A MITEL
PRODUCT
GUIDE

Mitel OpenScape Business

OpenScape Business V3

Documentación del administrador
11/2025

A31003-P3030-M100-63-76A9

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contenido

1 Historial de cambios..... 39
1.1 Historial de mejoras/correcciones..... 58

2 Introducción y notas importantes..... 70
2.1 Acerca de esta documentación..... 70
2.1.1 Documentación y destinatarios..... 71
2.1.2 Estructura de la documentación del administrador..... 72
2.1.3 Tipos de temas..... 74
2.1.4 Convenciones de representación..... 75
2.2 Indicaciones de seguridad y de aviso..... 75
2.2.1 Indicaciones de aviso: Peligro..... 76
2.2.2 Indicaciones de aviso: Advertencia..... 77
2.2.3 Advertencias: Atención..... 78
2.2.4 Indicaciones de aviso: Aviso..... 79
2.2.5 Indicaciones de seguridad nacionales..... 79
2.2.5.1 Indicaciones de seguridad para Australia..... 80
2.2.5.2 Indicaciones de seguridad para Brasil..... 80
2.2.5.3 Indicaciones de seguridad para EE. UU..... 80
2.2.5.4 Indicaciones de seguridad para Canadá..... 83
2.3 Avisos importantes..... 84
2.3.1 Comportamiento en caso de emergencia..... 84
2.3.2 Uso adecuado..... 85
2.3.3 Eliminación y reciclaje adecuados..... 85
2.3.4 Normas y pautas relativas a la instalación..... 86
2.3.4.1 Conexión de OpenScape Business X al circuito de alimentación eléctrica..... 86
2.3.4.2 Conexión de OpenScape Business S y OpenScape Business UC Booster Server con el circuito de alimentación eléctrica..... 86
2.3.4.3 Cableado blindado para conexiones LAN y WAN de OpenScape Business X..... 87
2.3.4.4 Normativa de protección antiincendios..... 87
2.3.4.5 Requisitos de protección contra descargas..... 88
2.3.4.6 Identificaciones para OpenScape Business X..... 89
2.3.5 Indicaciones sobre interferencias electromagnéticas y radio interferencias de OpenScape Business X..... 89
2.3.6 Privacidad y seguridad de los datos..... 89
2.3.7 Normas técnicas y conformidad de OpenScape Business X..... 90
2.3.7.1 Conformidad CE..... 90
2.3.7.2 Conformidad con normas estadounidenses y canadienses..... 90
2.3.7.3 Conformidad con las normas internacionales..... 91
2.3.8 Condiciones de servicio..... 91
2.3.8.1 Condiciones de servicio de OpenScape Business X..... 91
2.3.8.2 Condiciones de servicio de OpenScape Business S y OpenScape Business UC Booster Server..... 92

3 Visión general del sistema..... 93
3.1 Aspectos destacados..... 93
3.2 Comunicaciones Unificadas..... 93
3.2.1 Funciones de UC (vista general)..... 94
3.2.2 Acceso de usuario a funciones de UC (clientes de UC)..... 101
3.2.3 Integración en aplicaciones de negocio..... 104
3.3 OpenScape Business - Modelos..... 105
3.3.1 Niveles de ampliación disponibles a través de Ventas..... 105

3.3.2 Modelos de hardware de UC....108
3.3.3 Hardware UC Booster....109
3.3.4 Modelos de software de UC (softswitch)....110
3.3.5 Estructura y condiciones ambientales....110
3.3.6 Teléfonos compatibles....110
3.4 Información adicional....112
3.4.1 Idiomas admitidos....112
3.4.2 Enlaces de Internet....114

4 Principio de administración....115
4.1 OpenScape Business Assistant (Gestión basada en Web, WBM)....115
4.1.1 Requisitos para la Gestión basada en Web (WBM)....115
4.1.2 Página de inicio de la Gestión basada en Web (WBM)....115
4.1.3 Introducción a la Gestión basada en Web (WBM)....117
4.1.3.1 Cómo iniciar sesión en el WBM....119
4.1.3.2 Cómo cerrar sesión de la Gestión basada en Web (WBM)....119
4.1.4 Gestión de usuarios de WBM....120
4.1.4.1 Cómo agregar un administrador....123
4.1.4.2 Cómo editar un administrador....123
4.1.4.3 Cómo modificar su propria contraseña de administrador....123
4.1.4.4 Cómo borrar al administrador....124
4.1.4.5 Cómo cambiar una contraseña de administrador de Manager E....124
4.1.5 Asistentes....124
4.1.5.1 Asistentes – Configuración básica....125
4.1.5.2 Asistentes – Red / Internet....125
4.1.5.3 Asistentes – Teléfonos / Suscriptores....126
4.1.5.4 Asistentes – Telefonía central....126
4.1.5.5 Asistentes – Telefonía de usuario....127
4.1.5.6 Asistentes – Seguridad....128
4.1.5.7 Asistentes – UC Smart (solo con UC Smart)....128
4.1.5.8 Asistentes – UC Suite (solo con UC Suite)....128
4.1.5.9 Asistentes – Directorio Unificado....129
4.1.5.10 Asistentes - Servicios en la nube....129
4.1.6 Centro de servicios....130
4.1.6.1 Centro de servicios – **Documentos**....130
4.1.6.2 Centro de servicios – **Software** 130
4.1.6.3 Centro de servicios – **Inventario** > **Sistema**....131
4.1.6.4 Centro de servicios – **Inventario** > **Números de llamada**....131
4.1.6.5 Centro de servicios – **Inventario** > **Resumen de red**....131
4.1.6.6 Centro de servicios – **Actualización de software**....131
4.1.6.7 Centro de servicios – **Transferencia de correos electrónicos**....131
4.1.6.8 Centro de servicios – **Acceso remoto**....131
4.1.6.9 Centro de servicios – **Reiniciar / Volver a cargar**....131
4.1.6.10 Centro de servicios – **Diagnóstico** > **Estado**....131
4.1.6.11 Centro de servicios – **Diagnóstico** > **Visor de sucesos**....132
4.1.6.12 Centro de servicios – **Diagnóstico** > **Seguimiento**....132
4.1.6.13 Centro de servicios – Diagnóstico > Registro de servicio....132
4.1.7 Modo Experto....132
4.1.8 Ayuda online....132
4.1.8.1 Cómo acceder a la ayuda online sensible al contexto....133
4.2 Manager E....133
4.2.1 Cómo cargar la memoria de datos de cliente (KDS) en el Manager E....134
4.2.2 Cómo guardar la memoria de datos de cliente (KDS) de nuevo en el sistema de comunicación....135

5 Configuración inicial de OpenScape Business X....136
5.1 Requisitos para la instalación inicial....137

5.2 Componentes....138
5.3 Plan de numeración....139
5.4 Esquema de direcciones IP....140
5.5 Puesta en servicio inicial....142
5.5.1 Cómo iniciar el sistema de comunicación....142
5.5.2 Cómo conectar el PC de administración con el sistema de comunicación....143
5.5.3 Cómo iniciar WBM....144
5.6 Integración en la LAN de clientes....146
5.6.1 Cómo iniciar el asistente de instalación inicial....146
5.6.2 Configuración de sistema....147
5.6.2.1 Cómo definir el logotipo de pantalla y la designación de producto....147
5.6.2.2 Cómo definir las direcciones IP (opcional)....148
5.6.2.3 Cómo especificar el nombre de dispositivo....149
5.6.3 Configuración de DHCP....149
5.6.3.1 Cómo deshabilitar el servidor DHCP interno....150
5.6.3.2 Cómo habilitar y configurar el servidor DHCP interno....150
5.6.3.3 Cómo habilitar DHCP solo para dispositivos Mitel/Unify....152
5.6.4 Configuración de país y hora....153
5.6.4.1 Cómo seleccionar el código de país y el idioma para los registros de sucesos....154
5.6.4.2 Cómo introducir la identificación del sistema DECT....155
5.6.4.3 Configuración manual de fecha y hora....155
5.6.4.4 Obtención de la fecha y hora de un servidor SNTP....156
5.6.5 Solución UC....157
5.6.5.1 Cómo establecer la solución UC....157
5.6.6 Conexión del sistema de comunicación en la LAN de clientes....158
5.6.6.1 Cómo conectar el sistema de comunicación en la LAN de clientes....158
5.7 Configuración básica....159
5.7.1 Cómo iniciar el Asistente Configuración básica....159
5.7.2 Números de teléfono del sistema e interconexión....160
5.7.2.1 Cómo introducir el número de teléfono del sistema para una conexión de centralita....160
5.7.2.2 Cómo introducir los números de teléfono del sistema para un acceso individual....161
5.7.2.3 Cómo activar o desactivar la interconexión....162
5.7.3 Datos de extensión....163
5.7.3.1 Cómo mostrar los datos de extensión....164
5.7.3.2 Cómo borrar todos los números de llamada....164
5.7.3.3 Adaptar los números de teléfono preconfigurados al plan de numeración individual....165
5.7.3.4 Cómo importar los datos de extensión mediante un archivo XML....166
5.7.3.5 Cómo mostrar datos masivos....166
5.7.4 Configuración RDSI....167
5.7.4.1 Cómo configurar la conexión de extensiones RDSI....168
5.7.4.2 Cómo configurar la conexión de centralita RDSI....169
5.7.4.3 Cómo configurar el acceso individual RDSI....169
5.7.4.4 Cómo desactivar la configuración RDSI....170
5.7.5 Acceso a Internet....170
5.7.5.1 Cómo configurar el acceso a Internet a través de un router de Internet externo mediante la conexión LAN....173
5.7.5.2 Cómo configurar el acceso a Internet a través de un router de Internet externo mediante la conexión WAN....174
5.7.5.3 Cómo configurar el acceso a Internet a través de un ISP preconfigurado....175
5.7.5.4 Cómo configurar el acceso a Internet a través del PPPoE ISP estándar....177
5.7.5.5 Cómo configurar el acceso a Internet a través de un PPTP ISP estándar....179
5.7.5.6 Cómo configurar el acceso a Internet a través de un enrutador de Internet externo sobre la LAN con un puerto WAN dedicado a ITSP....181
5.7.5.7 Cómo desactivar el acceso a Internet....182
5.7.6 Telefonía Internet....183
5.7.6.1 Cómo configurar un ITSP predefinido....184

5.7.6.2 Cómo desactivar telefonía Internet....189
5.7.7 Extensiones....190
5.7.7.1 Cómo configurar extensiones RDSI 190
5.7.7.2 Cómo configurar extensiones analógicas....193
5.7.7.3 Cómo configurar extensiones UP0....196
5.7.7.4 Cómo configurar extensiones DECT....199
5.7.7.5 Cómo configurar extensiones IP y SIP....202
5.7.8 Configuración de UC Suite....205
5.7.8.1 Cómo configurar la Suite UC....205
5.7.9 Configuración de los buzones de voz de UC Smart....206
5.7.9.1 Cómo configurar los buzones de voz de UC Smart....206
5.7.10 Ajustes del servidor de conferencias....207
5.7.10.1 Cómo modificar los ajustes del servidor de conferencias....207
5.7.11 Envío de correo electrónico (opcional)....208
5.7.11.1 Cómo configurar el envío de correo electrónico....208
5.8 Tareas finales....211
5.8.1 Cómo activar y asignar las licencias....212
5.8.2 Cómo proporcionar el cliente UC Smart para la instalación....214
5.8.3 Cómo preparar los clientes de UC Suite para la instalación....214
5.8.4 Cómo realizar la copia de seguridad....216
5.9 Puesta en servicio de los teléfonos IP....216
5.9.1 Cómo configurar teléfono IP....218
5.9.2 Cómo configurar un teléfono SIP....219
5.10 Cómo recopilar seguimientos de diagnóstico para incidentes de error....221
5.11 Reflashing....222

6 Puesta en servicio inicial por OpenScape Business S....225
6.1 Requisitos para la puesta en servicio inicial....225
6.2 Componentes....228
6.3 Esquema de direcciones IP....229
6.4 Plan de numeración....229
6.5 Instalación del software de comunicación....230
6.5.1 Cómo instalar el software de comunicación....232
6.6 Puesta en servicio....234
6.6.1 Cómo iniciar el asistente de instalación inicial....234
6.6.2 Configuración de sistema....234
6.6.2.1 Cómo definir el logotipo de pantalla y la designación de producto....235
6.6.2.2 Cómo seleccionar el código de país y el idioma para los registros de seguimiento....236
6.6.2.3 Cómo activar un puerto LAN adicional como interfaz WAN....236
6.6.2.4 Cómo cambiar el plan de marcado a 4 dígitos....237
6.6.3 Solución UC....238
6.6.3.1 Cómo establecer la solución UC....238
6.7 Configuración básica....239
6.7.1 Cómo iniciar el Asistente Configuración básica....239
6.7.2 Números de teléfono del sistema e interconexión....240
6.7.2.1 Cómo introducir el número de teléfono del sistema para una conexión de centralita....240
6.7.2.2 Cómo introducir los números de teléfono del sistema para un acceso individual....241
6.7.2.3 Cómo activar o desactivar la interconexión....242
6.7.2.4 Cómo configurar el flujo ascendente de su conexión a Internet....243
6.7.3 Datos de extensión....243
6.7.3.1 Cómo mostrar los datos de extensión....245
6.7.3.2 Cómo borrar todos los números de llamada....245
6.7.3.3 Adaptar los números de teléfono preconfigurados al plan de numeración individual....246
6.7.3.4 Cómo importar los datos de extensión mediante un archivo XML....246
6.7.4 Acceso a Internet....247

6.7.4.1 Cómo configurar el acceso a Internet a través de un enrutador de Internet externo sobre la LAN con un puerto WAN dedicado a ITSP....247
6.7.5 Telefonía Internet 248
6.7.5.1 Cómo configurar un ITSP predefinido....249
6.7.5.2 Cómo desactivar telefonía Internet....254
6.7.6 Extensiones....255
6.7.6.1 Cómo configurar extensiones IP y SIP....255
6.7.7 Configuración de UC Suite....258
6.7.7.1 Cómo configurar la Suite UC....258
6.7.8 Configuración de los buzones de voz de UC Smart....259
6.7.8.1 Cómo configurar los buzones de voz de UC Smart....259
6.7.9 Ajustes del servidor de conferencias....260
6.7.9.1 Cómo modificar los ajustes del servidor de conferencias....260
6.7.10 Envío de correo electrónico (opcional)....261
6.7.10.1 Cómo configurar el envío de correo electrónico....261
6.8 Tareas finales....264
6.8.1 Cómo activar y asignar las licencias....265
6.8.2 Cómo proporcionar el cliente UC Smart para la instalación....267
6.8.3 Cómo preparar los clientes de UC Suite para la instalación....267
6.8.4 Cómo realizar la copia de seguridad....268
6.9 Puesta en servicio de los teléfonos IP....269
6.9.1 Cómo configurar teléfono IP....270
6.9.2 Cómo configurar un teléfono SIP....271
6.10 Desinstalación del software de comunicación....273
6.10.1 Cómo desinstalar el software de comunicación....274
6.11 Puertos utilizados....274
6.12 Cómo recopilar seguimientos de diagnóstico para incidentes de error....276
6.13 Reflashing....277

7 Configuración inicial de OpenScape Business UC Booster....280
7.1 Requisitos para la puesta en servicio inicial....282
7.2 Copia de seguridad de los datos de configuración del sistema de comunicación....285
7.2.1 Cómo realizar la copia de seguridad....285
7.3 Puesta en servicio de la UC Booster Card....286
7.3.1 Montaje de la UC Booster Card....286
7.3.2 Configuración de la UC Booster Card....286
7.3.3 Actualización de software para la UC Booster Card....287
7.3.3.1 Cómo ejecutar una actualización de software....287
7.4 Puesta en servicio del UC Booster Server....288
7.4.1 Instalación del software de comunicación....288
7.4.1.1 Cómo instalar el software de comunicación....289
7.4.2 Configuración del UC Booster Server....291
7.4.2.1 Comunicar la dirección IP del sistema de comunicación....292
7.4.3 Actualización de software para el UC Booster Server....294
7.5 Configuración básica....295
7.6 Tareas finales....295
7.7 Desinstalación del software de comunicación....296
7.7.1 Cómo desinstalar el software de comunicación....296
7.8 Actualización de UC Booster Card a UC Booster Server....296
7.9 Puertos utilizados....298

8 Registro de licencia....301
8.1 Procedimiento de activación de licencia....302
8.2 Licencias....304
8.2.1 Licencia básica....305
8.2.2 Licencias de usuario....306

8.2.3 Licencias orientadas a usuarios (User)..... 307
8.2.4 Licencias de sistema.....309
8.2.5 Licencias de evaluación.....311
8.2.6 Licencias de upgrade.....313
8.2.7 Combinaciones de licencias posibles.....313
8.3 Registro de licencia de un sistema de comunicación (independiente).....316
8.3.1 CLS Connect.....317
8.3.1.1 Cómo activar CLS Connect.....317
8.3.1.2 Pasar de CLS connect..... 318
8.3.2 Activación de licencia (Standalone).....318
8.3.2.1 Cómo activar licencias en línea (Standalone).....319
8.3.2.2 Cómo activar licencias offline (Standalone)..... 320
8.3.3 Asignación de licencias (independiente).....321
8.3.3.1 Cómo registrar licencias para suscriptores (independientes).....323
8.3.3.2 Cómo registrar licencias para líneas (Standalone)..... 326
8.4 Registro de licencia de varios sistemas de comunicación (interred).....327
8.4.1 Activación de licencia (interred).....329
8.4.1.1 Cómo activar licencias sin conexión (interred).....329
8.4.1.2 Cómo reunir archivos de licencia en un archivo de licencia de red.....331
8.4.2 Asignación de licencias (interred).....332
8.4.2.1 Cómo registrar licencia para extensiones (interred).....334
8.4.2.2 Cómo registrar licencias para líneas (interred)..... 337
8.4.2.3 Cómo asignar licencias de sistema a un nodo..... 337
8.4.2.4 Cómo asignar la licencia del sistema "Redes" a un nodo.....338
8.5 Información de licencia.....338
8.5.1 Información de licencia sin interred (Standalone)..... 339
8.5.1.1 Cómo mostrar información de licencia.....339
8.5.2 Información de licencia en la interred 339
8.5.2.1 Cómo mostrar todas las licencias de la interred.....340
8.5.2.2 Cómo mostrar las licencias vinculadas a un nodo.....340
8.5.2.3 Cómo mostrar todas las licencias en uso común de la interred..... 341
8.5.2.4 Cómo mostrar licencias orientadas a usuarios (User) o de extensión por nodos..... 341
8.6 Asignación de perfiles de licencia 341
8.6.1 Cómo añadir un perfil de licencia.....342
8.6.2 Cómo modificar un perfil de licencia..... 343
8.6.3 Cómo asignar un perfil de licencia a extensiones.....343
8.6.4 Cómo borrar un perfil de licencia..... 344
8.7 Rehost tras intercambio de hardware.....345
8.7.1 Cómo ejecutar un Rehost después de sustituir el hardware.....346
8.8 Servidor de licencias (Central License Server, CLS) 346
8.8.1 Cómo consultar o modificar la dirección IP del servidor de licencias.....346
8.8.2 Cómo comprobar la conexión de Central License Server (CLS)..... 347
8.9 Agente de licencias (Customer License Agent, CLA).....347
8.9.1 Cómo configurar la conexión con el agente de licencias local.....348
8.9.2 Cómo modificar la conexión con el agente de licencias central.....348
8.10 ID de bloqueo e ID de bloqueo avanzado.....348
8.10.1 Cómo consultar el ID de bloqueo del sistema de comunicación.....350
8.10.2 Cómo consultar el ID de bloqueo del softswitch..... 350
8.10.3 Cómo consultar el ID de bloqueo avanzado del softswitch.....350
8.11 Cómo migrar de Placa base V2 a Placa base V3 (sistema autónomo).....350
8.12 Cómo migrar de Placa base V2 a Placa base V3 como nodo maestro de un sistema conectado en red..... 353
8.13 Cómo migrar de Placa base V2 a Placa base V3 el nodo esclavo de un sistema conectado en red..... 353
8.14 Migración de sistemas HiPath 3000 al software OSBiz V3 con placa base V3.....354
8.15 Actualización de V2 a V3 con **CLS Connect**.....354
8.16 Actualización de V2 a V3 sin **CLS Connect**..... 354

9 Integración en la red de datos interna (LAN)....356
9.1 Interfaz LAN....356
9.1.1 Dirección IP y máscara de red de la interfaz LAN....356
9.1.1.1 Cómo modificar la dirección IP y la dirección de red de la plataforma de hardware....357
9.1.1.2 Cómo modificar la dirección IP de la UC Booster Card....358
9.1.1.3 Cómo modificar la dirección IP y la máscara de red del softswitch....358
9.1.2 Área de direcciones IP interna de la interfaz LAN....359
9.1.2.1 Cómo modificar el área de direcciones IP interna de la plataforma de hardware....359
9.1.2.2 Cómo restablecer el área de direcciones IP interna de la plataforma de hardware....360
9.2 DHCP....360
9.2.1 Agente DHCP Relay....360
9.2.1.1 Cómo configurar la plataforma de hardware como agente de retransmisión DHCP....361
9.2.2 Servidor DHCP 361
9.2.2.1 Cómo habilitar y configurar el servidor DHCP de la plataforma de hardware....363
9.2.2.2 Cómo deshabilitar el servidor DHCP de la plataforma de hardware....365
9.2.2.3 Cómo activar y configurar el servidor DHCP del softswitch....365
9.2.2.4 Cómo desactivar el servidor DHCP del softswitch....366
9.2.2.5 Cómo habilitar DHCP solo para dispositivos Mitel/Unify....366
9.3 DNS - Resolución de nombre....367
9.3.1 Cómo establecer un servidor DNS externo....369
9.4 Encamin. IP....369
9.4.1 Cómo activar o desactivar el router estándar....370
9.4.2 Cómo añadir ruta estática....370
9.4.3 Cómo borrar rutas estáticas....371
9.5 Deployment Service (DLI y DLS)....371
9.5.1 Cómo configurar un servidor DLS externo en el servidor DHCP interno....374
9.5.2 Cómo activar el DLI interno....374
9.5.3 Cómo configurar el sistema de comunicación como cliente de implementación y licencias (Deployment & Licensing Client)....375

10 Conexión al proveedor de servicios....377
10.1 Acceso a Internet....377
10.1.1 Acceso a Internet a través de un router Internet externo 379
10.1.1.1 Cómo configurar el acceso a Internet a través de un router de Internet externo mediante la conexión LAN....380
10.1.1.2 Cómo configurar el acceso a Internet a través de un router de Internet externo mediante la conexión WAN....381
10.1.1.3 Cómo configurar el acceso a Internet a través de un enrutador de Internet externo sobre la LAN con un puerto WAN dedicado a ITSP....382
10.1.2 Acceso a Internet a través de un módem Internet 383
10.1.2.1 Cómo configurar el acceso a Internet a través de un ISP preconfigurado....384
10.1.2.2 Cómo configurar el acceso a Internet a través de un PPPoE ISP estándar....386
10.1.2.3 Cómo configurar el acceso a Internet a través de un PPTP ISP estándar....388
10.1.3 Interfaz WAN....391
10.1.4 DynDNS....391
10.1.4.1 Cómo configurar el servicio DynDNS....392
10.1.4.2 Cómo definir Mail Exchanger....394
10.2 Línea urbana mediante ITSP....394
10.2.1 Configuración de un ITSP....396
10.2.1.1 Cómo configurar un ITSP predefinido....397
10.2.1.2 Cómo agregar un nuevo ITSP....403
10.2.1.3 Cómo configurar Multisite mediante ITSP 410
10.2.1.4 Cómo guardar una plantilla ITSP preconfigurada como una nueva plantilla....411
10.2.1.5 Cómo adaptar una plantilla de ITSP preconfigurada....412
10.2.1.6 Cómo actualizar manualmente una plantilla de ITSP preconfigurada....412
10.2.2 STUN (Simple Traversal of UDP through NAT)....413

10.2.2.1 Cómo definir el modo STUN 414
10.3 Acceso a línea urbana mediante líneas analógicas y digitales 414
10.3.1 Líneas 415
10.3.1.1 Cómo configurar el acceso a línea urbana RDSI 416
10.3.1.2 Cómo configurar el acceso analógico a línea urbana 417
10.3.1.3 Cómo mostrar todas las líneas 418
10.3.1.4 Cómo mostrar líneas individuales 418
10.3.1.5 Cómo modificar código de línea 419
10.3.1.6 Cómo asignar MSN a una línea 419
10.3.1.7 Cómo modificar el protocolo RDSI 419
10.3.1.8 Cómo modificar el modo de asignación del canal B 420
10.3.1.9 Cómo modificar el procedimiento de marcación 420
10.3.2 Rutas 420
10.3.2.1 Cómo modificar la asignación de ruta 424
10.3.2.2 Cómo modificar el nombre de ruta 424
10.3.2.3 Cómo modificar el código de ruta 424
10.3.2.4 Cómo configurar una ruta de desbordamiento si LCR está desactivado 425
10.3.2.5 Cómo configurar una ruta de desbordamiento con LCR activado 425
10.3.2.6 Cómo configurar el tipo de ocupación 425
10.3.2.7 Cómo introducir números de teléfono del sistema entrantes y salientes 425
10.3.2.8 Cómo configurar el formato del número de teléfono transmitido 426
10.3.2.9 Cómo configurar el tipo de número de teléfono transferido 426
10.3.2.10 Cómo configurar el prefijo de ruta 427
10.3.2.11 Cómo definir una ruta para la interconexión y cómo registrar un segundo código urbano 427
10.3.3 Supervisión de tono de marcación 428
10.3.3.1 Cómo configurar el tiempo de retardo de la supervisión del tono de marcación 429
10.3.3.2 Cómo configurar Tiempo supervisión tono marcación 429
10.3.3.3 Cómo configurar el tiempo de marcación de dígitos 430
10.3.3.4 Cómo activar o desactivar la evaluación del segundo tono de marcación 430
10.4 Prioridad de la ocupación de línea urbana con LCR activado 431
10.4.1 Cómo asignar prioridades a la ocupación de línea urbana 431

11 Estaciones 432
11.1 Plan de numeración 432
11.1.1 Plan de numeración estándar 433
11.1.2 Plan de numeración individual 434
11.1.2.1 Cómo borrar o modificar números de teléfono estándar 435
11.1.2.2 Cómo modificar números de teléfono estándar 436
11.1.2.3 Cómo importar números de teléfono y datos de extensión 437
11.2 Requisitos a la telefonía LAN 438
11.2.1 Códecs de sonido 438
11.2.1.1 Cómo configurar parámetros de códec de sonido 439
11.2.1.2 Cómo asignar parámetros de códec de sonido a un destino 440
11.2.2 Transmisión de tonos MF a RFC2833 440
11.2.2.1 Cómo activar o desactivar la transferencia de tonos de fax y módem según RFC2833 441
11.2.2.2 Cómo activar o desactivar la transferencia de MF según RFC2833 441
11.2.3 Calidad del servicio 442
11.2.3.1 Cómo configurar Quality of Service 444
11.3 Extensiones IP 444
11.4 Estaciones SIP 446
11.5 Extensiones UP0 448
11.6 Extensiones DECT 449
11.7 Estaciones SIP DECT de Mitel 450
11.8 Extensiones RDSI 450
11.8.1 Cómo configurar interfaces S_0 para extensiones RDSI 452
11.8.2 Cómo permitir solo números configurados para MSN 452

11.9 Ext. analógicas....453
11.10 Ext. virtuales....455
11.11 Programación de teclas....455
11.11.1 Cómo programar las teclas de función de los teléfonos de sistema....456
11.12 Perfiles de extensión....457
11.13 Configuración de las extensiones....458
11.13.1 Cómo configurar extensiones IP....460
11.13.2 Cómo configurar extensiones SIP....463
11.13.3 Cómo configurar estaciones UP0....467
11.13.4 Cómo configurar extensiones DECT....470
11.13.5 Cómo configurar estaciones SIP DECT de Mitel mediante aprovisionamiento....474
11.13.5.1 Cómo configurar estaciones SIP a través del modo experto....476
11.13.6 Cómo configurar extensiones RDSI....477
11.13.7 Cómo configurar extensiones analógicas....479
11.13.8 Cómo definir el nombre de las extensiones....482
11.14 Configuración de los perfiles de extensiones....483
11.14.1 Cómo crear un nuevo perfil de extensiones....484
11.14.2 Cómo mostrar perfiles de extensiones y sus miembros....485
11.14.3 Cómo agregar miembros a un perfil de extensiones....485
11.14.4 Cómo borrar miembros de un perfil de extensiones....486
11.14.5 Cómo importar o exportar un perfil de extensiones individual....486
11.14.6 Cómo modificar valores y ajustes de configuración de un perfil de extensiones....487
11.14.7 Cómo importar o exportar todos los perfiles de extensiones....488
11.15 Configuración de los datos de autenticación en el teléfono SIP....489
11.15.1 Cómo configurar los datos de autenticación mediante la Gestión basada en Web (WBM) del teléfono SIP....489
11.15.2 Cómo configurar los datos de autenticación en el display del teléfono SIP....492
11.16 Exportación de datos de extensión....493
11.16.1 Cómo exportar los datos de extensión....493

12 UC Smart....494
12.1 Ajustes básicos para UC Smart....495
12.1.1 Cómo activar UC Smart....495
12.1.2 Cómo configurar UC Smart....496
12.1.3 Cómo configurar conferencias controladas por aplicación....497
12.1.4 Cómo determinar las direcciones IP de los componentes del sistema....498
12.1.5 Cómo determinar el estado de UC Smart....499
12.2 Clientes de UC Smart....499
12.2.1 myPortal @work....499
12.2.1.1 Requisitos para myPortal @work....502
12.2.1.2 Configuración de usuario de myPortal @work....503
12.2.1.3 Pasos de configuración para utilizar myPortal @work a través de Internet....511
12.2.1.4 Otras recomendaciones & ajustes de configuración....512
12.2.1.5 Guía para la resolución de problemas....514
12.2.1.6 Más sugerencias....516
12.3 Usuarios de UC Smart....517
12.3.1 Cómo configurar un usuario de UC Smart....518
12.3.2 Cómo cambiar la contraseña de un usuario de UC Smart....518
12.4 Presencia....519
12.5 Directorios y diario....520
12.5.1 Directorios....520
12.5.1.1 Cómo configurar directorios para teléfonos de sistema....521
12.5.2 Directorio interno....521
12.5.2.1 Cómo activar o desactivar la indicación de una extensión en el directorio interno....522
12.5.3 Lista de favoritos....522
12.5.4 Listín del sistema....522

12.5.5 Directorio Unificado....523
12.5.5.1 Prestaciones....524
12.5.5.2 Reglas y convenciones....527
12.5.5.3 Capítulo 11.5.5.3 Límites funcionales....528
12.5.5.4 Directorio Unificado en sistemas interconectados....529
12.5.6 Diario....530
12.6 Llamadas....530
12.6.1 Formatos de números de teléfono....530
12.6.2 Requisitos previos para recibir llamadas a través de VoIP en myPortal to go para usar CallKit en su iPhone....531
12.7 Conferencias....531
12.8 Web Collaboration....533
12.8.1 Cómo configurar la conexión con el servidor de Web Collaboration (Public Server)....534
12.8.2 Cómo desactivar la conexión con el servidor de Web Collaboration....535
12.9 Mensajería instantánea....535
12.9.1 Mensajería instantánea....535
12.10 Buzón de voz (SmartVM)....535
12.10.1 Configuración del buzón de voz (SmartVM)....538
12.10.1.1 Cómo activar o desactivar el buzón de voz....539
12.10.1.2 Cómo configurar el buzón de voz (SmartVM)....539
12.10.1.3 Cómo añadir un buzón estándar para una extensión....541
12.10.1.4 Cómo modificar el grupo de clases de servicio de un puerto de buzón de voz....541
12.10.1.5 Cómo modificar la estructura del menú telefónico del buzón de voz....542
12.10.1.6 Cómo cargar, guardar y borrar saludos sueltos....542
12.10.1.7 Cómo guardar y recuperar saludos y mensajes....543
12.10.2 Servicio de notificación de nuevos mensajes....544
12.10.2.1 Cómo activar o desactivar las notificaciones de email....544

13 UC Suite....546
13.1 Configuración básica para la UC Suite....546
13.1.1 Cómo activar la UC Suite....547
13.1.2 Cómo restringir la clase de servicio de las llamadas UC iniciadas por parte del sistema....547
13.2 Clientes de UC Suite....547
13.2.1 myPortal for Desktop....548
13.2.2 myPortal @work....549
13.2.3 myPortal for Outlook....549
13.2.4 Fax Printer....549
13.2.5 myAttendant....550
13.2.6 Requisitos para los clientes de PC de UC Suite....550
13.2.7 Instalación/desinstalación silenciosa para clientes de PC de la UC Suite....554
13.2.7.1 Cómo realizar la instalación silenciosa....555
13.2.7.2 Cómo realizar la desinstalación silenciosa....556
13.2.8 Actualizaciones automáticas....557
13.3 Usuarios y perfiles de usuario de la UC Suite....557
13.3.1 Usuarios de UC Suite....558
13.3.1.1 Cómo configurar un usuario de la UC Suite....561
13.3.1.2 Cómo restablecer un usuario de la UC Suite....561
13.3.1.3 Cómo configurar un usuario de la UC Suite como agente (myAgent)....561
13.3.1.4 Cómo modificar el estado de presencia de un usuario de la UC Suite....562
13.3.1.5 Cómo modificar la contraseña para un usuario de UC Suite....562
13.3.1.6 Cómo modificar la longitud de la contraseña un usuario de la UC Suite....563
13.3.2 Perfil de usuario de UC Suite....563
13.3.2.1 Cómo añadir un perfil de usuario de la UC Suite....565
13.3.2.2 Cómo modificar un perfil de usuario de UC Suite....565
13.3.2.3 Cómo mostrar los perfiles de usuario de la UC Suite....566
13.3.2.4 Cómo añadir miembros a un perfil de usuario de UC Suite....566

13.3.2.5 Cómo borrar miembros de un perfil de usuarios de la UC Suite..... 566
13.3.2.6 Cómo borrar un perfil de usuario de la UC Suite.....567
13.4 Estado de presencia y servicio CallMe.....567
13.4.1 Presencia.....567
13.4.2 Servicio CallMe..... 570
13.4.3 Desvío de llamadas relativo al estado.....571
13.4.4 Desvío de llamadas basado en reglas..... 571
13.5 Directorios y diario.....572
13.5.1 Directorios.....572
13.5.1.1 Cómo configurar directorios para teléfonos de sistema.....575
13.5.2 Directorio interno.....575
13.5.2.1 Cómo activar o desactivar la indicación de extensiones analógicas en el directorio interno.....576
13.5.2.2 Cómo activar o desactivar la búsqueda en el directorio interno únicamente..... 576
13.5.3 Directorio externo.....577
13.5.3.1 Cómo importar un archivo CSV desde el sistema de archivos local en el directorio externo..... 578
13.5.3.2 Cómo añadir acceso a una base de datos externa para el directorio externo..... 580
13.5.3.3 Cómo exportar un archivo CSV desde el directorio externo.....580
13.5.4 Directorio offline externo (LDAP)..... 581
13.5.4.1 Cómo añadir un Directorio offline externo (LDAP) para clientes PC.....582
13.5.4.2 Cómo borrar un Directorio offline externo (LDAP) para clientes PC.....583
13.5.4.3 Cómo añadir un directorio offline externo (LDAP) para teléfonos de sistema.....583
13.5.5 Listín del sistema..... 584
13.5.6 Directorio Unificado.....584
13.5.6.1 Prestaciones.....585
13.5.6.2 Reglas y convenciones.....588
13.5.6.3 Capítulo 11.5.5.3 Límites funcionales.....589
13.5.6.4 Directorio Unificado en sistemas interconectados.....590
13.5.6.5 Cómo importar contactos a un Directorio Unificado.....591
13.5.6.6 Cómo editar o agregar nuevos contactos al Directorio Unificado..... 592
13.5.7 Departamentos..... 593
13.5.7.1 Cómo agregar un departamento..... 593
13.5.7.2 Cómo asignar extensiones a un departamento.....593
13.5.7.3 Cómo editar un departamento.....594
13.5.7.4 Cómo eliminar un departamento..... 594
13.5.8 Lista de favoritos.....594
13.5.9 Diario..... 595
13.5.9.1 Cómo modificar el tiempo máximo de retención para el diario..... 596
13.6 Llamadas..... 597
13.6.1 Marcación de escritorio y clipboard..... 597
13.6.2 Ventanas emergentes..... 597
13.6.3 Grabación de llamadas.....598
13.6.3.1 Cómo activar o desactivar la grabación de llamadas..... 598
13.6.3.2 Cómo activar o desactivar el anuncio grabado de una grabación..... 599
13.6.3.3 Cómo activar o desactivar el tono de aviso para la grabación..... 599
13.7 Conferencias.....600
13.7.1 Gestión de conferencias..... 600
13.7.1.1 Cómo modificar el número de acceso telefónico para la sala de conferencias virtual..... 604
13.7.1.2 Cómo autorizar o desaprobar la presencia de varios participantes de conferencia externos.....604
13.7.1.3 Cómo activar o desactivar el tono de advertencia.....605
13.7.1.4 Cómo modificar el intervalo de tiempo para la finalización automática de conferencias.....605
13.7.1.5 Cómo consultar información detallada sobre una conferencia memorizada.....606
13.7.1.6 Cómo borrar una conferencia guardada..... 606
13.7.1.7 Cómo configurar la grabación de conferencias.....606
13.7.2 Conferencia Ad-hoc.....607
13.7.3 Conferencia programada.....607
13.7.4 Conferencia permanente.....609

13.7.5 Conferencia abierta....610
13.8 Web Collaboration....611
13.8.1 Cómo configurar la conexión con el servidor de Web Collaboration (Custom Server)....612
13.8.2 Cómo configurar la conexión con el servidor de Web Collaboration (Public Server)....613
13.8.3 Cómo desactivar la conexión con el servidor de Web Collaboration....614
13.9 Mensajería instantánea....614
13.9.1 Mensajería instantánea....614
13.9.1.1 Cómo activar o desactivar los mensajes instantáneos....615
13.10 AutoAttendant....616
13.10.1 AutoAttendant personal....616
13.11 Mensajes de voz y de fax....616
13.11.1 Buzón de voz....616
13.11.1.1 Cómo configurar el número de teléfono del buzón de voz....619
13.11.1.2 Cómo configurar la transferencia automática diferida al buzón de voz....619
13.11.1.3 Cómo configurar parámetros del buzón de voz....619
13.11.1.4 Cómo configurar periodos de retención para los mensajes de voz....620
13.11.1.5 Cómo activar o desactivar la solicitud de contraseña del buzón de voz....620
13.11.1.6 Cómo configurar la información para mensajes de voz recibidos....621
13.11.1.7 Cómo configurar la tecla de buzón para consultar mensajes de voz....621
13.11.2 Anuncios grabados del buzón de voz....621
13.11.2.1 Cómo importar anuncios grabados para el buzón de voz....623
13.11.2.2 Cómo modificar el idioma de los anuncios grabados del buzón de voz....624
13.11.3 Buzón de fax....624
13.11.3.1 Cómo añadir un buzón de fax para extensiones....625
13.11.3.2 Cómo configurar el tipo de archivo para los mensajes de fax memorizados (UC Suite)....625
13.11.4 Envío de mensajes de fax con Fax Printer....626
13.11.4.1 Cómo agregar una portada de fax central....627
13.11.4.2 Cómo editar una portada de fax central....627
13.11.4.3 Cómo añadir encabezados para Fax Printer....627
13.11.4.4 Cómo cambiar encabezados para Fax Printer....628
13.11.4.5 Cómo borrar un encabezado para Fax Printer....629
13.11.5 Servicio de notificación de nuevos mensajes (UC Suite)....629
13.11.6 Envío de correo electrónico....630
13.11.6.1 Cómo configurar el envío de correo electrónico....630
13.11.7 Plantillas SMS....631
13.11.7.1 Cómo agregar plantillas SMS....632
13.11.7.2 Cómo editar plantillas SMS....633
13.11.7.3 Cómo eliminar plantillas SMS....633
13.11.8 Fax over IP (T.38 / G.711 Fax)....634
13.11.8.1 Cómo activar o desactivar Fax over IP (Fax T.38)....634
13.12 Descripción general de la integración de Microsoft Office 365....635
13.12.1 Cómo conectar el sistema OpenScape Business a Microsoft Office 365 mediante autenticación básica....636
13.12.2 Cómo conectar el sistema OpenScape Business a Microsoft Office 365 con el método de autenticación moderna....641
13.12.3 Cómo comprobar que las funciones de integración de Microsoft Office 365 están configuradas....641

14 Funciones del teléfono....644
14.1 Llamar....644
14.1.1 Marcación de dígitos....644
14.1.2 Marcación en bloque....644
14.1.3 Marc. tecl. num....644
14.1.4 Identificación de fin de marcación....645
14.1.5 Editar marcación....645
14.1.5.1 Cómo activar o desactivar Editar marcación....646
14.1.6 Remarcar botón....646

14.1.6.1 Cómo activar o desactivar la repetición de llamada automática..... 647
14.1.7 Marcación abreviada central..... 647
14.1.7.1 Cómo añadir un destino de marcación abreviada..... 649
14.1.7.2 Importar destinos de marcación abreviada de un archivo XML..... 649
14.1.7.3 Cómo exportar destinos de marcación abreviada a un archivo XML..... 650
14.1.7.4 Cómo editar destinos de marcación abreviada..... 650
14.1.8 Marcación abreviada individual (KWI)..... 651
14.1.9 Llamada directa..... 651
14.1.10 Mensaje directo / Contestación directa..... 652
14.1.10.1 Cómo activar o desactivar el bloqueo de mensaje directo para extensiones..... 653
14.1.11 Marcación asoc..... 653
14.1.12 Reserva de línea..... 654
14.1.12.1 Cómo activar o desactivar la reserva de línea..... 654
14.1.13 Línea privada..... 655
14.2 Señalización de llamadas, Indicación del número de teléfono..... 655
14.2.1 Señalización de llamadas diferencial..... 655
14.2.2 Transmisión del número de teléfono del llamante (CLIP)..... 656
14.2.2.1 Cómo activar o desactivar CLIP ajustable..... 656
14.2.3 Supresión de la indicación del número llamante (CLIR)..... 657
14.2.3.1 Cómo activar o desactivar la supresión del número de teléfono de la extensión..... 657
14.2.4 Presentación de identificación de línea conectada (COLP)..... 658
14.2.4.1 Cómo activar o desactivar Transmisión del número de teléfono del llamado..... 658
14.2.5 Supresión de la indicación del número llamado (COLR)..... 658
14.2.6 CLIP no screening (transmisión de información de número de teléfono específico del cliente)..... 659
14.2.6.1 Cómo configurar CLIP no screening..... 659
14.2.7 CLIP para terminales analógicos..... 660
14.2.8 Llamada silenciosa / reposo..... 660
14.2.9 Conversión de números de teléfono en nombres en la marcación abreviada central..... 660
14.3 Funciones durante la conexión..... 660
14.3.1 Retener..... 661
14.3.2 Aparcamiento..... 661
14.3.3 Consulta..... 662
14.3.4 Alternar..... 662
14.3.5 Transferir..... 663
14.3.6 Llamada recordatoria..... 664
14.3.7 Supervisión de llamadas..... 664
14.3.7.1 Cómo activar o desactivar la supervisión de llamadas para una extensión..... 665
14.3.8 Mensaje discreto..... 666
14.3.9 Grabación de llamadas (grabación de voz)..... 667
14.4 Control de accesibilidad..... 668
14.4.1 Desvíos de llamadas 669
14.4.1.1 Cómo configurar una transferencia automática diferida..... 670
14.4.2 Transferencia diferida..... 672
14.4.2.1 Cómo activar o desactivar el desvío de llamadas a través de líneas urbanas analógicas..... 674
14.4.2.2 Cómo activar o desactivar el desvío de llamadas tras desvío de llamadas a un destino externo..... 674
14.4.3 Desvío de llamadas diferido..... 674
14.4.4 Transferencia automática diferida en línea urbana (no disponible para EE. UU.)..... 675
14.4.5 Asignación de llamadas..... 676
14.4.5.1 Cómo configurar la asignación de llamadas..... 676
14.4.6 Timbre adicional..... 676
14.4.7 Rechazo de llamadas..... 678
14.4.8 Reposición de una llamada..... 678
14.4.9 No molestar..... 678
14.5 Optimización de la comunicación..... 679
14.5.1 Devolución de llamada..... 679

14.5.2 Aviso llam. en espera..... 680
14.5.2.1 Cómo activar o desactivar el aviso de llamada en espera.....681
14.5.2.2 Cómo activar o desactivar el aviso de llamada en espera inmediato a través del puesto de operadora..... 682
14.5.3 Intercalar (Intrusión)..... 682
14.5.3.1 Cómo autorizar a una extensión interna para la intercalación.....683
14.5.3.2 Cómo autorizar el puesto de interceptación para la intercalación.....684
14.5.4 Mensajes por ausencia..... 684
14.5.4.1 Cómo modificar el mensaje por ausencia.....684
14.5.5 Mensajes de texto.....684
14.5.5.1 Cómo modificar un mensaje de texto.....685
14.5.6 Servicios asociados.....685
14.5.6.1 Cómo activar o desactivar servicios asociados.....686
14.5.7 DISA..... 686
14.5.7.1 Cómo activar o desactivar la autorización DISA para un usuario..... 687
14.5.7.2 Cómo configurar el número DISA..... 688
14.5.7.3 Cómo configurar el modo de seguridad DISA..... 688
14.5.8 Flex Call/Pin móvil..... 688
14.5.9 Reasignación.....689
14.5.9.1 Cómo liberar la reasignación de números de teléfono a nivel de sistema.....690
14.5.10 Restablecimiento de las prestaciones activadas..... 690
14.5.11 Procedimientos..... 690
14.5.12 Equipo de despertador y citas.....692
14.6 Descripción general de funciones y códigos..... 692

15 Trabajar en equipo (Grupos).....697
15.1 Grupo de telecaptura, Llamada de grupo y Línea colectiva.....697
15.1.1 Grupo de telecaptura 697
15.1.2 Llamada de grupo.....699
15.1.3 Línea colectiva..... 703
15.1.4 Configuración de grupos de telecaptura, llamadas de grupo y líneas colectivas mediante asistentes 706
15.1.4.1 Configurar grupo de telecaptura.....707
15.1.4.2 Cómo añadir o borrar miembros de un grupo de telecaptura.....708
15.1.4.3 Cómo agregar una llamada de grupo (grupo).....708
15.1.4.4 Cómo modificar una llamada de grupo (grupo).....709
15.1.4.5 Cómo borrar una llamada de grupo (grupo)..... 710
15.1.4.6 Cómo agregar o borrar miembro a llamada de grupo (grupo)..... 711
15.1.4.7 Cómo agregar una línea colectiva..... 711
15.1.4.8 Cómo modificar una línea colectiva..... 713
15.1.4.9 Cómo borrar una línea colectiva..... 714
15.1.4.10 Cómo agregar o borrar miembro de línea colectiva.....714
15.1.5 Configuración de grupos de telecaptura, llamadas de grupo y líneas colectivas mediante el modo Experto.....715
15.1.5.1 Cómo activar o desactivar la indicación del número de teléfono y del nombre del llamante.....715
15.1.5.2 Cómo activar o desactivar tono de advertencia.....716
15.1.5.3 Cómo activar o desactivar la telecaptura de llamadas recordatorias.....716
15.1.5.4 Cómo agregar llamada de grupo (caso de libre o aviso de llamada en espera).....717
15.1.5.5 Cómo mostrar o modificar llamada de grupo (Caso de libre o Aviso de llamada en espera)..... 718
15.1.5.6 Cómo borrar llamada de grupo (caso de libre o aviso de llamada en espera).....718
15.1.5.7 Cómo agregar o borrar miembro a llamada de grupo (caso de libre o aviso de llamada en espera).....718
15.1.5.8 Cómo activar o desactivar el bloqueo de avisos de llamada en espera para miembro de grupo.....719
15.2 Configuración de equipo / Grupo Team y Jefe/Secretaria / Grupo Top..... 720
15.2.1 Configuración de equipo / Grupo Team.....720

15.2.2 Jefe/Secretaria / Grupo Top....724
15.2.3 Configuración de configuraciones de equipo / grupos Team y funciones Jefe/Secretaria / grupos Top mediante asistentes 728
15.2.3.1 Cómo añadir configuración de equipo / Grupo Team....729
15.2.3.2 Cómo modificar la configuración de equipo / Grupo Team....730
15.2.3.3 Cómo borrar configuración de equipo / Grupo Team....731
15.2.3.4 Cómo agregar grupos Jefe/secretaria / Top....732
15.2.3.5 Cómo modificar grupos Jefe/Secretaria / Top....733
15.2.3.6 Cómo borrar grupos Jefe/Secretaria /grupo Top....734
15.2.4 Configuración de configuraciones de equipo / grupos Team y funciones Jefe/Secretaria / grupos Top mediante el modo Experto....734
15.2.4.1 Cómo agregar o borrar un miembro a configuración de equipo / Grupo Team....735
15.2.4.2 Cómo modificar miembro de una configuración de equipo / Grupo Team....735
15.2.4.3 Cómo modificar las propiedades de los miembros de una configuración de equipo / Grupo Team....736
15.2.4.4 Cómo modificar la ocupación de teclas telefónicas para Configuración de equipo / Grupo Team....736
15.2.4.5 Cómo agregar un buzón de fax a la configuración de equipo / grupo Team....737
15.2.4.6 Cómo agregar o borrar un miembro a Jefe/secretaria (grupo Top)....737
15.2.4.7 Cómo modificar miembro de un Jefe/Secretaria (grupo Top)....738
15.2.4.8 Cómo modificar propiedades de los miembros de Jefe/secretaria (grupo Top)....738
15.2.4.9 Cómo agregar un buzón de fax a Jefe/secretaria (grupo Top)....739
15.3 MULAP básico y MULAP Jefe....739
15.3.1 MULAP básico....739
15.3.2 MULAP Jefe....742
15.3.3 Configuración de MULAP básicos y MULAP Jefe....744
15.3.3.1 Cómo agregar MULAP básico....745
15.3.3.2 Cómo mostrar o modificar MULAP básico....746
15.3.3.3 Cómo borrar MULAP básico....746
15.3.3.4 Cómo agregar o borrar miembro de MULAP básico....746
15.3.3.5 Cómo modificar miembro de un MULAP básico....747
15.3.3.6 Cómo agregar un MULAP Jefe....747
15.3.3.7 Cómo mostrar o modificar MULAP Jefe....748
15.3.3.8 Cómo borrar MULAP Jefe....748
15.3.3.9 Cómo agregar o borrar miembro de MULAP Jefe....749
15.3.3.10 Cómo modificar miembro de un MULAP Jefe....749
15.3.3.11 Cómo agregar un MULAP básico a un grupo....750
15.4 Grupo de buzón de voz y Grupo de buzón de fax....751
15.4.1 Grupo de buzón de voz....751
15.4.2 Grupo de buzón de fax....751
15.4.3 Configuración de grupos de buzón de voz y grupos de buzón de fax....752
15.4.3.1 Cómo añadir un grupo de buzón de voz....752
15.4.3.2 Cómo mostrar o modificar un grupo de buzón de voz....753
15.4.3.3 Cómo borrar un grupo de buzón de voz....753
15.4.3.4 Cómo agregar o borrar un miembro de un grupo de buzón de voz....754
15.4.3.5 Cómo modificar miembro de un grupo de buzón de voz....754
15.4.3.6 Cómo configurar un grupo de buzón de fax....755
15.4.3.7 Cómo mostrar o modificar un grupo de buzón de fax....756
15.4.3.8 Cómo borrar un grupo de buzón de fax....756
15.4.3.9 Cómo agregar o borrar un miembro de un grupo de buzón de fax....756
15.5 Mensajes directos para grupos....757
15.5.1 Mensaje a grupo....757
15.5.2 Transferencia a grupo desde mensaje....757
15.6 UCD (Uniform Call Distribution)....758
15.6.1 Distribución de llamadas (UCD)/Grupo UCD....759
15.6.1.1 Cómo configurar distribución de llamadas / Grupos UCD....760

15.6.2 Agentes UCD..... 761
15.6.2.1 Cómo agregar o eliminar agentes UCD..... 762
15.6.3 Tratamiento posterior..... 763
15.6.3.1 Cómo modificar el tiempo administrativo automático..... 763
15.6.4 Asignación de llamadas según prioridad..... 764
15.6.4.1 Cómo modificar la Asignación de llamadas según prioridad..... 765
15.6.5 Aceptar automáticamente llamadas UCD..... 765
15.6.5.1 Cómo modificar la aceptación automática de llamadas UCD..... 765
15.6.6 Cola de espera UCD..... 766
15.6.6.1 Cómo modificar cola de espera UCD..... 766
15.6.7 Desbordamiento UCD..... 767
15.6.7.1 Cómo modificar el desbordamiento UCD..... 768
15.6.8 Servicio nocturno UCD..... 768
15.6.9 Anuncios grabados/ música en espera en UCD..... 769
15.6.9.1 Cómo modificar anuncios grabados/ música en espera en UCD..... 769
15.6.10 Transferencia a grupos UCD..... 770
15.6.10.1 Cómo modificar el tiempo para la llamada recordatoria para llamadas transferidas a grupos UCD..... 771
15.6.11 Liberación de llamadas UCD a través de líneas analógicas..... 771
15.6.11.1 Cómo modificar el tiempo de liberación para llamadas UCD a través de líneas analógicas..... 771

16 Encaminamiento de llamadas..... 773
16.1 Clases de servicio (Control de marcación)..... 773
16.1.1 Grupos de clases de servicio y clases de servicio..... 773
16.1.1.1 Cómo modificar el nombre de un grupo de clases de servicio..... 774
16.1.1.2 Cómo modificar las clases de servicio de un grupo de clases de servicio..... 774
16.1.1.3 Cómo mostrar todos los usuarios de un grupo de clases de servicio..... 775
16.1.2 Listas de números prohibidos y autorizados..... 775
16.1.2.1 Cómo crear una lista de números de emergencia..... 776
16.1.2.2 Cómo crear una lista de números autorizados y de números prohibidos..... 777
16.1.2.3 Cómo crear más listas de números autorizados..... 777
16.1.2.4 Cómo crear más listas de números prohibidos..... 778
16.1.2.5 Cómo mostrar todos los números de teléfono de una lista de números prohibidos..... 778
16.1.2.6 Cómo mostrar todos los números de teléfono de una lista de números autorizados..... 779
16.1.2.7 Cómo modificar filtro de evaluación para lista de números prohibidos..... 779
16.1.3 Lista negra..... 779
16.1.3.1 Cómo crear una lista negra para las llamadas entrantes en el modo Experto..... 781
16.1.3.2 Cómo editar/eliminar números de llamada en la lista negra..... 781
16.1.3.3 Cómo mostrar los números de llamada en la lista negra..... 782
16.1.3.4 Cómo crear una lista negra para las llamadas entrantes en la Configuración..... 782
16.1.4 Serv. nocturno..... 783
16.1.4.1 Cómo asignar clases de servicio para el servicio nocturno manual..... 784
16.1.4.2 Cómo borrar clases de servicio para el servicio nocturno manual..... 784
16.1.4.3 Cómo configurar el servicio nocturno controlado por tiempo..... 785
16.1.4.4 Cómo configurar un Día especial para el servicio nocturno controlado por tiempo..... 785
16.1.4.5 Cómo borrar un día especial para el servicio nocturno controlado por tiempo..... 786
16.1.5 Conmutación de clase de servicio automática diferida..... 786
16.1.5.1 Plan horario..... 787
16.1.6 VBZ (Relaciones de tráfico)..... 788
16.1.6.1 Grupos VBZ (Grupos de relaciones de tráfico)..... 789
16.1.6.2 Asignación de números de marcación abreviada (KWZ) a grupos de relaciones de tráfico (VBZ)..... 789
16.1.6.3 Cómo asignar extensiones a un grupo de relaciones de tráfico (VBZ)..... 790
16.1.6.4 Cómo asignar una línea a un grupo de relaciones de tráfico (VBZ)..... 790
16.1.6.5 Cómo modificar una matriz VBZ..... 791
16.1.7 Candado telefónico central, Conmutación de clase de servicio..... 791

16.1.8 Candado telefónico individual (Candado Sí)..... 791
16.1.8.1 Cómo restablecer el candado personalizado..... 792
16.1.9 Bloqueo de llamadas a cobro revertido por línea urbana (solo para Brasil)..... 792
16.1.10 Bloqueo de llamadas a cobro revertido por extensión (solo Brasil)..... 793
16.2 LCR (Least Cost Routing, Ruta más económica)..... 793
16.2.1 Funcionalidad LCR..... 793
16.2.1.1 Cómo liberar LCR..... 796
16.2.2 Plan de marcación LCR..... 797
16.2.2.1 Cómo editar el plan de marcación..... 798
16.2.3 Tabla de rutas LCR..... 799
16.2.3.1 Cómo editar tablas de rutas..... 800
16.2.4 Autorización LCR..... 800
16.2.4.1 Cómo asignar y modificar autorizaciones LCR..... 801
16.2.5 Reglas de marcación LCR..... 801
16.2.5.1 Cómo editar reglas de marcación..... 803
16.2.6 Ofertante de red..... 804
16.2.7 Ocupación selectiva de líneas urbanas..... 805
16.2.7.1 Cómo configurar el código para la asignación selectiva de líneas urbanas RDSI..... 805
16.2.7.2 Cómo mostrar los códigos para la ocupación de línea urbana selectiva..... 806
16.3 Evaluación de marcación y encaminamiento de llamadas..... 806
16.3.1 Vista general de Call Routing / LCR..... 807
16.3.2 Diagrama de flujo de evaluación de marcación..... 809
16.3.3 Call Routing y LCR en la interred..... 810
16.3.3.1 Gateway dedicado..... 812
16.3.4 Escenarios: Evaluación de marcación y Call Routing (encaminamiento de llamadas)..... 813
16.3.4.1 La extensión A llama a la extensión B con el número de teléfono interno..... 814
16.3.4.2 La extensión A llama a la extensión B mediante un número de teléfono público..... 816
16.3.4.3 La extensión A llama a una extensión externa a través de la línea urbana..... 819
16.3.4.4 La línea urbana RDSI llama a la extensión A..... 820
16.3.4.5 Configuraciones especiales..... 820
16.3.4.6 La extensión A llama a la extensión C con un número interno..... 823
16.3.4.7 La extensión A llama a la extensión C con el número de teléfono público en la interred..... 824
16.3.4.8 La línea urbana RDSI llama a la extensión C..... 827
16.3.4.9 El gateway 1 de línea urbana RDSI llama a la extensión D..... 828
16.3.4.10 La extensión D llama a una extensión externa mediante la línea urbana..... 831
16.4 Llamadas de emergencia..... 833
16.4.1 Llamada de socorro / Hotline..... 834
16.4.1.1 Cómo configurar y modificar el destino de hotline..... 835
16.4.1.2 Cómo modificar el Tiempo de llamada de socorro..... 835
16.4.1.3 Cómo configurar la llamada de socorro o el hot-line para una extensión..... 835
16.4.2 Corte de línea para una llamada de emergencia..... 836
16.4.2.1 Cómo activar o desactivar Corte de línea para una llamada de emergencia..... 836
16.4.3 Solo para EE. UU., Canadá: Servicio de emergencia E911..... 837
16.4.3.1 Cómo editar CLIP / Lin..... 837
16.4.4 Llamadas de emergencia en combinación con Mobile Logon..... 838
16.4.4.1 Configuración del escenario de llamada de emergencia..... 838
16.4.5 Servicio de llamada de emergencia E112 para Europa..... 841
16.4.5.1 Cómo añadir un ID de ubicación ITSP a una extensión..... 841
16.5 Servicio de control de llamadas (Call Admission Control)..... 842
16.5.1 Restricción del número de llamadas simultáneas por ITSP..... 842
16.5.2 Restricción del ancho de banda necesario en llamadas de gateway..... 842
16.5.3 Restricción del número de llamadas en los escenarios de interconexión..... 842
16.6 Central compartida..... 843
16.6.1 Marcación abreviada central en centrales compartidas..... 844

17 Attendants..... 846

17.1 AutoAttendant ... 846
17.1.1 Company AutoAttendant (UC Smart) ... 848
17.1.1.1 Cómo configurar un Company AutoAttendant ... 849
17.1.1.2 Cómo configurar un Company AutoAttendant nuevo ... 850
17.1.2 Company AutoAttendant (UC Suite) ... 852
17.1.2.1 Planes horarios ... 852
17.1.2.2 Plantillas ... 861
17.2 OpenStage Attendant ... 862
17.3 OpenScape Business Attendant ... 863
17.3.1 OpenScape Business BLF ... 866
17.3.2 Ejemplos de configuración para OpenScape Business Attendant y OpenScape Business BLF ... 867
17.3.2.1 Escenario 1: OpenScape Business Attendant conectado a un sistema único OpenScape Business ... 867
17.3.2.2 Escenario 2: Dos o más OpenScape Business Attendant con un sistema individual OpenScape Business ... 872
17.3.2.3 Escenario 3: Interconexión de OpenScape Business con Attendants OpenScape Business propios (estado de presencia y BLF a nivel de red mediante WSI) ... 874
17.3.2.4 Escenario 4: Interconexión de OpenScape Business con el Attendant central de OpenScape Business (estado de presencia y BLF a nivel de red mediante WSI) ... 874
17.3.2.5 Escenario 5: OpenScape Business BLF conectado a un sistema individual OpenScape Business ... 875
17.3.2.6 Escenario 6: OpenScape Business BLF conectado en una interred OpenScape Business (estado de presencia y BLF mediante WSI) ... 877
17.4 myAttendant ... 877
17.4.1 Administración de extensiones ... 879
17.4.2 Centro de mensajes ... 879
17.4.3 Escenario 1: Cómo configurar myAttendant en un sistema individual OpenScape Business ... 880
17.4.4 Escenario 2: Cómo configurar uno o varios myAttendant en un sistema individual OpenScape Business ... 881
17.4.5 Escenario 3: Cómo configurar una interconexión OpenScape Business con myAttendant central ... 882
17.5 Puesto de interceptación ... 883
17.5.1 Cómo configurar criterios de interceptación y puesto de interceptación ... 885
17.5.2 Cómo configurar puesto de interceptación central ... 886
17.5.3 Cómo configurar la interceptación en caso de candado telefónico ... 886
17.5.4 Cómo configurar interceptación en caso de anuncio grabado ... 886

18 Multimedia Contact Center ... 888
18.1 Clientes de Contact Center ... 888
18.1.1 myAgent ... 889
18.1.2 Requisitos para myAgent ... 890
18.1.3 myReports ... 892
18.1.3.1 Cómo restablecer la contraseña de administrador de myReports ... 894
18.1.4 Requisitos para myReports ... 894
18.1.5 Observaciones sobre el uso simultáneo de myAgent y clientes de UC Suite ... 896
18.2 Agentes ... 897
18.2.1 Funciones según la clase de servicio para agentes ... 897
18.2.2 Agentes preferidos ... 898
18.2.3 Agente en varias colas de espera ... 899
18.2.4 Pausas de Contact Center ... 899
18.2.5 Inicio/Cierre de sesión de agente mediante el teléfono ... 899
18.3 Colas de espera y planes horarios ... 902
18.3.1 Colas de espera ... 902
18.3.2 Planes horarios ... 904
18.3.3 Terminar ... 913
18.3.4 Nivel de servicio ... 913
18.3.5 Tablero (Wallboard) ... 914

18.3.6 Devolución de llamadas de agentes....914
18.4 Asesoramiento VIP....914
18.4.1 Prioridad de llamantes VIP....915
18.4.2 Lista de llamadas VIP....915
18.5 Solución de respaldo (solución Fallback)....916
18.6 Configuración del Contact Center....919
18.6.1 Ejemplo de configuración de Contact Center....919
18.6.1.1 Cómo configurar grupos UCD para el ejemplo de Contact Center....921
18.6.1.2 Cómo configurar una solución de respaldo (solución Fallback) para el ejemplo de Contact Center....922
18.6.1.3 Cómo configurar extensiones como Agente para el ejemplo de Contact Center....923
18.6.1.4 Cómo grabar anuncios grabados para el ejemplo de Contact-Center....924
18.6.1.5 Cómo cargar anuncios grabados para el ejemplo de Contact Center....925
18.6.1.6 Cómo agregar el plan horario Standard Schedule XYZ para el ejemplo de Contact Center....925
18.6.1.7 Cómo agregar el plan horario Standard Schedule Hotline para el ejemplo de Contact Center...930
18.6.1.8 Cómo agregar colas de espera para el ejemplo de Contact Center....932
18.6.1.9 Cómo asignar agentes a las colas del ejemplo de Contact-Center....935
18.6.2 Procedimiento de configuración....936
18.6.2.1 Cómo configurar grupos UCD para el Contact Center....937
18.6.2.2 Cómo configurar extensiones como agentes....937
18.6.2.3 Cómo grabar un anuncio grabado personalizado para el Contact Center....938
18.6.2.4 Cómo cargar un anuncio grabado personalizado para el Contact Center....939
18.6.2.5 Cómo agregar un plan horario....939
18.6.2.6 Cómo modificar un plan horario....943
18.6.2.7 Cómo borrar un plan horario....944
18.6.2.8 Cómo guardar reglas (CCV) como archivo PDF....944
18.6.2.9 Cómo guardar reglas (CCV) como archivo PDF....945
18.6.2.10 Cómo cargar una regla descargada (CCV) en un formato de archivo de copia de seguridad...945
18.6.2.11 Cómo agregar una cola....946
18.6.2.12 Cómo modificar una cola....950
18.6.2.13 Cómo activar o desactivar la cola de espera....953
18.6.2.14 Cómo configurar un piloto para los mensajes de fax entrantes en colas....953
18.6.2.15 Cómo establecer valores nominales para el nivel de servicio....954
18.6.2.16 Cómo definir la prioridad de llamantes VIP....954
18.6.2.17 Cómo editar la lista de llamantes VIP....955
18.6.2.18 Cómo establecer agentes preferidos....956
18.6.2.19 Cómo borrar agentes preferidos....956
18.6.2.20 Cómo agregar una pausa de Contact Center....957
18.6.2.21 Cómo modificar la pausa de Contact Center....957
18.6.2.22 Cómo borrar pausas de Contact Center....958
18.6.2.23 Cómo agregar un motivo de tratamiento posterior para el "Tratamiento posterior simple"....958
18.6.2.24 Cómo modificar el motivo de tratamiento posterior para el "Tratamiento posterior simple"....958
18.6.2.25 Cómo borrar el motivo de tratamiento posterior para el "Tratamiento posterior simple"....959
18.6.2.26 Cómo agregar un motivo de tratamiento posterior para el "Tratamiento posterior múltiple"....959
18.6.2.27 Cómo modificar el motivo de tratamiento posterior para el "Tratamiento posterior múltiple"....960
18.6.2.28 Cómo borrar el motivo de tratamiento posterior para el "Tratamiento posterior múltiple"....961
18.6.2.29 Cómo asignar un agente a una cola....961
18.6.2.30 Cómo eliminar un agente de una cola....962
18.7 Observaciones sobre el uso del Contact Center....962
18.7.1 Restricciones de servicio del Contact Center....963
18.8 Observaciones sobre el uso de teléfonos DECT....966
18.9 Informes....967
18.9.1 Plantillas de informe predefinidas....968

19 Mobility....969
19.1 Soluciones de movilidad integradas....969

19.2 Movilidad fuera de casa/la oficina....969
19.2.1 myPortal to go....970
19.2.1.1 RequisitosmyPortal to go....972
19.2.2 Mobility Entry....974
19.2.3 Comparación entre extensiones móviles y Mobility Entry....975
19.2.4 Interdependencias para extensiones móviles y Mobility Entry....977
19.2.5 One Number Service (Servicio de número único)....979
19.2.6 Telefonía Dual-Mode....979
19.2.7 Configuración de myPortal to go y Mobility Entry....980
19.2.7.1 Cómo integrar un teléfono móvil GSM....981
19.2.7.2 Cómo integrar un teléfono Dual-Mode (GSM/WLAN) con cliente HFA o SIP....982
19.2.7.3 Cómo activar la interfaz Web para teléfonos móviles y clientes Web....984
19.2.7.4 Cómo borrar la integración de teléfono móvil....984
19.3 Movilidad en la oficina....985
19.3.1 Escritorio compartido....985
19.3.2 Solución Cordless integrada....986
19.3.2.1 Visión general del sistema....987
19.3.2.2 Conexión de módulos Cordless....988
19.3.2.3 Configuración del sistema....989
19.3.2.4 Teléfonos DECT/Cordless....991
19.3.2.5 Significado de los resultados de la prueba de área de cobertura....991
19.3.3 Configuración de la solución Cordless integrada....993
19.3.3.1 Cómo indicar la identificación de sistema DECT y configurar otros parámetros Cordless (datos a nivel del sistema)....993
19.3.3.2 Cómo configurar extensiones base Cordless....994
19.3.3.3 Cómo configurar por primera vez teléfonos DECT....994
19.3.3.4 Cómo iniciar sesión con un teléfono DECT (OpenStage/Gigaset-Mobilteil) en Cordless....995
19.3.3.5 Cómo añadir otros teléfonos DECT....997
19.3.3.6 Cómo borrar teléfonos DECT....997
19.3.3.7 Cómo configurar el parámetro Multi-SLC....998
19.3.3.8 Cómo consultar los datos de las extensiones base....999
19.3.3.9 Cómo activar el tono de aviso de MWI (Message Waiting Indication) para los teléfonos DECT....999
19.3.3.10 Cómo consultar el estado de registro de los teléfonos DECT....999
19.3.4 Cordless IP....1000
19.3.5 Teléfonos WLAN y puntos de acceso....1000
19.3.5.1 Requisitos de la WLAN....1000
19.4 Movilidad en el hogar....1001
19.4.1 Configuración de VPN....1002
19.4.2 Configuración de Equipo SIP@Home....1002
19.4.3 Configuración de Dispositivo de sistema@Casa....1004
19.4.4 Cómo activar Equipo@Home....1006
19.4.5 Cómo actualizar software para dispositivos de sistema (HFA) @Casa....1007
19.4.6 Cómo indicar un servidor STUN para Equipo@Home....1009

20 Seguridad....1010
20.1 Firewall....1010
20.1.1 Porthandling....1010
20.1.1.1 Liberación de puerto....1011
20.1.1.2 Cómo configurar Liberación de puerto....1011
20.1.1.3 Administración de puertos....1012
20.1.1.4 Cómo editar ajustes globales del Administrador de puertos....1012
20.1.2 NAT....1013
20.1.2.1 Cómo configurar regla NAT....1013
20.1.2.2 Cómo configurar varias reglas NAT con el editor de tablas NAT....1014
20.1.2.3 Cómo borrar regla NAT....1015

20.1.3 Cortafuegos de aplicaciones....1015
20.1.3.1 Cómo mostrar la configuración del Firewall de aplicación....1016
20.1.3.2 Cómo restringir servicios mediante el firewall de aplicación....1017
20.1.3.3 Cómo borrar la configuración del Firewall de aplicación....1017
20.1.4 Administración de servicios (OpenScape Business S)....1017
20.1.4.1 Cómo agregar o bloquear servicios....1018
20.2 Cifrado de datos de señalización y carga útil (SPE)....1019
20.2.1 Cómo activar o desactivar el soporte SPE....1021
20.2.2 Cómo modificar los ajustes de seguridad SPE....1021
20.2.3 Cómo importar el certificado SPE y la clave privada (PKCS#12)....1021
20.2.4 Cómo importar un certificado de entidad emisora SPE....1022
20.2.5 Cómo activar o desactivar SPE para una extensión....1022
20.3 Red privada virtual VPN 1023
20.3.1 Requisitos para VPN....1024
20.3.2 Conexión de teletrabajadores a través de VPN....1026
20.3.2.1 Cómo configurar conexión de teletrabajadores a través de VPN....1027
20.3.2.2 Cómo exportar los datos de teletrabajador....1029
20.3.3 Interconexión de sistemas de comunicación mediante VPN....1029
20.3.3.1 Cómo configurar la red mediante VPN....1030
20.3.3.2 Cómo exportar e importar datos de topología de una red VPN....1032
20.3.4 Mecanismos de seguridad VPN....1033
20.3.5 Certificados VPN....1035
20.3.5.1 VPN - Cómo generar certificados de entidad emisora Lightweight....1036
20.3.5.2 VPN - Administración de certificados - Cómo mostrar certificado....1037
20.3.5.3 VPN - Cómo importar certif. de entidad emisora de confianza (X.509)....1038
20.3.5.4 VPN - Certificados de par - Cómo generar Solicitud de certificado (CSR)....1038
20.3.5.5 Cómo generar un certificado de par de VPN (PKCS#12)....1039
20.3.5.6 VPN - Cómo importar certificado de par (PKCS#12)....1039
20.3.6 Clientes VPN....1040
20.3.6.1 Configuración de cliente VPN NCP....1041
20.3.6.2 Cómo configurar un cliente VPN NCP....1043
20.3.6.3 Cómo configurar un cliente VPN Shrew Soft....1044
20.3.6.4 Cómo configurar un cliente VPN iOS o Android....1044
20.3.6.5 Cómo configurar un cliente VPN Mac OSX....1045
20.3.7 VPN - Servicios....1046
20.3.7.1 VPN - Servicios activos - Cómo mostrar servicios IPSec....1046
20.3.7.2 VPN - Servicios activos - Cómo mostrar servicio IPSec especial....1046
20.3.7.3 VPN - Servicios configurados - Cómo mostrar servicios IPSec....1046
20.3.7.4 VPN - Servicios configurados - Cómo editar servicio IPSec....1047
20.3.7.5 VPN - Servicios configurados - Cómo cambiar nombre a servicio IPSec....1047
20.3.7.6 VPN - Servicios configurados - Cómo borrar servicio IPSec....1048
20.3.8 VPN - Túnel....1048
20.3.8.1 VPN - Túneles act. - Cómo mostrar datos generales de túnel....1048
20.3.8.2 VPN - Túneles act. - Cómo mostrar reglas de todos túneles....1049
20.3.8.3 VPN - Túneles config. - Cómo mostrar datos generales de túnel....1049
20.3.8.4 VPN - Túneles config. - Cómo mostrar reglas de todos túneles....1050
20.3.8.5 VPN - Cómo añadir túnel configurado....1050
20.3.9 VPN - Reglas....1052
20.3.9.1 VPN - Reglas activas - Cómo mostrar reglas....1052
20.3.9.2 VPN - Reglas activas - Cómo mostrar regla especial....1053
20.3.9.3 VPN - Reglas configuradas - Cómo mostrar todas las reglas....1053
20.3.9.4 VPN - Reglas configuradas - Cómo añadir regla....1053
20.3.9.5 VPN - Cómo editar regla....1054
20.3.9.6 VPN - Cómo añadir regla para dirección opuesta....1054
20.3.9.7 VPN - Cómo borrar regla....1055
20.3.10 Servidor PKI....1055

20.3.10.1 VPN - Cómo mostrar servidor PKI....1055
20.3.10.2 VPN - Cómo añadir servidor PKI....1056
20.4 Gestión de certificados....1056
20.4.1 Introducción....1057
20.4.2 Cómo generar certificado de entidad emisora....1058
20.4.3 Cómo generar certificado con firma automática....1059
20.4.4 Cómo generar una solicitud de certificado (CSR)....1059
20.4.5 Cómo importar un certificado de servidor (PKCS#12)....1061
20.4.6 Cómo importar certificados de servidor (PEM)....1062
20.4.7 Cómo mostrar certificados....1062
20.4.8 Cómo borrar un certificado....1063
20.4.9 Cómo exportar un certificado (X.509)....1063
20.4.10 Cómo importar certificado renovado (X.509)....1063
20.4.11 Cómo activar un certificado....1064
20.4.12 Gestión de certificados para Booster Server....1064
20.5 Seguridad Web....1065
20.5.1 Conexiones con el servidor Web....1065
20.5.1.1 Cómo configurar las conexiones con el servidor Web (UC Suite)....1065
20.5.1.2 Cómo configurar las conexiones con el servidor Web (UC Smart)....1066
20.5.2 Protocolo admin....1066
20.5.2.1 Cómo cargar protocolo admin....1066
20.5.2.2 Cómo modificar el idioma del protocolo de administración....1067
20.6 Seguridad SQL....1067
20.6.1 Nodo único....1067
20.6.2 Varios nodos....1068
20.6.3 Cómo configurar contraseñas para la base de datos SQL....1069
20.7 Protección frente a ataques SIP (SIP Attack Protection)....1069

21 Interconexión de OpenScape Business....1071
21.1 Plan de interconexión....1072
21.1.1 Redes homogéneas y no homogéneas....1072
21.1.1.1 Cómo mostrar la vista general de todos los nodos OpenScape Business....1073
21.1.2 Gateway único y multigateway....1073
21.2 Prestaciones a nivel de red....1074
21.2.1 Prestaciones a nivel de red de las soluciones de UC....1074
21.2.2 Prestaciones de voz a nivel de red....1077
21.3 Registro de licencia de una interconexión....1079
21.4 Requisitos de la interconexión....1079
21.4.1 Requisitos a la interconexión LAN....1080
21.4.2 Plan de numeración en la red....1081
21.4.2.1 Marcación de números de teléfono públicos en la red....1082
21.5 Optimización de rutas (Path Replacement)....1083
21.5.1 Cómo activar o desactivar la optimización de rutas (Path Replacement)....1083
21.6 Escenarios de interconexión....1084
21.6.1 Interdependencias y restricciones....1084
21.6.2 Interconexión de varios OpenScape Business X....1085
21.6.2.1 Cómo configurar la instalación básica para el nodo 1 (maestro)....1089
21.6.2.2 Cómo configurar la interconexión para el nodo 1 (maestro)....1090
21.6.2.3 Cómo configurar la instalación básica para el nodo 2 (esclavo)....1091
21.6.2.4 Cómo configurar la interconexión para el nodo 2 (esclavo)....1092
21.6.2.5 Cómo controlar la función de interconexión del maestro....1092
21.6.2.6 Cómo configurar parámetros de ruta y rutas (línea urbana RDSI para el maestro)....1093
21.6.2.7 Cómo configurar direcciones y parámetros de ruta (Ruta 16) (maestro)....1094
21.6.2.8 Cómo configurar LCR para la interconexión (maestro)....1094
21.6.2.9 Cómo configurar la dirección y parámetros de ruta (esclavo)....1095
21.6.2.10 Cómo configurar LCR para la interconexión (esclavo)....1096

21.6.3 Interconexión de OpenScape Business X con OpenScape Business S (Gateway único)....1097
21.6.3.1 Cómo configurar la instalación básica para el nodo 1 (maestro)....1103
21.6.3.2 Cómo configurar la interconexión para el nodo 1 (maestro)....1104
21.6.3.3 Cómo configurar la instalación básica para el nodo 2 (esclavo)....1105
21.6.3.4 Cómo configurar la interconexión para el nodo 2 (esclavo)....1106
21.6.3.5 Cómo configurar la instalación básica para el nodo 3 (esclavo)....1107
21.6.3.6 Cómo controlar la función de interconexión del maestro....1108
21.6.3.7 Configuración de la interconexión para el nodo 3 (esclavo)....1108
21.6.3.8 Cómo configurar LCR para la interconexión (nodo 3, esclavo)....1109
21.6.3.9 Cómo configurar LCR para la interconexión (nodo 2)....1110
21.6.3.10 Cómo configurar direcciones y parámetros de ruta (nodo 1, maestro)....1112
21.6.3.11 Cómo configurar direcciones y parámetros de ruta (Ruta 16) (Nodo 1)....1112
21.6.3.12 Cómo configurar LCR para la interconexión (nodo 1)....1113
21.6.4 Interconexión de OpenScape Business X y OpenScape Business S (multigateway)....1115
21.6.4.1 Cómo configurar la instalación básica para el nodo 4 (OpenScape Business S, maestro)....1123
21.6.4.2 Cómo configurar la interconexión para el nodo 4 (maestro)....1124
21.6.4.3 Cómo configurar la instalación básica para el nodo 1 (esclavo)....1124
21.6.4.4 Cómo configurar la interconexión para el nodo 1 (esclavo)....1125
21.6.4.5 Cómo configurar la instalación básica para el nodo 2 (esclavo)....1126
21.6.4.6 Cómo configurar la interconexión para el nodo 2 (esclavo)....1127
21.6.4.7 Cómo configurar la instalación básica para el nodo 3 (esclavo)....1127
21.6.4.8 Cómo configurar la interconexión para el nodo 3 (esclavo)....1128
21.6.4.9 Cómo controlar la función de interconexión del maestro....1129
21.6.4.10 Cómo configurar multi-gateway para el nodo 4 (maestro)....1129
21.6.4.11 Cómo configurar la dirección y los parámetros de ruta (nodo 1, esclavo)....1130
21.6.4.12 Cómo configurar LCR para la interconexión (nodo 1, esclavo)....1131
21.6.4.13 Cómo configurar la dirección y los parámetros de ruta (nodo 2, esclavo)....1133
21.6.4.14 Cómo configurar LCR para la interconexión (nodo 2, esclavo)....1134
21.6.4.15 Cómo configurar la dirección y los parámetros de ruta (nodo 3, esclavo)....1136
21.6.4.16 Cómo configurar LCR para la interconexión (nodo 3, esclavo)....1136
21.6.4.17 Cómo configurar la dirección y parámetros de ruta (nodo 4, maestro)....1138
21.6.4.18 Cómo configurar LCR para la interconexión (nodo 4, maestro)....1139
21.6.5 Interconexión de OpenScape Business en entornos de hosting....1142
21.6.6 Interconexión de OpenScape Business X y OpenScape 4000....1145
21.6.7 Interconexión de OpenScape Business X y OpenScape Voice....1152
21.6.8 Conectar equipo auxiliar externo con OpenScape Business mediante la interconexión SIP....1155
21.6.9 Numeración abierta en redes OpenScape Business X....1156
21.6.9.1 Cómo configurar la numeración abierta....1157
21.6.10 Interconexión mediante RDSI....1159
21.6.11 Interred OpenScape Business con conexión central de línea urbana ITSP....1160
21.7 Puesto de interceptación central en la interred (no para EE. UU.)....1162
21.7.1 Cómo configurar un puesto de interceptación central en una interred multigateway....1163
21.8 Gestor de presencia....1165
21.9 Estado de sincronización en la interred....1165
21.9.1 Sincronización manual en la interred....1166
21.9.2 Cómo iniciar la sincronización manual....1167
21.10 Supervivencia....1167
21.10.1 Cómo configurar Survivability....1169
21.11 Eliminación de un nodo de la interred....1170

22 Equipo externo....1171
22.1 Equipo de anuncios grabados analógico....1171
22.1.1 Cómo añadir un equipo de anuncios grabados analógico....1172
22.1.2 Cómo modificar el retraso de anuncio grabado....1173
22.2 Portero eléctrico y Abrepuertas....1173
22.2.1 DoorLine a/b T01-T04....1173

22.2.1.1 Cómo configurar el puerto de extensión del Doorline a/b T01-T04....1174
22.2.1.2 Cómo configurar la extensión para Doorline a/b T01-T04....1175
22.2.2 DoorCom Analog....1175
22.2.2.1 Cómo configurar el puerto de extensión del DoorCom analógico....1176
22.2.2.2 Cómo configurar la extensión para el DoorCom Analog....1176
22.2.3 Dispositivo de portero eléctrico con amplificador (TFE-S)....1176
22.2.3.1 Cómo configurar el Portero eléctrico....1178
22.2.4 Altavoz....1178
22.2.4.1 Cómo configurar la interfaz de extensión analógica para un altavoz....1179
22.2.4.2 Cómo configurar la interfaz de extensión analógica para conectar un amplificador en el módulo TFE S....1180
22.3 Contactos....1180
22.3.1 Cómo configurar un contacto....1182
22.4 Sensores....1182

23 Application Connectivity....1185
23.1 CSTA....1185
23.1.1 Cómo modificar el número de puerto para CSTA....1187
23.1.2 Cómo activar o desactivar el CMD para utilizar TAPI 120....1188
23.1.3 Cómo activar o desactivar el servidor DSS para utilizar teclas DSS a nivel de red....1188
23.1.4 Cómo activar o desactivar el CSP....1189
23.1.5 Cómo activar o desactivar el Media Extension Bridge....1189
23.2 OpenScape Business TAPI 120/170....1190
23.2.1 OpenScape Business TAPI 120....1191
23.2.2 OpenScape Business TAPI 170....1195
23.3 Interfaz de Web Services....1200
23.4 Open Directory Service....1201
23.4.1 Cómo activar o desactivar Open Directory Service....1206
23.4.2 Cómo reiniciar Open Directory Service....1206
23.4.3 Cómo configurar la contraseña ara acceder a Open Directory Service....1206
23.4.4 Cómo configurar el ODBC-ODBC Bridge Server....1207
23.4.5 Cómo añadir una fuente de datos externa para Open Directory Service....1209
23.4.6 Cómo ejecutar una vista preliminar de los resultados de búsqueda LDAP para el Open Directory Service....1212
23.4.7 Cómo borrar una fuente de datos externa para Open Directory Service....1212
23.5 Servicio de integración de Active Directory....1213
23.5.1 Cómo configurar el servicio de Active Directory....1214
23.6 Application Launcher....1215
23.6.1 Requisitos para Application Launcher....1216
23.6.2 Perfil con datos de configuración de Application Launcher....1216
23.6.2.1 Cómo ofrecer un perfil con datos de configuración desde Application Launcher....1217
23.7 Descripción general de myPortal for Teams....1217
23.7.1 Cómo configurar MyPortal para Teams....1218
23.7.2 Cómo cargar myPortal para Teams en la tienda de Teams....1218
23.8 Unify Phone....1219
23.8.1 Cómo configurar la conectividad del Unify Phone....1220
23.8.2 Cómo configurar la instancia de usuario de Unify Phone....1221
23.8.3 Cómo gestionar usuarios de Unify Phone....1221
23.8.3.1 Cómo crear nuevos usuarios de Unify Phone....1222
23.8.3.2 Cómo agregar usuarios existentes de Unify Phone....1222
23.8.3.3 Cómo editar los datos de usuario de Unify Phone....1223
23.8.3.4 Cómo eliminar o eliminar usuarios de Unify Phone....1224
23.8.3.5 Cómo configurar las opciones de número alternativo y encaminamiento de llamadas para interconectividad de Unify Phone....1225
23.9 Servicio Let's Encrypt....1225
23.9.1 Cómo configurar el servicio Let's Encrypt....1225

23.10 CloudLink Service....1226
23.10.1 Cómo configurar CloudLink Service....1227
23.10.2 Cómo abrir la interfaz web de CloudLink Daemon....1227
23.10.3 Cómo configurar la interfaz web de CloudLink Daemon....1228
23.10.4 Cómo habilitar/configurar el conector SIP para conectarse a Workflow Studio....1228
23.11 Números piloto de CloudLink....1229
23.11.1 Cómo configurar los números piloto de CloudLink....1229

24 Accounting....1231
24.1 Datos de conexión....1231
24.1.1 Registro de datos de conexión....1231
24.1.1.1 Cómo activar o desactivar el registro de datos de conexión....1232
24.1.1.2 Cómo activar o desactivar el registro de la duración de la conexión....1232
24.1.1.3 Cómo configurar la protocolización de importes o unidades de tarificación....1233
24.1.1.4 Cómo configurar Factor de tarificación, Moneda y Exactitud del cálculo....1233
24.1.1.5 Cómo activar o desactivar la protocolización de las cuatro últimas cifras....1234
24.1.1.6 Cómo activar o desactivar la protocolización de llamadas salientes sin conexión....1234
24.1.1.7 Cómo activar o desactivar la protocolización de conexiones entrantes....1234
24.1.1.8 Cómo activar o desactivar el protocolo de conexión....1235
24.1.1.9 Cómo activar o desactivar la protocolización de los MSN....1235
24.1.1.10 Cómo activar o desactivar el formato decimal....1236
24.1.2 Códigos de proyecto....1236
24.1.2.1 Cómo configurar un código de proyecto....1237
24.1.2.2 Cómo configurar un procedimiento de prueba de código de proyecto (PRO)....1237
24.1.2.3 Cómo activar o desactivar la rellamada con PRO....1238
24.2 Indicación y transferencia de datos de conexión....1238
24.2.1 Transmisión de importes (no para los EE. UU.)....1238
24.2.1.1 Cómo configurar la transmisión de importes....1239
24.2.2 Indicación de los gastos de conexión en el teléfono....1239
24.2.3 Indicación de la duración de la conexión en el teléfono....1240
24.2.3.1 Cómo activar o desactivar la muestra la duración de la conexión....1240
24.2.4 Transmisión de datos de conexión....1240
24.2.4.1 Cómo seleccionar el formato....1248
24.2.4.2 Cómo activar o desactivar la transferencia de datos de conexión por HTTPS....1248
24.3 Control de gastos....1248
24.3.1 Aviso de rutas de enlace caras....1249
24.3.1.1 Cómo configurar una advertencia para rutas de enlace poco económicas....1249
24.3.2 Protección ante abuso en las tarifas....1249
24.3.2.1 Cómo activar o desactivar la protección contra el abuso de tasas....1249
24.4 Accounting-Tools....1250
24.4.1 Accounting Manager....1250
24.4.2 Teledata Office....1250

25 Mantenimiento....1251
25.1 Configuración de telefonía....1251
25.1.1 Fecha y hora....1251
25.1.1.1 Cómo configurar la fecha y hora manualmente....1252
25.1.1.2 Cómo configurar la zona horaria....1252
25.1.1.3 Cómo configurar el formato de fecha....1253
25.1.2 SNTP....1253
25.1.2.1 Cómo obtener la fecha y hora de un servidor SNTP....1253
25.1.3 Logotipos telefónicos....1254
25.1.3.1 Cómo cargar un logotipo telefónico en el sistema....1254
25.1.3.2 Cómo distribuir un logotipo telefónico a teléfonos del sistema....1255
25.1.3.3 Cómo borrar un logotipo telefónico....1255
25.1.4 Indicación en display personalizada....1255

25.1.4.1 Cómo modificar la indicación en display específica de cliente (Nombre del sistema)....1256
25.1.5 Salida de texto multilingüe....1256
25.1.6 Menús flexibles....1256
25.1.6.1 Cómo cambiar el menú flexible....1257
25.1.7 Música en espera....1257
25.1.7.1 Cómo importar la música en espera interna....1258
25.1.7.2 Cómo configurar la función de música en espera interna....1259
25.1.7.3 Cómo modificar la música en espera interna para cada grupo de relaciones de tráfico....1259
25.1.8 Anuncio grabado....1260
25.1.8.1 Cómo configurar anuncios (UC Suite)& Refuerzo de UC)....1261
25.1.8.2 Cómo configurar anuncios (UC Smart)....1262
25.1.9 Señalización de usuario a usuario....1263
25.1.10 Protección de señalización en el canal telefónico....1263
25.1.11 Parámetros de tiempo....1263
25.1.12 Control de prestaciones Centrex....1263
25.1.12.1 Cómo activar o desactivar el control de prestaciones Centrex....1264
25.2 Capítulo 24.2 Copia de seguridad y recuperación de datos....1264
25.2.1 Conjuntos de copias de seguridad....1265
25.2.1.1 Cómo ver los conjuntos de copias de seguridad....1266
25.2.1.2 Cómo borrar conjuntos de copias de seguridad....1266
25.2.2 Medios de copia de seguridad....1266
25.2.2.1 Agregar un medio de copia de seguridad....1267
25.2.2.2 Cómo editar un medio de copia de seguridad....1269
25.2.2.3 Cómo borrar un medio de copia de seguridad....1269
25.2.3 Almacenamiento inmediato....1269
25.2.3.1 Cómo guardar un conjunto de copias de seguridad inmediatamente....1270
25.2.4 Copia de seguridad programada....1271
25.2.4.1 Cómo guardar un conjunto de copias de seguridad programado....1272
25.2.5 Recuperar....1272
25.2.5.1 Cómo recuperar un conjunto de copias de seguridad....1273
25.3 Actualizaciones....1273
25.3.1 Uso de un servidor Web local....1275
25.3.1.1 Cómo configurar el acceso al servidor Web local....1276
25.3.2 Actualización del sistema de comunicación....1277
25.3.2.1 Cómo actualizar el sistema a través de un servidor Web....1278
25.3.2.2 Cómo actualizar el sistema con un soporte USB....1280
25.3.2.3 Cómo actualizar el sistema mediante una carga de archivo....1281
25.3.2.4 Cómo actualizar el sistema mediante un soporte USB sin acceso a la Gestión basada en Web (WBM)....1282
25.3.3 Actualización de los teléfonos de sistema....1283
25.3.3.1 Cómo cargar el software de teléfono en el sistema....1284
25.3.3.2 Cómo distribuir el software telefónico a los teléfonos del sistema....1284
25.3.3.3 Cómo borrar el software telefónico....1285
25.3.3.4 Cómo activar o desactivar la distribución automática del software telefónico....1285
25.3.3.5 Cómo configurar la reactualización automática....1286
25.3.4 Estado de software....1287
25.3.4.1 Cómo consultar el estado de software....1287
25.4 Restart, Reload, Shutdown....1288
25.4.1 Reinicio (Restart) de OpenScape Business....1288
25.4.1.1 Cómo activar un reinicio (Restart) de OpenScape Business....1289
25.4.2 Recarga (Reload) de OpenScape Business....1289
25.4.2.1 Cómo activar una recarga (Reload) de OpenScape Business....1290
25.4.3 Shutdown (apagado) de OpenScape Business X....1291
25.4.3.1 Cómo apagar OpenScape Business X....1291
25.4.4 PIN para el apagado controlado (Shutdown) de OpenScape Business X....1291
25.4.4.1 Cómo configurar un PIN para el apagado controlado (Shutdown) de OpenScape Business X.1292

25.4.5 Reiniciar (Restart) de la UC Booster Card (Tablero de aplicaciones OCAB)....1292
25.4.5.1 Cómo iniciar un reinicio (Restart) de la UC Booster Card (Tablero de aplicaciones OCAB)....1292
25.4.6 Recarga (Reload) de la UC Booster Card (Tablero de aplicaciones OCAB)....1293
25.4.6.1 Cómo iniciar un recarga (reload) de la UC Booster Card (Tablero de aplicaciones OCAB)....1293
25.4.7 Reinicio (Restart) de la aplicación de UC....1294
25.4.7.1 Cómo activar un reinicio (Restart) de la aplicación de UC....1294
25.5 Gestión de inventario....1294
25.5.1 Estado del sistema 1295
25.5.1.1 Cómo consultar el estado de extensiones....1296
25.5.1.2 Cómo consultar el estado del establecimiento de conexión....1296
25.5.1.3 Cómo consultar el estado de ITSP....1297
25.5.1.4 Cómo mostrar direcciones IP....1297
25.5.2 Inventario....1298
25.5.2.1 Cómo consultar el inventario de OpenScape Business X....1299
25.5.2.2 Cómo consultar el inventario de OpenScape Business S....1301
25.6 Acciones automát....1301
25.6.1 Acción automática Garbage Collection....1301
25.6.1.1 Cómo modificar la acción automática Garbage Collection....1302
25.6.1.2 Cómo iniciar la acción automática Garbage Collection (activación)....1303
25.6.1.3 Cómo detener la acción automática Garbage Collection (desactivación)....1303
25.6.2 Acción automática Notificación DLS....1303
25.6.2.1 Cómo modificar la acción automática Notificación DLS....1304
25.6.2.2 Cómo iniciar la acción automática Notificación DLS (activación)....1304
25.6.2.3 Cómo detener la acción automática Notificación DLS (desactivación)....1305
25.6.3 Mecanismo de advertencia para la vida útil de la tarjeta SDHC....1305
25.6.3.1 Cómo establecer una notificación en caso de errores en la tarjeta SDHC....1307
25.6.3.2 Cómo iniciar la acción automática "Mecanismo de advertencia para la vida útil de la tarjeta SDHC"....1307
25.6.3.3 Cómo clonar y cambiar una tarjeta SDHC....1308
25.6.3.4 Cómo crear un archivo de copia de seguridad de datos SDHC....1309
25.6.3.5 Cómo sustituir una tarjeta SDHC....1311
25.7 Gestión de energía....1313
25.7.1 Cómo activar o desactivar la gestión de energía....1314
25.7.2 Cómo modificar el modo Ethernet-Link de las interfaces LAN....1315
25.8 Supervisión y mantenimiento de OpenScape Business....1315
25.8.1 Comprobación de una conexión de red de OpenScape Business X....1316
25.8.1.1 Cómo enviar ping....1316
25.8.1.2 Cómo comprobar Traceroute....1316
25.8.2 SNMP (Simple Network Management Protocol)....1317
25.8.2.1 Cómo mostrar todas las comunidades....1329
25.8.2.2 Cómo añadir comunidad....1329
25.8.2.3 Cómo editar comunidad....1330
25.8.2.4 Cómo borrar comunidad....1330
25.8.2.5 Cómo mostrar traps....1330
25.8.2.6 Cómo mostrar detalles de una trap....1331
25.8.3 Acciones manuales....1331
25.8.3.1 Cómo descargar Datos de diagnóstico / Protocolos de diagnóstico....1334
25.8.4 Traces....1335
25.8.4.1 Cómo descargar un archivo de protocolo de de trace del sistema....1341
25.8.4.2 Cómo borrar un archivo de protocolo de trace del sistema....1342
25.8.4.3 Cómo restablecer los valores estándar de los ajustes Trace....1342
25.8.4.4 Cómo mostrar todos perfiles trace....1343
25.8.4.5 Cómo iniciar o detener un perfil trace....1344
25.8.4.6 Cómo mostrar o modificar la configuración de formato trace....1344
25.8.4.7 Cómo mostrar o modificar las interfaces de salida trace....1345
25.8.4.8 Cómo mostrar o modificar el protocolo Visor de sucesos / protocolo Trace de cliente....1345

25.8.4.9 Cómo descargar o abrir protocolo Visor de sucesos / protocolo Trace de cliente....1345
25.8.4.10 Cómo borrar protocolo Visor de sucesos / protocolo trace de cliente....1346
25.8.4.11 Cómo mostrar los componentes trace M5T....1346
25.8.4.12 Cómo iniciar o detener un componente trace M5T....1347
25.8.4.13 Cómo editar componentes M5T-Trace....1347
25.8.4.14 Cómo iniciar o detener Secure Trace....1347
25.8.4.15 Cómo consultar el estado de Secure Trace....1348
25.8.4.16 Cómo modificar la contraseña para el Secure Trace....1348
25.8.4.17 Cómo importar el certificado para el Secure Trace a partir de un archivo X.509....1349
25.8.4.18 Cómo mostrar o modificar una configuración Trace de pila H.323....1349
25.8.4.19 Cómo editar módulos H.323....1349
25.8.4.20 Cómo descargar o abrir Protocolo trace de pila H.323....1350
25.8.4.21 Cómo borrar protocolo trace pila H.323....1350
25.8.4.22 Cómo modificar el trace de componentes de licencia....1350
25.8.4.23 Cómo mostrar detalles de un perfil Trace....1351
25.8.4.24 Cómo detener todos los perfiles trace....1351
25.8.4.25 Cómo agregar perfil Trace....1352
25.8.4.26 Cómo mostrar los componentes trace....1352
25.8.4.27 Cómo mostrar detalles de un componente Trace....1352
25.8.4.28 Cómo iniciar o detener un componente trace....1353
25.8.4.29 Cómo detener todos los componentes trace....1353
25.8.4.30 Cómo restablecer los valores estándar de los ajustes Trace....1353
25.8.4.31 Cómo editar componentes trace....1354
25.8.4.32 Cómo reenviar archivos de protocolo del sistema automáticamente....1354
25.8.4.33 Cómo iniciar el servicio de datos Kernel Crash....1355
25.8.4.34 Cómo detener el servicio de datos de Kernel Crash....1356
25.8.4.35 Cómo iniciar el Trace del servidor de medios....1356
25.8.4.36 Cómo detener el Trace del servidor de medios....1356
25.9 TCP Dump....1357
25.9.1 Cómo iniciar TCP Dump....1357
25.9.2 Cómo detener TCP Dump....1357
25.9.3 Cómo borrar TCP Dump....1358
25.10 Daemon RPCAP....1358
25.10.1 Cómo activar RPCAP Daemon....1359
25.10.2 Cómo desactivar RPCAP Daemon....1359
25.11 Sucesos....1359
25.11.1 Cómo modificar la protocolización de sucesos por LAN....1361
25.11.2 Cómo descargar el archivo de protocolo de sucesos....1362
25.11.3 Cómo borrar archivo de protocolo de sucesos....1362
25.11.4 Cómo modificar configuración de correo electrónico por sucesos....1362
25.11.5 Cómo mostrar la Tabla reacción sucesos....1363
25.11.6 Cómo modificar la configuración de reacción de un suceso....1363
25.11.7 Cómo modificar la configuración de reacción de varios sucesos....1364
25.11.8 Cómo descargar o abrir protocolos de diagnóstico....1365
25.11.9 Cómo borrar protocolos diagnóstico....1365
25.11.10 Cómo definir los destinos para la señalización de alarmas....1366
25.12 Datos de configuración para el diagnóstico....1366
25.12.1 Cómo crear datos de configuración para el diagnóstico....1367
25.13 Card Manager....1368
25.13.1 Cómo escribir con el Card Manager el software de comunicación en M.2 SATA SSD....1369
25.13.2 Cómo escribir con el Card Manager el software de comunicación en la tarjeta SDHC....1371
25.13.3 Cómo escribir con el Card Manager el software de comunicación en el disco duro OCAB....1373
25.14 Supervisión y mantenimiento de la UC Suite....1375
25.14.1 Protocolización....1375
25.14.1.1 Cómo activar o desactivar el registro de los protocolos de sistema....1377
25.14.1.2 Cómo activar o desactivar el registro de los Client-Logs a nivel de sistema....1377

25.14.1.3 Cómo activar o desactivar el registro de los Client-Logs a nivel de extensión....1378
25.14.1.4 Cómo configurar la ruta de almacenamiento para los archivos de registro de cliente....1378
25.14.1.5 Cómo activar o desactivar la memorización central de los registros de cliente en el disco duro....1379
25.14.1.6 Cómo descargar Client Logs de todas las extensiones internas....1380
25.14.2 Notificación....1380
25.14.2.1 Cómo configurar notificaciones por correo electrónico de errores del sistema....1382
25.14.3 Mantenimiento....1383
25.14.3.1 Cómo configurar la hora para el mantenimiento....1384
25.14.3.2 Cómo configurar el periodo de retención de los archivos de protocolo....1385
25.14.3.3 Cómo ejecutar un mantenimiento del sistema inmediato....1385
25.14.3.4 Cómo configurar el tiempo de retención para los datos del Contact Center....1386
25.15 Supervisión de UC Smart....1386
25.15.1 Cómo consultar el estado actual de UC Smart....1386
25.16 Servicios remotos....1386
25.16.1 RSP.servicelink....1387
25.16.1.1 Cómo instalar, configurar y registrar el plugin RSP.servicelink....1390
25.16.1.2 Cómo activar el plugin RSP.servicelink....1391
25.16.1.3 Cómo desactivar el plugin RSP.servicelink....1392
25.16.1.4 Cómo restablecer el plugin de servicio RSP....1392
25.16.1.5 Cómo configurar un PIN para activar y desactivar el plugin RSP.servicelink....1393
25.16.2 Acceso remoto....1393
25.16.2.1 Cómo activar el acceso remoto por RDSI....1394
25.16.2.2 Cómo configurar un PC con Microsoft Windows Vista para el acceso remoto a través de RDSI....1394
25.16.2.3 Cómo configurar un PC con Microsoft Windows 7 para el acceso remoto a través de RDSI..1396
25.16.2.4 Cómo activar el acceso remoto a través de acceso a Internet con dirección IP fija....1397
25.16.2.5 Cómo activar el acceso remoto a través de acceso a Internet sin dirección IP fija....1398
25.16.2.6 Cómo desactivar el acceso remoto....1399
25.16.3 Usuario online....1399
25.16.3.1 Cómo iniciar el Usuario online....1400

26 Migración....1401
26.1 Actualización de software para sistemas OpenScape Business X....1402
26.1.1 Actualización de software de OpenScape Business X V2 a OpenScape Business X V3....1403
26.1.1.1 Actualización de software de sistemas con licencia permanente con CLS Connect....1404
26.1.1.2 Actualización de software de sistemas con licencia permanente sin CLS Connect....1404
26.1.1.3 Actualización de software de sistemas con licencia PayGo....1405
26.2 Actualización de software de UC Booster Server a OpenScape Business X V3....1405
26.2.1 Cómo actualizar UC Business Booster Server v2 a v3....1405
26.3 Migración de hardware/software de los sistemas OpenScape Business X a V3....1407
26.3.1 Migración de OpenScape Business X V2 a OpenScape Business X V3....1408
26.3.1.1 Cómo migrar con CLS Connect a los sistemas con licencia permanente V3....1409
26.3.1.2 Cómo migrar sin CLS Connect a los sistemas con licencia permanente V3....1410
26.3.1.3 Cómo migrar a los sistemas con licencia PayGo V3....1411
26.4 Migración de un sistema OpenScape Business X V3 de placa base V2 a placa base V3....1412
26.4.1 Cómo migrar con CLS Connect a los sistemas con licencia permanente de placa base V3....1414
26.4.2 Cómo migrar sin CLS Connect a los sistemas con licencia permanente de placa base V3....1415
26.4.3 Cómo migrar a los sistemas con licencia PayGo de placa base V3....1416
26.5 Actualización de software de OpenScape Business S....1416
26.5.1 Actualización de software de OpenScape Business S V2 a OpenScape Business S V3....1417
26.5.1.1 Cómo actualizar con CLS Connect a los sistemas con licencia permanente V3....1418
26.5.1.2 Cómo actualizar a sistemas con licencia PayGo V3....1419
26.5.2 Actualización de software de OpenScape Business S V2 a OpenScape Business S V3....1419
26.6 Migración/actualización de una red OpenScape Business V2 a V3....1420

26.6.1 Escenario 1: Migración de hardware de nodo maestro; actualización de software de nodos esclavos.....1422
26.6.1.1 Migración/actualización con CLS Connect en el nodo maestro.....1422
26.6.1.2 Migración/actualización sin CLS Connect en el nodo maestro.....1423
26.6.2 Escenario 2: Actualización de software de todos los sistemas en la red a V3.....1424
26.6.2.1 Actualización de software con CLS Connect en el nodo maestro.....1424
26.6.2.2 Actualización de software sin CLS Connect en el nodo maestro.....1425
26.6.3 Escenario 3a: Actualización de software de todos los nodos.....1426
26.6.4 Escenario 3b: Actualización de software en el nodo maestro; migración de hardware de los nodos esclavos.....1426
26.6.4.1 Migración/actualización con CLS Connect en el nodo maestro.....1426
26.6.4.2 Migración/actualización sin CLS Connect en el nodo maestro.....1427
26.7 Migración de HiPath 3000 a OpenScape Business V3.....1428
26.7.1 Migración de HiPath 33xx, 35xx, 3800 a OpenScape Business X3/X5/X8 V3.....1430
26.7.1.1 Cómo cargar la memoria de datos de cliente (KDS) desde HiPath 3000.....1434
26.7.1.2 Cómo consultar los ajustes de configuración de HG1500.....1435
26.7.1.3 Cómo convertir la memoria de datos de cliente (KDS) de HiPath 3000.....1435
26.7.1.4 Cómo sustituir el hardware de HiPath 3300/3500.....1436
26.7.1.5 Cómo sustituir el hardware de HiPath 3350/3550.....1437
26.7.1.6 Cómo sustituir el hardware con el HiPath 3800.....1438
26.7.1.7 Cómo ejecutar la la instalación inicial.....1439
26.7.1.8 Cómo cargar la memoria de datos de cliente (KDS) convertida en el nuevo sistema.....1440
26.7.1.9 Cómo generar un nuevo archivo de licencia.....1440
26.7.1.10 Cómo activar el archivo de licencia sin conexión.....1442
26.7.1.11 Cómo asignar licencias.....1442
26.7.1.12 Cómo restablecer las entradas LCR.....1442
26.7.2 Migración de un sistema HiPath 3000 con OpenScape Office V3 HX a OpenScape Business V3 con placa base V3.....1443
26.7.3 Migración de un sistema HiPath 3000 con OpenScape Office V3 HX a OpenScape Business V3 con UC Booster Server.....1444
26.7.3.1 Cómo convertir un conjunto de copias de seguridad de OpenScape Office V3 HX.....1446
26.7.4 Migración de una red HiPath 3000 a una red OpenScape Business.....1447
26.7.5 Migración de una interred HiPath 3000 V9 con HiPath 5000 RSM.....1449
26.7.6 Prestaciones e interfaces modificadas/descartadas de HiPath 3000.....1452
26.8 Migración en OpenScape Business V3.....1459
26.9 Migración de módulos de hardware.....1460
26.9.1 Sustitución de SLMO24N con SLMU.....1461
26.9.2 Sustitución de SLM8N con SLMU.....1461
26.9.3 Sustitución de SLCN con SLMUC (SLMU + CMAe).....1461
26.10 Migración de OpenScape Business X1 V2 a OpenScape Business X1W V3.....1462
26.10.1 Cómo migrar con CLS Connect a los sistemas con licencia permanente X1W V3.....1463
26.10.2 Cómo migrar con CLS Connect a los sistemas sin licencia permanente X1W V3.....1464

27 Límites de ampliación y capacidades.....1466
27.1 Valores máximos para extensiones.....1466
27.2 Valores máximos para líneas.....1469
27.3 Valores máximos de los recursos.....1471
27.3.1 Detalles sobre el uso de canales DSP.....1473
27.3.2 Información detallada sobre el uso de los canales proxy RTP.....1474
27.4 Valores máximos para prestaciones.....1475
27.4.1 Conexión al proveedor de servicios.....1475
27.4.2 Extensiones.....1476
27.4.3 Niveles de ampliación de UC Smart.....1476
27.4.4 Niveles de ampliación de Smart Voicemail.....1479
27.4.5 Niveles de ampliación de UC Suite.....1481
27.4.6 Funciones del teléfono.....1491

27.4.7 Trabajar en equipo (Grupos)....1493
27.4.8 Encaminamiento de llamadas....1498
27.4.9 Multimedia Contact Center....1499
27.4.10 Límites de expansión de Mobility....1500
27.4.11 Seguridad....1501
27.4.12 Interconexión de OpenScape Business....1502
27.4.13 Application Connectivity....1503
27.4.14 Accounting....1505

28 Modo Experto....1506
28.1 Convenciones de representación para descripciones de parámetros....1506
28.2 **Mantenimiento**....1507
28.2.1 **Configuración**....1507
28.2.1.1 **Configuración > Música en espera (MoH) > Cargar al gateway**....1507
28.2.1.2 **Configuración > Anuncios > Cargar el Gateway**....1508
28.2.1.3 **Configuración > Configuración de puerto**....1509
28.2.1.4 **Configuración > SmartVM**....1509
28.2.1.5 **Configuración > SmartVM > Operaciones de buzón**....1509
28.2.1.6 **Configuración > SmartVM > Operaciones en archivo**....1510
28.2.1.7 **Configuración > Marca**....1512
28.2.1.8 **Configuración > Dirección IP del gateway**....1512
28.2.2 **Imagen software**....1513
28.2.2.1 **Imagen de software > Software del sistema > Actualización a través de Internet**....1513
28.2.2.2 **Imagen software > Software del sistema > Actualización a través de Carga de archivo**....1514
28.2.2.3 **Imagen software > Software del sistema > Actualización vía lápiz USB**....1515
28.2.2.4 **Imagen software > Imágenes de teléfono > Cargar**....1515
28.2.2.5 **Imagen software > Imágenes de teléfono > Distribuir**....1516
28.2.2.6 **Imagen de software > Imágenes de teléfono > Distribuir por dispositivo**....1516
28.2.2.7 **Imagen software > Logotipos de imagen de teléfono > Cargar**....1517
28.2.2.8 **Imagen software > Logotipos de imagen de teléfono > Distribuir**....1517
28.2.3 **Inalámbrico (Cordless)**....1518
28.2.3.1 **Extensiones base > Cordless**....1518
28.2.4 **Estado de puerto/módulos**....1520
28.2.4.1 **Estado de puerto/módulos > Estado de módulos**....1520
28.2.4.2 **Estado de puerto/módulos > Fuera de servicio**....1521
28.2.5 **Traces**....1522
28.2.5.1 **Traces > Configuración de formato trace**....1522
28.2.5.2 **Traces > Interfaces de salida trace**....1523
28.2.5.3 **Traces > Protocolo trace**....1524
28.2.5.4 **Traces > Loopback digital**....1524
28.2.5.5 **Traces > Protocolo trace de cliente**....1524
28.2.5.6 **Traces > Componente trace M5T**....1525
28.2.5.7 **Traces > Secure Trace**....1525
28.2.5.8 **Traces > Secure Trace > Certificado Secure Trace**....1526
28.2.5.9 **Traces > Secure Trace > Ajustes Secure Trace**....1526
28.2.5.10 **Traces > Trace pila H.323**....1527
28.2.5.11 **Traces > Supervisión de llamadas**....1528
28.2.5.12 **Traces > Componente de licencia**....1530
28.2.5.13 **Traces > Perfiles trace**....1530
28.2.5.14 **Traces > Componentes trace**....1531
28.2.5.15 **Traces > TCP Dump**....1531
28.2.5.16 **Traces > rpcap Daemon**....1532
28.2.5.17 **Rastros > Datos de colisiones del kernel**....1533
28.2.5.18 **Traces > Trace del servidor de medios**....1534
28.2.6 **Sucesos**....1534
28.2.6.1 **Sucesos > Config. sucesos**....1534

28.2.6.2 **Sucesos** > **Protocolo sucesos** 1535
28.2.6.3 **Sucesos** > **Correo electrónico**....1535
28.2.6.4 **Sucesos** > **Tabla reacción** 1536
28.2.6.5 **Sucesos** > **Protocolos diagnóstico** 1536
28.2.6.6 **Sucesos** > **Señalización de alarmas** 1537
28.2.7 **Reiniciar / Volver a cargar**....1537
28.2.7.1 **Reiniciar / Volver a cargar** > **Reiniciar / Volver a cargar**....1537
28.2.8 **SNMP**....1539
28.2.8.1 **SNMP** > **Comunidades** 1539
28.2.8.2 **SNMP** > **Comunidades** > **Comunidades lectura** 1539
28.2.8.3 **SNMP** > **Comunidades** > **Comunidades escritura** 1540
28.2.8.4 **SNMP** > **Comunidades** > **Comunidades trap** 1540
28.2.8.5 **SNMP** > **Traps** 1540
28.2.9 **Protocolo admin.**....1541
28.2.9.1 **Protocolo admin.** > **Configuración** 1541
28.2.9.2 **Protocolo admin.** > **Datos protocolo admin.** 1541
28.2.10 **Acciones**....1542
28.2.10.1 **Acciones** > **Acciones manuales** > **Protocolos de diagnóstico** 1542
28.2.10.2 **Acciones** > **Acciones manuales** > **Mantenimiento DLI**....1544
28.2.10.3 **Acciones** > **Acciones automát.** > **Garbage Collection** 1544
28.2.10.4 **Acciones** > **Acciones automát.** > **Notificación DLS** 1545
28.2.10.5 **Acciones > Acciones automát. > Comprobación de mantenimiento SDHC**....1545
28.2.11 **Diagnóstico de plataforma**....1545
28.2.12 **Diagnóstico de aplicación**....1545
28.2.12.1 **Diagnóstico de aplicación** > **Configuración del desarrollador** > **Salida de consola trace** 1546
28.2.12.2 **Diagnóstico de aplicación** > **Configuración del desarrollador** > **Asumir permiso de escritura** 1546
28.2.12.3 **Diagnóstico de aplicación** > **Placa base** 1546
28.2.12.4 Diagnóstico de aplicación > Configuración del desarrollador > Perfiles de proveedor SIP....1546
28.2.13 **Diagnóstico de IP**....1546
28.2.13.1 **Diagnóstico de IP** > **Placa base** > **Protocolo ARP** 1546
28.2.13.2 **Diagnóstico de IP** > **Placa base** > **Solicitud ICMP** > **Ping** 1547
28.2.13.3 **Diagnóstico de IP** > **Placa base** > **Solicitud ICMP** > **Traceroute** 1547
28.2.14 **Usuario online**....1548
28.2.14.1 **Usuario online** 1548
28.3 **Telefonía**....1548
28.3.1 **Ajustes básicos**....1548
28.3.1.1 **Ajustes básicos** > **Sistema** > **Flags del sistema**....1548
28.3.1.2 **Ajustes básicos** > **Sistema** > **Parámetros de tiempo** 1557
28.3.1.3 **Ajustes básicos** > **Sistema** > **Display**....1563
28.3.1.4 **Ajustes básicos** > **Sistema** > **DISA** 1567
28.3.1.5 **Configuración básica** > **Sistema** > **Interceptación/PO/Hot-line**....1568
28.3.1.6 **Ajustes básicos** > **Sistema** > **LDAP**....1571
28.3.1.7 **Ajustes básicos** > **Sistema** > **Textos** 1572
28.3.1.8 **Ajustes básicos** > **Sistema** > **Menús flexibles** 1573
28.3.1.9 **Ajustes básicos** > **Sistema** > **Destinos de marcación abreviada**....1573
28.3.1.10 **Ajustes básicos** > **Sistema** > **Códigos de servicio**....1574
28.3.1.11 **Ajustes básicos** > **Sistema > Contraseña de registro HFA**....1575
28.3.1.12 **Ajustes básicos** > **Gateway** 1576
28.3.1.13 **Ajustes básicos** > **DynDNS** > **Servicio DynDNS** 1577
28.3.1.14 **Ajustes básicos** > **DynDNS** > **Tiempo actualiz. nombres DNS** 1578
28.3.1.15 **Ajustes básicos** > **Calidad del servicio** 1579
28.3.1.16 **Ajustes básicos** > **Fecha y hora** > **Fecha y hora** 1580
28.3.1.17 **Ajustes básicos** > **Fecha y hora** > **Ajustes zona horaria** 1580
28.3.1.18 **Ajustes básicos** > **Fecha y hora** > **Ajustes SNTP** 1580

28.3.1.19 **Ajustes básicos** > **Administración de puertos** 1581
28.3.1.20 **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Formato de salida** 1582
28.3.1.21 **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Factores** 1584
28.3.1.22 **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Códigos de proyecto** 1585
28.3.1.23 **Ajustes básicos** > **Reproductor para mensajes de voz / anuncios** 1586
28.3.1.24 **Configuración básica** > **Implementación de parámetros del teléfono** 1586
28.3.1.25 **Ajustes básicos** > **Gestión de energía** 1589
28.3.1.26 Instalación básica > Datos masivos 1589
28.3.2 **Seguridad** 1591
28.3.2.1 **Cortafuegos de aplicaciones** > **de seguridad** 1591
28.3.2.2 **Seguridad** > **Deployment and Licensing Client (DLSC)** 1593
28.3.2.3 **Seguridad** > **Deployment and Licensing Client (DLSC)** > **Certificado de cliente DLSC** 1593
28.3.2.4 **Seguridad** > **Deployment and Licensing Client (DLSC)** > **Certificado de entidad emisora DLSC** 1594
28.3.2.5 **Seguridad** > **Cifrado de señalización y carga útil** 1596
28.3.2.6 **Seguridad** > **Cifrado de señalización y carga útil** > **Certificado SPE** 1596
28.3.2.7 **Seguridad** > **Cifrado de señalización y carga útil** > **Certificados de entidad emisora SPE** 1597
28.3.2.8 **Seguridad** > **VPN** 1597
28.3.2.9 **Seguridad** > **VPN** > **Entidad emisora Lightweight** 1598
28.3.2.10 **Seguridad** > **VPN** > **Admin. certificados** 1599
28.3.2.11 **Seguridad** > **VPN** > **Admin. certificados** > **Certif. de entidad emisora de confianza** > **Certificados activ.** 1599
28.3.2.12 **Seguridad** > **VPN** > **Admin. certificados** > **Certif. de entidad emisora de confianza** > **Certificados configurados** 1600
28.3.2.13 **Seguridad** > **VPN** > **Certificados de par** 1601
28.3.2.14 **Seguridad** > **VPN** > **Servicios** > **Servicios activos** 1602
28.3.2.15 **Seguridad** > **VPN** > **Servicios** > **Servicios configurados** 1602
28.3.2.16 **Seguridad** > **VPN** > **Túnel** > **Túneles activos** 1603
28.3.2.17 **Seguridad** > **VPN** > **Túnel** > **Túneles config.** 1606
28.3.2.18 **Seguridad** > **VPN** > **Reglas** > **Reglas activas** 1610
28.3.2.19 **Seguridad** > **VPN** > **Reglas** > **Reglas configuradas** 1611
28.3.2.20 **Seguridad** > **VPN** > **Public Key Infrastructure (PKI)** 1613
28.3.2.21 **Seguridad** > **SSL** > **Generación de certif.** 1613
28.3.2.22 **Seguridad** > **SSL** > **Admin. certificados** 1614
28.3.2.23 **Seguridad** > **SSL** > **Admin. certificados** > **Certificados de servidor** 1615
28.3.2.24 **Seguridad** > **Seguridad Web** 1616
28.3.2.25 **Seguridad** > **Seguridad SQL** 1616
28.3.3 **Interfaces de red** 1617
28.3.3.1 **Interfaces de red** > **Placa base** > **Nombre de host** 1617
28.3.3.2 **Interfaces de red** > **Placa base** > **LAN 1 (WAN)** 1617
28.3.3.3 **Interfaces de red** > **Placa base** > **LAN 2** 1622
28.3.3.4 **Interfaces de red** > **Placa base** > **LAN 3 (Admin)** 1623
28.3.3.5 **Interfaces de red** > **Placa base** > **Servidor FTP** 1624
28.3.3.6 **Interfaces de red** > **Placa base** > **Modo DHCP** 1624
28.3.3.7 **Interfaces de red** > **Placa base** > **Modo DHCP** > **Servidor DHCP** > **Parámetros globales** 1625
28.3.3.8 **Interfaces de red** > **Placa base** > **Modo DHCP** > **Servidor DHCP** > **Grupos de direcciones IP** 1626
28.3.3.9 **Interfaces de red** > **Placa base** > **Modo DHCP** > **Servidor DHCP** > **Direcciones IP estáticas** 1628
28.3.3.10 **Interfaces de red** > **Placa base** > **Modo DHCP** > **Servidor DHCP** > **Últimas concesiones activas** 1629
28.3.3.11 **Interfaces de red** > **Placa base** > **Modo DHCP** > **Servidor DHCP** > **Todos los leases** 1630
28.3.3.12 **Interfaces de red** > **Tablero de aplicaciones** > **Nombre de host** 1630
28.3.3.13 **Interfaces de red** > **Tablero de aplicaciones** > **LAN 1** 1631
28.3.3.14 **Interfaces de red** > **Tablero de aplicaciones** > **LAN 2** 1631

28.3.4 **Encaminamiento** ... 1632
28.3.4.1 **Encaminamiento > Encamin. IP > Placa base > Rutas estáticas** ... 1633
28.3.4.2 **Encaminamiento > Encamin. IP > Placa base > Router estándar** ... 1633
28.3.4.3 **Encaminamiento > Encamin. IP > Placa base > Servidor DNS** ... 1633
28.3.4.4 **Encaminamiento > Encamin. IP > Tablero de aplicaciones > Rutas estáticas** ... 1634
28.3.4.5 **Encaminamiento > Encamin. IP > Tablero de aplicaciones > Router estándar** ... 1634
28.3.4.6 **Encaminamiento > NAT** ... 1635
28.3.4.7 **Encaminamiento > PSTN** ... 1636
28.3.4.8 **Encaminamiento > PSTN > Protocolo PPP** ... 1637
28.3.4.9 **Encaminamiento > PSTN > Colateral PSTN** ... 1637
28.3.5 **LCR** ... 1640
28.3.5.1 **LCR > Flags LCR** ... 1641
28.3.5.2 **LCR > Clases de servicio** ... 1641
28.3.5.3 **LCR > Plan de marcación** ... 1641
28.3.5.4 **LCR > Tabla de rutas** ... 1643
28.3.5.5 **LCR > Regla de marcación** ... 1644
28.3.5.6 **LCR > Multisitio** ... 1646
28.3.6 **Gateway voz** ... 1647
28.3.6.1 **Gateway voz > Parámetros SIP** ... 1647
28.3.6.2 Gateway de voz > Ajustes de ID de ubicación ITSP ... 1648
28.3.6.3 **Gateway voz > Parámetros códec** ... 1650
28.3.6.4 **Gateway voz > Parám. códec destino** ... 1652
28.3.6.5 **Gateway de voz > Proveedor de servicios de telefonía por Internet** ... 1652
28.3.6.6 **Gateway voz > Redes > Nodos** ... 1664
28.3.6.7 **Gateway voz > Redes > Encaminamiento** ... 1664
28.3.6.8 **Gateway voz > Interconexión SIP-Q** ... 1665
28.3.6.9 **Voice Gateway > Línea de servidor SIP nativo** ... 1666
28.3.7 **Extensiones** ... 1672
28.3.7.1 **Extensiones > Extensiones > Extensiones UP0** ... 1672
28.3.7.2 **Estación > Estación > Clientes IP** ... 1674
28.3.7.3 **Extensión > Extensión > Extensiones analógicas** ... 1678
28.3.7.4 **Extensión > Extensión > Extensiones RDSI** ... 1679
28.3.7.5 **Extensión > Extensión > Extensiones DECT > SLC Número de llamada** ... 1680
28.3.7.6 **Extensiones > Extensiones > Extensiones DECT > Extensiones DECT** ... 1681
28.3.7.7 **Extensión > Extensión > Puertos IVM/EVM > EVM** ... 1682
28.3.7.8 **Extensiones > Extensiones > Extensiones virtuales** ... 1684
28.3.7.9 **Extensión > Extensión > Parámetros de extensión** ... 1684
28.3.7.10 **Extensión > Extensión > UC Applications** ... 1696
28.3.7.11 **Extensiones > Extensiones > Perfiles/Plantillas** ... 1697
28.3.7.12 **Extensiones > Extensiones > Extensiones de marcación directa (DID)** ... 1699
28.3.7.13 **Extensión > Extensión > Mobility Entry** ... 1699
28.3.7.14 **Extensión > Extensión > Usuario de SfB** ... 1701
28.3.7.15 **Extensión > Extensión > Vista general de extensiones** ... 1702
28.3.7.16 **Extensiones > Programación de teclas** ... 1702
28.3.8 **Cordless** ... 1703
28.3.8.1 **Cordless > Para todo el sistema** ... 1703
28.3.8.2 **Cordless > SLC** ... 1705
28.3.8.3 **Cordless > Multi-SLC** ... 1707
28.3.8.4 **Cordless > Extensión base** ... 1707
28.3.9 **Llamadas entrantes** ... 1708
28.3.9.1 **Llamadas entrantes > Grupos/Grupos de caza** ... 1708
28.3.9.2 **Llamadas entrantes > Miembros del grupo** ... 1711
28.3.9.3 **Llamadas entrantes > Team/Top** ... 1713
28.3.9.4 **Llamadas entrantes > Telecaptura de llamadas** ... 1716
28.3.9.5 **Llamadas entrantes > UCD** ... 1716
28.3.9.6 **Llamadas entrantes > Desvío de llamadas** ... 1719

28.3.10 **Líneas/Interconexión**....1722
28.3.10.1 **Líneas/Interconexión > Líneas** 1722
28.3.10.2 **Troncales/Enrutamiento > Grupo troncal**....1725
28.3.10.3 **Líneas/Interconexión > Prestaciones QSIG** 1733
28.3.10.4 **Líneas/Interconexión > Asignar MSN** 1734
28.3.10.5 **Líneas/Interconexión > Parámetros RDSI** 1734
28.3.11 **Clases de servicio**....1735
28.3.11.1 **Clases de servicio > Extensiones**....1735
28.3.11.2 **Clases de servicio > Día: Grupos de clase de servicio** 1735
28.3.11.3 **Clases de servicio > Servicio nocturno: Grupos de clase de servicio** 1736
28.3.11.4 **Clases de servicio > Listas de nos. permitidos** 1737
28.3.11.5 **Clases de servicio > Listas de nos. prohibidos** 1738
28.3.11.6 **Clases de servicio > Lista negra** 1738
28.3.11.7 **Clases de servicio > Servicio nocturno** 1739
28.3.11.8 **Clases de servicio > Asignación de grupos VBZ** 1739
28.3.11.9 **Clases de servicio > Matriz VBZ** 1740
28.3.11.10 **Clases de servicio > Servicio autom. nocturno**....1741
28.3.11.11 **Clases de servicio > Días especiales**....1741
28.3.12 **Conexiones**....1742
28.3.12.1 **Equipo auxiliar > Música en espera**....1742
28.3.12.2 **Equipo auxiliar > Correo telefónico**....1743
28.3.12.3 **Anuncios > de equipos auxiliares**....1743
28.3.12.4 **Equipo auxiliar > Abridor de puerta**....1745
28.3.12.5 **Equipo auxiliar > SmartVM**....1746
28.3.13 **Payload**....1750
28.3.13.1 **Payload > Dispositivos** 1750
28.3.13.2 **Payload > Media Stream Control (MSC)** 1750
28.3.13.3 **Payload > Módulos hardware** 1751
28.3.14 **Estadísticas**....1754
28.3.14.1 **Estadísticas > Estadísticas de gateway > Placa base > Estadísticas disposit.** 1754
28.3.14.2 **Estadísticas > Estadísticas de gateway > Placa base > Estadísticas MSC** 1754
28.3.14.3 **Estadísticas > Estadística SNMP** 1755
28.3.14.4 **Estadísticas > Estadísticas de telefonía > Textos del sistema** 1755
28.3.14.5 **Estadísticas > Estadísticas de telefonía > Agentes UCD** 1755
28.3.14.6 **Estadísticas > Estadísticas de telefonía > Estado de línea**....1756
28.3.14.7 **Estadísticas > Estadísticas de telefonía > Desvío** 1756
28.3.14.8 **Estadísticas > Estadísticas de telefonía > Extensiones** 1757
28.4 **Aplicaciones**....1759
28.4.1 **Selección de aplicación**....1759
28.4.1.1 **Selección de aplicación** 1759
28.4.2 **Servicio de integración de Active Directory**....1759
28.4.2.1 **Servicio de integración de Active Directory**....1759
28.4.3 **UC Smart**....1760
28.4.3.1 **UC Smart > Ajustes básicos** 1760
28.4.3.2 **UC Smart > Gestión de usuarios**....1761
28.4.3.3 **Estado > UC Smart**....1762
28.4.4 **OpenScape Business UC Suite**....1763
28.4.4.1 **OpenScape Business UC Suite** 1763
28.4.4.2 **OpenScape Business, UC Suite > Directorio de usuario**....1763
28.4.4.3 **OpenScape Business UC Suite > Departamentos**....1766
28.4.4.4 **OpenScape Business UC Suite > Grupos**....1766
28.4.4.5 **OpenScape Business UC Suite > Plantillas**....1768
28.4.4.6 **Directorio externo de > OpenScape Business UC Suite**....1768
28.4.4.7 **OpenScape Business UC Suite > Configuración de proveedores externos**....1769
28.4.4.8 **OpenScape Business UC Suite > Contact Center**....1771
28.4.4.9 **OpenScape Business UC Suite > Planes horarios**....1780

28.4.4.10 **OpenScape Business UC Suite** > **Carga de archivo** ... 1781
28.4.4.11 **OpenScape Business UC Suite** > **En conferencia** ... 1782
28.4.4.12 **OpenScape Business UC Suite** > **Lista de ubicaciones** ... 1783
28.4.4.13 **OpenScape Business UC Suite** > **Servidor** ... 1783
28.4.4.14 **OpenScape Business UC Suite** > **Perfiles** ... 1790
28.4.4.15 **OpenScape Business UC Suite** > **Encabezados de fax** ... 1792
28.4.5 **Web Services** ... 1792
28.4.5.1 **Web Services** > **Web Collaboration** ... 1793
28.4.6 **Open Directory Service** ... 1793
28.4.6.1 **Open Directory Service** > **Ajustes básicos** ... 1794
28.4.6.2 **Fuentes de datos** > **Open Directory Service** > **Usuarios OpenScape Business** ... 1794
28.4.6.3 **Open Directory Service** > **Fuentes de datos** > **LXV3** ... 1794
28.4.6.4 **Open Directory Service** > **Fuentes de datos** > **LXV3** ... 1795
28.4.6.5 **Open Directory Service** > **Mantenimiento** ... 1795
28.4.7 **Application Launcher** ... 1795
28.4.7.1 **Application Launcher** ... 1795
28.5 **Middleware** ... 1796
28.5.1 Reproductor de anuncios ... 1796
28.5.2 Distribuidor de mensajes CSTA (CMD) ... 1796
28.5.3 Proveedor de servicios CSTA (CSP) ... 1797
28.5.4 Servidor DSS ... 1797
28.5.5 Media Extension Bridge (MEB) ... 1798

29 Anexo ... 1799
29.1 Estándares admitidos ... 1799
29.2 Prestaciones Euro-RDSI ... 1801
29.3 Puertos utilizados ... 1803
29.4 Planificación de proyecto de los canales DSP para los sistemas de comunicación OpenScape Business X3/X5/X8 ... 1805

30 Glosario ... 1816
30.1 Glosario ... 1816

Índice ... 1832

1 Historial de cambios

Los cambios que se mencionan en este capítulo son acumulativos.

Cambios en V3R4 FR3

Capítulos afectados	Descripción de los cambios	Número de edición	Fecha
Troncales/EnrutamientoGrupo troncal en la página 1725	Fijo para COLP (temas ITSP)	62	Octubre de 2025
Asistentes - Servicios en la nube en la página 129 CloudLink Service en la página 1226 Cómo configurar CloudLink Service en la página 1227 Cómo configurar la interfaz web de CloudLink Daemon en la página 1228 Cómo habilitar/configurar el conector SIP para conectarse a Workflow Studio en la página 1228 (nuevo) Números piloto de CloudLink en la página 1229 (nuevo) Cómo configurar los números piloto de CloudLink en la página 1229 (nuevo)	Compatibilidad con contenedores, habilitar conector SIP y números piloto CL	62	Septiembre de 2025
Inventario en la página 1298	Rediseño de hardware de OCCe	62	Septiembre de 2025

Cambios en V3R4 FR2

Capítulos afectados	Descripción de los cambios	Número de edición	Fecha
Migración de OpenScape Business X V2 a OpenScape Business X V3 en la página 1408	Se ha añadido una nota relativa a la dirección IP del DSP no predeterminada durante la migración.	61	10 de septiembre de 2025
Anuncios de equipos auxiliares en la página 1743	Se ha añadido un enlace a Configuración > Anuncios > Cargar en la puerta de enlace en el parámetro de archivo WAVE.	60	Septiembre de 2025
Movilidad en el hogar en la página 1001	Se agregó una nota sobre la limitación con múltiples dispositivos SIP/HFA y NAT.	56	Julio 2025
Open Directory Service en la página 1201	Se ha añadido una nota relativa a la integración de Microsoft Excel con la base de datos ODS.	56	Julio 2025

Capítulos afectados	Descripción de los cambios	Número de edición	Fecha
Llamadas entrantesGrupos/ Grupos de caza en la página 1708	Se agregó una nota sobre la dependencia con el desvío de llamadas (*1) a otro grupo de búsqueda, grupo de espera de llamadas y grupo RNA.	56	Julio 2025
Requisitos para los clientes de PC de UC Suite en la página 550	Actualizaciones para sistemas operativos, aplicaciones de Office/Outlook, software adicional (ej. Java / OpenJDK).	56	Julio 2025
Asistentes – Teléfonos / Suscriptores en la página 126 Estructura de la documentación del administrador en la página 72 Estaciones en la página 432 Estaciones SIP DECT de Mitel en la página 450 nuevo Cómo configurar estaciones SIP DECT de Mitel mediante aprovisionamiento en la página 474 nuevo ExtensiónExtensiónParámetros de extensión en la página 1684 Cómo configurar estaciones SIP a través del modo experto en la página 476 nuevo	Actualizaciones para el aprovisionamiento de MITEL SIP-DECT	55	Mayo-junio de 2025
Conexiones en la página 1742 Anuncios de equipos auxiliares en la página 1743 Equipo auxiliar Correo telefónico en la página 1743 Cómo configurar anuncios (UC Suite)& Refuerzo de UC) en la página 1261 Cómo configurar anuncios (UC Smart) en la página 1262	Actualizaciones para la configuración de Anuncios	55	Mayo-junio de 2025
Gateway de vozProveedor de servicios de telefonía por Internet en la página 1652	Actualizaciones para perfiles ITSP	55	Mayo-junio de 2025

Cambios en V3R4 FR1

Capítulos afectados	Descripción de los cambios
Configuración de equipo / Grupo Team en la página 720 MULAP básico en la página 739	Se modificó el párrafo "Ordenamiento de dispositivos miembros de Mulap" para LAN/WAN con UP.
Instalación del software de comunicación en la página 230	Se agregó una nota sobre la calificación de la configuración de DHCP desde yast o WBM.
Gestión de usuarios de WBM en la página 120	Se agregó nota para el registro de roles de administrador.
Estaciones SIP en la página 446 Llamada de grupo en la página 699 Línea colectiva en la página 703	Actualizaciones en la lista de códigos de servicio compatibles con dispositivos SIP.
Acceso a Internet en la página 170 Cómo configurar el acceso a Internet a través de un enrutador de Internet externo sobre la LAN con un puerto WAN dedicado a ITSP en la página 181 Cómo configurar el acceso a Internet a través de un enrutador de Internet externo sobre la LAN con un puerto WAN dedicado a ITSP en la página 247 Gateway de vozProveedor de servicios de telefonía por Internet en la página 1652	Actualizaciones sobre LAN/WAN e ITSP en WAN.
Cómo habilitar y configurar el servidor DHCP interno en la página 150 Cómo habilitar DHCP solo para dispositivos Mitel/Unify en la página 152 Cómo habilitar y configurar el servidor DHCP de la plataforma de hardware en la página 363 Interfaces de red Placa base Modo DHCP Servidor DHCP Parámetros globales en la página 1625 Interfaces de red Placa base Modo DHCP Servidor DHCP Grupos de direcciones IP en la página 1626 Interfaces de red Placa base Modo DHCP Servidor DHCP Direcciones IP estáticas en la página 1628	Actualizaciones para el manejo de subredes DHCP para dispositivos Mitel/Unify y opción de retransmisión.

Cambios en V3R4

Capítulos afectados	Descripción de los cambios
MULAP básico en la página 739	Se eliminaron los teléfonos SIP de la lista de miembros básicos de MULAP.
Detalles sobre el uso de canales DSP en la página 1473	Actualizaciones sobre Seguridad e ITSP.
Fuentes de datos de Open Directory Service Usuarios OpenScape Business en la página 1794	Actualizaciones sobre ODS Light.

Capítulos afectados	Descripción de los cambios
Voice Gateway Línea de servidor SIP nativo en la página 1666	Cifrado directo de medios y carga útil para Unify Phone.
Unify Phone en la página 1219	Se agregó myAgent a los clientes UC de control de llamadas de terceros.
Modelos de software de UC (softswitch) en la página 110 Hardware UC Booster en la página 109 Cómo instalar el software de comunicación en la página 232 Requisitos para la puesta en servicio inicial en la página 225 Puesta en servicio inicial por OpenScape Business S en la página 225 Requisitos para la puesta en servicio inicial en la página 282 Configuración inicial de OpenScape Business UC Booster en la página 280 Configuración inicial de OpenScape Business UC Booster en la página 280 Cómo actualizar UC Business Booster Server v2 a v3 en la página 1405	Compatibilidad de SLES 15 con OpenScape Business S y UC Booster Server.

Cambios en la actualización V3R3 FR2 GA

Capítulos afectados	Descripción de los cambios
Escritorio compartido en la página 985	Corrección de la nota relativa a la función de compartir escritorio.
Puertos utilizados en la página 274	Consolidación y corrección de los puertos utilizados para las comprobaciones de CAR Alive.
Fuentes de datos de Open Directory Service Usuarios OpenScape Business en la página 1794	Corrección de los valores mínimos y máximos para las longitudes internas máximas y externas mínimas y botón Ocultar llamadas abiertas en el diario.
Imagen de softwareSoftware del sistema Actualización a través de Internet en la página 1513	Se agregó el botón Limpiar almacenamiento antes de transferir que faltaba.
Unify Phone en la página 1219 Cómo agregar usuarios existentes de Unify Phone en la página 1222	Se agregó información sobre Unify Phone y aplicaciones de terceros.
OpenScape Business, UC SuiteDirectorio de usuario en la página 1763 OpenScape Business UC SuiteServidor en la página 1783	Se agregaron dos notas sobre diferentes longitudes de contraseñas de usuario y Restablecer todas las contraseñas de usuario.

Capítulos afectados	Descripción de los cambios
CloudLink Service en la página 1226 Cómo configurar CloudLink Service en la página 1227 Cómo abrir la interfaz web de CloudLink Daemon en la página 1227 Cómo configurar la interfaz web de CloudLink Daemon en la página 1228	Se agregaron nuevos capítulos para CloudLink Service.

Cambios en V3R3 FR2

Capítulos afectados	Descripción de los cambios
Capítulo 24.2 Copia de seguridad y recuperación de datos en la página 1264	Se agregó una nota sobre la limitación con la sincronización de Unify Phone Cloud.
-	Capturas de pantalla de la interfaz de usuario modificadas en todo el documento.
Servicio Let's Encrypt en la página 1225	Se eliminó BETA y se agregó nueva funcionalidad para el servicio Let's Encrypt.
Teléfonos compatibles en la página 110 Prestaciones en la página 524 Cómo cargar un logotipo telefónico en el sistema en la página 1254	Actualizaciones para los nuevos dispositivos compatibles CP205T/CP405T (TDM).

Cambios en V3R3 FR1

Capítulos afectados	Descripción de los cambios
Unify Phone en la página 1219 Cómo configurar la conectividad del Unify Phone en la página 1220 Cómo crear nuevos usuarios de Unify Phone en la página 1222 Cómo agregar usuarios existentes de Unify Phone en la página 1222 Cómo editar los datos de usuario de Unify Phone en la página 1223	Actualizaciones para acceso al directorio y diario, pantalla de esquema de numeración y campo de código de acceso a troncales.
Asistentes - Servicios en la nube en la página 129 Servicio Let's Encrypt en la página 1225	Se agregó el asistente 'Servicios en la nube' y el servicio 'Vamos a cifrar'.
Open Directory Service en la página 1201	Se agregó la sección 'Open Directory Service y OpenScape Business Mainboards'.

Capítulos afectados	Descripción de los cambios
Cómo gestionar usuarios de Unify Phone en la página 1221 Cómo crear nuevos usuarios de Unify Phone en la página 1222 Cómo agregar usuarios existentes de Unify Phone en la página 1222 Cómo editar los datos de usuario de Unify Phone en la página 1223	Se agregó 'Cómo crear nuevos usuarios de Unify Phone' y se actualizaron los demás capítulos en consecuencia.
Cómo personalizar una interfaz de usuario moderna alternativa para myPortal for Desktop Configuración de la máscara de OpenScape Business UC Suite Asistentes – UC Suite (solo con UC Suite) en la página 128	Se eliminaron archivos y menciones para 'Configuración de máscara'.
Cómo importar un archivo CSV desde el sistema de archivos local en el directorio externo en la página 578 Cómo añadir una fuente de datos externa para Open Directory Service en la página 1209	Actualizaciones sobre el campo 'customer_id' para importación y exportación de datos.
UC SmartAjustes básicosUC SmartAjustes básicos en la página 1760	Se agregó información sobre CloudService y otros campos faltantes.
Cómo configurar el servicio nocturno controlado por tiempo en la página 785	Se agregó información sobre el mensaje del modo nocturno en la página de inicio del portal de administración.
RequisitosmyPortal to go en la página 972	Se agregó soporte a través de conexiones de datos 4G/5G y recomendación de plan de datos de tarifa plana.
Llamadas entrantesGrupos/Grupos de caza en la página 1708	Se agregó información sobre las conversiones de tipos de grupos.
Cómo eliminar o eliminar usuarios de Unify Phone en la página 1224	Se editó la función de eliminar o eliminar para los usuarios de Unify Phone.
Cómo agregar un plan horario en la página 939 Cómo modificar un plan horario en la página 943	Se agregó una nota para explicar la vinculación de uno a muchos de las colas a los horarios.
Trabajar en equipo (Grupos) en la página 697	Se eliminó el capítulo "17.1.3 Xpressions Compact" y sus entradas del documento. Actualización para grupos de caza reservados.
Restricción del número de llamadas simultáneas por ITSP en la página 842	Se agregaron entradas para llamadas de Unify Phone y my Portal for Teams.
Clases de servicioExtensiones en la página 1735 Cómo modificar el grupo de clases de servicio de un puerto de buzón de voz en la página 541	Se agregaron notas sobre la configuración de idioma de los grupos de clase de servicio y los textos del puerto EVM.

Capítulos afectados	Descripción de los cambios
Cómo agregar el plan horario Standard Schedule XYZ para el ejemplo de Contact Center en la página 925 Cómo agregar el plan horario Standard Schedule Hotline para el ejemplo de Contact Center en la página 930 Plantillas en la página 861 Planes horarios en la página 852	Cambio de imagen y reemplazo de Contact Center. Se reintrodujo una imagen comentada para el capítulo Horarios.
Planes horarios en la página 904	Se eliminó UCD (incluido el Contact Center) y se agregó una línea sobre la transferencia al objeto CVV de cola.

Cambios en V3R3 X1R

Capítulos afectados	Descripción de los cambios
Accounting en la página 1505 Application Connectivity en la página 1503 Encaminamiento de llamadas en la página 1498 Conexión al proveedor de servicios en la página 1475 Valores máximos para extensiones en la página 1466 Estructura y condiciones ambientales en la página 110 Modelos de hardware de UC en la página 108 Extensiones DECT en la página 449 Funciones del teléfono en la página 1491 Valores máximos para líneas en la página 1469 Valores máximos de los recursos en la página 1471 Límites de expansión de Mobility en la página 1500 Multimedia Contact Center en la página 1499 Interconexión de OpenScape Business en la página 1502 Seguridad en la página 1501 Niveles de ampliación de Smart Voicemail en la página 1479 Extensiones en la página 1476 Niveles de ampliación de UC Smart en la página 1476 Trabajar en equipo (Grupos) en la página 1493	Actualizaciones para X1R

Cambios en V3R3

Capítulos afectados	Descripción de los cambios
Migración en la página 1401	Se agregó una nota sobre la eliminación de usuarios de Unify Phone.
Actualizaciones en la página 1273 Registro de licencia en la página 301 Interconexión de OpenScape Business en la página 1071	Se agregó información sobre la red: licencias al actualizar sistemas.
Reflashing en la página 222 Reflashing en la página 277	Se agregaron dos nuevos capítulos sobre la función de actualización.
Procedimiento de activación de licencia en la página 302 Puertos utilizados en la página 274 Cómo activar CLS Connect en la página 317	Se eliminaron menciones del puerto obsoleto 7780
Traces en la página 1335 Traces en la página 1522	Sección eliminada para RtpProxy Trace, ya que este seguimiento ya no está disponible en WBM
Traces Trace del servidor de medios en la página 1534 Cómo iniciar el Trace del servidor de medios en la página 1356 Cómo detener el Trace del servidor de medios en la página 1356	Nuevos capítulos para Media Server
OpenScape Business, UC SuiteDirectorio de usuario en la página 1763 OpenScape Business UC SuiteServidor en la página 1783	Actualizaciones sobre el formato de fecha y hora
Cómo eliminar o eliminar usuarios de Unify Phone en la página 1224	Actualizaciones sobre el reemplazo de la tarjeta SDHC
Descripción general de myPortal for Teams en la página 1217	myPortal for Teams: soporte de control de llamadas
Configuración básicaImplementación de parámetros del teléfono en la página 1586	Actualizaciones para la configuración de dial canónico
Migración en la página 1401	Se agregaron dos notas sobre buenas prácticas de migración y puntos de falla.
Cómo registrar licencias para suscriptores (independientes) en la página 323 Licencias orientadas a usuarios (User) en la página 307	Se agregaron dos notas sobre la asignación de licencias de correo de voz.

Capítulos afectados	Descripción de los cambios
Imagen softwareSoftware del sistema Actualización a través de Carga de archivo en la página 1514 Cómo actualizar el sistema mediante una carga de archivo en la página 1281	Se agregó información sobre la nueva bandera para actualizar mediante la carga de archivos.
Terminar en la página 913 Cómo agregar un motivo de tratamiento posterior para el "Tratamiento posterior múltiple" en la página 959	Se agregó información sobre múltiples resúmenes y grupos.
Cómo activar un puerto LAN adicional como interfaz WAN en la página 236 Cómo seleccionar el código de país y el idioma para los registros de seguimiento en la página 236 Cómo definir el logotipo de pantalla y la designación de producto en la página 235	Se reemplazó la captura de pantalla de la interfaz de usuario para mostrar la marca con impacto en los capítulos vinculados.
Cómo configurar la conectividad del Unify Phone en la página 1220 Asistentes - Servicios en la nube en la página 129 Cómo configurar el acceso a Internet a través de un PPPoE ISP estándar en la página 386 Restricción del número de llamadas simultáneas por ITSP en la página 842 Licencias de sistema en la página 309 Valores máximos para extensiones en la página 1466 Cómo configurar un ITSP predefinido en la página 184 Cómo configurar el acceso a Internet a través de un ISP preconfigurado en la página 175 ExtensiónExtensiónParámetros de extensión en la página 1684	Se eliminaron capítulos y referencias al producto Circuit.

Cambios en V3R2 FR1

Capítulos afectados	Descripción de los cambios
Cómo configurar la grabación de conferencias en la página 606 Cómo activar o desactivar la grabación de llamadas en la página 598	Nueva casilla de verificación para habilitar o deshabilitar la grabación de conferencias
Rastros Datos de colisiones del kernel en la página 1533 Cómo iniciar el servicio de datos Kernel Crash en la página 1355 Cómo detener el servicio de datos de Kernel Crash en la página 1356	Nuevo servicio de datos de fallos del kernel

Capítulos afectados	Descripción de los cambios
Combinaciones de licencias posibles en la página 313	Se agregó información sobre las licencias activas necesarias para utilizar las funciones del Contact Center y del Asistente automático de la empresa
ExtensiónExtensiónParámetros de extensión en la página 1684	Mencione que el campo **Número de llamada de estación externa confiable** es obligatorio
OpenScape Business UC SuiteServidor en la página 1783	Nueva opción para eliminar después de un período de tiempo específico mensajes de devolución de llamada, llamadas grabadas en vivo, llamadas de fax y correos electrónicos asociados con llamadas
Cómo guardar reglas (CCV) como archivo PDF en la página 945 Cómo cargar una regla descargada (CCV) en un formato de archivo de copia de seguridad en la página 945	Nuevos capítulos para descarga y carga de una regla (CCV)
UC Suite en la página 546 Multimedia Contact Center en la página 888 Mantenimiento en la página 1251 Modo Experto en la página 1506	Actualizaciones de la interfaz de usuario en capítulos completos afectados
Cómo configurar el envío de correo electrónico en la página 208 OpenScape Business UC SuiteConfiguración de proveedores externos en la página 1769 OpenScape Business UC Suite Contact Center en la página 1771 Cómo agregar colas de espera para el ejemplo de Contact Center en la página 932 Cómo agregar una cola en la página 946 Cómo modificar una cola en la página 950 Cómo conectar el sistema OpenScape Business a Microsoft Office 365 mediante autenticación básica en la página 636 Cómo conectar el sistema OpenScape Business a Microsoft Office 365 con el método de autenticación moderna en la página 641	Soporte para autenticación OAuth 2.0
myReports en la página 892	Los administradores de myReports ya no pueden configurar la cuenta de correo electrónico que se utilizará para enviar informes por correo electrónico
Descripción general de myPortal for Teams en la página 1217	myPortal for Teams: soporte para teclado de marcación y favoritos
RequisitosmyPortal to go en la página 972	Requisitos previos actualizados para myPortal to go iOS cliente

Capítulos afectados	Descripción de los cambios
Administración de extensiones en la página 879	En myAttendant, la cantidad predeterminada de botones de usuario aumentó y se puede cambiar
Usuarios de UC Suite en la página 558 OpenScape Business, UC SuiteDirectorio de usuario en la página 1763	Lista actualizada de formatos de archivo admitidos para cargar una imagen
Acceso de usuario a funciones de UC (clientes de UC) en la página 101 Teléfonos compatibles en la página 110 Deployment Service (DLI y DLS) en la página 371 Clientes de UC Smart en la página 499 Requisitos para myPortal @work en la página 502 Cómo configurar directorios para teléfonos de sistema en la página 521 Prestaciones en la página 524 Requisitos para los clientes de PC de UC Suite en la página 550 Configuración de equipo / Grupo Team en la página 720 OpenScape Business Attendant en la página 863 myAttendant en la página 877 Requisitos para myAgent en la página 890 Cómo cargar un logotipo telefónico en el sistema en la página 1254 Cómo configurar la reactualización automática en la página 1286 Actualización de software para sistemas OpenScape Business X en la página 1402 Cómo actualizar UC Business Booster Server v2 a v3 en la página 1405 Migración de hardware/software de los sistemas OpenScape Business X a V3 en la página 1407 Actualización de software de OpenScape Business S en la página 1416 Niveles de ampliación de UC Smart en la página 1476 Niveles de ampliación de UC Suite en la página 1481 Application Connectivity en la página 1503	Nuevos teléfonos compatibles: • OpenScape Desk Phone CP 210 • OpenScape Desk Phone CP 710
Teléfonos compatibles en la página 110	Nuevos módulos clave compatibles: • Módulo de llave OpenScape 410 • Módulo de llave OpenScape 710

Capítulos afectados	Descripción de los cambios
Ajustes básicosSistema LDAP en la página 1571	Se agregó una nota sobre la visualización de fuentes LDAP.
DISA en la página 686	Se agregó una nota sobre las llamadas a números DISA en OSBiz S y OSBiz X.
OpenScape Business UC SuiteServidor en la página 1783	Se eliminó la entrada de la tabla DB.
Open Directory Service en la página 1201	Se modificaron fuentes de datos externas y se agregó información sobre el campo 'Descripción'.
Cómo migrar de Placa base V2 a Placa base V3 (sistema autónomo) en la página 350	Se agregó texto sobre problemas con la funcionalidad UC Fax.
Migración de OpenScape Business X1 V2 a OpenScape Business X1W V3 en la página 1462	Se agregaron capítulos sobre la migración de X1 V2 a X1W V3.
Pasar de CLS connect en la página 318	Se presentó el capítulo Cambio desde CLS connect.
Cómo migrar de Placa base V2 a Placa base V3 (sistema autónomo) en la página 350	Migración OCCLA independiente
Acceso remoto en la página 1393 Descripción general de funciones y códigos en la página 692 Esquema de direcciones IP en la página 140 Cómo activar el acceso remoto por RDSI en la página 1394 Cómo configurar un PC con Microsoft Windows Vista para el acceso remoto a través de RDSI en la página 1394 Cómo configurar un PC con Microsoft Windows 7 para el acceso remoto a través de RDSI en la página 1396	Se cambiaron los métodos de acceso remoto obsoletos y se eliminaron los últimos tres capítulos.
Migración de OpenScape Business X1 V2 a OpenScape Business X1W V3 en la página 1462	Se agregaron capítulos sobre la migración de X1 V2 a X1W V3.
Voice Gateway Línea de servidor SIP nativo en la página 1666	Se agregaron entradas de tabla para seguridad de transporte y medios.
OpenScape Business UC SuiteServidor en la página 1783	Se agregó texto sobre el reinicio de la aplicación UC.
Pasar de CLS connect en la página 318	Se agregó un capítulo sobre el cambio desde CLS Connect.
OpenScape Business UC SuiteServidor en la página 1783	Se agregó texto sobre el reinicio de la aplicación UC.
Voice Gateway Línea de servidor SIP nativo en la página 1666	Se agregaron entradas de tabla para seguridad de transporte y medios.
Acceso remoto en la página 1393	Se eliminaron métodos de acceso remoto obsoletos.

Capítulos afectados	Descripción de los cambios
Pasar de CLS connect en la página 318	Se agregó un capítulo sobre el cambio desde CLS Connect.

Cambios en V3R2

Capítulos afectados	Descripción de los cambios
Teléfonos compatibles en la página 110 Requisitos para myPortal @work en la página 502 Prestaciones en la página 524 Requisitos para los clientes de PC de UC Suite en la página 550 OpenScape Business Attendant en la página 863 myAttendant en la página 877 Requisitos para myAgent en la página 890 Cómo configurar la reactualización automática en la página 1286 Significado de los resultados de la prueba de área de cobertura en la página 991	Nuevos teléfonos compatibles: • OpenScape Desk Phone CP 110 • Teléfono DECT OpenScape S6/SL6/R6
Descripción general de myPortal for Teams en la página 1217	myPortal for Teams: soporte de diario
Niveles de ampliación disponibles a través de Ventas en la página 105 Valores máximos para extensiones en la página 1466 Niveles de ampliación de UC Smart en la página 1476 Niveles de ampliación de UC Suite en la página 1481 Límites de expansión de Mobility en la página 1500 Application Connectivity en la página 1503	myPortal for Teams: Límites de configuración y capacidades
myPortal @work en la página 499	Los escenarios de campamento son compatibles con myPortal @work

Capítulos afectados	Descripción de los cambios
Unify Phone en la página 1219 Cómo configurar la conectividad del Unify Phone en la página 1220 Cómo gestionar usuarios de Unify Phone en la página 1221 Cómo agregar usuarios existentes de Unify Phone en la página 1222 Cómo editar los datos de usuario de Unify Phone en la página 1223 Cómo configurar las opciones de número alternativo y encaminamiento de llamadas para interconectividad de Unify Phone en la página 1225 Ajustes básicos Sistema Flags del sistema en la página 1548	Capítulos nuevos/actualizados para la conectividad de Unify Phone
Licencias en la página 304 Combinaciones de licencias posibles en la página 313 Licencias de usuario en la página 306 Licencias orientadas a usuarios (User) en la página 307 Licencias de sistema en la página 309 Asignación de licencias (independiente) en la página 321 Cómo registrar licencias para suscriptores (independientes) en la página 323 Asignación de licencias (interred) en la página 332 Cómo registrar licencia para extensiones (interred) en la página 334	Nueva licencia de Unify Phone
Información detallada sobre el uso de los canales proxy RTP en la página 1474	Agregue información sobre los canales proxy RTP requeridos por llamada de Unify Phone
Presencia en la página 567	Se agregó una nota sobre la visibilidad del estado de presencia.
Usuarios de UC Suite en la página 558	Se agregó una nota sobre la restricción al cambiar el nombre de usuario.
Registro de licencia en la página 301	Se cambió el nombre de OCCLA y OCCL a placa base V3 y placa base V2 respectivamente, en los capítulos 8.11 a 8.14

Cambios en V3R1 FR2

Capítulos afectados	Descripción de los cambios
RequisitosmyPortal to go en la página 972	myPortal to go: compatibilidad con el kit de llamadas de iOS

Capítulos afectados	Descripción de los cambios
RSP.servicelink en la página 1387	Almacene las credenciales de RSP en el conjunto de copias de seguridad
OpenScape Business UC SuiteGrupos en la página 1766 OpenScape Business UC SuitePerfiles en la página 1790	UC Suite: Grupos de favoritos
Troncales/EnrutamientoGrupo troncal en la página 1725 ExtensiónExtensiónParámetros de extensión en la página 1684	SBC de confianza
myPortal @work en la página 499	myPortal @work: soporte de telecaptura
Descripción general de myPortal for Teams en la página 1217 Cómo configurar MyPortal para Teams en la página 1218 Cómo cargar myPortal para Teams en la tienda de Teams en la página 1218	myPortal for Teams

Cambios en V3R1 FR1

Capítulos afectados	Descripción de los cambios
Cómo añadir una Excepción en CCV en la página 860	Se ha añadido un nuevo tipo de excepción CCV
OpenScape Business UC SuiteServidor en la página 1783	Se ha añadido el parámetro **Desactivar el seguimiento de conversaciones**
OpenScape Business UC SuiteServidor en la página 1783	Se ha añadido el parámetro **La caché de búsqueda del directorio caduca en**

Cambios en V3R1

Capítulos afectados	Descripción de los cambios
• Teléfonos compatibles en la página 110 • Requisitos para myPortal @work en la página 502 • Deployment Service (DLI y DLS) en la página 371 • Prestaciones en la página 524 • myAttendant en la página 877 • Requisitos para myAgent en la página 890 • OpenScape Business Attendant en la página 863 • Cómo configurar la reactualización automática en la página 1286 • Actualización de software para sistemas OpenScape Business X en la página 1402 • Migración de hardware/software de los sistemas OpenScape Business X a V3 en la página 1407 • Actualización de software de OpenScape Business S en la página 1416 • Niveles de ampliación de UC Smart en la página 1476 • Niveles de ampliación de UC Suite en la página 1481 • Application Connectivity en la página 1503	Nuevo teléfono compatible OpenScape Deskphone CP 700 y CP 700X
Teléfonos compatibles en la página 110	Nuevo teléfono compatible OpenScape WLAN Phone WL4/WL4 Plus
• Gateway de vozProveedor de servicios de telefonía por Internet en la página 1652 • Voice Gateway Línea de servidor SIP nativo en la página 1666 • EstadísticasEstadísticas de telefonía Estado de línea en la página 1756	Mejores de ITSP
Directorio externo de OpenScape Business UC Suite en la página 1768	Nuevo botón **Eliminar todo**
OpenScape Business UC SuiteServidor en la página 1783	Nuevo flag **Mostrar nombres de los agentes en enlace de cola de myAgent** para mostrar los nombres de usuario junto con sus números de extensión.
Cómo mostrar datos masivos en la página 166	Datos masivos también está disponible en el menú de nivel superior de Configuración - Asistentes.
Instalación básica > Datos masivos en la página 1589	Adición de dos columnas de menús: **N.º llam. móvil** y **Dirección de correo electrónico**
Clases de servicioServicio autom. nocturno en la página 1741	Adición de la funcionalidad **Servicio de copia**.

Capítulos afectados	Descripción de los cambios
• Valores máximos para extensiones en la página 1466 • Valores máximos para líneas en la página 1469 • Conexión al proveedor de servicios en la página 1475 • Niveles de ampliación de UC Smart en la página 1476 • Niveles de ampliación de Smart Voicemail en la página 1479 • Niveles de ampliación de UC Suite en la página 1481 • Trabajar en equipo (Grupos) en la página 1493 • Límites de expansión de Mobility en la página 1500 • Application Connectivity en la página 1503	Actualización de los valores máximos de las placas nuevas
• Cómo configurar el envío de correo electrónico en la página 208 • Cómo modificar configuración de correo electrónico por sucesos en la página 1362 • SucesosCorreo electrónico en la página 1535	Notificar llamadas de emergencia a la seguridad in situ
• Cómo actualizar UC Business Booster Server v2 a v3 en la página 1405 • Actualización de software de OpenScape Business S en la página 1416	Seguridad - OpenSSL V1.1.1
Cómo reenviar archivos de protocolo del sistema automáticamente en la página 1354	Envío externo de archivos syslog de Linux
Instalación básica > Datos masivos en la página 1589	Adición del número de UC Mobile a la configuración del asistente de datos masivos
Cómo recopilar seguimientos de diagnóstico para incidentes de error en la página 221	Recopilación y transferencia automáticas de datos de diagnóstico

Cambios en V3

Capítulos afectados	Descripción de los cambios
Modelos de software de UC (softswitch) en la página 110 Hardware UC Booster en la página 109 Cómo instalar el software de comunicación en la página 232 Requisitos para la puesta en servicio inicial en la página 225 Puesta en servicio inicial por OpenScape Business S en la página 225 Requisitos para la puesta en servicio inicial en la página 282 Configuración inicial de OpenScape Business UC Booster en la página 280	Actualización a SLES 12 SP5.
Circuit Cómo configurar un número de buzón de voz de Circuit Cómo configurar un número alternativo y encaminamiento de llamadas para interconectividad de Circuit	Mejoras de interconectividad de Circuit
UC Smart Gestión de usuarios en la página 1761 Migración en OpenScape Business V3 en la página 1459 Combinaciones de licencias posibles en la página 313 Licencias orientadas a usuarios (User) en la página 307 Licencias de sistema en la página 309 Escenario 5: OpenScape Business BLF conectado a un sistema individual OpenScape Business en la página 875 Escenario 6: OpenScape Business BLF conectado en una interred OpenScape Business (estado de presencia y BLF mediante WSI) en la página 877 OpenScape Business BLF en la página 866 OpenScape Business TAPI 120 en la página 1191 Ajustes básicos para UC Smart en la página 495 myPortal @work en la página 499	Licencias UC Suite para clientes de UC Smart
Cómo migrar de Placa base V2 a Placa base V3 (sistema autónomo) en la página 350	Bloqueo de los dispositivos OptiPoint en la evolución de OCC V3.
Cómo iniciar sesión en el WBM en la página 119	Refuerzo del acceso externo a WBM.

Capítulos afectados	Descripción de los cambios
Cómo migrar de Placa base V2 a Placa base V3 (sistema autónomo) en la página 350 Cómo migrar de Placa base V2 a Placa base V3 como nodo maestro de un sistema conectado en red en la página 353 Cómo migrar de Placa base V2 a Placa base V3 el nodo esclavo de un sistema conectado en red en la página 353 Migración de sistemas HiPath 3000 al software OSBiz V3 con placa base V3 en la página 354 Actualización de V2 a V3 con CLS Connect en la página 354 Actualización de V2 a V3 sin CLS Connect en la página 354	Evolución de OCC.
Cómo cargar un logotipo telefónico en el sistema en la página 1254	Soporte en la carga de logotipo de teléfono CP con WBM
Actualizaciones automáticas en la página 557 myPortal @work en la página 499 myPortal @work en la página 549	Actualizaciones respecto a myPortal @work

Cambios en V2R7

Capítulos afectados	Descripción de los cambios
Asistentes – Telefonía central Servicio de integración de Active Directory Cómo configurar el servicio de Active Directory Servicio de integración de Active Directory	Se ha añadido información sobre el servicio de integración de Active Directory
Estación > Estación > Parámetros de la estación	Se ha eliminado la opción de desactivación del control de PW
Circuit	Se han añadido llamadas pull/push, llamadas en conferencia y una funcionalidad de información de ocupado en una llamada
OpenScape Business UC Suite > Servidor	Se ha añadido el flag Deshabilitar la edición de nombres
OpenScape Business, UC Suite > Perfiles	Se ha añadido un grupo Teclas de acceso rápido en ajustes Perfiles de UC Suite
myPortal @work	Se ha añadido la disponibilidad en Mac OS

Capítulos afectados	Descripción de los cambios
Modelos de software de UC (softswitch) Hardware UC Booster Migración de un sistema independiente HiPath 3000 con OpenScape Office V3 HX Cómo instalar el software de comunicación Requisitos para la puesta en servicio inicial Puesta en servicio inicial por OpenScape Business S Requisitos para la puesta en servicio inicial Configuración inicial de OpenScape Business UC Booster	Se ha añadido la compatibilidad de SLES 12 SP3
Voice Gateway > Proveedores de servicio de telefonía internet Voice Gateway > Troncal del servidor SIP nativo	Se ha añadido información en la wiki (ITSP)

Cambios en V2R6FR2

Nota: Este documento puede contener descripciones de prestaciones que aún puede estar en estado beta. Para obtener información detallada, consulte la información de ventas y las notas de la versión.

- Combinaciones de licencias posibles
  - Se han añadido licencias para telefonía VoIP de myPortal @work
- myPortal @work
  - Se ha añadido información sobre VoIP
- Requisitos para myPortal @work
  - Se ha añadido información sobre VoIP
- Música en espera
  - Uso de música en espera (MOH) importada en UC Suite
- Cómo importar la música en espera interna
  - Uso de música en espera (MOH) importada en UC Suite
- OpenScape Business UC Suite > Servidor
  - Se ha añadido el flag Cerrar la conversación después

1.1 Historial de mejoras/correcciones

Los cambios que se mencionan en este capítulo son acumulativos.

Cambios en V3R4 FR2

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados	Número de edición
PRB000086522	23 de octubre de 2025	Se ha añadido una sección con directrices para cuando se aumenta el rango de subredes.	Configuración inicial de OpenScape Business X en la página 136	63
PRB000086522	26 de agosto de 2025	Se ha añadido una declaración sobre la conexión simultánea de dos proveedores de servicios de telecomunicaciones (ITSP) en la red local (LAN) y la red WAN.	Cómo configurar el acceso a Internet a través de un enrutador de Internet externo sobre la LAN con un puerto WAN dedicado a ITSP en la página 181	58
PRB000081445	18 de agosto de 2025	Se han añadido notas relativas a la generación automática de canales multimedia.	Cómo configurar la Suite UC en la página 205 Cómo configurar la Suite UC en la página 258	58
PRB000082631	15 de julio de 2025	Se agregó información sobre el mecanismo de clasificación en Clientes IP > Información del dispositivo, pestaña WBM	EstaciónEstaciónClientes IP en la página 1674	57

Cambios en V3R4 FR1

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000082944	22 de abril de 2025	Se agregó una nota respecto a que los datos de usuario de Unify Phone no forman parte del archivo de exportación.	ConfiguraciónConfiguración de puerto en la página 1509

Cambios en V3R4

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000080604	19 de febrero de 2025	Se modificó la oración sobre el número de teléfono que se utilizará para llamadas salientes cuando no haya ningún número DID de la persona que llama disponible.	Cómo configurar un ITSP predefinido en la página 184 Cómo configurar un ITSP predefinido en la página 397
PRB000080170	15 ene 2025	Corrección en la descripción del nombre para mostrar/entrada de la tabla de algoritmos.	Ajustes básicos Sistema Display en la página 1563
PRB000077322	09 de diciembre de 2024	Corrección de ambos valores máximos para Estaciones y estaciones TDM para X1R/W.	Valores máximos para extensiones en la página 1466

Cambios en la actualización V3R3 FR2 GA

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000079549	15 de septiembre de 2024	Corrección en el paso 5 de notificaciones por correo electrónico.	Cómo configurar notificaciones por correo electrónico de errores del sistema en la página 1382
PRB000076788	13 de septiembre de 2024	Se agregó nota sobre la calificación del Firewall de aplicaciones.	Cortafuegos de aplicacionesde seguridad en la página 1591 Cortafuegos de aplicaciones en la página 1015 Supervivencia en la página 1167
PRB000075233	18 de julio de 2024	Correcciones sobre la prioridad de los horarios y sus excepciones.	Cómo añadir una Excepción en CCV en la página 860
PRB000077767	28 de agosto de 2024	Se agregó nota sobre el reenvío de llamadas al buzón de correo de voz.	Presencia en la página 567
PRB000078194	18 de julio de 2024	Corrección de los valores de los puertos utilizados en los controles activos de CAR	Puertos utilizados en la página 274

Cambios en V3R3 FR2

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000078191	13 de junio de 2024	Corrección de los valores para anuncios X1 a/b y canales MEB para X1W/R	Valores máximos para líneas en la página 1469 Valores máximos de los recursos en la página 1471
PRB000076108	13 de junio de 2024	Corrección en los puertos CLS y nueva sección al final del capítulo	Puertos utilizados en la página 274

Cambios en V3R3 FR1

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000072445	1 de abril de 2024	Se agregó la "Longitud máxima del número local" en la Configuración de marcación canónica	Configuración básicaImplementación de parámetros del teléfono en la página 1586
PRB000074047	15 de marzo de 2024	Se agregó una nota para explicar cómo funciona el indicador "eliminar datos antes de importar".	Cómo importar un archivo CSV desde el sistema de archivos local en el directorio externo en la página 578
PRB000072007	1 de abril de 2024	Se agregó un nuevo capítulo "Cómo cambiar el plan de marcado a 4 dígitos" e información relacionada.	Cómo cambiar el plan de marcado a 4 dígitos en la página 237, Configuración de sistema en la página 234

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000074908	8 de abril de 2024	Se agregó capacidad de usuarios con respecto a recordatorios cronometrados.	Equipo de despertador y citas en la página 692
PRB000073511	14 de abril de 2024	Correcciones y solución de problemas con excepciones recurrentes anualmente.	Cómo agregar un plan horario en la página 939 Cómo añadir una Excepción en CCV en la página 860

Cambios en V3R3

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000068453	27 de junio de 2023	Se agregó información sobre SMTP autenticado y OAuth 2.0.	Cómo configurar el envío de correo electrónico en la página 208
PRB000066465	17 de julio de 2023	Se agregó información sobre el nuevo puerto en el firewall para CLS Connect.	Activación de licencia (Standalone) en la página 318, Procedimiento de activación de licencia en la página 302, Puertos utilizados en la página 274, Cómo activar CLS Connect en la página 317
PRB000068453	17 de julio de 2023	Formatos de imagen compatibles actualizados.	OpenScape Business, UC SuiteDirectorio de usuario en la página 1763, Usuarios de UC Suite en la página 558
PRB000071258	18 Oct 2023	Se agregaron límites de longitud para datos CSV.	Cómo importar un archivo CSV desde el sistema de archivos local en el directorio externo en la página 578
PRB000061414	20 Oct 2023	Se agregó una nueva bandera: Usar ruta estática dedicada.	Imagen de softwareSoftware del sistema Actualización a través de Internet en la página 1513
PRB000064083	26 Oct 2023	Se agregaron valores faltantes para el campo Aplicar autenticación para dispositivos HFA.	Ajustes básicosSistema > Contraseña de registro HFA en la página 1575

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000071163	24 de noviembre de 2023	Se agregaron nuevos capítulos e información sobre el manejo de certificados.	Introducción en la página 1057 (nuevo) Cómo importar certificados de servidor (PEM) en la página 1062 (nuevo) Gestión de certificados para Booster Server en la página 1064 (nuevo) Cómo generar una solicitud de certificado (CSR) en la página 1059 Cómo generar certificado de entidad emisora en la página 1058 Cómo importar un certificado de servidor (PKCS#12) en la página 1061 Gestión de certificados en la página 1056
PRB000072442	04 ene 2023	Se agregó una nota sobre el comportamiento de DND en equipos.	Configuración de equipo / Grupo Team en la página 720
PRB000069431	05 ene 2024	Se agregó información sobre UC Suite, enrutamiento CLI y MS Teams.	Planes horarios en la página 852 Planes horarios en la página 904
PRB000054882	02 de febrero de 2024	Se agregó información para la sección faltante 'Autorización de troncal conmutada'.	Configuración básicaSistema Interceptación/PO/Hot-line en la página 1568
PRB000073109	22 de febrero de 2024	Se agregó ITSP a la fila de canales troncales SIP en las tablas.	Valores máximos para líneas en la página 1469
PRB000073818	1 de marzo de 2024	Corrección de los valores predeterminados para los parámetros Recuento de alarmas de cola, Tiempo de alarma de cola, Tiempo de espera de llamadas perdidas y Umbral de llamadas abandonadas.	OpenScape Business UC Suite Contact Center en la página 1771

Cambios en V3R2 FR1

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000066080	11 de mayo de 2023	Se agregó una nota sobre el campamento sobre el comportamiento.	Cómo activar o desactivar el aviso de llamada en espera inmediato a través del puesto de operadora en la página 682

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000067262	12 de mayo de 2023	Se corrigieron los valores del rango del temporizador de retardo de MOH.	Ajustes básicosSistema Parámetros de tiempoParámetros de tiempo, Modo ExpertoAjustes básicosSistema, Modo Experto en la página 1557
PRB000065660	29 de junio de 2023	Se agregó una nota sobre cómo agregar y eliminar contactos de UC.	Directorios en la página 520, Directorios en la página 572
PRB000067012	01 de agosto de 2023	Se agregó una nota sobre las reglas de restricción de llamadas y marcación rápida del sistema.	Marcación abreviada central en la página 647
PRB000056655	05 de septiembre de 2023	Se agregó una nota sobre la actualización de la información de la pantalla después de transferir una llamada.	Transferir en la página 663

Cambios en V3R2

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000052166	20 de junio de 2022	Sección eliminada para Auto DSP Trace, ya que este seguimiento ya no está disponible en WBM	Traces en la página 1522
PRB000058845	01 de julio de 2022	Información actualizada sobre el soporte de SPE en redes	Deployment Service (DLI y DLS) en la página 371
PRB000058415	22 de agosto de 2022	Se eliminó la sección para placas y dispositivos no compatibles, ya que esta sección se trasladó a la documentación de servicio.	Anexo en la página 1799
PRB000058021	22 de agosto de 2022	Información actualizada sobre los componentes a reemplazar	Migración de hardware/software de los sistemas OpenScape Business X a V3 en la página 1407
PRB000061111	27 de octubre de 2022	Se agregó una nota sobre el comportamiento de VoIP de myPortal@work	Clientes de UC Smart en la página 499
PRB000062363	25 de noviembre de 2022	Se agregaron capítulos y subcapítulos sobre la migración de placas HW	Migración de módulos de hardware en la página 1460
PRB000063445	30 de noviembre de 2022	Se agregó una nota sobre el grupo UCD de respaldo en la solución alternativa básica	Solución de respaldo (solución Fallback) en la página 916
RB000055773, PRB000055775	12 de enero de 2023	Se agregó una nota sobre la adición de una nueva fuente de datos en ODS.	Cómo añadir una fuente de datos externa para Open Directory Service en la página 1209
PRB000061481	12 de enero de 2023	Se agregó una nota y un subcapítulo sobre la eliminación de usuarios de Unify Phone	Unify Phone en la página 1219

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000063445	12 de enero de 2023	Nota agregada en Solución alternativa básica	Solución de respaldo (solución Fallback) en la página 916
PRB000062971	25 de ene de 2023	Eventos eliminados que no están presentes en WBM. Nota agregada y tabla modificada para ajustarse al contenido.	SNMP (Simple Network Management Protocol) en la página 1317
PRB000065939	5 de abril de 2023	Cambios en la bandera 'Desactivar correo electrónico de invitación de myPortal'.	OpenScape Business UC SuiteServidor en la página 1783
PRB000065939	5 de abril de 2023	Cambios en la bandera 'Desactivar correo electrónico de invitación de myPortal'.	OpenScape Business UC SuiteServidor en la página 1783
PRB000067211	26 de abril de 2023	Se agregó una sección sobre limitaciones de migración y soluciones alternativas.	Migración de un sistema OpenScape Business X V3 de placa base V2 a placa base V3 en la página 1412

Cambios en V3R1

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000052438	20 de abril de 2021	Sección añadida para OCCLA y modo UC Suite / Smart	Cómo migrar de Placa base V2 a Placa base V3 (sistema autónomo) en la página 350
PRB000051654	14 de mayo de 2021	Se han añadido capítulos nuevos Integración de MS Office 365	Descripción general de la integración de Microsoft Office 365 en la página 635
PRB000051803	19 de mayo de 2021	Se ha añadido una nota para escenarios en espera	myPortal @work en la página 499
PRB000052202	02 de septiembre de 2021	Se ha añadido información sobre llamadas por Internet	Restricción del número de llamadas simultáneas por ITSP en la página 842

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000054381	03 de septiembre de 2021	Se han eliminados las entradas de myPortal Smart	• Funciones de UC (vista general) en la página 94 • Niveles de ampliación disponibles a través de Ventas en la página 105 • Idiomas admitidos en la página 112 • Programación de teclas en la página 455 • UC Smart en la página 494 • Clientes de UC Smart en la página 499 • Presencia en la página 519 • Interconexión de OpenScape Business X y OpenScape 4000 en la página 1145 • Prestaciones e interfaces modificadas/descartadas de HiPath 3000 en la página 1452 • Acceso de usuario a funciones de UC (clientes de UC) en la página 101 • Cómo registrar licencias para suscriptores (independientes) en la página 323 • myPortal @work en la página 499 • myPortal to go en la página 970 • Actualización de software para sistemas OpenScape Business X en la página 1402
PRB000054046	06 de septiembre de 2021	Nota agregada sobre dispositivos	Configuración de equipo / Grupo Team en la página 720Jefe/ Secretaria / Grupo Top en la página 724
PRB000053988	06 de septiembre de 2021	Se agregó una nota sobre la búsqueda de nombres de grupos en myPortal @work	Prestaciones en la página 524

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000054258	10 de septiembre de 2021	Se han actualizado capítulos para configurar teléfonos DECT	Cómo indicar la identificación de sistema DECT y configurar otros parámetros Cordless (datos a nivel del sistema) en la página 993 Cómo configurar extensiones base Cordless en la página 994 Cómo configurar por primera vez teléfonos DECT en la página 994 Cómo iniciar sesión con un teléfono DECT (OpenStage/Gigaset-Mobilteil) en Cordless en la página 995 Cómo añadir otros teléfonos DECT en la página 997 Cómo borrar teléfonos DECT en la página 997 Cómo configurar el parámetro Multi-SLC en la página 998 Cómo consultar los datos de las extensiones base en la página 999 Cómo activar el tono de aviso de MWI (Message Waiting Indication) para los teléfonos DECT en la página 999 Cómo consultar el estado de registro de los teléfonos DECT en la página 999
PRB000051960, PRB000052019	11 de octubre de 2021	Se ha añadido una nota sobre la cuenta de usuario myPortal @work bloqueada en el modo UC Suite	Configuración de usuario de myPortal @work en la página 503
PRB000053691	18 de octubre de 2021	Se ha actualizado la tabla sobre cómo se realiza la búsqueda LDAP	Ajustes básicosSistema LDAP en la página 1571
PRB000054934	12 de noviembre de 2021	Se agregó información sobre la cantidad de conversaciones que se muestran en el cliente	myPortal @work en la página 499
PRB000054816	03 de febrero de 2022	Nota agregada sobre el servicio CallMe	Servicio CallMe en la página 570
PRB000054995/ PRB000055780	18 de febrero de 2022	Nota agregada para ODBC a ODBC Bridge Server	Cómo configurar el ODBC-ODBC Bridge Server en la página 1207
PRB000055651	28 de febrero de 2022	Se agregó información sobre la finalización del proceso de registro del teléfono DECT	Cómo iniciar sesión con un teléfono DECT (OpenStage/Gigaset-Mobilteil) en Cordless en la página 995

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000056047	15 de marzo de 2022	Nota agregada para RSP	RSP.servicelink en la página 1387
PRB000055842	30 de marzo de 2022	Se agregó información sobre los formatos de archivo admitidos y el límite de tamaño para cargar una imagen	Usuarios de UC Suite en la página 558 OpenScape Business, UC SuiteDirectorio de usuario en la página 1763

Cambios en V3

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
NA16738104	19 de agosto de 2020	Adición de una nota sobre rellenar tanto el campo Nombre como el campo Apellidos en el directorio externo	Directorio externo en la página 577
NA16759874	13 de noviembre de 2020	Adición de información sobre la compatibilidad del modo dúplex con OCCLA	Cómo migrar de Placa base V2 a Placa base V3 (sistema autónomo) en la página 350 Gestión de energía en la página 1313Interfaces de redPlaca base LAN 2LAN 2, Modo ExpertoInterfaces de red Placa base, Modo Experto en la página 1622Interfaces de redPlaca base LAN 3 (Admin)LAN 3 (Administrador), Modo ExpertoInterfaces de red Placa base, Modo Experto en la página 1623Interfaces de redTablero de aplicacionesLAN 1LAN 1, Modo ExpertoInterfaces de red Tablero de aplicaciones, Modo Experto en la página 1631Interfaces de redTablero de aplicacionesLAN 2LAN 2, Modo ExpertoInterfaces de red Tablero de aplicaciones, Modo Experto en la página 1631Interfaces de red Placa base LAN 1 (WAN) en la página 1617
PRB000050351	12 de noviembre de 2020	Se ha corregido una nota sobre los teléfonos CP0.	Cómo configurar un PIN para el apagado controlado (Shutdown) de OpenScape Business X en la página 1292
PRB000050248	12 de noviembre de 2020	Se han añadido entradas para CAR en la tabla	Puertos utilizados en la página 274

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
NA16756853/ PRB000049732	10 de diciembre de 2020	Adición de una nota sobre reiniciar Booster Server en caso de cambios en la configuración de la transferencia de correos electrónicos.	Cómo configurar el envío de correo electrónico en la página 630
PRB000050722	15 de diciembre de 2020	Adición de información sobre activar la opción Conversión de número para los números de marcación abreviada mediante LDAP.	Reglas y convenciones en la página 527
PRB000051401	09 de febrero de 2021	Adición de una nota sobre los ajustes de firewall en Device@Home.	Configuración de Dispositivo de sistema@Casa en la página 1004
PRB000050983	11 de febrero de 2021	Adición de una nota sobre el número de usuarios de Circuit por sistema.	Valores máximos para extensiones en la página 1466
PRB000051647	11 de febrero de 2021	Adición de información sobre Desvío de llamadas tras Deflect call/Transferencia paso individual y Determinación del destino mediante lista de destinos con Deflect call/Transferencia paso individual.	Ajustes básicos Sistema Flags del sistema en la página 1548
PRB000051165	19 de febrero de 2021	Corrección de nota con el tipo de dispositivo.	MULAP Jefe en la página 742
PRB000050983	15 de febrero de 2021	Se ha añadido una nota para función no compatible	Estaciones SIP en la página 446

Cambios en V2R7

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
NA16740815	11 de agosto de 2020	Adición de una nota a pie de página sobre el número máximo de llamadas simultáneas en MOH.	Valores máximos de los recursos en la página 1471
NA16653104	2 de junio de 2020	Actualización de documentación sobre puertos utilizados	Puertos utilizados en la página 274
NA16692823	30 de abril de 2020	Se agregó la opción para utilizar FQDN también en el campo WAN de MyPortal @work	Requisitos para myPortal @work en la página 502
NA16652178	8 de abril de 2020	Adición de una nota sobre la apertura del puerto 8101 en un proxy para el correcto funcionamiento de `CommunicationsServer.exe`.	Cómo realizar la desinstalación silenciosa en la página 556 Cómo realizar la instalación silenciosa en la página 555

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
NA16582432	6 de abril de 2020	Se agregó información sobre la activación de **Supervisión de llamadas**.	Supervisión de llamadas en la página 664

2 Introducción y notas importantes

La introducción ofrece una visión general de la estructura de esta documentación. Le ayudará a encontrar más rápidamente información sobre distintos temas. Antes de comenzar con el montaje y puesta en servicio del sistema de comunicación, consulte las indicaciones de seguridad y advertencias y las observaciones importantes.

Consejo: Las indicaciones de seguridad y las advertencias ofrecen información sobre las indicaciones de seguridad y de aviso que debe tener en cuenta. Las observaciones importantes incluyen indicaciones sobre el comportamiento en caso de emergencia, normas y pautas relativas a la instalación y propiedades de radio interferencia del sistema de comunicación. Además, incluyen información sobre la eliminación y el reciclaje adecuados.

Nota: This document may contain descriptions for features which may still be in beta status. For details see sales info and release notes.

2.1 Acerca de esta documentación

Este documento describe la administración de OpenScape Business™.

Incluya los modelos de hardware OpenScape Business X1, OpenScape Business X3, OpenScape Business X5 y OpenScape Business X8,. así como el modelo de software OpenScape Business S (softswitch). La solución de Comunicaciones Unificadas UC Smart está integrada en todos los modelos OpenScape Business. La solución de Comunicaciones Unificadas UC Suite se ofrece para los modelos de hardware con UC Booster Card o con UC Booster Server; en el softswitch se puede elegir entre UC Smart o UC Suite.

Nota: Los modelos de hardware OpenScape Business X1/ X3/X5/X8 (abreviado: OpenScape Business X) y el softswitch OpenScape Business S también se denominan "sistemas de comunicación" en este documento.

UC Suite designa las funciones avanzadas de Comunicaciones Unificadas, con el Multimedia Contact Center.

La información de esta documentación incluye descripciones generales de las opciones técnicas. Estas opciones no están presentes en todos los casos. Las prestaciones deseadas se deben definir para cada caso en el momento de cerrar el contrato.

Si una función no está disponible según la descripción, puede haber varios motivos:

- La prestación no está disponible en el sistema de comunicación.
- La licencia disponible no está disponible o no está activa.

2.1.1 Documentación y destinatarios

Los documentos relativos a OpenScape Business están dirigidos a distintos grupos.

Ventas y planificación de proyectos

El documento siguiente está dirigido a ventas y planificación de proyectos.

- Descripción de prestaciones

  Este documento describe todas las prestaciones. Este documento es un extracto de la Documentación para el administrador.

Instalación y servicio

El documento siguiente está dirigido a técnicos de servicio.

- OpenScape Business X1/X1W, Guía de instalación

  Este documento describe la instalación del hardware y la instalación inicial de OpenScape Business X1.
- OpenScape Business X3/X5/X8, Instrucciones de instalación

  Este documento describe la instalación del hardware y la instalación inicial de OpenScape Business X3/X5/X8.
- OpenScape Business S, Instrucciones de instalación

  Este documento describe la instalación inicial del softswitch OpenScape Business S.
- OpenScape Business X1/X1W, Documentación de servicio

  Este documento describe el hardware de OpenScape Business X1
- OpenScape Business X3/X5/X8, Documentación de servicio

  Este documento describe el hardware de OpenScape Business X3/X5/X8.
- OpenScape Business X1R, guía de instalación y servicio Documentación de servicio

  Este documento describe la instalación del hardware, la instalación inicial y el servicio de OpenScape Business X1R.

Administración

La siguiente documentación está dirigido a los administradores.

- Documentación del administrador

  Este documento describe la configuración de las prestaciones que se configuran mediante el OpenScape Business Assistant (GESTIÓN BASADA EN WEB, WBM). La documentación para el administrador está disponible en el sistema como ayuda online.
- Configuración para administradores de cliente, documentación para el administrador

  Este documento describe la configuración de las prestaciones que se pueden configurar con el OpenScape Business Assistant (administración basada en web, WBM) con el perfil de administrador **Básico**.
- Manager E, Documentación para el administrador

  Este documento describe la configuración de las prestaciones que se configuran con el Manager E.

Clientes de UC / Telephone User Interfaces (TUI)

Este documento está dirigido a usuarios de Comunicaciones unificadas (UC).

- myPortal for Desktop, Instrucciones de uso

  Este documento describe la instalación, la configuración y el funcionamiento del cliente de Comunicaciones unificadas (UC) myPortal for Desktop.
- myPortal for Outlook, Instrucciones de uso

  Este documento describe la instalación, la configuración y el funcionamiento del cliente de Comunicaciones unificadas (UC) myPortal for Outlook.
- myPortal@work, Instrucciones de uso

  Este documento describe la instalación, la configuración y el funcionamiento del cliente de UC myPortal @work.
- Impresora de fax, Instrucciones de uso

  Este documento describe la instalación, la configuración y el funcionamiento de Fax Printer.
- myPortal to go, Instrucciones de uso

  Este documento describe la configuración y el funcionamiento del cliente de Comunicaciones unificadas (UC) myPortal to go para smartphones y tabletas.
- myAgent, Instrucciones de uso

  Este documento describe la instalación, la configuración y el funcionamiento del cliente de Contact Center myAgent.
- myReports, Instrucciones de uso

  Este documento describe la instalación, la configuración y el funcionamiento del cliente de Contact Center myReports.
- myAttendant, Instrucciones de uso

  Este documento describe la instalación, la configuración y el funcionamiento del puesto de operadora myAttendant.
- OpenScape Business Attendant, Instrucciones de uso

  El documento describe la instalación, la configuración y el manejo del puesto de operadora OpenScape Business Attendant.
- UC Smart Telefon User Interface (TUI), Instrucciones breves

  Este documento describe el menú telefónico de buzón de voz de la solución de Comunicaciones Unificadas UC Smart.
- UC Suite Telefon User Interface (TUI), Instrucciones breves

  Este documento describe el menú telefónico de buzón de voz de la solución de Comunicaciones Unificadas UC Suite.

2.1.2 Estructura de la documentación del administrador

Esta sección le muestra cómo está estructurado el contenido de la Documentación del Administrador. El hardware se describe en la Documentación de servicio.

Sección	Contenido
Introducción y notas importantes	Descripción general de la estructura de esta documentación e información importante/ de seguridad que se debe tener en cuenta durante la instalación y el funcionamiento
Descripción general del sistema	Descripción general del sistema de comunicación para un inicio rápido
Concepto de administración	Descripción general de los programas de administración y roles de usuario en WBM
Instalación inicial de OpenScape Business X	Integración de OpenScape Business X3/ X5/X8 en la LAN del cliente y configuración básica mediante asistentes
Instalación inicial de OpenScape Business S	Integración de OpenScape Business S en la LAN del cliente y configuración básica mediante asistentes
Instalación inicial de OpenScape Business UC Booster	Integración de OpenScape UC Business Booster en la LAN del cliente y configuración básica mediante asistentes
Registro de licencia	Procedimientos de licencia y licencias
Integración en la red interna de datos (LAN)	Interfaz LAN/WAN, resolución de nombres, enrutamiento de datos, DLI y DLS
Conexión con el proveedor de servicios	Acceso a Internet, telefonía IP, acceso troncal
Extensión	Plan de marcación, estaciones IP, estaciones UP0, estaciones DECT, estaciones SIP-DECT de Mitel, estaciones ISDN y analógicas, estaciones virtuales, usuarios de clientes UC, perfiles de usuario
UC Smart	Clientes y funciones de la solución de comunicaciones unificadas UC Smart, incluido Smart Voicemail. Estado de presencia, directorios y diario, conferencias, funciones de equipo, mensajes de voz
UC Suite	Clientes y funciones de la solución de comunicaciones unificadas UC Suite: Estado de presencia y CallMe, directorios y diario, conferencias y colaboración web, mensajes de voz y fax, mensajería instantánea
Funciones en el teléfono	Realizar llamadas, señalización de llamadas, identificación de la línea que llama, funciones durante la llamada, optimización de la comunicación
Trabajar en equipo (grupos)	Grupo de captura de llamadas, llamada de grupo, grupo de búsqueda, equipo/superior, MULAP, UCD

Sección	Contenido
Encaminamiento de llamadas	Clases de servicio, restricción de peaje, sistema de inquilinos, LCR, llamadas de emergencia
Asistentes	Asistentes automáticos, asistentes OpenStage, asistentes basados en PC, posición de intercepción
Centro de contacto multimedia	Clientes y funciones del Contact Center: agentes, colas y horarios, atención VIP, fallback, informes
Movilidad	myPortal to go, Mobility Entry, Servicio de un solo número, telefonía de modo dual, movilidad IP, inalámbrico/DECT
Seguridad	Cortafuegos, SPE, VPN, certificados
Interconexión de OpenScape Business	Plan de red, escenarios de red, posición de intercepción central, capacidad de supervivencia
Conexiones	Dispositivos de anuncio, portero automático y portero automático, actuadores y sensores
Conectividad de aplicaciones	CSTA, TAPI, Lanzador de aplicaciones
Contabilidad	Grabación de detalles de llamadas, cargos y duración de llamadas, control de costos
Mantenimiento	Copia de seguridad y restauración, actualización, reinicio, recarga, apagado, restablecimiento de fábrica, inventario, acciones, servicios remotos
Migración	Actualización de HiPath 3000 a OpenScape Business
Límites de configuración y capacidades	Valores máximos para los límites de configuración y capacidades de los diferentes sistemas de comunicación
Modo experto	Descripción de referencia de las ventanas/ máscaras en el modo Experto
Apéndice	Lista de estándares admitidos, las características de Euro-ISDN y los protocolos IP y números de puerto utilizados
Glosario	Breves descripciones de términos de uso común

2.1.3 Tipos de temas

Los tipos de temas incluyen conceptos y tareas.

Tipo de tema	Descripción
Concepto	Explica el "qué" y ofrece una visión general de las relaciones e información básica, por ejemplo, sobre prestaciones.
Tarea (Instrucciones de uso)	Describe el "cómo" de casos de aplicación orientados a tareas y presupone el conocimiento previo de los conceptos teóricos correspondientes. Las tareas se pueden identificar por el formato de título **Cómo...**.

2.1.4 Convenciones de representación

Esta documentación utiliza distintos medios para representar los distintos tipos de información.

Tipo de información	Visualización	Ejemplo
Elementos de la interfaz de usuario	negritas	Haga clic en **Aceptar**.
Secuencia de menú	>	**Archivo** > **Salir**
Énfasis especial	negritas	El nombre **no se puede borrar**.
Referencia cruzada	cursiva	Encontrará más información en la sección *Red*.
Salida	Fuente con espaciado de letra fijo, por ejemplo, Courier	`Comando no encontrado.`
Entrada	Fuente con espaciado de letra fijo, por ejemplo, Courier	`Introducir` LOCAL como nombre de archivo.
Combinación de teclas	Fuente con espaciado de letra fijo, por ejemplo, Courier	`<Ctrl>+<Alt>+<Esc>`

2.2 Indicaciones de seguridad y de aviso

Las indicaciones de seguridad y aviso identifican situaciones que pueden provocar la muerte, lesiones graves, daños materiales y/o pérdida de datos.

En los sistemas de comunicación y en los dispositivos **solo** pueden trabajar personas cualificadas.

En estas indicaciones de seguridad y aviso, el personal cualificado son aquellas personas autorizadas a poner en servicio, poner a tierra y etiquetar los

sistemas, equipos y líneas según los procedimientos y estándares de seguridad vigentes.

Es imprescindible que lea y tenga en cuenta las siguientes indicaciones de seguridad y de advertencia antes de comenzar con el montaje y la puesta en servicio del sistema de comunicación.

Lea además todas las indicaciones de aviso y de seguridad del sistema de comunicación y de los dispositivos, y sígalas cuidadosamente.

Infórmese también de cuáles son los números de emergencia.

Tipos de advertencias de seguridad y avisos

En esta documentación se utilizan los siguientes grados de indicaciones de seguridad y aviso:

PELIGRO: Identifica una situación de riesgo inmediato que podría causar la muerte o lesiones graves.

Atención: Identifica una situación de riesgo general que podría causar la muerte o lesiones graves.

PRECAUCIÓN: Identifica una situación de riesgo que podría causar lesiones.

Nota: Identifica situaciones que podrían causar daños materiales y/o pérdida de datos.

Símbolos adicionales para una descripción más detallada de la fuente de peligro

El siguiente símbolo no se suele utilizar en esta documentación, pero puede aparecer en los dispositivos o embalajes.



Componentes sometidos a cargas electrostáticas (EGB)

Conceptos relacionados

Avisos importantes en la página 84

2.2.1 Indicaciones de aviso: Peligro

Las indicaciones de tipo Peligro identifican una situación de riesgo inmediato que podría producir la muerte o lesiones graves.

PELIGRO: Descarga eléctrica al tocar los cables con tensión

- Recuerde: ¡la tensión por encima de 30 V c.a. (corriente alterna) ó 60 V c.c. (corriente continua) es peligrosa!
- Solo pueden realizar trabajos en la red de baja tensión (<1000 V ca) técnicos eléctricos con la calificación pertinente. Se deben cumplir todas las normativas nacionales y locales relativas a conexiones eléctricas.

2.2.2 Indicaciones de aviso: Advertencia

Las indicaciones del tipo Advertencia identifican una situación de riesgo general que podría producir la muerte o lesiones graves.



Atención: Descarga eléctrica al tocar los cables con tensión

- Conecte a tierra los sistemas de comunicación OpenScape Business X3R, X3W, X5R y X5W con un conductor de protección de tierra independiente. Conecte el sistema de comunicación antes de la puesta en servicio y de la conexión de teléfonos y líneas con el conductor de protección de tierra.
- Conecte a tierra todos los armarios del sistema del sistema de comunicación OpenScape Business X8 con un conductor de protección de tierra independiente. Conecte el sistema de comunicación antes de la puesta en servicio y de la conexión de teléfonos y líneas con el conductor de protección de tierra.
- Utilice solo sistemas, equipos y medios operativos que se encuentren en perfecto estado. Está prohibido poner en servicio dispositivos con daños externos.
- Sustituya inmediatamente los elementos de seguridad defectuosos (cubiertas, etiquetas adhesivas y cables de protección).
- Cambie inmediatamente el cable de red si presenta algún tipo de daño.
- Ponga los sistemas de comunicación y los sistemas de comunicación en servicio solo con enchufes con contacto de protección conectado.
- Durante una tormenta no conecte ni extraiga nunca las líneas ni monte o extraiga los módulos.
- Desconecte toda la alimentación eléctrica si el suministro de corriente del sistema de comunicación no es necesario para determinadas tareas (por ejemplo, al modificar el cableado). Extraiga los enchufes de red del sistema de comunicación y asegúrese de que el sistema de comunicación no recibe alimentación de una fuente de tensión adicional (por ejemplo, un suministro de corriente continuo).

  Antes de empezar a trabajar, compruebe que el sistema de comunicación no tiene tensión. Nunca dé por sentado que al apagar un fusible o un interruptor principal quedan interrumpidos de forma fiable todos los circuitos de corriente.
- Tenga en cuenta que pueden producirse corrientes de fuga desde la red de telecomunicaciones. Desconecte todos los cables de telecomunicaciones del sistema de comunicación antes de desconectar el conductor de protección de tierra obligatorio.

- Si el suministro de corriente está conectado, ponga extremo cuidado al efectuar las mediciones en las piezas conductoras de tensión, así como los trabajos de mantenimiento en módulos o cubiertas.

  Las superficies con recubrimiento metálico (p. ej. espejos) son conductoras de corriente, si se tocan existe el peligro de una descarga eléctrica o de un cortocircuito.

2.2.3 Advertencias: Atención

Las indicaciones del tipo Atención identifican una situación peligrosa que podría provocar daños.

PRECAUCIÓN: Si la batería o las pilas no se sustituyen correctamente, pueden producirse explosiones

- Utilice únicamente baterías autorizadas.
- Sustituya la batería de litio con una idéntica o con un tipo recomendado por el fabricante.

PRECAUCIÓN: Peligro de incendio

- Utilice solo líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o más.
- No deposite documentos ni otros objetos incendiables en el sistema de comunicación.

PRECAUCIÓN: Riesgo de accidente o lesión general en el puesto de trabajo

- Una vez finalizadas las tareas de prueba y de mantenimiento, vuelva a instalar todos los dispositivos de seguridad en el lugar correcto y vuelva a cerrar la tapa y la caja.
- Tienda los cables de tal manera que no puedan surgir accidentes (peligro de tropezar con ellos) ni se dañen.
- Cerciórese de que tanto el sistema de comunicación como el servidor estén constantemente vigilados mientras están abiertos cuando son manipulados.
- Utilice siempre herramientas adecuadas para levantar objetos o cargas pesados.
- Compruebe el estado de sus herramientas con regularidad. Utilice solo herramientas que se encuentren en perfecto estado.
- Cuando realice trabajos en los sistemas, evite llevar ropa holgada y si tiene el cabello largo, recójaselo.
- No se ponga joyas, correas de reloj metálicas ni lleve tampoco, p. ej., aplicaciones o remaches metálicos en su ropa.
- Utilice siempre durante el trabajo la protección de los ojos correspondiente.
- Utilice siempre un casco en todos los lugares en los que exista peligro de caída de objetos.

- Asegúrese de que el puesto de trabajo esté bien iluminado y ordenado.

2.2.4 Indicaciones de aviso: Aviso

Las indicaciones del tipo Aviso identifican situaciones que podrían provocar daños materiales y/o pérdida de datos.

Siga las siguientes indicaciones para evitar daños materiales y/o pérdidas de datos:

- Antes de la puesta en servicio, compruebe que la tensión nominal de la red de alimentación coincida con la tensión nominal del sistema de comunicación o del servidor (placa de características).
- Siga estas medidas de protección antiestática para proteger los componentes:
  - Antes de iniciar cualquier trabajo en los componentes y módulos, póngase la muñequera de toma de tierra de la forma reglamentaria.
  - Ponga siempre los módulos y componentes sobre una superficie conductora y con toma de tierra.
  - Los componentes del sistema de comunicación (por ejemplo, módulos) siempre se deben enviar en un embalaje adecuado.
- Utilice solo accesorios originales. De no hacerlo, pueden ocasionarse averías en el sistema de comunicación o incumplirse las indicaciones de seguridad o de compatibilidad electromagnética establecidas.
- Si la temperatura cambia repentinamente puede condensarse la humedad ambienta. Si, por ejemplo, el sistema de comunicación o el servidor es llevado desde un entorno frío a un espacio cálido, puede darse condensación de humedad. Espere hasta que la temperatura se normalice y el sistema de comunicación y el servidor estén completamente secos antes de ponerlos en servicio.
- Conecte los cables solo en los puntos de conexión indicados.
- Si no hay disponible un suministro eléctrico de emergencia o si en caso de caída eléctrica no se pueden utilizar teléfonos de emergencia, el sistema de comunicación no permitirá realizar llamadas de emergencia en caso de caída del suministro eléctrico.
- Antes de comenzar con el montaje mural, compruebe si la pared tiene una capacidad de carga suficiente. Utilice siempre medios de instalación o sujeción adecuados para montar de forma segura los sistemas de comunicación y los equipos.
- No permita que se depositen materiales altamente inflamables junto al sistema de comunicación.

2.2.5 Indicaciones de seguridad nacionales

Aquí encontrará información sobre las indicaciones de seguridad para el montaje, la puesta en servicio y la operación del sistema de comunicación en algunos países.

2.2.5.1 Indicaciones de seguridad para Australia

Durante el montaje, la puesta en servicio y el funcionamiento de los sistemas de comunicación OpenScape Business X y OpenScape Business S y del servidor OpenScape Business UC Booster Server (servidor de aplicaciones) en Australia hay que tener siempre en cuenta las siguientes indicaciones de seguridad:

- Solo personal técnico autorizado puede hacer la instalación y el mantenimiento de los sistemas de comunicación OpenScape Business X y OpenScape Business S y del servidor OpenScape Business UC Booster Server (servidor de aplicaciones).
- Los sistemas murales OpenScape Business deben instalarse cerca de un enchufe de pared para el suministro de tensión al sistema de comunicación correspondiente. La caja de conexión de pared debe estar accesible. Es imprescindible asegurarse de que el contacto de tierra de la caja de conexión de pared esté en perfectas condiciones.
- Hay que configurar los sistemas de comunicación OpenScape Business X y OpenScape Business S y el servidor OpenScape Business UC Booster Server (servidor de aplicaciones) de forma que se puedan marcar en todo momento números de emergencias (por ejemplo, 000).
- Si se produce una caída de la tensión de red, no se pueden realizar llamadas de emergencia a través del sistema de comunicación si no hay un suministro de emergencia o no se puede conmutar a teléfonos de emergencia analógicos (conmutación de línea urbana).
- Los equipos de música en espera y de búsqueda deben conectarse al sistema de comunicación mediante una Line Isolation Unit autorizada por la ACA (Australian Communications Authority).

2.2.5.2 Indicaciones de seguridad para Brasil

Durante el montaje, la puesta en servicio y el funcionamiento de los sistemas de comunicación OpenScape Business X y OpenScape Business S y del servidor OpenScape Business UC Booster Server (servidor de aplicaciones) en Brasil hay que tener siempre en cuenta estas indicaciones de seguridad:

- Es imprescindible utilizar la regleta con protección contra sobretensiones con el código C39334-Z7052-C33. La conexión de tensión de red de los sistemas de comunicación OpenScape Business X y OpenScape Business S y del servidor OpenScape Business UC Booster Server (servidor de aplicaciones) debe realizarse mediante la regleta con protección contra sobretensiones.
- Es obligatorio el uso de cables Ethernet blindados para las conexiones/interfaces LAN/WAN de las placas base OCCL, OCCM y OCCMR y de la UC Booster Card OCAB (Tablero de aplicaciones).

2.2.5.3 Indicaciones de seguridad para EE. UU.

Durante el montaje, la puesta en servicio y el funcionamiento de los sistemas de comunicación OpenScape Business X y OpenScape Business S y del servidor OpenScape Business UC Booster Server (servidor de aplicaciones) en los EE. UU., hay que tener siempre en cuenta estas indicaciones de seguridad:

- Interrupciones de red y fallo de T1

  En una interconexión de sistemas de comunicación mediante T1 (1,544 MBit/S), hay que informar a la compañía telefónica (Federal Communications Commission FCC) si se retira de la red un sistema de comunicación.

  Si alguno de los sistemas de comunicación de Unify Software and Solutions GmbH & Co. KG. descritos en esta documentación afecta al funcionamiento de la red de telecomunicaciones pública, la compañía telefónica está autorizada a bloquear de forma provisional el acceso a la línea urbana. Por norma general, se informa previamente al respecto a la compañía telefónica. Si no es posible, se lo comunicará posteriormente lo antes posible. En este contexto, usted será informado al mismo tiempo de que puede presentar una reclamación a la compañía telefónica.
- Modificación de equipos de telecomunicación

  La compañía telefónica está facultada para adaptar en caso necesario sus propios equipos, procedimientos operativos y procesos. Las modificaciones de este tipo pueden afectar, en su caso, al servicio de sus sistemas de comunicación. Por norma general recibirá un aviso previo para que no se vea interrumpido el servicio de telecomunicaciones.
- Equipos de reproducción de voz

  Los dispositivos de reproducción de voz (por ejemplo, dispositivos de música en espera y de grabación de voz) deben estar autorizados por Unify Software and Solutions GmbH & Co. KG y estar registrados según las directrices y disposiciones de las normas FCC, parte 68, subsección C.

  Los dispositivos no autorizados para la reproducción de voz solo se pueden conectar con circuitos de protección autorizados por Unify Software and Solutions GmbH & Co. KG y registrados según las directrices y disposiciones de las normas FCC, parte 68, subsección C.
- Ringer Equivalence Number REN

  El valor de conexión (Ringer Equivalence Number, REN) determina cuántos equipos se conectan simultáneamente a una línea telefónica y pueden señalizar una llamada si se marca el número en cuestión. En la mayoría de las áreas, pero no en todas, pueden conectarse como máximo cinco equipos a una línea (REN = 5). Diríjase en su caso a su compañía telefónica local para saber cuántos REN se soportan en su área de llamada.
- Nuevos códigos urbanos y de red local

  La prestación Ruta más económica (Least Cost Routing LCR) se debe configurar de forma que se puedan detectar y tomar en consideración automáticamente los cambios en los códigos de red local y de línea urbana. De lo contrario, después de cambios en los códigos no se podrán utilizar para llamadas.
- Compatibilidad con audífonos

  Los teléfonos de emergencias y los teléfonos públicos (p. ej., los teléfonos que se encuentren en recibidores, habitaciones de hospital, ascensores y habitaciones de hotel) deben tener microteléfonos compatibles con el uso de audífonos acoplados magnéticamente. Si es necesario, para personas con problemas de audición que no se encuentren en zonas públicas deben suministrarse, microteléfonos adecuados.

  Todos los teléfonos digitales de Unify Software and Solutions GmbH & Co. KG fabricados después del 16 de agosto de 1989 son

compatibles con audífonos y cumplen los requisitos de las normas FCC, parte 68, secciones 68.316 y 68.317.

- Funciones de marcación programadas

  Si desea programar números de teléfono de emergencia o establecer una conexión de prueba con un número de teléfono de emergencia mediante un producto de Unify Software and Solutions GmbH & Co. KG con funciones de marcación programadas, deberá retener la comunicación y explicar brevemente a la persona responsable la razón de su llamada antes de colgar. Se recomienda realizar estas medidas en momentos en los que no haya mucho tráfico (por ejemplo, a primera hora de la mañana o última hora de la tarde).
- Conexión de extensiones externas

  Los clientes que quieran conectar extensiones externas (Off-Premises Station OPS), deben informar a la compañía telefónica de la clase OPS en la que están registrados los dispositivos correspondientes y de cuál será el tipo de conexión.
- Supervisión de la aceptación de llamadas con marcación directa

  Los clientes que operen uno de los sistemas de comunicación de Unify Software and Solutions GmbH & Co. KG descritos en esta comunicación sin una supervisión adecuada de la aceptación de llamadas están incumpliendo la parte 68 de las disposiciones FCC.

  Los sistemas de comunicación de Unify Software and Solutions GmbH & Co. KG. descritos en esta documentación retornan una supervisión de llamadas correcta a la red telefónica pública conmutada (PSTN) cuando las llamadas de marcación directa:

  – son aceptadas por el usuario llamado.
  – son aceptadas por personal de conmutación.
  – son desviadas a un anuncio grabado administrado en el lado del cliente.

  Además, los sistemas de comunicación de Unify Software and Solutions GmbH & Co. KG. descritos en esta documentación retornan una supervisión de llamadas correcta para las llamadas de marcación directa transferidas a la PSTN. Excepciones permitidas:

  – No se contesta una llamada.
  – Hay señalización de ocupado.
  – Se recibe un tono de congestión (reorder tone).
- Requisitos para el acceso equitativo

  En áreas con un elevado tráfico (hoteles, hospitales, aeropuertos, centros escolares), hay que suministrar a las extensiones códigos de acceso equitativos para los proveedores deseados. Los códigos actuales para el acceso equitativo (también llamados "Códigos de acceso de operador" [CACs]), son 10xxx y 101xxxx, 800/888 y 950, donde xxx o xxxx corresponde al código de proveedor respectivo.

  Para establecer una conexión a través de un determinado proveedor, el usuario debe introducir primero antes del número de teléfono del interlocutor deseado un código de acceso específico del proveedor. También se puede

acceder al acceso equitativo a través de los números 800/888 o 950 del proveedor deseado.

Mediante códigos de acceso equitativos, los sistemas de comunicación descritos de Unify Software and Solutions GmbH & Co. KG. descritos en esta documentación permiten el acceso a proveedores interestatales.

La modificación de estas funciones representa una violación de la norma Telephone Operator Consumer Services Improvement Act de 1990, así como de la parte 68 de las normas FCC.

2.2.5.4 Indicaciones de seguridad para Canadá



PELIGRO: Descarga eléctrica al tocar los cables con tensión

Solo pueden realizar trabajos en la red de baja tensión (<1000 V ca) técnicos eléctricos con la calificación pertinente. Se deben cumplir todas las normativas nacionales y locales relativas a conexiones eléctricas.

Durante el montaje, la puesta en servicio y el manejo de los sistemas de comunicación OpenScape Business X y OpenScape Business S y del servidor OpenScape Business UC Booster Server (servidor de aplicaciones) en Canadá, hay que tener siempre en cuenta estas indicaciones de seguridad:

- Ringer Equivalence Number REN

  El valor de conexión (Ringer Equivalence Number, REN) determina cuántos equipos pueden conectarse simultáneamente a una línea telefónica. La terminación de interfaz puede abarcar un combinación de equipos cualquiera – siempre que la cantidad REN sea inferior o igual a cinco.
- Restricciones para la conexión de dispositivos

  La etiqueta de Innovation, Science and Economic Development Canada (ISED) identifica a los equipamientos certificados. Esta certificación garantiza que los dispositivos cumplen ciertos requisitos relativos a la protección, el manejo y la seguridad de redes de telecomunicaciones. Los requisitos están documentos en el documento de Terminal Equipment Technical Requirements. Innovation, Science and Economic Development Canada (ISED) no ofrece ninguna garantía de que los dispositivos certificados vayan a funcionar en todo momento de forma satisfactoria para los clientes.

  Antes de instalar los componentes y los dispositivos descritos en esta documentación, el usuario debería cerciorarse de que se dispone de una conexión a los equipos de la compañía telefónica local. Además, al instalar los sistemas de comunicación y servidores hay que procurar elegir un procedimiento de conexión adecuado. Se debería hacer notar al cliente que, aunque se cumplan todas las normas descritas, en determinadas situaciones pueden producirse pérdidas de potencia.

  Las reparaciones que se realicen en dispositivos certificados deben estar coordinadas por un técnico de servicio del fabricante o del proveedor. La compañía telefónica puede solicitar al usuario que desinstale los dispositivos correspondientes, si el usuario realiza reparaciones o modificaciones en

los dispositivos y componentes descritos en esta documentación, o si estos presentan algún tipo de avería.

Por su propia seguridad, el usuario debería asegurarse de que las conexiones eléctricas de puesta a tierra del suministro de corriente, de las líneas telefónicas y de la red de cañerías metálicas internas (si las hay) estén conectadas entre sí. Esta medida de seguridad puede ser importante sobre todo en zonas rurales.

2.3 Avisos importantes

Los Avisos importantes ofrecen información sobre el comportamiento en caso de emergencia, la eliminación y el reciclaje correctos, el uso adecuado y las condiciones de servicio de los sistemas de comunicación y servidores. Además, ofrecen información sobre normas y pautas relativas a la instalación, propiedades de radio interferencia del sistema de comunicación, protección y seguridad de datos.

Conceptos relacionados

Indicaciones de seguridad y de aviso en la página 75

2.3.1 Comportamiento en caso de emergencia

Aquí encontrará información sobre las medidas a tomar en caso de emergencia.

Comportamiento en caso de accidente

Primeros auxilios

Llamada de emergencia

Comunicación de accidentes

- Mantenga la calma en todo momento y actúe con prudencia.
- Antes de tocar a la víctima del accidente, desconecte siempre la tensión.
- En caso de que no pueda desconectar la tensión inmediatamente, toque a la víctima solamente con materiales no conductores (p. ej. palo de escoba de madera), e intente primeramente aislarla de la fuente de tensión.
- En caso de accidente por descarga eléctrica debe estar familiarizado con los principios elementales de primeros auxilios. Para estos casos de emergencia es indispensable tener conocimientos básicos de las diversas medidas de reanimación ante paro respiratorio o cardíaco, así como de primeros auxilios en caso de quemaduras.
- En caso de paro respiratorio, ejecute sin demora la respiración artificial (boca a boca o boca-nariz).
- Si dispone de la capacitación correspondiente, realice un masaje cardíaco en caso de paro cardíaco.

Llame inmediatamente a una ambulancia o al médico de urgencia. Realice la llamada de emergencia y comunique lo sucedido en el siguiente orden:

- Lugar del suceso
- Qué ha sucedido
- Número de heridos
- Tipo de heridas
- Preste atención a las preguntas que puedan hacerle.
- Comunique sin demora a sus superiores todos los accidentes, los "casi accidentes" y las fuentes potenciales de peligro.
- Notifique cualquier descarga eléctrica aunque haya sido mínima.

2.3.2 Uso adecuado

Los sistemas de comunicación y servidores solo se pueden utilizar con las opciones de uso descritas en esta documentación y en combinación con los dispositivos y componentes adicionales recomendados y autorizados por Unify Software and Solutions GmbH & Co. KG.

El uso adecuado de los sistemas de comunicación supone el transporte, el almacenamiento, el montaje y la puesta en servicio adecuados y a manos de expertos, y el manejo y mantenimiento cuidadosos.

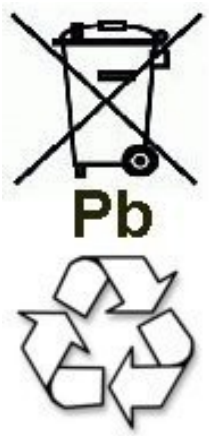
Nota: Limpie la carcasa del sistema de comunicación y del servidor solamente con un paño suave y ligeramente humedecido. No utilice detergentes agresivos ni esponjas agresivas.

2.3.3 Eliminación y reciclaje adecuados

Aquí obtendrá información sobre la eliminación y reciclaje correctos de dispositivos eléctricos y electrónicos y de baterías y pilas usadas.



No está permitido eliminar junto con la basura doméstica los equipos eléctricos o electrónicos. Se deben utilizar los puestos de eliminación de residuos previstos por la ley. La eliminación de residuos y la recogida por separado de los equipos en desuso ayuda a reducir los daños potenciales a la salud y al medio ambiente. Son requisito para la reutilización y el reciclaje de los equipos eléctricos y electrónicos. Si desea información más detallada sobre la eliminación de sus equipos, entre en contacto con las autoridades municipales, con el servicio de recogida de basuras, con la tienda en la que adquirió el producto o con su representante de ventas. Estas indicaciones solo son válidas para dispositivos adquiridos e instalados en los países de la Unión Europea y adheridos a la directiva europea 2012/19/UE. En los países que no formen parte de la Unión Europea puede haber otras normativas para la eliminación y tratamientos de equipos eléctricos o electrónicos.



Las baterías y pilas usadas con este símbolo son bienes reutilizables y deben ser sometidas al proceso de reciclaje. Las baterías y pilas usadas que no son sometidas a un proceso de reciclaje deben ser eliminadas siguiendo todas las normas para los desechos especiales.

2.3.4 Normas y pautas relativas a la instalación

Aquí encontrará información sobre las pautas a observar en la conexión de los sistemas de comunicación a un circuito eléctrico y en el cableado blindado para conexiones LAN y WAN.

2.3.4.1 Conexión de OpenScape Business X al circuito de alimentación eléctrica

Los sistemas de comunicación OpenScape Business X están homologados para la conexión con sistemas de suministro de energía TN-S. Asimismo se admite la conexión a un sistema de alimentación de energía TN-C-S, en el que el conductor PEN está dividido respectivamente en un conductor de protección y un conductor neutro. TN-S y TN-C-S se consideran con arreglo a la definición en las normas estándar IEC 60364-1 y IEC60364-5-51.

Los trabajos en la red de baja tensión solo pueden ser llevados a cabo por parte de un técnico eléctrico autorizado. Estas actividades de instalación dedicadas a conectar los sistemas de comunicación deben realizarse bajo cumplimiento de las normas IEC 60364-1 e IEC 60364-4-41 o cualquier otra normativa legal o prescripciones de ámbito nacional (por ejemplo, en los EE. UU. y Canadá).

2.3.4.2 Conexión de OpenScape Business S y OpenScape Business UC Booster Server con el circuito de alimentación eléctrica

Consulte los datos de conexión de OpenScape Business S y OpenScape Business UC Booster Server (servidor de aplicaciones) con el circuito de alimentación eléctrica en la documentación del fabricante del PC de servidor y demás componentes.

Los trabajos en la red de baja tensión solo pueden ser llevados a cabo por parte de un técnico eléctrico autorizado. Estas actividades de instalación dedicadas a conectar OpenScape Business S y OpenScape Business UC Booster Server deben realizarse bajo cumplimiento de las normas IEC 60364-1 e IEC 60364-4-41 o cualquier otra normativa legal o prescripciones de ámbito nacional (por ejemplo, en los EE. UU. y Canadá).

2.3.4.3 Cableado blindado para conexiones LAN y WAN de OpenScape Business X

El cumplimiento de los requisitos de la CE sobre compatibilidad electromagnética de los sistemas de comunicación OpenScape Business X y sus conexiones LAN y WAN supone la siguiente condición:

- Los sistemas de comunicación solo se pueden operar con cableado de conexión blindado. Esto significa que entre los conectores hembra LAN y WAN blindados de los sistemas de comunicación y la conexión a la instalación del edificio o la conexión a componentes activos externos se debe utilizar un cable de la categoría 5 (cable CAT.5) blindado con una longitud mínima de 3 m. En el extremo del cable conectado a la instalación del edificio o al componente activo externo, el blindaje del cable debe ponerse a tierra (enlace para la conexión equipotencial del edificio).
- En el caso de enlaces más cortos con un componente activo externo (conmutador LAN o similar) también se debe utilizar un cable de la categoría 5 blindado (cable CAT.5). No obstante, el componente activo deberá disponer de una conexión LAN blindada pertinente cuya conexión de blindaje esté puesta a tierra (enlace para la conexión equipotencial del edificio).
- Las propiedades de blindaje de los componentes de cableado deben cumplir como mínimo los requisitos de la norma europea EN 50173-1[*)] "Tecnología de la información - Sistemas de cableado genéricos" (y las referencias mencionadas en ella).[***)]
- Las instalaciones en edificios provistas de cableado de cobre simétrico blindado convencional según los requisitos de la clase D[**)] de la normativa EN 50173-1 cumplen la condición mencionada antes.[***)]

2.3.4.4 Normativa de protección antiincendios

La normativa de protección antiincendios está regulada en las ordenanzas de edificación de cada país. Deben respetarse las disposiciones vigentes en cada caso.

Para garantizar el cumplimiento de la normativa legal de protección antiincendios y compatibilidad electromagnética, los sistemas de comunicación OpenScape Business X solo pueden operarse cuando se encuentran cerrados. La apertura no está permitida sino de forma provisional para fines de montaje y mantenimiento.

---

*) La norma europea EN 50173-1 se deriva del estándar global ISO/IEC 11801.

**) La clase D se consigue entre otras cosas si hay instalados componentes (cables, cajas de conexión, cables de conexión, etc.) de la categoría 5 (CAT.5).

***) En el mercado norteamericano hay instalado mayoritariamente cableado UTP (norma US EIA/TIA 568 A/B), lo que implica los siguientes factores para las conexiones LAN y WAN de los sistemas de comunicación: Los sistemas solo se pueden operar con cableado de conexión blindado. Esto significa que entre los conectores hembra LAN y WAN blindados de los sistemas de comunicación y la conexión a la instalación del edificio o la conexión a componentes activos externos se debe utilizar un cable de la categoría 5 (cable CAT.5) blindado con una longitud mínima de 3 m. En el extremo del cable conectado a la instalación del edificio o al componente activo externo, el blindaje del cable debe ponerse a tierra (enlace para la conexión equipotencial del edificio).

Los cables de sistema OpenScape-Business siguen las exigencias del estándar internacional IEC 60332-1 respecto a comportamiento en caso de incendio. Los siguientes estándares incluyen requisitos equivalentes respecto al comportamiento en caso de incendio de cables:

IEC 60332-1 Aviso: IEC 60332-1 es equivalente al método de verificación UL VW-1	EN 60332-1-1 y EN 60332-2-1	DIN EN 60332-1-1 (VDE 0482-332-1-1) y DIN EN 60332-2-1 (VDE 0482-332-2-1)

El área responsable de la proyección y el servicio técnico debe verificar si el estándar IEC 60332-1 cumple las ordenanzas de edificios correspondientes y posibles disposiciones adicionales.

2.3.4.5 Requisitos de protección contra descargas

La protección de los sistemas de comunicación contra sobretensiones eléctricas requiere una conexión de tierra de baja resistencia conforme a las indicaciones recogidas en las *Instrucciones de instalación de OpenScape Business*.

Nota: Una vez realizada la puesta a tierra de protección de un sistema de comunicación hay que comprobar la conexión a tierra de baja resistencia del sistema mediante el conductor de protección del circuito de suministro de tensión de red y la conexión de baja resistencia del conductor de toma de tierra de protección adicional y con conexión permanente con a las líneas de compensación de potencial del edificio.

Nota:

Peligro de incendio por sobretensión

Las líneas de telecomunicaciones de más de 500 m o las líneas de telecomunicaciones que salen del edificio se deben conducir por una protección contra descargas externa adicional.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje adecuado de conductores de descarga de sobretensión (con gas) en el distribuidor principal, en el panel de conexiones o en el punto de entrada de la línea en el edificio. Para ello, hay que conmutar a tierra un conductor de descarga de sobretensión con una tensión nominal de 230 V desde cada uno de los conductores que se quieren proteger.

Sin esta protección primaria adicional, los módulos pueden quedar destruidos en caso de descarga eléctrica por rayos. Esto a su vez puede producir la caída de todo el sistema de comunicación y el sobrecalentamiento de los elementos constructivos (peligro de incendio).

2.3.4.6 Identificaciones para OpenScape Business X



La marca CE confirma el cumplimiento del equipo con las directrices de la UE. Puede consultar esta declaración de conformidad, otras declaraciones de conformidad existentes e información adicional sobre normativas que restringen el uso de sustancias o que afectan a la declaración de sustancias utilizadas en productos, en la WIKI para expertos de Unify, que encontrará en.

2.3.5 Indicaciones sobre interferencias electromagnéticas y radio interferencias de OpenScape Business X

Los sistemas de comunicación OpenScape Business X son dispositivos de la clase B según la normativa EN 55032.

2.3.6 Privacidad y seguridad de los datos

Siga la información sobre la protección y seguridad de los datos.

Los sistemas de comunicación y servidores descritos en esta documentación trabajan, entre otros, con datos privados y los utilizan, por ejemplo, para el registro de tarifas, indicaciones en pantalla y el registro de datos de clientes.

Para el procesamiento y utilización de estos datos personales, en Alemania rige lo establecido por la Ley Federal de Privacidad de Datos (BDSG). Para los demás países deberá tenerse en cuenta la legislación vigente en cada uno de ellos.

Mediante la privacidad de datos se pretende evitar que el uso indebido de los datos personales de los clientes afecte a sus derechos individuales.

Se pretende, además, evitar el uso indebido de los datos en las diferentes fases de su procesamiento e impedir todo abuso sobre asuntos propios o ajenos dignos de protección.

Consejo: El cliente es responsable de que la instalación, puesta en servicio y mantenimiento de los sistemas de comunicación y servidores cumple con la normativa vigente en materia de protección de datos y derecho laboral y de seguridad en el trabajo.

Empleados de Unify Software and Solutions GmbH & Co. KG están sujetos a las normas internas que exigen un trato confidencial de los secretos empresariales y de los datos confidenciales.

A fin de actuar siempre conforme a las normas legales debe tener presentes en todo momento (también en las tareas de asistencia técnica, ya sea en visitas al cliente o al efectuar la teleasistencia) las reglas indicadas a continuación. De

esta forma, no sólo protegerá los intereses de sus y nuestros clientes, sino que evitará igualmente consecuencias para su persona.

Colabore para garantizar la privacidad y seguridad de los datos, actuando con la responsabilidad que ello requiere:

- Ponga especial atención en que solo las personas autorizadas tengan acceso a los datos de los clientes.
- Aproveche siempre las posibilidades que le ofrece la asignación de contraseñas; evite que éstos puedan quedar al alcance de personas no autorizadas, p. ej., al apuntarlos en notas.
- Tome las medidas necesarias para impedir que las personas no autorizadas hagan uso de los datos de cliente o los procesen en la forma que sea (almacenar, modificar, transferir, bloquear, borrar).
- Evite el acceso de personas no autorizadas a los soportes de datos, tales como CD/DVD de copia de seguridad o impresos de protocolo. tanto al realizar las tareas de asistencia técnica como en el transporte y en el almacenamiento.
- Elimine por completo los soportes de datos que ya no se necesiten y no deje nunca documentos al alcance de personas no autorizadas.
- Colabore con el cliente: creará así una base de confianza y gozará de mayor credibilidad.

2.3.7 Normas técnicas y conformidad de OpenScape Business X

Aquí encontrará información sobre el cumplimiento de las exigencias establecidas (conformidad) por los sistemas de comunicación OpenScape Business X.

2.3.7.1 Conformidad CE

La certificación de conformidad (marcado) CE se basa en: Directiva sobre baja tensión 2014/35/UE; (Diario Oficial de la UE L96, 29/03/2014, págs. 357-374) Directiva sobre compatibilidad electromagnética 2014/30/UE; (Diario Oficial de la UE L96, 29/03/2014, págs. 79-106) Directiva sobre restricción de uso de ciertas sustancias peligrosas 2011/65/UE; (Diario Oficial de la UE L174, 01/07/2011, págs. 88–110)

	Referencias normativas
Safety	EN 62368-1
Compatibilidad electromagnética CE	EN55032 (EMC Emission) EN55024 (EMC Immunity Residential)

2.3.7.2 Conformidad con normas estadounidenses y canadienses

	Referencias normativas
Seguridad en EE. UU. y Canadá	CSA/UL 62368-1

	Referencias normativas
Compatibilidad de emisiones electromagnéticas EMC Canadá	ICES-003 Apartado 6 Clase B
Compatibilidad de emisiones electromagnéticas EMC EE. UU.	FCC 47 CFR Parte 15 Subparte B Clase B

Número de registro FCC y valor de conexión

En la trasera de la carcasa de los sistemas de comunicación hay una etiqueta con el número de registro FCC, el valor de conexión (Ringer Equivalence Number, REN) y más información. Si se solicita, esta información se puede transferir a la compañía telefónica.

2.3.7.3 Conformidad con las normas internacionales

	Referencias normativas
Safety	IEC 60950-1 and IEC 62368-1
EMC Emission (Emisión CE)	CISPR 32

2.3.8 Condiciones de servicio

Respete las condiciones climáticas y mecánicas para el funcionamiento de los sistemas de comunicación OpenScape Business X y OpenScape Business S y del servidor Business UC Booster Server (servidor de aplicaciones).

2.3.8.1 Condiciones de servicio de OpenScape Business X

Se indican las condiciones climáticas y mecánicas para el servicio de los sistemas de comunicación OpenScape Business X.

Condiciones de servicio climáticas

Margen de servicio límite:

- Temperatura ambiente: + 5 a + 40 °C (41 a 104 °F)
- Humedad absoluta del aire: 1 a 25 g H_2O/m^3
- Humedad relativa del aire: 5 a 80%

La ventilación de los sistemas de comunicación se hace por convección. Con OpenScape Business X5W es obligatorio el uso de ventilación forzada si hay más de 32 interfaces a/b.

Nota: Daños por aumentos locales de temperatura

Evite que los sistemas de comunicación reciban la acción directa de los rayos del sol o que aumente de temperatura por fuentes de calor.

Nota: Daños por condensación de humedad del aire

Evite por todos los medios que durante el funcionamiento se produzca condensación por humedad ambiental sobre o en los sistemas de comunicación.

El sistema de comunicación tiene que estar totalmente seco antes de proceder a la puesta en servicio.

Condiciones de servicio mecánicas

Los sistemas de comunicación se han diseñado básicamente para su uso estacionario.

2.3.8.2 Condiciones de servicio de OpenScape Business S y OpenScape Business UC Booster Server

Puede consultar los datos sobre las condiciones mecánicas y climáticas para el funcionamiento de OpenScape Business S y OpenScape Business UC Booster Server (servidor de aplicaciones) en la documentación del fabricante del PC de servidor y de los demás componentes.

3 Visión general del sistema

OpenScape Business responde a las necesidades de comunicación de las pequeñas y medianas empresas, y lo hace a través de una única solución, versátil y adaptable. La arquitectura de soluciones OpenScape Business permite el empleo independientemente de la infraestructura de telefonía disponible: telefonía clásica por IP o DECT. OpenScape Business proporciona siempre la solución adecuada para cada necesidad, desde su potente telefonía hasta la solución completa e integral de Comunicaciones Unificadas (UC).

Versátil, ampliable y potente

OpenScape Business reúne lo mejor de HiPath 3000 y OpenScape Office en una nueva plataforma de soluciones.

3.1 Aspectos destacados

OpenScape Business es la solución integral para pequeñas y medianas empresas. Ofrece los siguientes aspectos destacados.

Aspectos destacados

- Servicios de voz integrados, gestión de presencia (estado de presencia), conferencia Drag&Drop, buzón de voz visual (Voicemail), puesto de operadora automático (AutoAttendant), Multimedia Contact Center, IM (Instant Messaging, mensajes instantáneos), Mobility, acceso a directorios con conexión de base e datos, fax, integración en procesos de negocio y mucho más
- Clientes de UC personalizables al puesto de trabajo y a la forma de trabajo
- Integración de interfaces de OpenScape Web Collaboration
- Para clientes con una ubicación o como solución a nivel de red con varias ubicaciones
- OpenScape Business ofrece una arquitectura de solución unitaria.
- En función de la infraestructura presente, hay disponibles diferentes modelos OpenScape Business para diferentes tamaños de ampliación. Como alternativa, existe también la opción de operar el software OpenScape Business en un servidor estándar (softswitch) (por supuesto también en entornos totalmente virtualizados).
- La solución de Comunicaciones Unificadas UC Smart está preintegrada en la placa base. La solución de Comunicaciones Unificadas aditiva UC Suite respalda un mayor número de usuarios UC y ofrece un conjunto ampliado de prestaciones de Comunicaciones Unificadas. Para ello se requiere una UC Booster Card o un UC Booster Server.
- Ya se incluyen todas las interfaces de comunicación para todo tipo de requisitos: IP, digital, analógica y DECT y todas las interfaces habituales de línea urbana para la comunicación de voz

3.2 Comunicaciones Unificadas

Unified Communications (UC) es una tecnología para mejorar la comunicación en las empresas e integra diferentes soportes de comunicación en un entorno de aplicaciones unificado. Unified Communications simplifica los procesos de negocio en las empresas mediante una gestión de presencia integral

(p.ej., las llamadas se desvían automáticamente al teléfono móvil si está fuera de casa). Esta solución unificada también unifica el aprovisionamiento de conferencias de acceso telefónico, buzón de voz personal (Voicemail), buzón de faz personal, mensajería instantánea (IM, Instant Messaging), uso del teléfono móvil como extensión del sistema de comunicación, Contact Center, Video y Web Collaboration.

Con el enfoque flexible de Comunicaciones Unificadas de OpenScape Business, se ofrecen diferentes soluciones de UC según los requisitos del puesto de trabajo y de la infraestructura existente. En la solución de UC, seleccione entre UC Smart y UC Suite (UC Smart y UC Suite no se pueden utilizar en paralelo).

La solución UC Smart ya integrada en OpenScape Business se puede migrar en cualquier momento a la solución ampliada UC Suite mediante una licencia de upgrade. Según el número de extensiones UC, hay que ampliar el sistema OpenScape Business con el módulo interno "UC Booster Card" o con el servidor Linux externo "UC Booster Server". Como softswitch puro está disponible OpenScape Business S, como solución de servidor con la UC Smart o la UC Suite.

3.2.1 Funciones de UC (vista general)

En función de la solución de UC seleccionada (UC Smart o UC Suite) tiene a su disposición diferentes funciones de UC.

Las siguientes tablas le ayudarán a optar por una solución de UC adecuada. Encontrará información detallada sobre las condiciones marco en los capítulos correspondientes (UC Smart, UC Suite, Attendants) de la Descripción de prestaciones o la Documentación para el administrador.

Función de UC	**UC Smart**	**UC Suite**			**Notas**
	myPortal to g	**myPortal for Desktop/ Outlook**	**myPortal @w**	**myPortal to g**	
Estado de presencia					
Presencia (gestión de presencia)	x	x	x	x	
Modificación del estado de presencia mediante cliente	x	x	x	x	
Modificación del estado de presencia mediante TUI	-	x	-	-	
Desvío de llamadas basado en el estado	x	x	x	destinos definidos con myPortal	UC Smart permite seleccionar cualquier número como destino. UC Suite solo permite seleccionar un número de la preselección

Función de UC	UC Smart	UC Suite			Notas
	myPortal to g	myPortal for Desktop/ Outlook	myPortal @w	myPortal to g	
Indicación de estado en favoritos	x	x	x	x	
Indicación de estado en los directorios	x	x	x	x	
Indicación de estado en el diario	-	x	-	-	
Activar servicio CallMe	-	x	x	x	
Integración de calendario (Outlook)	-	x	-	-	
Integración de calendario, iCal (solo myPortal for Desktop)	-	x	-	-	
Favoritos					
Indicación del estado de la llamada	x	x	x	x	
Creación de grupos	x	x	-	-	
Indicación compacta de los favoritos	-	x	-	-	
Directorios					
Directorio personal	x	x	x	x	
Directorio interno	x	x	x	x	
Directorio externo	-	x	x	x	
Búsqueda en directorios	x	x	x	x	
Acceso a destinos marcación abrev. (KWZ) definidos en sistema	x	-	x	x	
Importar/Administrar contactos personales (CSV/XML)	-	x	-	-	
Acceso a contactos de Outlook	-	x	-	-	
Importación de contactos personales (Mac OS) (myPortal for Desktop)	-	x	-	-	
Integración del servidor de directorios externos por LDAP	-	x	-	-	
Diario					
Todas las llamadas	x	x	-	x	
Llamadas abiertas	-	x	-	-	
Llamadas perdidas	x	x	-	x	
Llamadas contestadas	x	x	-	x	
Llamadas programadas	-	x	-	-	

Función de UC	UC Smart	UC Suite			Notas
	myPortal to g	myPortal for Desktop/ Outlook	myPortal @w	myPortal to g	
Buzón de voz	x	x	-	x	
Diario de fax	-	x	-	-	
Conversaciones					
Chat	-	-	-	-	
Diario	-	-	x	-	
Buzón de voz	-	-	x	-	
Llamadas					
Marcación manual	x	x	x	x	
Marcación de escritorio (Click to Call)	-	x	-	-	
Desvío	x	x	x	x	
Retener	x	x	x	x	
Grabación de llamadas (Voice Recording)	-	x	-	-	
Enviar un email	x	x	x	x	
Enviar SMS	x	-	-	x	
Enviar un mensaje instantáneo	-	x	-	-	
Popups	-	x	-	-	
Conferencias					
Conferencia AdHoc	x	x	x	x	
Conferencias programadas	-	x	-	-	
Conferencias permanentes y abiertas (conferencia Drag&Drop)	-	x	-	-	
Integración de Web Collaboration	-	x			
Mensajes de voz y de fax					
Buzón de voz (buzón de voz visual)	x	x	x	x	Funciones de mensajería vocal para extensiones (IP, TDM)
Escuchar por teléfono	x	x	x	x	
Escuchar por tarjeta de sonido PC	-	x	-	-	
Cómo enviar un mensaje de voz como electrónico	x	x	-	-	

Función de UC	UC Smart	UC Suite			Notas
	myPortal to g	myPortal for Desktop/ Outlook	myPortal @w	myPortal to g	
Fax	-	x	-	-	
Mensajería instantánea					
Mensajería instantánea (chat)	-	x	-	-	

myPortal to go permite acceder también a los contactos locales del smartphone.

Centro de contactos

Función de UC	UC Smart	UC Suite		Notas
		myAgent	myReports	
Agentes, colas de espera y planes horarios	-	x	-	
Fax y correo electrónico	-	x	-	
Plantillas de informe/ Reports predefinidos	-	x	x	
Creación controlada por tiempo de informes/ reports	-	-	x	

Una opción es conectar el OpenScape Contact Center.

Attendants (puestos de operadora)

Función de UC	UC Smart	UC Suite	Notas
	Business Attendant	myAttendant	
Indicación de las llamadas en espera, con tipo de llamada, nombre y número de llamada	x	x	
Indicación del estado de la conexión	x	x	
Conmutación rápida de llamadas	x	x	
Marcación abreviada por campos de ocupado/botones de usuario. Configuración individual de campos de ocupado/botones de usuario con número de teléfono o nombre	x	x	
Ver el estado de presencia de otras extensiones	x	x	Con OpenStage Business Attendant se requiere UC Booster Card/Server o Business S para la funcionalidad de Presencia

Función de UC	UC Smart	UC Suite	Notas
	Business Attendant	myAttendant	
Modificar el estado de presencia de otras extensiones	x	x	
Directorio personal	-	x	
Directorio interno	x	x	
Directorio externo	x	x	
Contactos Outlook	x	x	
Acceso LDAP	x	x	
Diario	-	x	
Conferencia AdHoc	x	x	
Conferencias planificadas, permanentes y abiertas (conferencia Drag&Drop)	-	x	
Centro de mensajes	-	x	En el Centro de mensajes se administran y registran los mensajes de voz y fax, los mensajes instantáneos, SMS y correos electrónicos.
Acceso a mensajes de voz y de fax de otras extensiones	-	x	Debe activarlo la extensión correspondiente
Mensajería instantánea (chat)	-	x	
Servicio nocturno	x	x	

El cliente de Attendant recomendado para la UC Suite es myAttendant. OpenScape Business Attendant también se puede utilizar con la UC Suite.

Voicemail & Company AutoAttendant

Función de UC	UC Smart	UC Suite	Nota
Funcionalidad básica de Voicemail & Company AutoAttendant de UC Smart	x	-	
Funcionalidad básica de Voicemail & Company AutoAttendant de UC Suite	-	x	Se requiere UC Booster Card/Server o Business S
Prestaciones de UC			
Control gráfico del buzón de voz para extensiones (interfaz web o interfaz de cliente)	x	x	
Anuncios grabados de buzón de voz para función de presencia	x	x	Anuncios grabados diferentes según presencia configurada para UC

Función de UC	UC Smart	UC Suite	Nota
Reglas personales para saludos por cada buzón de voz	-	x	El usuario establece reglas detalladas para seleccionar sus anuncios grabados personales
Buzón de voz a correo electrónico	x	x	El mensaje de voz se añade como archivo adjunto en formato Wave al correo electrónico
Funciones de AutoAttendant			
Buzones de puesto de operadora (Basic AutoAttendants)	100	20	
Company AutoAttendant	x	x	Puesto de operadora central y buzón de voz central con anuncios grabados alternativos según la extensión
Anuncios grabados antes de contestar/ Señalización en paralelo	x	x	Anuncio grabado al llamante mientras se llama a la extensión Con la UC Suite esta función solo está disponible con el Contact Center
Destinos de marcación para 4 secciones de día/Calendario para AutoAttendant	x	x	Conmutación automática variable según la hora La función de calendario con UC Smart disponible mediante servicio nocturno automático
Calendario central para buzón de voz	x	x	Anuncios grabados y tratamiento de llamadas para eventos a nivel de empresa (festivos, vacaciones, etc.).
Perfil individual para buzón y AutoAttendant personal	-	x	Tratamiento de llamadas en función de la presencia, configurable por extensión
Planes horarios	Servicio de día y noche	Plan horario con reglas (Call Control Vector CCV)	
Plantillas	1 AutoAttendant configurado de forma predeterminada	5 plantillas personalizables	
Editor de reglas gráfico (Editor CCV)	-	x	

Función de UC	UC Smart	UC Suite	Nota
Encadenamiento de buzones/ AutoAttendant multipaso	x	-	La llamada se transfiere en cadena de un buzón a otro y siempre se reproduce el anuncio grabado correspondiente
Marcar por nombre (Dial by Name)	-	x	
Marcar por extensión (Dial by Extension)	x	x	
Prestaciones del buzón de voz			
Saludos individuales por buzón de voz	4	10	Guardar y configurar diferentes anuncios grabados
Transferencia de mensajes de voz	-	x	Transferir mensaje a otras extensiones/buzones
Devolución de llamada desde el buzón de voz	x	x	Devolución de llamada al llamante del mensaje activable
Mensaje en espera	-	x	Si hay un mensaje, se llama a un destino externo, p.ej., un móvil
Función de suplente	-	x	Transferencia del llamante al suplente, con anuncio grabado personal
Buzón de voz según llamante/ Encaminamiento CLI	-	x	Tratamiento en función de número de llamada, p.ej. saludo en el idioma del llamante
Buzón de grupo central	x	x	Con anuncios grabados para departamentos/grupos
Grabación de la llamada	-	x	Grabación de llamadas con funciones de seguridad Cuando se usa la grabación de comunicaciones de UC en OpenScape Business S, G.729A no se tiene en cuenta.
Guardar mensajes	-	x	Los usuarios pueden guardar mensajes propios de buzón de voz
Borrado automático de mensajes	x	x	Los mensajes de voz se borran al cabo de un tiempo, para liberar memoria
Cambio de idioma de buzón de voz, personalizado	-	x	Selección de los anuncios grabados automáticos en idioma personalizado

Conceptos relacionados

UC Smart en la página 494

3.2.2 Acceso de usuario a funciones de UC (clientes de UC)

El acceso a las funciones de UC se hace mediante clientes de UC. A Presencia (UC Suite) y Buzón de voz (UC Smart y UC Suite) también se puede acceder con la TUI (interfaz de usuario de telefonía).

Hay disponibles clientes de UC para los sistemas operativos habituales. Para ello, consulte los requisitos de los clientes en las notas de la versión correspondientes.

Clientes de comunicación (clientes de escritorio y groupware)

Cliente	recomendado para		Descripción
	UC Smart	UC Suite	
myPortal @work	x	x	Cliente de escritorio de UC para Microsoft Windows y Mac OS X
myPortal for Desktop	-	x	Clientes de escritorio de UC avanzado para Microsoft Windows y Apple Mac
myPortal for Outlook	-	x	Cliente de groupware de UC para la integración de Microsoft Outlook
OpenScape Desk Phone CP 400/600/600E/ 700/700X/710 HFA (software Cliente a teléfono integrado)	x	x	Control de presencia y acceso al listín para UC Suite y UC Smart

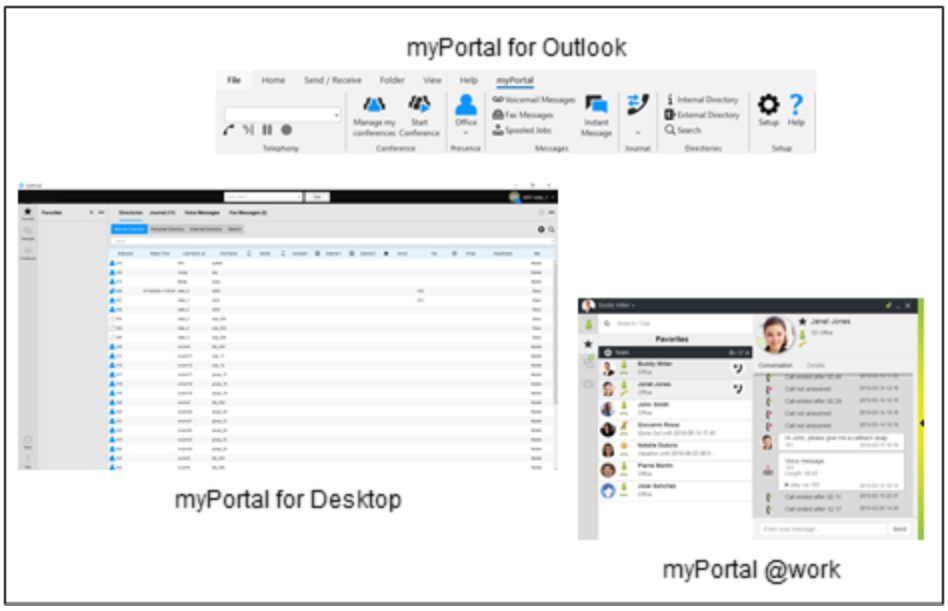


Figura 1: myPortal for Desktop / myPortal for Outlook y myPortal @work

Mobility Clients

Cliente	recomendado para		Descripción
	UC Smart	UC Suite	
myPortal to go	x	x	Aplicación móvil para smartphones y tabletas myPortal to go está disponible con un abanico de funciones solo ligeramente diferente para UC Smart y UC Suite



Figura 2: myPortal to go

Clientes de Contact Center

Cliente	recomendado para		Descripción
	UC Smart	UC Suite	
myAgent	-	x	Cliente de Contact Center
myReports	-	x	Informes/Interfaz de evaluación para Contact Center myReports también se puede utilizar para las estadísticas del sistema, con independencia del Contact Center

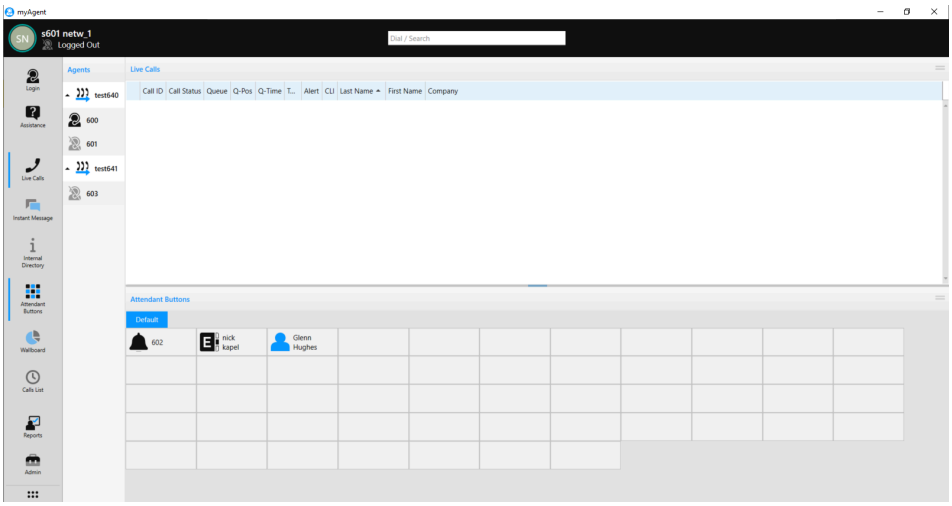


Figura 3: myAgent

Attendants/Puestos de operadora

Cliente	recomendado para		Descripción
	UC Smart	UC Suite	
OpenScape Business Attendant	x	-	Puesto de operadora de UC, con Presencia
myAttendant	-	x	Puesto de operadora de UC avanzado para UC Suite

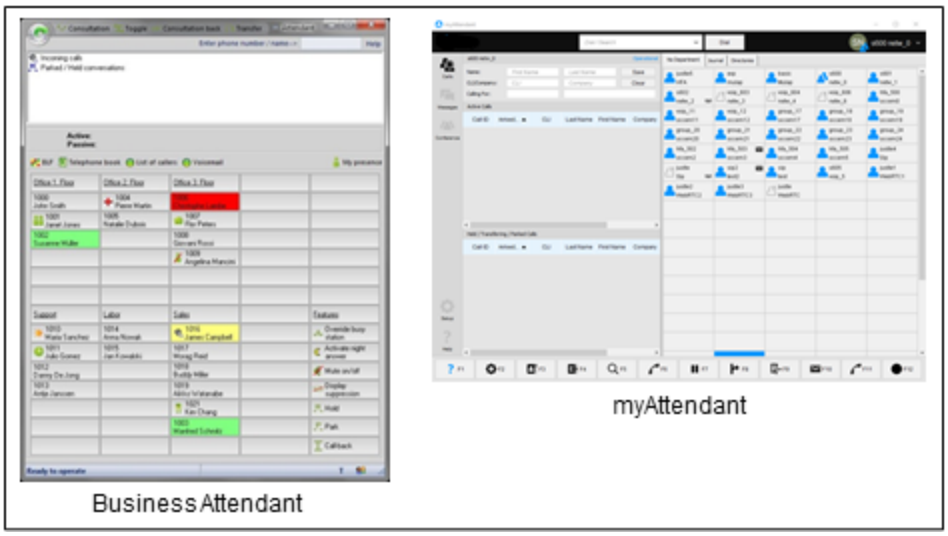


Figura 4: myAttendant

3.2.3 Integración en aplicaciones de negocio

OpenScape Business se puede integrar en las infraestructuras de TI y en las aplicaciones empresariales existentes.

Aplicaciones

- Application Launcher para una interacción activa con aplicaciones CRM/ERP
- Accounting Software para evaluar tarifas

Servicios integrados

- Servicios de directorio (Directory Services) para información sobre llamantes y buscar en directorios internos y externos
- Gestión de presencia y mensajería instantánea (MI) en redes sociales
- Servicios Web (Web Services) para interactuar con aplicaciones basadas en Web, por ejemplo en teléfonos móviles y tabletas

CTI-Middleware

- First- and Third-party TAPI Service Provider para control de llamadas desde aplicaciones CTI o CRM/ERP

Interfaces y protocolos

- CSTA para la supervisión y el control de diferentes aplicaciones
- SIP para la conexión con aplicaciones basadas en tronqueo SIP
- LDAP para la conexión de directorios externos o clientes LDAP externos
- HTTP y HTTPS para el acceso a funciones de UC del servidor Web integrado
- TCP/IP como protocolo básico para todas las conexiones de Ethernet
- Conector SQL para la conexión de bases de datos SQL (Microsoft SQL Server, PostgreSQL, Sybase SQL Server)
- Conector LDAP para servidores LDAP externos, como por ejemplo, Active Directory

3.3 OpenScape Business - Modelos

Para utilizar las funciones de telefonía y de UC se ofrecen diferentes modelos de despliegue. Puede elegir entre modelos de hardware o modelos puros de software que se operen en servidores estándares o en un entorno virtual con VMware vSphere.

Las funciones de Comunicaciones Unificadas para UC Smart ya están integradas en OpenScape Business. UC Suite requiere además el módulo insertable interno "UC Booster Card" o el servidor Linux externo "UC Booster Server". El softswitch OpenScape Business S admite UC Smart o UC Suite de forma opcional.

3.3.1 Niveles de ampliación disponibles a través de Ventas

Los modelos de OpenScape Business tienen diferentes grados de ampliación.

	X1	X3R/X3W	X5R/X5W	X8	S
Conexión al proveedor de servicios					
Canales ITSP (Proveedor SIP)	30	60	60	60	180
Número máximo de proveedores SIP activos	8	8	8	8	8
RDSI S_0 (BRI)	4	20	52	128	-
	por placa base	X3R: 2* STLSX4R X3W: 2* STLSX4	X5R: 6* STLSX4R X5W: 6* STLSX4	Límite de software (en función del número de módulos STDM3)	
RDSI S_{2M} (PRI)	-	30	30	120	-
			1* TS2	3* DIUT3	
Cantidad máxima de canales de línea (ITSP, SIP-Q, SIP nativo, líneas TDM, MEB)	250	250	250	250	250
Extensiones					
RDSI	4	20	52	128	-
	por placa base	X3R: 2* STLSX4R X3W: 2* STLSX4	X5R: 6* STLSX4R X5W: 6* STLSX4	8* STMD3	
Analógico	4	20	52/68	384	-
	por placa base	X3R: 2* SLAV8R X3W: 1* SLAV16	X5R: 6* SLAV8R X5W: 4* SLAV16	16* SLMA	
Digital ($U_{P0/E}$)	8	24	56	384	-
	por placa base	2* SLU8(R)	6* SLU8(R)	16* SLMO2	

	X1	X3R/X3W	X5R/X5W	X8	S
Extensiones IP	20[1]	500	500	500	2000 (máx. 500 extensiones SIP)
Cordless/DECT(CMI)	16	32	32/64	250	-
	1-7 extensiones base mediante placa base	1-7 extensiones base mediante placa base + 8-15 mediante SLUN	1-7 extensiones base mediante placa base + 8-15 mediante SLUN	4* SLMUC	
Núm. máx. extensiones	30[1]	500	500	500	2000
Comunicaciones Unificadas (UC Smart)					
UC Smart VoiceMail (Smart VM)	30	500/320[2]	500/320[2]	500/320[2]	1500
Núm. máx. clientes UC Smart activos simultáneamente (Total de myPortal to go, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF y clientes WSI de terceros)	30	250/50[2]	250/50[2]	250/50[2]	250
OpenScape Business Attendant	8	8	8	8	8
OpenScape Business BLF	30	250	250	250	250
	Máx. 350 teclas BLF	Máx. 350 teclas BLF	Máx. 350 teclas BLF	Máx. 350 teclas BLF	Máx. 350 teclas BLF
Número máximo de extensiones móviles	30	250/50[2]	250/50[2]	250/50[2]	250
Número de usuarios Mobility Entry	30	150	150	150	250
myPortal to go	30	250/50[2]	250/50[2]	250/50[2]	250
myPortal for Teams	-	-	-	-	250
N.º máximo canales para conferencias UC	30	30	30	30	60
Comunicaciones Unificadas (UC Suite)					
VoiceMail de UC Suite	-	500	500	500	1500
Núm. máx. clientes UC Suite activos simultáneamente (Total de myPortal for Desktop, myPortal for Outlook, myAttendant y myAgent)	-	500/150[3]	500/150[3]	500/150[3]	1500

	X1	X3R/X3W	X5R/X5W	X8	S
Núm. máx. otros clientes activos simultáneamente (Total de myPortal to go, myPortal for Teams, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF y clientes WSI de terceros)	-	-	-	-	500
myPortal for Desktop	-	500/150[3]	500/150[3]	500/150[3]	1500
myPortal for Outlook	-	500/150[3]	500/150[3]	500/150[3]	1500
myAttendant	-	20	20	20	20
OpenScape Business Attendant	8	8	8	8	8
OpenScape Business BLF	30	250	250	250	500
	Máx. 350 teclas BLF	Máx. 350 teclas BLF	Máx. 350 teclas BLF	Máx. 350 teclas BLF	Máx. 350 teclas BLF
myAgent	-	192 configurables/64 activas en paralelo	192 configurables/64 activas en paralelo	192 configurables/64 activas en paralelo	192 configurables/64 activas en paralelo
Número máximo de extensiones móviles	-	250/150[3]	250/150[3]	250/150[3]	250
Número de usuarios Mobility Entry	-	150	150	150	250
myPortal to go	-	250/100[3]	250/100[3]	250/100[3]	250
myPortal for Teams	-	-	-	-	250
myReports	-	1	1	1	1
Número máx. canales fax simultáneos	-	8	8	8	8
N.º máximo usuarios de fax	-	500/150[3]	500/150[3]	500/150[3]	1500
N.º máximo canales para conferencias UC	-	20	20	20	60
Comunicaciones Unificadas (CRM, conexión de base de datos)					
Application Launcher	30 configurables/ 30 activas en paralelo	500 configurables/ 50 activas en paralelo	500 configurables/ 50 activas en paralelo	500 configurables/ 50 activas en paralelo	500
Usuarios TAPI 120/170 (mediante CSTA, se requiere UC Booster Server/Card)	-	500/150[3]	500/150[3]	500/150[3]	1500
Usuarios TAPI 120 (en modo UC Smart por placa base sin CSTA)	30	30	30	30	-

	X1	X3R/X3W	X5R/X5W	X8	S
Directory Service Connector (requiere UC Booster Card/ Server)	-	4	4	4	4

Para una descripción detallada de los niveles/límites de ampliación, véase también Límites de configuración y capacidades.

Interconexión de UC de OpenScape Business

OpenScape Business ofrece muy diversas opciones de interconexión de UC:

- Interconexión de voz y UC entre los distintos OpenScape Business X (si se establece una interconexión UC se requiere UC Booster Card/Server) y OpenScape Business S
- Con varios edificios en las instalaciones de la empresa
- Con ubicaciones distribuidas
- Administración central, incluyendo licencias (no se requiere HiPath 5000 RSM)
- Interconexión de voz con OpenScape Enterprise en preparación

En la interconexión de voz se admiten interconexiones con hasta 32 nodos. En una interconexión de UC se admiten interconexiones con máx. 8 nodos y hasta 1000 extensiones (1500 extensiones con OpenScape Business S). Además, se pueden realizar lanzamientos específicos de proyecto.

Para una descripción detallada de los escenarios de interconexión, véase Límites de configuración y capacidades.

3.3.2 Modelos de hardware de UC

Los sistemas de comunicación OpenScape Business X son muy versátiles en cuanto a estructura y prestaciones. Según el modelo de OpenScape Business X se admiten hasta 500 extensiones para IP, digital (RDSI), analógico (a/b) e inalámbrico (Cordless, DECT), así como la conexión con la red pública mediante ITSP (SIP), RDSI (BRI y PRI), CAS, analógico y onboard-IP (preintegrado en la placa base).

- OpenScape Business X1W

  Sistema de comunicación en caja para montaje mural.
- OpenScape Business X1R

  Sistema de comunicación que viene en una carcasa de rack de 19 pulgadas y puede instalarse en un rack de 19 pulgadas, como unidad independiente (operación de escritorio) o montado en la pared.

[1] Número máx. total de usuarios de IP y Deskshare = 20 (limitado por configuración) - Total máx. de extensiones IP, Deskshare, analógicas y digitales = 30 (limitado por licencias)
[2] Primer valor: ampliación máxima con UC Booster Server / Segundo valor: ampliación máxima con placa base o UC Booster Card
[3] Primer valor: ampliación máxima con UC Booster Server / Segundo valor: ampliación máxima con UC Booster Card

- OpenScape Business X3W

  Sistema de comunicación en caja para montaje mural.
- OpenScape Business X3R

  Sistema de comunicación que viene en una carcasa de rack de 19 pulgadas y puede instalarse en un rack de 19 pulgadas, como unidad independiente (operación de escritorio) o montado en la pared.
- OpenScape Business X5 W

  Sistema de comunicación en caja para montaje mural.
- OpenScape Business X5R

  Sistema de comunicación que viene en una carcasa de rack de 19 pulgadas y puede instalarse en un rack de 19 pulgadas, como unidad independiente (operación de escritorio) o montado en la pared.
- OpenScape Business X8

  Sistema de comunicación modular que se puede utilizar como sistema de box único (box base) o de box doble (box base + box de ampliación). El sistema de comunicación se puede montar de forma autónoma o en un armario de 19 pulgadas.



Figura 5: Plataformas de hardware

3.3.3 Hardware UC Booster

UC Booster Hardware para OpenScape Business X.

- Tarjeta OpenScape Business UC Booster

  Placa para OpenScape Business X si UC Suite se va a utilizar como solución UC con hasta 150 usuarios UC.
- OpenScape Business UC Booster Server

  UC Booster Server externo (Linux) para OpenScape Business X si UC Suite se utilizará como solución UC con hasta 500 usuarios UC.

  En el UC Booster Server se utiliza SLES 12 SP5 de 64 bits o SLES 15 SP6 de 64 bits. El UC Booster Server también puede ejecutarse en un entorno virtual con VMware vSphere.

  Cuando se utiliza el UC Booster Server, no es necesaria la tarjeta UC Booster.

- Tarjeta OpenScape Business Voice Channel Booster

  Dos módulos opcionales para la ampliación de OpenScape Business X con canales DSP adicionales (por ejemplo, para conexiones de voz simultáneas con transiciones IP/TDM).

  La placa base incluye ocho canales DSP. La tarjeta Voice Channel Booster Card OCCB/1 proporciona otros 48 canales DSP, y la tarjeta Voice Channel Booster Card OCCB/3 proporciona hasta 128 canales DSP.

3.3.4 Modelos de software de UC (softswitch)

Solución de software UC todo en uno basada en servidor que admite hasta 1000 estaciones IP con conexiones a la red pública mediante ITSP (SIP).

Independientemente de la plataforma utilizada, OpenScape Business S puede instalarse en un servidor Linux. SLES 12 SP5 64 bits o SLES 15 SP6 64 bits, se utilizan como sistemas operativos. OpenScape Business S también puede ejecutarse en un entorno virtual con VMware vSphere. Si se necesitan interfaces TDM para la conexión a teléfonos TDM o troncales TDM, los sistemas OpenScape Business X pueden utilizarse como pasarela.

3.3.5 Estructura y condiciones ambientales

	X1	X1R	X3W	X3R	X5W	X5R	X8
Estructura	Sistema mural	Rack	Sistema mural	Rack	Sistema mural	Rack	Sistema estándar (también se puede montar en rack)
Dimensiones (AlxAnxPr en mm)	470x370x80	450x460x130	450x460x130	89x440x380 (2U)	450x460x200	155x440x380 (3,5U)	490x440x430
Peso	aprox. 2,8 kg	aprox. 6 kg	aprox. 6 kg	aprox. 6 kg	aprox. 8 kg	aprox. 8 kg	aprox. 34 kg (carga completa)
Color de la carcasa	Blanco	Negro	Blanco	Verde/Gris oscuro	Blanco	Verde/Gris oscuro	Verde/Gris oscuro
Fuente de alimentación	De forma predeterminada, los modelos están diseñados para el servicio de red • Tensión de entrada nominal (CA): 100 a 240 V • Frecuencia nominal: 50/60Hz • Alimentación de batería (CC): -48 V						
Consumo de potencia	En función de la plataforma de hardware y de la ampliación						
Condiciones ambientales	• Condiciones operativas: +5 a +40 °C (41 a 104 °F) • Humedad: 5 a 85%						

3.3.6 Teléfonos compatibles

OpenScape Business X permite telefonear mediante IP/HFA (HiPath Feature Access), SIP, TDM, a/b, Cordless/DECT y WLAN. Se pueden conectar teléfonos IP/HFA, SIP e inalámbricos a OpenScape Business S.

Teléfonos OpenStage (IP/ HFA, SIP T))	• OpenStage 5/10/15/20/30/40/60/80
OpenScape Desk Phone (IP/HFA, SIP, and T)	• OpenScape Desk Phone IP 35G/55G/35G Eco • OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA y SIP 200/400/205/405 TDM • OpenScape Desk Phone CP 110/210/410/710 HFA y SIP
Aparatos auxiliares	• Módulos OpenStage Key solo para OpenStage 15/40/60 • OpenStage BLF 40 (campo de lámpara de ocupado), solo para OpenStage 40 y OpenStage 30 T • OpenScape Key Module 400/600, sólo para CP 400/600/600E/700/700X • OpenScape Key Module 410/710, sólo para CP 710
OpenScape Business Cordless	• OpenStage M3 • OpenScape DECT Phone S6/SL6/R6
Clientes de PC (HFA, SIP)	• OpenScape Personal Edition (con SIP incl. vídeo)
Teléfonos SIP (UC Suite) / Adaptador AP	• Teléfonos SIP con compatibilidad de RFC 3725 • Mediatrix 4102 S (para conectar 2 teléfonos analógicos o equipos de fax)
Teléfonos WLAN	• OpenStage WL3 professional • Teléfono OpenScape WLAN WL4/WL4 Plus
Teléfonos analógicos y RDSI	• Teléfonos analógicos (a/b) • Teléfonos RDSI digitales (S_0)

Se admiten dispositivos más antiguos (como optiPoint 410/420/500, Gigaset M2/SL3/S4/SL4/S5 y optiPoint WL2 SIP). No se pueden operar dispositivos Optiset E.

Funciones y configuración de los teléfonos SIP

OpenScape Business ofrece un amplio abanico de funciones para la comunicación de voz para teléfonos OpenStage HFA. Muchas funciones también están disponibles para teléfonos SIP estándares.

Puede consultar una visión general de las prestaciones admitidas por los teléfonos OpenStage SIP y otras indicaciones en la wiki de Unifiy, en el enlace

`http://wiki.unify.com/wiki/Features_and_Configuration_of_SIP_Devices`

Para el control de las conexiones de voz para teléfonos SIP mediante CTI (3PCC), con OpenScape Business X3/X5/X8 se requiere una UC Booster Card o un UC Booster Server.

Para rack OpenScape Business X3/X5, el control de las conexiones de voz para teléfonos SIP mediante clientes UC Smart Clients se respalda con UC Booster Card.

Mediante las funciones DLI, los teléfonos OpenScape Desk Phone (SIP) se pueden administrar de forma centralizada y también reciben aprovisionamiento de software.

Conceptos relacionados

CSTA en la página 1185

3.4 Información adicional

Encontrará más información en Internet y en la extranet. En las notas de versión encontrará información sobre restricciones y cambios recientes.

3.4.1 Idiomas admitidos

Hay disponibles diferentes idiomas para los distintos componentes de software (clientes y WBM) y para la ayuda online y la documentación.

Estos idiomas se ofrecen como parte de la introducción específica de países.

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
Clientes de UC Smart										
myPortal @work (Cliente)	X	X	X	X	X	X	X	-	-	-
myPortal @work (Guía del usuario)	X	X	X	X	X	X	X	-	-	-
myPortal to go (Cliente)	X	X	X	X	X	X	X	X	X	–
myPortal to go (Instrucciones de uso/Ayuda online)	X	X	X	X	X	X	X	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	–	X	–	X
TUI (Instrucciones breves)	X	X	–	–	–	–	–	–	–	–
OpenScape Business Attendant / BLF (cliente)	X	X	–	–	–	X	–	–	–	–
OpenScape Business Attendant / BLF (Instrucciones de uso)	X	X	–	–	–	X	–	–	–	–
Clientes de UC Suite										
myPortal @work (Cliente)	X	X	X	X	X	X	X	-	-	-

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
myPortal @work (Guía del usuario)	X	X	X	X	X	X	X	-	-	-
myPortal for Desktop (Cliente)	X	X	X	X	X	X	X	X	X	X
myPortal for Desktop (Instrucciones de uso/ Ayuda online)	X	X	X	X	X	X	X	–	–	–
myPortal for Outlook (cliente)	X	X	X	X	X	X	X	X	X	X
myPortal for Outlook (Instrucciones de uso/ Ayuda online)	X	X	X	X	X	X	X	–	–	–
myPortal to go (Cliente)	X	X	X	X	X	X	X	X	X	–
myPortal to go (Instrucciones de uso/Ayuda online)	X	X	X	X	X	X	X	–	–	–
myAttendant (Cliente)	X	X	X	X	X	X	X	X	X	X
myAttendant (Instrucciones de uso/Ayuda online)	X	X	X	X	X	X	X	–	–	–
myAgent (Cliente)	X	X	X	X	X	X	X	X	X	X
myAgent (Instrucciones de uso/Ayuda online)	X	X	X	X	X	X	X	–	–	–
myReports (Cliente)	X	X	–	X	X	X	X	–	–	–
myReports (Instrucciones de uso/Ayuda online)	X	X	–	X	X	X	X	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	X	X	X	X
TUI (Instrucciones breves)	X	X	–	–	–	–	–	–	–	–
Administración										
OpenScape Business Assistant (WBM)	X	X	–	–	–	–	–	–	–	–
OpenScape Business Assistant (Documentación para el administrador/Ayuda online)	X	X (sin nl)	–	–	–	–	–	–	–	–
Manager E	X	X	X	X	X	X	X	–	–	–
Manager E (Documentación para el administrador/Online/Ayuda)	X	X	–	–	X	–	–	–	–	–

Además, la TUI de UC Smart está disponible en belga (flamenco) y esloveno.

Consejo: Es necesario disponer del sistema operativo Windows en versión rusa o china para poder utilizar la interfaz de usuario en idioma ruso o chino.

Las abreviaturas utilizadas en la tabla equivalen a los siguientes códigos de idioma (ISO 639-1):

- de = Alemán
- en = Inglés
- cs = Checo
- da = Danés
- es = Español
- fi = Finlandés
- fr = Francés
- hr = Croata
- hu = Húngaro
- it = Italiano
- nl = Holandés
- no = Noruego
- pl = Polaco
- pt = Portugués
- ru = Ruso
- sv = Sueco
- tr = Turco
- zh = Chino

3.4.2 Enlaces de Internet

Encontrará información adicional y más actual en la página web de Unify, en nuestra wiki de expertos y en el portal para socios de Unify.

Enlaces de Internet

- Página web de Unify:

  `http://www.unify.com`
- Wiki para expertos sobre temas de telefonía, sistemas de comunicación y UC:

  `http://wiki.unify.com`
- Portal para socios (se requiere registro):

  `https://www.unify.com/de/partners/partner-portal.aspx`

  o

  `https://www.unify.com/en/partners/partner-portal.aspx`

4 Principio de administración

El sistema de comunicación se administra con el OpenScape Business Assistant.

4.1 OpenScape Business Assistant (Gestión basada en Web, WBM)

El OpenScape Business Assistant está basado en Web y por ello también se denomina Gestión basada en Web (Web Based Management, WBM).

El ámbito de las tareas de administración ofrecidas depende del perfil de administrador que se utilice.

Para cada página de la Gestión basada en Web (WBM) hay disponible una ayuda en línea.

4.1.1 Requisitos para la Gestión basada en Web (WBM)

Para poder utilizar WBM necesita el software adecuado para el PC de administración.

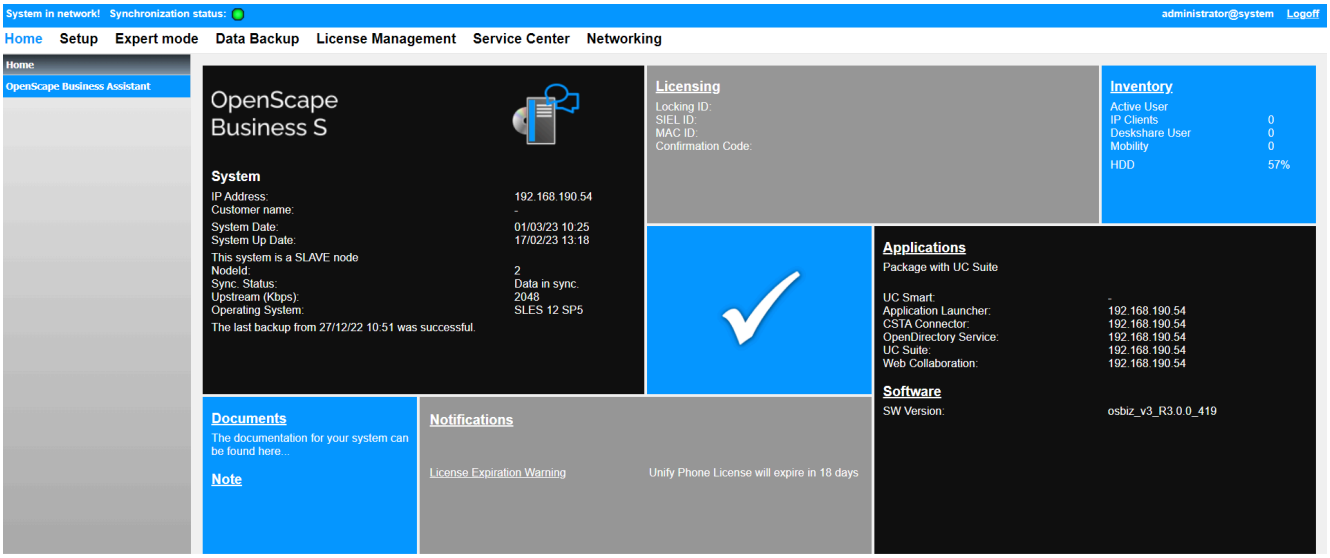
Navegadores Web compatibles:

- Microsoft Internet Explorer 10 o superior
- Microsoft Edge
- Mozilla Firefox 18 o superior
- Google Chrome

4.1.2 Página de inicio de la Gestión basada en Web (WBM)

La página de inicio de la Gestión basada en Web (WBM) muestra información importante del sistema distribuida en diferentes áreas. Además, ofrece indicaciones e información sobre errores del sistema, eventos y acciones.

La información del sistema ofrecida depende del perfil de administrador utilizado. Es posible hacer clic en los títulos subrayados de las distintas áreas, para acceder al tema correspondiente en la Gestión basada en Web (WBM).



Se muestra la siguiente información:

- Área: **Estado** (Centro)
  - Una marca de verificación blanca sobre fondo azul: el sistema de comunicación está operativo. Los mensajes resaltados en rojo en los demás campos indican acciones que se deberían ejecutar.
  - Una marca de exclamación blanca sobre fondo rojo: el sistema de comunicación no está totalmente operativo y el administrador debe realizar alguna acción. Los mensajes resaltados en rojo en los demás campos indican errores del sistema o eventos que hay que corregir.
- Área: **Sistema**
  - Brand
  - Dirección IP del sistema de comunicación
  - Fecha y hora actual
  - Fecha y hora del último reinicio del sistema
  - Indicaciones con servicio en una interred (el sistema es maestro o esclavo, ID de nodo)
  - Estado de sincronización
  - Ancho de banda de carga en kbps
  - Estado de mantenimiento SDHC
  - Notas sobre copia de seguridad y recuperación
  - Estado de Booster Card
- Área: **Documentos**
  - Enlaces a la documentación
- Área: **Notificaciones**
  - Diversas notificaciones sobre el sistema
- Área: **Observación**
  - Muestra la última información introducida por un administrador. Al hacer clic en el título subrayado se abre una ventana de texto en la que aparece toda la información y se pueden introducir otros datos.

    Los datos del campo Nota no están incluidos en el conjunto de copia de seguridad del sistema. En consecuencia, al recuperar un conjunto de copia de seguridad, no se recuperan esos datos.

- Área: **Registro de licencia**
  - ID de bloqueo para el registro de licencia
  - ID SIEL para el registro de licencia
  - Observación sobre el estado de licencia, para indicar si el sistema está en modo de licencia "Permanente" o en modo "Pago por uso".
- Área: **Inventario**
  - Tipo y número de las extensiones activas
  - Número de ITSP activados y un enlace al cuadro de diálogo de estado ITSP, en el Centro de servicios de extensiones activas
- Área: **Aplicaciones** y software

  Aplicaciones:
  - Paquete de aplicación utilizado (UC Smart o UC Suite) y sus componentes, incluidas las direcciones IP de los servidores utilizados.
  - Indicación de si se ha insertado una tarjeta UC Booster Card.

  Software:
  - Versión del software del sistema de comunicación instalado
  - Indicación de si se ha insertado una tarjeta UC Booster Card. Si además se puede acceder a través de una dirección IP, se muestra la versión del software de UC Booster Card instalado.

    La UC Booster Card y el sistema de comunicación siempre deben tener la misma versión de software.
  - Fecha de vencimiento del soporte de software de 3 años.

    Una vez superada la fecha de vencimiento, aparece un mensaje indicando que la licencia de asistencia de software ha caducado y se debe actualizar.
  - Nota sobre la nueva versión de software

4.1.3 Introducción a la Gestión basada en Web (WBM)

La Gestión basada en Web (WBM) es la aplicación basada en Web para la administración del sistema.

Idioma de la interfaz de usuario

Al iniciar sesión puede seleccionar uno de los siguientes idiomas:

- Alemán
- Inglés
- Francés
- Italiano
- Holandés (ayuda online solo disponible en inglés)
- Portugués
- Español

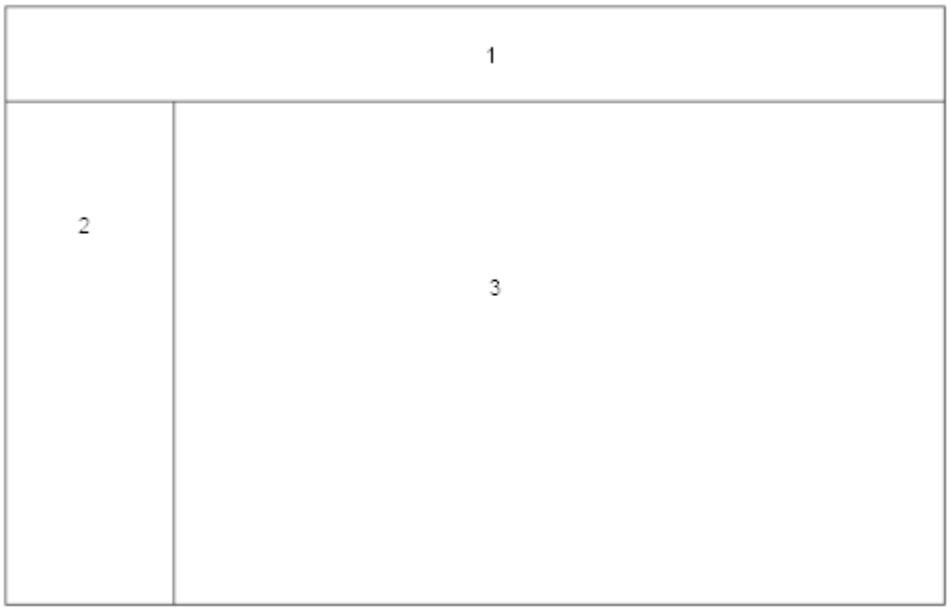
Clasificación de las interfaces de usuario descritas

Todas las tareas que se pueden ejecutar en un asistente solo se describen en el asistente correspondiente.

Las demás tareas que se pueden realizar en el Modo Experto se describen solo para ese modo.

Solo el resto de tareas se describen para el Manager E.

Elementos de la interfaz de usuario



- Barra de navegación (1)

  La navegación es la principal ayuda para la navegación y siempre muestra los mismos enlaces a los principales centros de tareas, es decir, **Inicio**, **Administradores**, **Configuración**, **Modo Experto**, **Copia de seguridad de datos**, **Gestión de licencias**, **Centro de servicio** así como el nombre de usuario actual y el enlace **Cerrar sesión**. Cuando haga clic en uno de los centros de tareas se abrirá en el área de navegación el árbol de navegación correspondiente. En el área de trabajo se abrirá la página de inicio del centro de tareas.
- Área de navegación (2)

  El área de navegación es la navegación secundaria e incluye el árbol de navegación con las opciones de menú del centro de tareas seleccionado. En la parte superior del árbol de navegación aparece el nombre del centro de tareas seleccionado. Bajo este nombre encontrará los grupos y opciones de menú desplegables. Los grupos de menú ofrecen diferentes opciones en función del contexto. Cuando haga clic en una de las opciones de menú aparecerá la página correspondiente en el área de trabajo.
- Área de trabajo (3)

  En el área de trabajo podrá realizar las tareas de administración con todo detalle. Por norma general, el área de trabajo se abre en una ventana independiente. El número y la selección de la información y acciones mostradas depende de la opción de menú seleccionada en el árbol de navegación. En el Modo experto aparece en el área de trabajo a la izquierda del grupo de menús.

Navegación en el grupo de menús

El grupo de menús sirve para navegar en el Modo Experto de la Gestión basada en Web (WBM). El árbol de menú contiene carpetas (p. ej., **Mantenimiento**) con elementos adicionales (p. ej., **Reiniciar / Recargar**).

Para navegar en el grupo de menús, haga clic en la carpeta (alternar entre desplegar y cerrar).

Fin de sesión diferido automático

La sesión se cerrará automáticamente pasados 30 minutos sin actividad. Para seguir trabajando con WBM deberá volver a iniciar sesión. Por motivos de seguridad, haga una pausa y, después, vuelva a cargar la página antes de realizar cambios para que no se pierdan por fin de sesión automático.

4.1.3.1 Cómo iniciar sesión en el WBM

Requisitos previos

Debe tener acceso a sus credenciales de usuario (nombre de usuario y contraseña). En caso contrario, obtenga esta información de su administrador.

TLS 1.2 está habilitado en la configuración de su navegador web.

Paso a paso

1) Abra la página de inicio de sesión en su navegador web ingresando la siguiente dirección: `https://<Dirección IP del sistema de comunicación>`. La dirección IP predeterminada es 192.168.1.2.
2) Haga clic en el código de idioma en la parte superior derecha y seleccione el idioma en el que se mostrará la interfaz de usuario del WBM en el menú. La página de inicio de sesión se mostrará en el idioma seleccionado.
3) Introduzca el nombre de usuario en **Iniciar sesión** en el primer campo. "@system" se agrega automáticamente al salir del campo.
4) Ingrese su contraseña en el segundo campo debajo de **Iniciar sesión**. Tenga en cuenta el uso de mayúsculas y minúsculas y el estado de la tecla **Num**. La contraseña se muestra con asteriscos (*).
5) Haga clic en **Iniciar sesión**.

Si ingresa credenciales no válidas, se mostrará un mensaje después del tercer intento fallido de inicio de sesión, informándole que la cuenta está bloqueada durante 5 minutos. Puede intentar iniciar sesión nuevamente después de este período de tiempo.

Para cualquier intento fallido de inicio de sesión adicional, este período de tiempo se duplica y llega a 160 minutos en el octavo intento fallido. Por cada intento fallido subsiguiente el tiempo de bloqueo de la cuenta es de 160 minutos.

4.1.3.2 Cómo cerrar sesión de la Gestión basada en Web (WBM)

Procedimiento

- En la parte superior derecha, haga clic en **Finalizar sesión**.

4.1.4 Gestión de usuarios de WBM

Puede configurar y administrar hasta 16 administradores para WBM (administración basada en web). A cada administrador se le asigna un perfil que especifica el alcance de su autorización. También puede cambiar la contraseña de un administrador de Manager E.

Los usuarios de WBM también se denominan administradores.

El administrador predeterminado es `administrator@system` con la contraseña predeterminada `administrator` y tiene el perfil **Avanzado**. Esta contraseña debe cambiarse la primera vez que inicie sesión. La contraseña de un administrador debe constar de al menos 8 caracteres y un máximo de 128 caracteres, de los cuales al menos un carácter debe ser un dígito. Además, para una contraseña segura, se debe incluir al menos una letra mayúscula, una letra minúscula y un carácter especial en la contraseña.

Nota: El acceso administrativo (incluido el rol de usuario administrador) se registra en el archivo de registro de mensajes/ syslog. Se puede acceder a través del menú**Rastreo** > **Diagnóstico**.

Perfiles

El WBM admite cuatro perfiles con diferentes clases de servicio (autorizaciones) para administradores con diferentes niveles de experiencia técnica y tareas.

Para evitar que ningún usuario malintencionado pueda iniciar sesión a través de ISDN y cambiar la contraseña predeterminada cuando inicie sesión por primera vez, es obligatorio que el usuario cambie la contraseña a través de Manager E como paso de instalación.

Nota: Una contraseña que consta de 5 caracteres (*****) no será aceptada por el sistema por razones de seguridad.

Tabla 1: Clases de perfil de servicio

Perfil	Clase de servicio
Básico Conocimientos básicos de configuración del sistema	Información del sistema en la página de inicio Asistente de **programación de teclas** Asistente para **agenda telefónica/marcación rápida** Asistente de **grabación de detalles de llamadas** Asistente para **música en espera/anuncios** Asistente para **nombre de estación y liberación** Acceso a **Administradores** (sólo para cambiar sus propias contraseñas) Acceso a **Gestión de licencia** > **Información de licencia** Acceso a **Centro de Servicio** > **Documentos** Acceso a **Centro de Servicio** > **Software**
Mejorado Buen conocimiento de la configuración del sistema	En cuanto al perfil **Básico**, más: Acceso a todos los asistentes (excepto asistentes de **Instalación Básica**, **UC Suite** y **UC Smart**) **Nota:** El acceso a todos los asistentes no es compatible con los sistemas OpenScape Business S. Acceso a **Administradores** (sólo para cambiar sus propias contraseñas) Acceso a **Copia de seguridad y restauración** Acceso a **gestión de licencias** (excluyendo registro, activación de licencias y configuración) Acceso a **Centro de Servicio** > **Inventario** Acceso a **Centro de Servicio** > **Reiniciar / Recargar** (sin recargar) Acceso a **Centro de Servicio** > **Diagnóstico** > **Estado** Acceso a **Centro de servicio** > **Diagnóstico** > **Visor de eventos**
Avanzado Usuarios capacitados	En cuanto al perfil **Mejorado**, más: Acceso a todos los asistentes Acceso a **Administradores** (sólo para cambiar sus propias contraseñas) Acceso a la **Gestión de Licencias** completa Acceso al **Centro de Servicio** completo Acceso a **Redes**

Perfil	Clase de servicio
Experto Técnicos de servicio capacitados	En cuanto al perfil **Avanzado**, más: Acceso a **Administradores** (completo) Acceso a **Modo experto**

Tabla 2: Gestión de perfiles

Perfil	Mantenimiento
Básico Conocimientos básicos de configuración del sistema	Puede cambiar su propia contraseña. No ve ningún otro administrador configurado excepto él mismo.
Mejorado Buen conocimiento de la configuración del sistema	Puede cambiar su propia contraseña. No ve ningún otro administrador configurado excepto él mismo.
Avanzado Usuarios capacitados	Puede cambiar su propia contraseña. No ve ningún otro administrador configurado excepto él mismo.
Experto Técnicos de servicio capacitados	Puede cambiar su propia contraseña y los nombres de usuario y contraseñas de otros administradores. Ve todos los administradores configurados. Puede agregar, editar y eliminar administradores.

Nota: Mientras no exista ningún administrador con el perfil **Experto**, los administradores con el perfil **Avanzado** pueden agregar, editar y eliminar otros administradores. Una vez que exista un administrador con el perfil **Experto**, solo los administradores con el perfil **Experto** podrán agregar, editar y eliminar otros administradores.

Gestión de administradores en la interconexión de redes

La gestión directa de administradores solo es posible en el WBM del nodo maestro. El menú **Administrador** no se muestra en los nodos esclavos. Todas las configuraciones del administrador se transmiten a los nodos esclavos. Sin embargo, es posible llamar al WBM del nodo maestro desde dentro del WBM del nodo esclavo a través de la Vista de nodo. Aquí se muestra el menú del **Administrador**, y solo se pueden mostrar los administradores.

Nota: No es posible agregar, editar o eliminar usuarios a través del acceso WBM en modo esclavo (sino solo a través del acceso WBM en modo maestro).

Administrador de contraseñas E

Un administrador puede cambiar (pero no crear un nuevo rol de usuario) la contraseña de los usuarios existentes que pueden acceder al sistema integrado a través de Manager E.

Se le solicitará al usuario que cambie las contraseñas solo de los usuarios existentes y no podrá cambiar el grupo del usuario y las opciones como Creado, Último uso no serán visibles. Esta es una característica de seguridad y, por lo tanto, no proporciona toda la pantalla de administración de Manager E.

4.1.4.1 Cómo agregar un administrador

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)). (Siempre que no haya ningún administrador con el perfil **Experto**.)

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**. (Si ya hay un administrador con el perfil **Experto**.)

Paso a paso

1) En la barra de navegación, haga clic en **Administradores**.
2) Haga clic en **Agregar...**.
3) Introduzca los siguientes datos: **Nombre de usuario**, **Nombre**, **Apellidos**, **Contraseña**, **Repetir contraseña**.
4) En la lista desplegable **Rol usuario**, seleccione el perfil de usuario deseado.
5) Haga clic en **OK & Continuar**.

4.1.4.2 Cómo editar un administrador

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Administradores**.
2) En la **Lista de administradores**, active la casilla de verificación del administrador deseado.
3) Haga clic en **Editar**.
4) Ajuste los datos (nombre de conexión, nombre y apellidos, contraseña y rol de usuario).
5) Haga clic en **OK & Continuar**.

4.1.4.3 Cómo modificar su propria contraseña de administrador

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Administradores**.
2) En el campo **Contraseña** y en el campo **Repetir contraseña** , introduzca la nueva contraseña.

   Nota: Por motivos de seguridad, el sistema no aceptará contraseñas que consistan en 5 asteriscos (*****).

3) Haga clic en **OK & Continuar**.

Conceptos relacionados

Almacenamiento inmediato en la página 1269

4.1.4.4 Cómo borrar al administrador

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Administradores**.
2) En la **Lista de administradores**, active la casilla de verificación del administrador correspondiente.
3) Haga clic en **Borrar...**.

4.1.4.5 Cómo cambiar una contraseña de administrador de Manager E

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Administradores**.
2) Clic **Lista admin. de Manager E**.
3) Modifique los datos (Identificaciones de usuario, Nueva contraseña o Confirmar contraseña) necesarios.
4) Clic **Guardar**.

   Nota: La contraseña debe tener como mínimo 5 dígitos. No se permite el uso de letras u otros caracteres. Contraseñas antiguas no reutilizab.

4.1.5 Asistentes

Los asistentes permiten instalar y configurar el sistema fácilmente.
Los asistentes permiten instalar y configurar el sistema fácilmente. Los administradores de cliente (perfil **Básico**) tienen a su disposición una parte de los asistentes, mientras que los administradores con conocimientos avanzados

o los técnicos de servicio expertos (perfil **Avanzado**) pueden acceder a todos los asistentes.

Los asistentes disponibles dependen de la configuración del sistema (UC Smart o UC Suite). Los asistentes pueden tener varias páginas consecutivas. Con OK & Continuar se guardan los cambios realizados y se pasa a la página siguiente del asistente. Los cambios que se guarden con OK & Continuar no se pueden descartar. Si no se ha guardado ningún cambio, **Anular** cierra el asistente. Al hacer clic en el símbolo **X** de la esquina superior derecha de la ventana del asistente, se cierra el asistente y se conservan los cambios que se hayan guardado previamente con OK & Continuar.

4.1.5.1 Asistentes – Configuración básica

Los asistentes de **Configuración básica** ayudan a realizar los ajustes de configuración básica fácilmente.

En **Configuración básica** están disponibles los siguientes asistentes:

- **Instalación inicial**

  Uso único en la configuración inicial. Inicialización del país, dirección IP del sistema y servidor DHCP.
- **Configuración básica**

  Configuración básica de sistema con datos de extensión, líneas urbanas, parámetros de red, Internet.
- **Registro de licencia**

  Activar licencias online a través del servidor de licencias.
- **Configuración de red**

  Configuración del sistema como parte de una red.
- **Gestión de energía**

  Configuración y activación de la gestión de energía.

4.1.5.2 Asistentes – Red / Internet

Los asistentes de **Red / Internet** ayudan a configurar la red y el acceso a Internet fácilmente.

En **Red/Internet** están disponibles los siguientes asistentes:

- **Configuración de red**

  Configurar DHCP, encaminamiento IP y servidor DNS.
- **Configuración de Internet**

  Parámetros de acceso para los datos de proveedor de Internet, por ejemplo, identificación de usuario y contraseña.
- **Configuración VPN**

  Conexión de puestos de trabajo a través de Internet.

4.1.5.3 Asistentes – Teléfonos / Suscriptores

Los asistentes bajo **Teléfonos / Suscriptores** apoyan la configuración sencilla de teléfonos y suscriptores.

Los siguientes asistentes están disponibles en **Teléfonos / Suscriptores**:

- **Dispositivos IP**

  Configure teléfonos IP y SIP específicos del sistema, números de llamada de FAX y adaptadores IP/analógicos.
- **Dispositivos UP0**

  Configurar teléfonos UP0, números de llamada de FAX.
- **Teléfonos DECT**

  Configurar números de llamada de FAX y teléfono DECT.
- **Mitel SIP DECT**

  Configuración de dispositivos Mitel SIP DECT RFP.
- **Dispositivos ISDN**

  Puertos ISDN sin alimentación para tarjetas ISDN/módems y estaciones S0.
- **Terminales analógicos**

  Puertos analógicos compatibles con DTMF y CLIP para fax y teléfono.
- **Programación de teclas**

  Programación de teclas de nombre y función para dispositivos IP específicos del sistema y teléfonos UP0.

4.1.5.4 Asistentes – Telefonía central

Los asistentes de **Telefonía central** ayudan a configurar fácilmente las prestaciones de telefonía central.

En **Telefonía central** están disponibles los siguientes asistentes:

- **Línea urbana RDSI / analógico / ITSP**

  Conexión de varios dispositivos (MSN) y número de teléfono del sistema para conexiones RDSI, así como asignación de líneas urbanas y de ITSP.
- **Telefonía Internet**

  Parámetros de acceso del proveedor de servicios de telefonía por Internet (ITSP), por ejemplo, identificación de usuario, contraseña, número de extensión SIP.
- **Listín / Marcación abreviada**

  Configuración de destinos centrales de marcación abreviada para el listín interno del sistema.
- **Grabación de detalles de llamada**

  Configurar los parámetros de conexión para grabación de detalles de llamada para las aplicaciones de detalle de llamadas.
- **Música en espera / Anuncios grabados**

  Grabar nuevas melodías y anuncios grabados para la música en espera y los anuncios previos a la respuesta.

- **Portero eléctrico**

  Configuración de la ubicación de llamada y la autorización de acceso para el terminal de entrada a la conexión de extensión analógica.
- **SmartVM**

  Configuración de un buzón de voz UC Smart (SmartVM).
- **Lista negra para llamadas entrantes**

  Defina una lista de números para bloquear a los llamantes no deseados de forma permanente.
- **Servicio de integración de Active Directory**

  Configure Active Directory.

4.1.5.5 Asistentes – Telefonía de usuario

Los asistentes de **Telefonía de usuario** ayudan a configurar las prestaciones de la telefonía de usuario fácilmente.

En **Telefonía de usuario** están disponibles los siguientes asistentes:

- **Clase de servicio**

  Configurar clases de servicio con los números externos que se pueden asignar a las extensiones, por ejemplo, números de emergencia, números permitidos, números prohibidos y asignación de la clase de servicio para servicio nocturno.
- **Versión y nombre de extensión**

  Editar nombres de grupo y extensión y restablecer código de bloqueo para extensiones individuales.
- **Llamada de grupo / Línea colectiva**

  Configurar llamadas entrantes para grupo de extensiones (orden de llamadas paralelo, lineal o cíclico).
- **Transferencia automática diferida**

  Configuración de asignaciones de números de extensión a nivel de sistema y de forma central, y desvío "diferido" y "en caso de ocupado".
- **Telecaptura de llamadas**

  Configuración de extensiones de un grupo de telecaptura de llamadas con la opción de responder las llamadas del resto.
- **Configuración de equipo**

  Configuración de extensiones que, en el caso de llamadas entrantes, pueden llamar en paralelo a la extensión principal y que, en el caso de una conexión saliente, pueden utilizar su número de teléfono.
- **Integración de teléfono móvil**

  Configuración de una conexión entre un teléfono móvil y una extensión interna en aras de la accesibilidad, en sentido entrante y saliente con un único número de teléfono (servicio de número único).
- **Jefe / Secretaria**

  Configurar en unlace entre uno o más teléfonos de jefe y uno o más teléfonos de secretaria para habilitar las transferencias de llamada simplicadas y las transferencias de timbre.

- **UCD**

  Configurar una distribución de llamadas automática inteligente a un grupo con extensiones seleccionadas.
- **Puesto de operadora**

  Configurar extensiones como números de consola PO y comportamiento de extensión para en caso de ocupado, marcación incorrecta y No contesta.
- **Perfiles de extensión**

  Asignar extensiones a un perfil e importar/exportar datos de perfil.

4.1.5.6 Asistentes – Seguridad

Los asistentes de **Seguridad** ayudan a configurar fácilmente el firewall.

En **Seguridad** están disponibles los siguientes asistentes:

- **Firewall**

  Configurar la apertura de puertos para restringir el tráfico de Internet.

4.1.5.7 Asistentes – UC Smart (solo con UC Smart)

Los asistentes de **UC Smart** ayudan a configurar la solución de Unified Communications UC Smart.

En **UC Smart** están disponibles los siguientes asistentes:

- **UC Smart**

  Configuración básica y configuración de usuarios de UC Smart.

4.1.5.8 Asistentes – UC Suite (solo con UC Suite)

Los asistentes de UC Suite ayudan a configurar la solución de Unified Communications **UC Suite**.

En **UC Suite** están disponibles los siguientes asistentes:

- **Directorio de usuario**

  Configuración de los usuarios.
- **Departamentos**

  Configuración de departamentos.
- **Grupos**

  Configuración de grupos de fax y buzón de voz.
- **Plantillas**

  Configuración de plantillas SMS.
- **Directorio externo**

  Inserción manual de contactos individuales en el directorio externo.
- **Configuración de proveedores externos**

  Entrada de datos de acceso del servidor Exchange o LDAP.

- **Contact Center**

  Configuración de Contact Center.
- **Planes horarios**

  Configuración de los planes horarios.
- **Carga de archivo**

  Carga de archivos de audio para anuncios grabados y música en espera.
- **En conferencia**

  Configuración de conferencias.
- **Perfiles**

  Creación de perfiles de usuario.
- **Encabezados de fax**

  Configuración de encabezados de fax.

4.1.5.9 Asistentes – Directorio Unificado

Los asistentes bajo el **Directorio Unificado** admiten la importación y edición de contactos de directorio.

En **Directorio Unificado** están disponibles los siguientes asistentes:

- **Importar contactos**

  El asistente le guiará por la importación de datos de contacto al Directorio global desde CSV.
- **Editar contactos**

  Añadir o editar manualmente registros de Directorio global.

4.1.5.10 Asistentes - Servicios en la nube

Los asistentes de **Servicios en la nube** admiten la funcionalidad admitida en la nube.

En **Servicios en la nube** están disponibles los siguientes asistentes:

- **Complemento del cliente de Microsoft Teams**

  Configure y descargue el complemento del cliente myPortal for Teams.
- **Conectividad de Unify Phone**

  Configuración de ajustes básicos para Unify Phone.
- **Instancia de usuario de Unify Phone**

  Configurar la instancia de usuarios de Unify Phone
- **Servicio Let's Encrypt**

  Configurar el servicio Let's Encrypt
- **CloudLink Service**

  Configurar CloudLink Service
- **Números piloto de CloudLink**

  Configurar números piloto para CloudLink

4.1.6 Centro de servicios

El **Centro de servicios** de la administración basada en web (WBM) ofrece diferentes funciones de mantenimiento, inicia la actualización de software y proporciona documentación y software.

4.1.6.1 Centro de servicios – Documentos

Documentos ofrece documentos, plantillas CSV y enlaces a información más detallada. Estos documentos se pueden consultar en formato PDF en todos los idiomas compatibles.

Estos son los contenidos disponibles en función de la configuración del sistema:

Contenido	UC Smart	UC Suite
Documentación del administrador (PDF)	-	x
Documentación del usuario (PDF)	-	x
Enlaces (Wiki)	x	x
Plantillas (Plantillas CSV) para importar datos para • Extensiones • Marcación abreviada central • Directorio externo	x	x
CLUF	x	x

Conceptos relacionados

Accounting-Tools en la página 1250

4.1.6.2 Centro de servicios – Software

Software ofrece el software para los clientes de UC, los controladores USB y las herramientas.

Están disponibles los contenidos siguientes:

Contenido	UC Smart	UC Suite
Archivos de instalación para el software de los clientes de UC	x	x
Controladores USB	x	x
Herramientas	x	x
Enlaces para el acceso directo a los archivos de instalación	-	x

4.1.6.3 Centro de servicios – Inventario > Sistema

Sistema ofrece una visión general de los datos de configuración básicos del sistema.

4.1.6.4 Centro de servicios – Inventario > Números de llamada

Números de llamada: lista de números de llamada asignados.

4.1.6.5 Centro de servicios – Inventario > Resumen de red

Resumen de red proporciona una lista con información sobre los sistemas que se encuentran actualmente en la red.

4.1.6.6 Centro de servicios – Actualización de software

Actualización de software comprueba si hay disponible una actualización de software en el servidor Web y realiza la actualización.

4.1.6.7 Centro de servicios – Transferencia de correos electrónicos

Transferencia de correos electrónicos permite el envío de correos electrónicos con mensajes del sistema desde la UC Suite al administrador, y el envío de correos electrónicos con mensajes de fax o de voz anexos a las extensiones.

4.1.6.8 Centro de servicios – Acceso remoto

Acceso remoto permite configurar el acceso para administrar el sistema con independencia de la ubicación.

4.1.6.9 Centro de servicios – Reiniciar / Volver a cargar

Reiniciar/Volver a cargar permite reiniciar el sistema y permite (de forma opcional) restablecer el sistema a la configuración de fábrica.

4.1.6.10 Centro de servicios – Diagnóstico > Estado

Estado ofrece información de estado sobre la red, las extensiones, el establecimiento de conexión, ITSP y VPN.

Véase también Gestión de inventario .

4.1.6.11 Centro de servicios – Diagnóstico > Visor de sucesos

Visor de sucesos registra los sucesos de sistema.

Véase también Traces .

4.1.6.12 Centro de servicios – Diagnóstico > Seguimiento

Seguimiento ofrece opciones para el registro de errores.

Véase también Traces .

4.1.6.13 Centro de servicios – Diagnóstico > Registro de servicio

El Registro de servicio registra varios datos del sistema en forma de evento de HiPath 3000.

Para actualizar o descargar el archivo, debe estar en el modo de vista de la administración basada en web (WBM).

4.1.7 Modo Experto

El Modo Experto ofrece menús con funciones para la configuración y el mantenimiento del sistema para los técnicos de servicio debidamente formados (perfil **Experto**).

Encontrará información detallada en el capítulo Modo Experto.

4.1.8 Ayuda online

La ayuda online integrada describe conceptos importantes e instrucciones de uso. En función del contexto, aparece el tema de ayuda correspondiente a la página de la Gestión basada en Web (WBM) que esté abierta.

Navegación

Los botones de la ayuda online tienen las siguientes funciones:

- **Contenido**

  ofrece una visión general de la estructura
- **Índice**

  permite acceder directamente a un tema a través de palabras clave
- **Buscar**

  le permite realizar una búsqueda de texto completo para localizar con precisión temas relevantes.

4.1.8.1 Cómo acceder a la ayuda online sensible al contexto

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

Procedimiento

- En la ventana abierta de la Gestión basada en Web (WBM), haga clic en el símbolo de la interrogación que aparece arriba a la derecha o en el botón de ayuda abajo a la izquierda.

4.2 Manager E

Manager E es una herramienta de servicio con ayuda integrada en Windows para tareas que no se pueden realizar en la Gestión basada en Web (WBM).

Manager E se puede utilizar para OpenScape Business X1, OpenScape Business X3, OpenScape Business X5 y OpenScape Business X8. OpenScape Business S no se puede administrar con Manager E.

Se recomienda hacer cambios de configuración a través de Manager E solo cuando no pueda realizarlos mediante WBM, por ejemplo, atenuación, pulso de timbre, frecuencia de tono, etc. Los cambios realizados a través de Manager E deben enviarse a través del modo delta.

Manager E está destinado a personal de servicio experto e incluye los siguientes bloques de funciones:

- Creación (también creación sin conexión)
- Copia de seguridad y recuperación de datos del cliente
- Consultas de servicio como, por ejemplo, reinicio de módulos
- Restablecimiento de prestaciones activadas
- Creación e impresión de:
  - Rótulos de teclas para optiPoint 500
  - Listas de datos de cliente
  - Asignaciones de distribuidores principales
- Administración de usuarios y contraseñas para el servicio
- Rutina de conversión para memoria de datos de clientes

El acceso al sistema con el Manager E se realiza con un nombre de usuario y una contraseña propios. Para agilizar los cambios menores, está disponible el modo en línea. Las funciones del modo en línea se corresponden con la interfaz de usuario de Assistant T.

Estas prestaciones ya no se pueden administrar con el Manager E:

- Registro de licencia

- Red
  - Colateral SNMP
  - Colateral PSTN
  - Encaminamiento
  - Mapping
  - Gatekeeper
  - Ext. H.323
  - Puertos IP
- Mantenimiento
  - Historial de errores
  - Protocolo de sucesos
  - Ajustes de Tracer
  - Error Reaction Table
  - Estado de V.24
  - DMA
- Traces

Pasos de trabajo con memoria de datos de cliente (KDS)

El procedimiento de trabajo básico incluye estos pasos:

- Cargar la memoria de datos de cliente (KDS) desde el sistema en el Manager E
- Hacer cambios en Manager E
- Guardar la memoria de datos de cliente (KDS) desde Manager E en el sistema

4.2.1 Cómo cargar la memoria de datos de cliente (KDS) en el Manager E

Siga estos pasos y, a continuación, haga las tareas de configuración en Manager E.

Paso a paso

1) Inicie Manager E en el PC de administración.
2) Introduzca **Nombre de usuario** para el Manager E.
3) Introduzca la **Contraseña** para el Manager E.
4) Haga clic en **Archivo** > **Transferir**.
5) Haga clic en la pestaña **Comunicación**.
6) En el área **Acceso** active la opción correspondiente al tipo de conexión del PC de administración con el sistema.
7) Active la opción **Leer/escribir KDS**.
8) Haga clic en **Instalación -> PC**.
9) Haga clic en **Aceptar**. La memoria de datos de cliente (KDS) se transfiere del sistema al Manager E.
10) Una vez terminada la transferencia, haga clic en **OK**.
11) Haga clic en **Cerrar**.

4.2.2 Cómo guardar la memoria de datos de cliente (KDS) de nuevo en el sistema de comunicación

Siga estos pasos para guardar de nuevo en el sistema las configuraciones realizadas en el Manager E.

Paso a paso

1) Haga clic en **Archivo** > **Transferir**.
2) Haga clic en la pestaña **Comunicación**.
3) En el área **Acceso** active la opción correspondiente al tipo de conexión del PC de administración con el sistema.
4) Active la opción **Leer/escribir KDS**.
5) Haga clic en **PC -> Sistema**.
6) Haga clic en **Aceptar**. La memoria de datos de cliente (KDS) se transfiere desde el Manager E al sistema.
7) Una vez terminada la transferencia, haga clic en **OK**.
8) Haga clic en **Cerrar**.

5 Configuración inicial de OpenScape Business X

Este capítulo describe la configuración inicial de OpenScape Business X1/X3/X5/X8. El sistema de comunicación y sus componentes están integrados en una infraestructura existente que consta de una LAN del cliente y una red de telefonía TDM. El acceso a Internet y la conexión troncal están configurados y las estaciones conectadas están configuradas.

La configuración inicial de OpenScape Business X1/X3/X5/X8 (es decir, el sistema de comunicación) se lleva a cabo utilizando el programa de administración OpenScape Business Assistant (gestión basada en web, también llamada WBM).

Aquí se describe la configuración inicial estándar de los componentes de uso común. Los pasos específicos de instalación dependen del sistema de comunicación y de los componentes involucrados (por ejemplo, la tarjeta UC Booster). Durante la configuración inicial, es posible que en algunos lugares deba elegir entre varias opciones o incluso omitir algunas configuraciones por completo. También es posible que los pasos de instalación descritos aquí no aparezcan en su sistema de comunicación.

Las configuraciones detalladas de las funciones no incluidas en la configuración inicial estándar se describen en los capítulos siguientes.

Para realizar la puesta en servicio inicial hay que crear un esquema de direcciones IP y un plan de numeración.

Los pasos más importantes para la instalación son los siguientes:

- Direcciones IP y configuración DHCP
- Configuración de país y hora
- Números de teléfono del sistema e interconexión
- Configuración ISDN
- Acceso a Internet
- Telefonía por Internet
- Configuración de extensiones
- Registro de licencia
- Endurecimiento del sistema
- Almacenamiento de datos

Directrices para aumentar el rango de subredes, para evitar posibles configuraciones erróneas

Entre las consideraciones clave que debe tener en cuenta antes de proceder con dichos cambios se incluyen:

Asegurar que ciertas redes no se superpongan con otras redes del sistema. Específicamente:

- Red DSP
- Red LAN1 (WAN)
- Red LAN2
- Red LAN3 (Administración)

Además, también debe asegurarse de que no haya conflictos con la dirección IP de la puerta de enlace predeterminada y, si se utiliza una tarjeta Booster, la interfaz LAN2 del sistema debe estar en la misma subred que la interfaz LAN2 de la tarjeta Booster.

5.1 Requisitos para la instalación inicial

Si se cumplen los requisitos para la instalación inicial, el sistema de comunicación funcionará correctamente.

General

Según el hardware utilizado (módulos, teléfonos, etc.) y la infraestructura, se aplican los siguientes requisitos generales:

- La infraestructura (LAN, red de telefonía TDM) está disponible y se puede utilizar.
- El hardware se ha montado y conectado correctamente.
- Para la integración de la placa base y la tarjeta UC Booster Card en la LAN de clientes, se requiere un puerto de LAN.
- El sistema de comunicación todavía no está conectado con la LAN.
- Si se utiliza la tarjeta UC Booster Card, hay que insertarla antes de la instalación inicial.
- Hay disponible acceso a Internet con un ITSP (Proveedor de servicios de Internet).
- Para usar un acceso de línea urbana RDSI, se requiere una conexión múltiplex primaria RDSI o S_0.
- Para usar un acceso de línea urbana CAS, se requiere una conexión de línea urbana CAS.
- Para usar un acceso de línea urbana analógico, se requiere una conexión urbana analógica.
- Hay disponible, y se conoce, un esquema de direcciones IP (véase Esquema de direcciones IP).
- Hay disponible, y se conoce, un plan de numeración (véase Plan de numeración).

PC de administración

El PC de administración (Admin-PC) con el que se ejecuta la instalación inicial y la posterior administración del sistema de comunicación debe cumplir estos requisitos:

- Interfaz de red:

  El PC de administración requiere un puerto de LAN libre.
- Sistema operativo:

  Si la configuración del sistema de comunicación se va a realizar con Manager E, se requiere un sistema operativo Windows (Windows XP y versiones posteriores).

  Por su parte, la configuración con Gestión basada en Web (WBM) se basa en navegador; por lo tanto, no depende de la plataforma.

- Navegador Web:

  Son compatibles estos navegadores Web:

  – Microsoft Internet Explorer a partir de la versión 10.
  – Microsoft Edge
  – Mozilla Firefox a partir de la versión 17.
  – Google Chrome

  Si hay instalada una versión anterior del navegador Web, deberá actualizarse para poder comenzar con la puesta en servicio.
- Java:

  Debe estar instalado Oracle Java 8 o superior, o bien OpenJDK 8. Si hay instalada una versión anterior, hay que actualizar a la versión más reciente para poder comenzar con la puesta en servicio.

5.2 Componentes

A continuación se describen y resumen los componentes del ejemplo de instalación.

El ejemplo de instalación incluye estos componentes:

- OpenScape Business X

  El sistema de comunicación se integra en la LAN de clientes existente mediante la interfaz LAN
- PC de administración

  El PC de administración también se conecta con el sistema de comunicación a través de una interfaz LAN.
- Extensiones IP (Clientes IP)

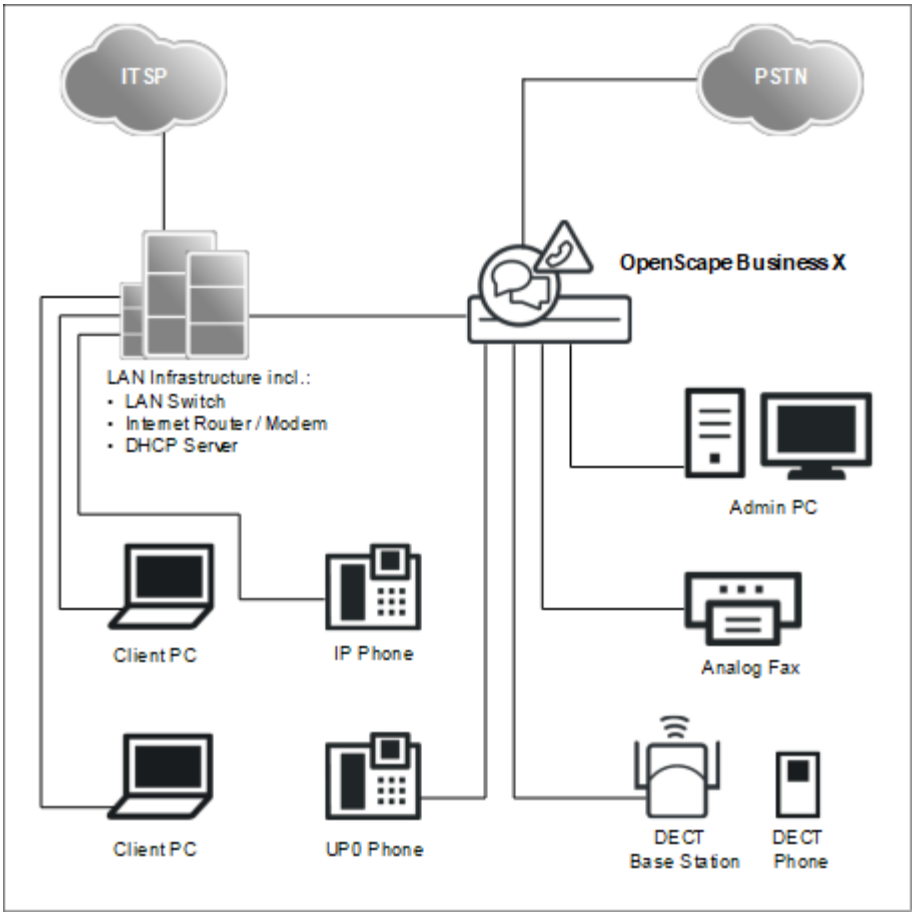
  Las extensiones IP (teléfonos IP del sistema, PC de cliente, puntos de acceso WLAN...) se integran en la LAN a través de uno o varios conmutadores.
- Extensiones UP0

  Las extensiones UP0 (p. ej., teléfono del sistema TDM OpenStage 60T) se conectan directamente con el sistema de comunicación.
- Extensiones analógicas

  Las extensiones analógicas (p. ej., fax analógico) se conectan directamente con el sistema de comunicación.
- Extensiones DECT

  Las extensiones DECT se registran en el sistema de comunicación a través de la extensión base.

Un servidor DHCP interno o externo (p. ej., router Internet) asigna las direcciones IP dinámicamente a los clientes IP.



5.3 Plan de numeración

Un plan de numeración es una lista de todos los números de teléfono disponibles en el sistema de comunicación. Incluye, entre otras cosas, números de teléfono internos, números de marcación directa y números de llamada de grupo.

Plan de numeración estándar

Los números de teléfono internos tienen preasignados valores estándar. Si es necesario, puede ajustar estos valores a sus necesidades (plan de numeración individual).

Extracto del plan de numeración estándar:

Tipo de los números de teléfono	**X1**	X3/X5/X8
Números de teléfono de extensión internos	11-30	100-742
Números de marcación directa de extensión	11-30	100-742
Números de teléfono de línea	700-703	desde 7801

Tipo de los números de teléfono	**X1**	X3/X5/X8
Códigos de ruta (códigos externos): Ruta 1 (línea urbana RDSI, analógica) Ruta 8 (UC Suite) Ruta 12-15 (línea urbana, ITSP) Ruta 16 (interconexión)	 0 = Mundial / 9 = EE. UU. - sin preasignar sin preasignar	 0 = Mundial / 9 = EE. UU. 851 855-858 859
Número de teléfono para el acceso remoto	sin preasignar	sin preasignar
Número de teléfono para mensajes de voz UC Smart UC Suite	351 -	351 sin preasignar

Plan de numeración individual

Se puede importar un plan de numeración individual durante la configuración básica a través de un archivo XML.

El archivo XML incluye varios pestañas. La pestaña "Cliente" incluye además del nombre y del número de teléfono de la extensión otros datos como, por ejemplo, los tipos de extensiones y las direcciones de correo electrónico.

Puede consultar un ejemplo de archivo XML con la correspondiente explicación en la Gestión basada en Web (WBM), en **Centro de servicios** > **Documentos** > **Plantillas CSV**. El archivo XML ahí guardado también se puede utilizar como plantilla para sus datos. Se puede editar, por ejemplo, con Microsoft Excel.

5.4 Esquema de direcciones IP

Un esquema de direcciones IP define cómo se asignan las direcciones IP de la LAN de clientes. Incluye las direcciones IP de PC, servidores, routers Internet, teléfonos IP, etc.

Para conseguir una mejor visión general en la asignación de direcciones IP, es conveniente crear un esquema de direcciones IP.

Ejemplo de un esquema de direcciones IP con un área de direcciones IP `192.168.1." -x`:

Área direcc. IP	**Clientes**
192.168.1.1 a **192.168.1.19**	Clientes con dirección IP fija:
192.168.1.1	Router interno (Gateway)
192.168.1.2	Sistema de comunicación
192.168.1.3	Tablero de aplicaciones (opcional)
192.168.1.10	Servidor de correo electrónico

Área direcc. IP	Clientes
192.168.1.50 a **192.168.1.254**	Clientes de PC y teléfonos IP, al mismo tiempo rango de dirección IP del servidor DHCP, la asignación de las direcciones IP a los clientes se realiza dinámicamente

Los siguientes rangos de direcciones IP están reservados de forma interna y no se pueden asignar:

Rangos de direcciones IP excluidos	Descripción
10.0.0.1; 10.0.0.2	reservados para el servidor de licencias
10.186.237.65; 10.186.237.66	Reservados para RDSI remota (obsoleto)
192.168.3.2	Dirección IP interna del sistema de comunicación
192.168.2.1	Dirección IP de la interfaz LAN3 (puerto de administración)

Esta lista también se puede encontrar en el WBM en **Centro de servicios** > **Diagnóstico** > **Estado** > **Resumen de direcciones IP**.

Ampliación de la máscara de red al utilizar el segmento de red predefinido

La dirección IP interna del sistema de comunicación y la dirección IP de la interfaz LAN3 (puerto de administración) no pueden estar en el mismo segmento de red que la dirección IP del sistema de comunicación.

Configuración del segmento de red predefinido:

- 192.168.1.2: Dirección IP del sistema de comunicación
- 255.255.255.0: Másc. red
- 192.168.3.2: Dirección IP interna del sistema de comunicación
- 192.168.2.1: Dirección IP de la interfaz LAN3 (puerto de administración)

Si al utilizar el segmento de red predefinido, la máscara de red se amplía de 255.255.255.0 a 255.255.0.0, por ejemplo, hay que modificar las direcciones IP señaladas arriba:

Ejemplo de configuración modificada:

- 192.168.1.2: Dirección IP del sistema de comunicación
- 255.255.**0**.0: Másc. red
- 192.**169**.3.2: Dirección IP interna del sistema de comunicación

  El cambio se realiza a través de **Modo experto** > **Telefonía** > **Payload** > **Módulos hardware** > **Editar ajustes DSP**
- 192.**170**.2.1: Dirección IP de la interfaz LAN3 (puerto de administración)

  El cambio se realiza a través de **Modo experto** > **Telefonía** > **Interfaces de red** > **Placa base** > **LAN 3 (Admin)**

5.5 Puesta en servicio inicial

La puesta en servicio inicial incluye el inicio del sistema de comunicación, la conexión y configuración del PC de administración y el primer arranque del programa de administración OpenScape Business Assistant (Gestión basada en Web, WBM).

Hay que realizar la puesta en servicio inicial del sistema de comunicación antes de integrar el sistema de comunicación en la LAN interna. Pueden darse problemas si la dirección IP preconfigurada del sistema de comunicación ya está presente en la LAN interna o si se ya utiliza un servidor DHCP. Para estos casos, hay que cambiar primero la configuración de la dirección IP del sistema de comunicación o desactivar el servidor DHCP del sistema de comunicación. Solo entonces se puede integrar el sistema de comunicación en la LAN interna.

Nota: Antes de la puesta en servicio inicial hay que observar las indicaciones sobre protección y seguridad de los datos.

PELIGRO: El OpenScape Business X8 solo se puede encender si la parte trasera de todos los armarios del sistema está cerrada con los paneles de conexiones y ciegos previstos para ello.

PELIGRO: El OpenScape Business X3R/X5R solo se puede encender si la parte delantera de la caja está cerrada. Los slots no equipados con módulos deberán cubrirse siempre con placas de protección (C39165-A7027-B115).

PELIGRO: El OpenScape Business X1W/X3W/X5W solo se puede encender si la carcasa está cerrada.

Conexión del PC de administración

Para configurar el sistema de comunicación, el PC de administración se conecta directamente con la interfaz LAN "LAN" del sistema de comunicación y se configura de forma que obtenga su dirección IP del servidor DHCP interno del sistema de comunicación. Después de finalizar la instalación, el PC de administración se puede integrar en la LAN interna sin necesidad de más cambios de configuración.

5.5.1 Cómo iniciar el sistema de comunicación

Requisitos previos

El montaje del hardware se ha realizado correctamente (véase *OpenScape Business, Instrucciones de instalación*).

La tarjeta de memoria (con el software del sistema) está insertada.

El sistema de comunicación no está integrado en la LAN de clientes.

Paso a paso

Conecte el sistema de comunicación con la alimentación eléctrica.



Atención:

Descarga eléctrica al tocar los cables con tensión

Asegúrese de que el sistema de comunicación (y con OpenScape Business X8 también cada armario del sistema) está conectado a tierra con un conductor de protección de tierra independiente (véase *OpenScape Business, Instrucciones de instalación*).

El sistema de comunicación arranca. En el proceso, los LED del sistema se encienden con distintos colores y secuencias (véase *OpenScape Business, Instrucciones de instalación*). Durante el encendido, no se puede desconectar la corriente del sistema de comunicación.

Una vez finalizado el arranque del sistema, el LED "Run" de la placa base parpadea en verde a intervalos de 1 Hz (0,5 s encendido/0,5 s apagado).

5.5.2 Cómo conectar el PC de administración con el sistema de comunicación

Requisitos previos

El sistema de comunicación está operativo.

Paso a paso

1) Arranque el PC de administración.
2) Compruebe si se puede asignar al PC una dirección IP dinámica. Si no es así, deberá cambiar la configuración del PC de administración. Para hacerlo necesita derechos de administrador.

   Nota: Los ajustes IP que se describen aquí son válidos para Windows 7. Si desea información más detallada sobre la configuración en otros sistemas operativos Windows, consulte las instrucciones del correspondiente sistema operativo.

   a) Seleccione **Inicio** > **Panel de control**, haga doble clic en **Redes e Internet** y, a continuación, haga clic en **Centro de redes y recursos compartidos**.
   b) En la red activa pertinente, haga clic en**Conexión de área local** y, a continuación, en **Propiedades**.
   c) En la pestaña **Funciones de red** haga clic con el botón izquierdo del ratón en la entrada **Protocolo de Internet versión 4 (TCP/IPv4)** y haga clic en **Propiedades**.
   d) Haga clic en la pestaña **General** y compruebe si el campo de opción **Obtener dirección IP automáticamente** está activado. Si la opción no está activada, hágalo.
   e) Cierre todas las ventanas abiertas pulsando **Aceptar**.

3) Con un cable LAN, conecte la interfaz LAN del PC de administración que acaba de configurar con la interfaz LAN "LAN" del sistema de comunicación. Con esta interfaz se asigna una dirección IP dinámica al PC de administración.

Nota: El PC de administración también se puede conectar con la interfaz LAN "Admin". No obstante, si se hace así, hay que asignarle una dirección IP fija del rango comprendido entre la dirección 192.168.2.xxx (por ejemplo, 192.168.2.40) y la máscara de red 255.255.255.0. El sistema de comunicación tiene la dirección IP 192.168.2.1 a través de la interfaz LAN "Admin" (muy importante para el acceso de WBM).

5.5.3 Cómo iniciar WBM

Requisitos previos

El sistema de comunicación está operativo. El LED "Run" de la placa base parpadea en verde a intervalos de 1 Hz 0,5 s encendido/ 0,5 s apagado).

El PC de administración y el sistema de comunicación se pueden comunicar entre sí a través de la LAN.

Paso a paso

1) En el PC de administración, inicie el navegador Web y abra la página de registro de OpenScape Business Assistant (WBM) con esta dirección:

```
https://192.168.1.2
```

Nota: Si no consigue iniciar Gestión basada en Web (WBM), compruebe la conexión LAN y vuelva a intentarlo. Si no diera resultados, compruebe si la dirección IP está bloqueada por la configuración del firewall interno de su PC. Encontrará información más detallada en la documentación de su firewall.

---

2) Si el navegador Web notifica un problema con un certificado de seguridad, instale el certificado (en el ejemplo se utiliza Internet Explorer V10).

a) Cierre el navegador Web.

b) Abra el navegador Web con derechos de administrador. Para ello, haga clic con el botón secundario del ratón en el símbolo del navegador

Web y en el menú contextual seleccione la entrada **Ejecutar como administrador**.

c) Autorice el control de cuentas de usuario.

d) Abra la página de registro del OpenScape Business Assistant (Gestión basada en Web, WBM) en la siguiente dirección:

`https://192.168.1.2`

e) Haga clic en **Continuar cargando este sitio Web**.

f) Haga clic en el mensaje **Error de certificado** en la barra de navegación del navegador Web.

g) Haga clic en **Mostrar certificados**.

h) Haga clic en **Instalar certificado** (solo visible con derechos de administrador).

i) Seleccione la opción **Ordenador local** y confirme la acción con **Continuar**.

j) Seleccione la opción **Colocar todos los certificados en el siguiente almacén**, haga clic en **Examinar** e introduzca **Entidades emisoras raíz de confianza**.

k) Confirme con **Aceptar** y, a continuación, con **Continuar** y **Finalizar**.

l) Confirme el certificado de importación con **Aceptar** y cierre la ventana del certificado con **Aceptar**.

m) Cierre el navegador Web.

n) Inicie de nuevo el navegador Web (sin derechos de administrador) y abra la página de registro de OpenScape Business Assistant (Gestión basada en Web, WBM) en la siguiente dirección:

`https://192.168.1.2`

3) Arriba a la derecha, haga clic en la abreviatura de idioma y en el menú seleccione el idioma para visualizar la interfaz de la Gestión basada en Web (WBM). La página de registro aparece en el idioma seleccionado.

4) En el primer campo en **Inicio de sesión**, introduzca el nombre de usuario estándar `administrador@sistema` para acceder como administrador.

Nota: Si después de introducir `Administrador` pasa al campo **Contraseña**, `@system` se añade automáticamente.

---

5) En el segundo campo en **Inicio de sesión**, indique la contraseña estándar `administrator` para acceder como administrador.

6) Haga clic en **Inicio de sesión**.

7) Estos pasos solo son necesarios una vez, al iniciar sesión por primera vez en la Gestión basada en Web (WBM):

a) En el campo **Contraseña**, vuelva a introducir la contraseña estándar `administrator`.

b) En los campos **Nueva contraseña** y **Confirmar nueva contraseña**, introduzca una nueva contraseña para proteger el sistema contra el uso indebido. Esta opción distingue entre mayúsculas y minúsculas;

compruebe también las teclas `Num` y `BloqMayús` (tecla de ajuste fijo). La contraseña aparece oculta con asteriscos (*).

> **Nota:** La contraseña debe tener una extensión mínima de 8 caracteres e incluir una cifra. Recuerde exactamente cuál es esa contraseña.

c) Haga clic en **Inicio de sesión**.
d) Seleccione la fecha actual e introduzca la hora correctamente.
e) Haga clic en **OK & Continuar**. La sesión de Gestión basada en Web (WBM) finaliza automáticamente.
f) En el primer campo en **Inicio de sesión**, introduzca el nombre de usuario estándar `administrador@sistema` para acceder como administrador.

> **Nota:** Si después de introducir `Administrador` pasa al campo **Contraseña**, `@system` se añade automáticamente.

g) En el segundo campo en **Inicio de sesión** introduzca la contraseña que acaba de definir para acceder como administrador.
h) Haga clic en **Inicio de sesión**. Se abre la página de inicio de la Gestión basada en Web (WBM).

Pasos siguientes

Iniciar la instalación inicial.

5.6 Integración en la LAN de clientes

La integración en la LAN de clientes se realiza con el asistente **Instalación inicial** de la Gestión basada en Web (WBM). Con ello se definen los ajustes básicos para integrar el sistema de comunicación en la LAN existente.

5.6.1 Cómo iniciar el asistente de instalación inicial

Requisitos previos

Se ha iniciado la Gestión basada en Web.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) Haga clic en **Editar** para iniciar el asistente **Instalación inicial**.

> **Nota:** Si el tamaño de la ventana del navegador no puede mostrar el área de trabajo completa a bajas resoluciones de pantalla, aparecerá a los lados una barra de deslizamiento horizontal o vertical para desplazarse hasta la sección deseada.

Pasos siguientes

Realice la instalación inicial tal y como se describe a continuación, paso a paso. Los campos que no se describen aquí están preestablecidos de acuerdo al caso estándar y solo hay que modificarlos cuando no coincidan con sus datos de red. Encontrará información detallada en la descripción de los distintos asistentes de la documentación del administrador.

5.6.2 Configuración de sistema

En la ventana **Configuración de sistema**, configure los ajustes del sistema de comunicación.

Para ello, siga este procedimiento:

1) Defina el logotipo en pantalla y la denominación de producto

   Puede definir un texto que se mostrará en el display de los teléfonos el sistema. También puede seleccionar la denominación de producto.
2) Definir direcciones IP (en caso necesario)

   El sistema de comunicación tiene asignada de forma predeterminada una dirección IP y una máscara de subred. En algunos casos hay que ajustar la dirección IP o la máscara de subred al área de direcciones IP propia.

   Además, puede indicar la dirección IP de su router estándar, por ejemplo, la dirección IP del router Internet.

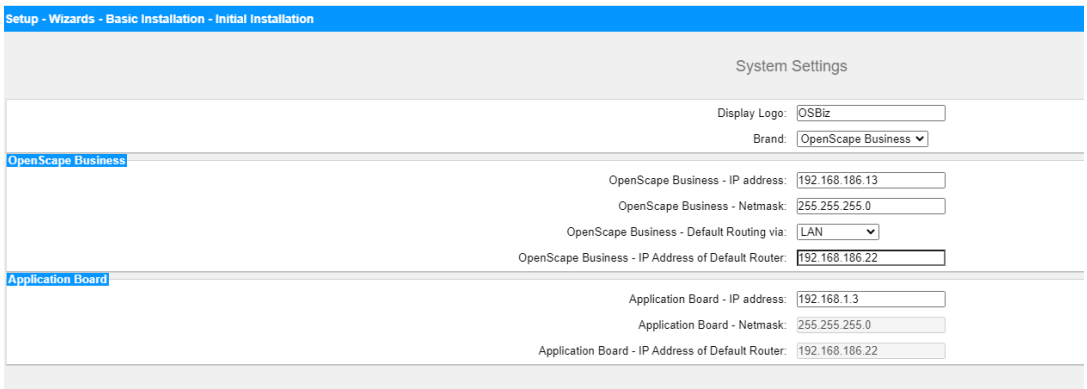
   El tablero de aplicaciones (UC Booster Card) también requiere una dirección IP. Esté montado o no, puede asignar una dirección IP de su área de direcciones IP.

Si desea ampliar la máscara de red (p.ej., de 255.255.**255**.0 a 255.255.**0**.0), hay que modificar la dirección IP interna del sistema de comunicación y la dirección IP de la interfaz LAN3 (puerto de administración), ya que no pueden estar en el mismo segmento de red que la dirección IP de los sistemas de comunicación (véase también Esquema de direcciones IP).

5.6.2.1 Cómo definir el logotipo de pantalla y la designación de producto

Requisitos previos

Se encuentra en la ventana **Configuración de sistema**.



Paso a paso

1) En el campo **Mostrar logotipo** introduzca el texto que usted elija (p. ej. OpenScape Biz). El texto puede tener como máximo 16 caracteres. Evite el uso de diéresis y caracteres especiales.
2) En la lista desplegable **Producto**, seleccione la denominación del producto.

Pasos siguientes

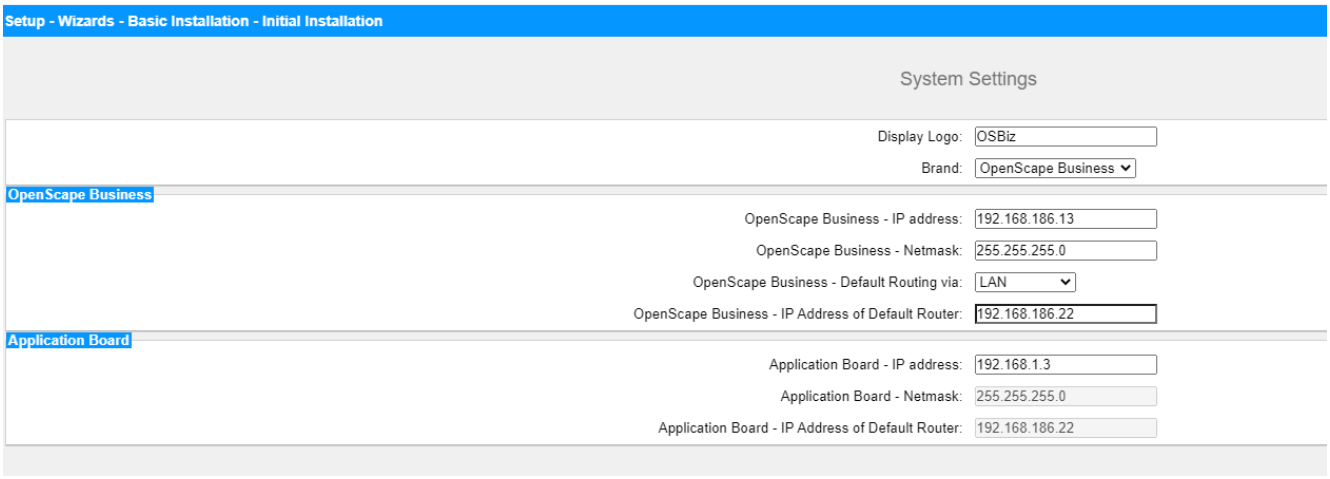
Modifique las direcciones IP (si es necesario) o configure DHCP.

5.6.2.2 Cómo definir las direcciones IP (opcional)

Requisitos previos

Conoce el área de direcciones IP de su red interna.

Se encuentra en la ventana **Configuración de sistema**.



Paso a paso

1) Definir la dirección IP del sistema de comunicación:
   a) En el campo **OpenScape Business - Dirección IP**, introduzca una dirección IP que se encuentre dentro del área de direcciones IP de su red interna (por ejemplo, red interna: `192.168.1.x`, OpenScape Business: `192.168.1.2`.

      Nota: La dirección IP de OpenScape Business no puede estar asignada a un cliente de red ya que, de lo contrario, se producirá un conflicto de direcciones IP.

   b) Introduzca la máscara de subred de su red interna (por ejemplo, `255.255.255.0`) en el campo **OpenScape Business - Máscara de subred**.
2) Definir la dirección IP del router predeterminado:
   a) En el campo **OpenScape Business - Enrutamiento por defecto a través de**, seleccione la entrada **LAN**.
   b) Introduzca la dirección IP de su router predeterminado en el campo **OpenScape Business - Dirección IP del router predeterminado**

(por ejemplo, red interna: `192.168.1.x`, enrutador de Internet como enrutador predeterminado: `192.168.1.1`.

3) Definir la dirección IP de la UC Booster Card (necesario si la tarjeta está insertada):
4) Haga clic en **OK & Continuar**.

Pasos siguientes

Configurar DHCP.

5.6.2.3 Cómo especificar el nombre de dispositivo

Requisitos previos

Se encuentra en la ventana **Configuración de sistema**.

El sistema está en modo DTAG.

Paso a paso

1) Marque la casilla de verificación **Registro automático RSP.servicelink**:

   el campo **Nombre del dispositivo** es editable.
2) Especifique el **Nombre del dispositivo**.

   Al seleccionar el registro automático RSP.servicelink, cada 10 minutos, el sistema intentará registrarse automáticamente y conectarse con servidores RSP mediante el nombre de dispositivo suministrado.
3) Haga clic en **OK y Continuar.**

Pasos siguientes

Configurar DHCP.

5.6.3 Configuración de DHCP

En la ventana **Ajustes globales DHCP**, active, configure o desactive el servidor DHCP interno del sistema de comunicación.

Un servidor DHCP asigna automáticamente una dirección IP a las extensiones IP (teléfonos IP, PC, etc.) y les suministra datos específicos de red (como, por ejemplo, la dirección IP del gateway estándar).

Como servidor DHCP se puede utilizar un servidor DHCP externo (por ejemplo, el servidor DHCP del router Internet) o el servidor DHCP interno integrado en el sistema de comunicación.

Para la actualización automática de software de los teléfonos IP del sistema se puede utilizar el DLI integrado en el sistema de comunicación o un servidor DLS externo (Deployment Service [DLI y DLS]). El servidor DHCP debe conocer la dirección IP del DLI integrado o del servidor DLS externo.

Tiene las siguientes opciones:

- Activar y configurar un servidor DHCP interno

  Si se utiliza el servidor DHCP interno del sistema de comunicación, hay que desactivar un servidor DHCP externo (por ejemplo, el servidor DHCP del

router Internet). Puede ser necesario adaptar los ajustes del servidor DHCP interno con la LAN de clientes. Si se utiliza el servidor DHCP interno y el DLI interno, los teléfonos del sistema se actualizan automáticamente. Si se utiliza un servidor DLS externo, hay que registrar su dirección IP en el servidor DHCP interno mediante el Modo Experto (Deployment Service (DLI y DLS)).

- Desactivar el servidor DHCP interno

  Si se utiliza un servidor DHCP externo, hay que desactivar el servidor DHCP interno del sistema de comunicación. Para suministrar el software telefónico actualizado automáticamente a todos los teléfonos IP del sistema, en el servidor DHCP externo hay que introducir los datos específicos de red como, por ejemplo, la dirección IP del DLI interno o del servidor DLS externo.

  Nota: ¡No todos los servidores DHCP externos admiten la entrada de datos específicos de red! En este caso, hay que introducir los datos manualmente en todos los teléfonos IP del sistema.

5.6.3.1 Cómo deshabilitar el servidor DHCP interno

Requisitos previos

Se habilita un servidor DHCP externo (por ejemplo, el servidor DHCP del enrutador de Internet) en la red interna.

Está en la ventana **Configuración global de DHCP**.

Paso a paso

1) Desmarque la casilla de verificación **Habilitar servidor DHCP.**
2) Haga clic en **Aceptar & Siguiente**.

Pasos siguientes

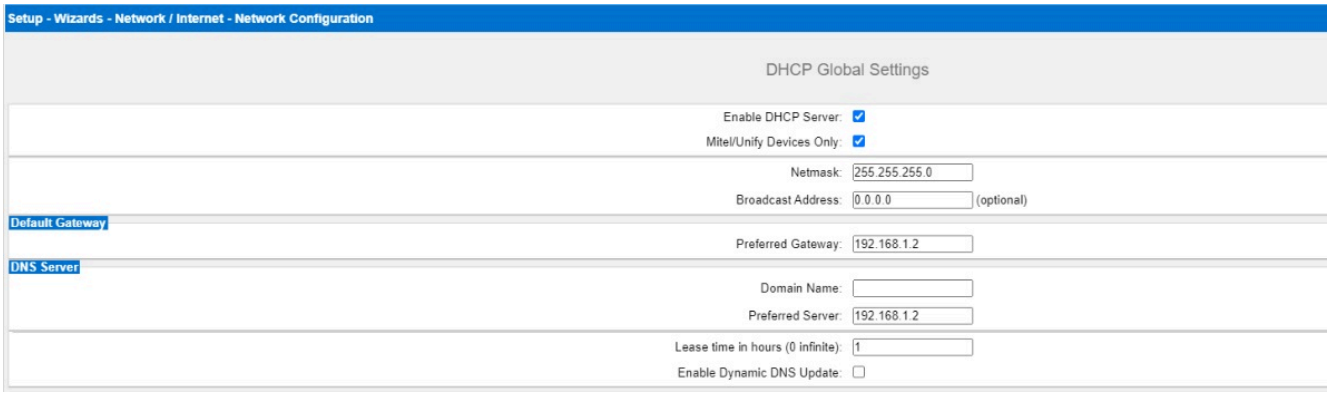
Configure los ajustes de país y hora.

5.6.3.2 Cómo habilitar y configurar el servidor DHCP interno

Requisitos previos

El servidor DHCP externo (por ejemplo, el servidor DHCP del enrutador de Internet) se ha deshabilitado en la red interna.

Está en la ventana **Configuración global de DHCP**.

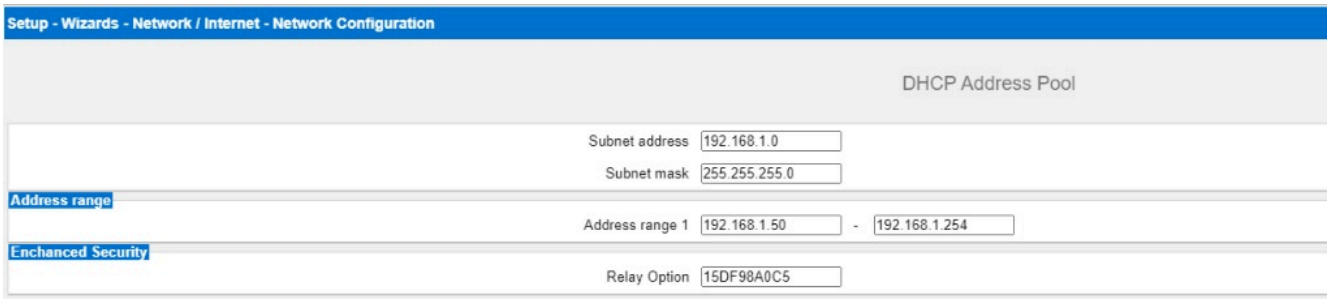


Paso a paso

1) Deje la casilla de verificación **Habilitar servidor DHCP** habilitada.
2) Si es necesario, habilite la casilla de verificación **Solo dispositivos Mitel/ Unify.**

   Nota: Esta opción sólo está disponible para placas base V3.

3) Vaya al campo **Máscara de red** y ajuste la máscara de subred a su rango de direcciones IP (por ejemplo, `255.255.255.0`).
4) En el campo **Gateway preferido**, ingrese la dirección IP del enrutador de Internet (por ejemplo, `192.168.1.1`).
5) En el campo **Servidor preferido**, ingrese la dirección IP del servidor DNS (por ejemplo, la dirección IP del enrutador de Internet, `192.168.1.1`.
6) Haga clic en **Aceptar & Siguiente**. Aparece la ventana del **grupo de direcciones DHCP**.



7) Especifique los valores para **Dirección de subred**, **Máscara de red** y **Rango de direcciones 1** para definir el rango de direcciones IP que administrará el servidor DHCP interno.

   Si la red interna utiliza direcciones IP estáticas (por ejemplo, para un servidor de impresora), se debe seleccionar el rango de direcciones IP

(grupo de direcciones DHCP) de modo que las direcciones IP fijas no se incluyan dentro de este rango.

Ejemplo:

Enrutador de Internet: `192.168.1.1`

OpenScape Business: `192.168.1.2`

Tarjeta de refuerzo UC: `192.168.1.3`

Dirección de subred: `192.168.1.0`

Máscara de subred: `255.255.255.0`

Servidor de impresión: `192.168.1.10`

Grupo de direcciones DHCP: `192.168.1.50` a `192.168.1.254`

8) Si es necesario, especifique el valor del campo **Opción de retransmisión.**

Nota: Esta opción sólo está disponible para placas base V3.

9) Haga clic en **Aceptar & Siguiente**.

Pasos siguientes

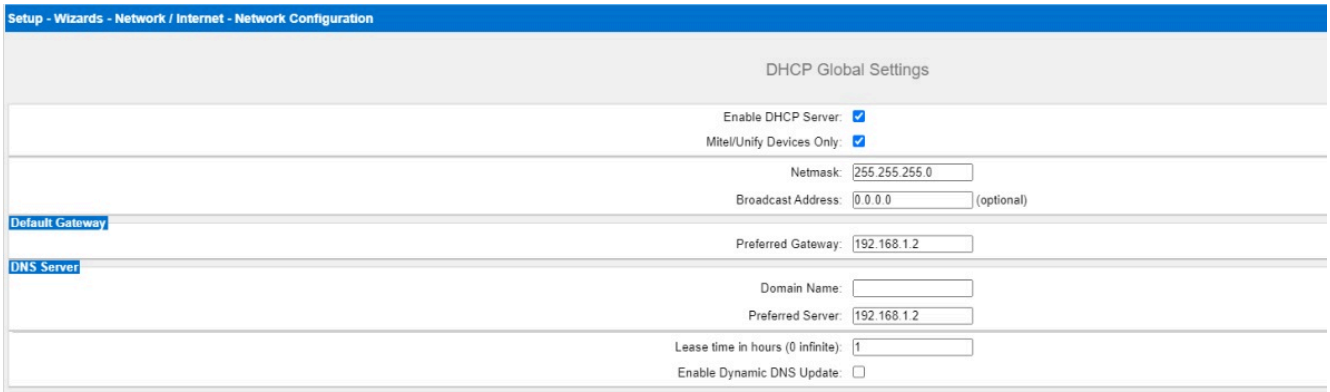
Configure los ajustes de país y hora.

5.6.3.3 Cómo habilitar DHCP solo para dispositivos Mitel/Unify

Esta opción permite al administrador del sistema activar el servicio DHCP de OpenScape Business exclusivamente para dispositivos Mitel y Unify.

Requisitos previos

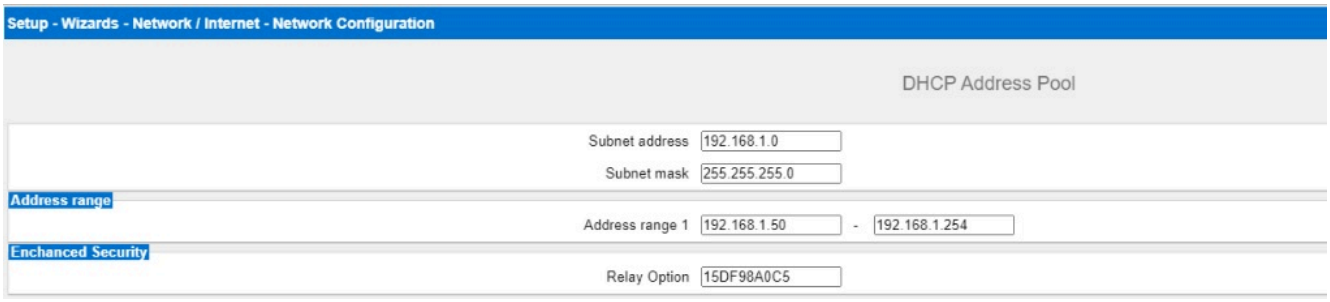
Está en la ventana **Configuración global de DHCP**.



Paso a paso

1) Deje la casilla de verificación **Habilitar servidor DHCP** habilitada.
2) Haga clic para habilitar la casilla de verificación **Solo dispositivos Mitel/ Unify.** Consulte Servidor DHCP > Parámetros globales para obtener más información sobre esta opción.
3) Vaya al campo **Máscara de red** y ajuste la máscara de subred a su rango de direcciones IP (por ejemplo, `255.255.255.0`).

4) En el campo **Gateway preferido**, ingrese la dirección IP del enrutador de Internet (por ejemplo, `192.168.1.1`).
5) En el campo **Servidor preferido**, ingrese la dirección IP del servidor DNS (por ejemplo, la dirección IP del enrutador de Internet, `192.168.1.1`.
6) Haga clic en **Aceptar & Siguiente**. Aparece la ventana del **grupo de direcciones DHCP**.



7) Especifique los valores para la dirección de subred , **Máscara de subred** y **Rango de direcciones 1** para definir el rango de direcciones IP que será administrado por el servidor DHCP interno.

   Si la red interna utiliza direcciones IP estáticas (por ejemplo, para un servidor de impresora), se debe seleccionar el rango de direcciones IP (grupo de direcciones DHCP) de modo que las direcciones IP fijas no se incluyan dentro de este rango.

   Ejemplo:

   Enrutador de Internet: `192.168.1.1`

   OpenScape Business: `192.168.1.2`

   Tarjeta de refuerzo UC: `192.168.1.3`

   Dirección de subred: `192.168.1.0`

   Máscara de subred: `255.255.255.0`

   Servidor de impresión: `192.168.1.10`

   Grupo de direcciones DHCP: `192.168.1.50` a `192.168.1.254`
8) Especifique el valor del campo **Opción de retransmisión**.
9) Haga clic en **Aceptar & Siguiente**.

Pasos siguientes

Configure los ajustes de país y hora.

5.6.4 Configuración de país y hora

En la ventana **Configuración básica** seleccione su país y el idioma para los registros de suceso y configure la fecha y la hora. Si utiliza la solución Cordless integrada, introduzca aquí la identificación del sistema DECT a nivel del sistema.

Para ello, siga este procedimiento:

1) Seleccionar el distintivo de país y el idioma para los registros de sucesos

   Para que la inicialización del país sea correcta, debe seleccionar el idioma en el que estará en servicio el sistema de comunicación. Además, puede seleccionar el idioma en el que se guardarán los registros de sucesos (protocolos de eventos del sistema, errores, etc).
2) Introducir la identificación del sistema DECT (solo con una solución Cordless integrada)

   Si utiliza la solución Cordless integrada, introduzca aquí la identificación del sistema DECT a nivel del sistema.
3) Configurar fecha y hora manualmente
   - Configuración manual de fecha y hora

     El sistema de comunicación y las extensiones (teléfonos IP, teléfonos TDM, PC de cliente) deben disponer de una base temporal única (fecha y hora). Si no conoce ningún servidor SNTP para la sincronización de hora, también puede introducir la fecha y la hora de forma manual.

     Nota: La fecha y hora se actualizan automáticamente cuando se establece una conexión por la línea urbana RDSI.
   - Obtener la fecha y hora de un servidor SNTP

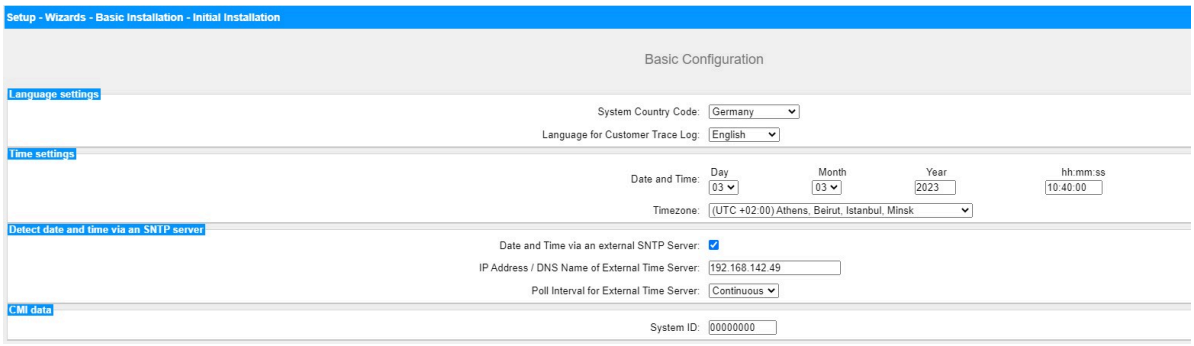
     El sistema de comunicación y las extensiones IP (teléfonos IP, PC de cliente) deben disponer de una base temporal única (fecha y hora). Esta base temporal se puede ofrecer por un servidor SNTP. El servidor SNTP puede encontrarse en la red interna o en Internet.

El sistema de comunicación envía automáticamente la fecha y hora a los teléfonos IP. Los PC de cliente en los que se ejecutan los clientes de UC deben configurarse de forma que tengan la hora sincronizada con el sistema de comunicación (vea las instrucciones del sistema operativo del PC cliente).

5.6.4.1 Cómo seleccionar el código de país y el idioma para los registros de sucesos

Requisitos previos

Se encuentra en la ventana **Configuración básica**.



Paso a paso

1) En la lista desplegable **Distintivo país sistema** seleccione el país en el que estará en funcionamiento el sistema de comunicación.
2) En el campo **Idioma para el Protocolo trace de cliente** seleccione el idioma para emitir los protocolos de sucesos de sistema, errores, etc.

Pasos siguientes

Introducir la identificación del sistema DECT (solo con una solución Cordless integrada)

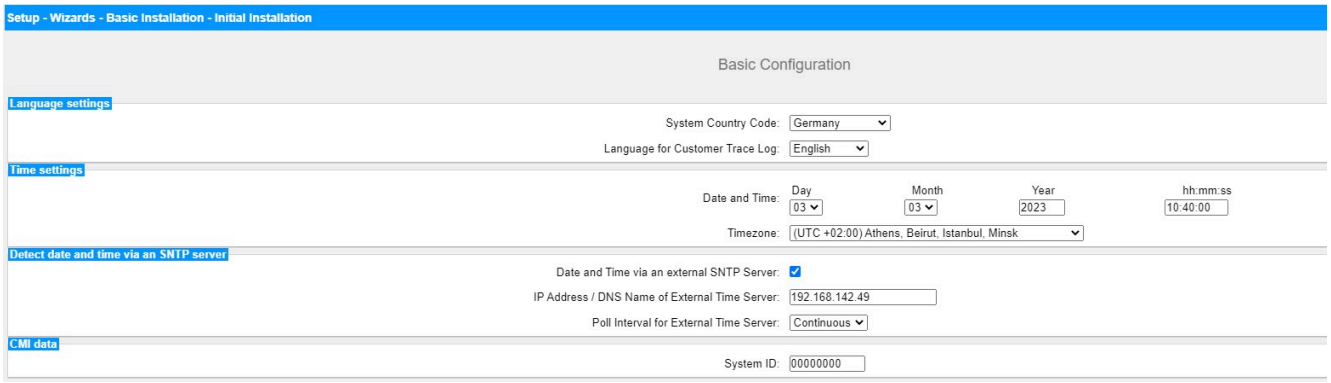
o

Configurar la fecha y la hora a mano o consultar la fecha y la hora desde un servidor SNTP.

5.6.4.2 Cómo introducir la identificación del sistema DECT

Requisitos previos

Se encuentra en la ventana **Configuración básica**.



Paso a paso

En la sección **Datos CMI**, en **ID del sistema**, indique el ID de sistema DECT hexadecimal de 8 dígitos que ha recibido al adquirir su solución Cordless (inalámbrica) integrada.

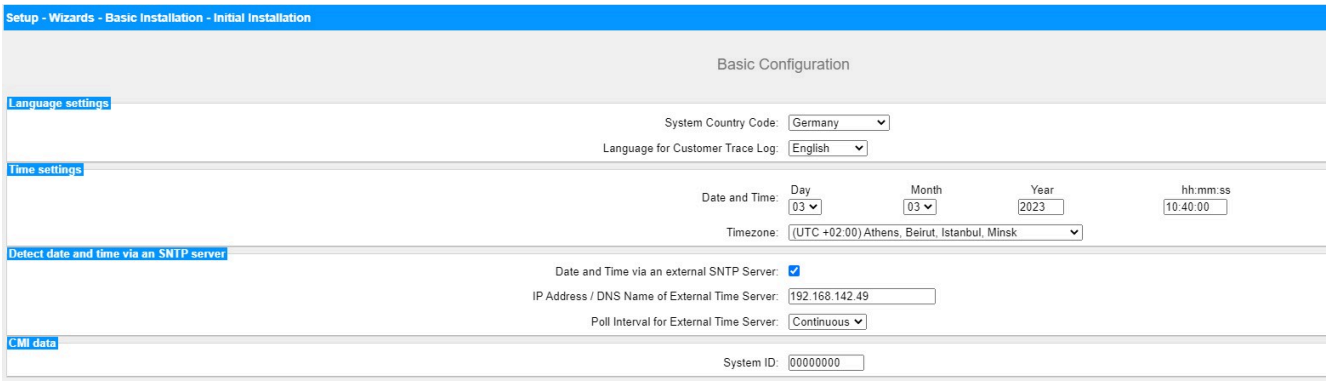
Pasos siguientes

Configurar la fecha y la hora a mano o consultar la fecha y la hora desde un servidor SNTP.

5.6.4.3 Configuración manual de fecha y hora

Requisitos previos

Se encuentra en la ventana **Configuración básica**.



Paso a paso

1) Indique los valores actuales para **Fecha y hora**.
2) En el campo **Zona horaria** establezca la zona horaria deseada.
3) Haga clic en **OK & Continuar**.

Nota: Si se cambia la zona horaria, el **sistema se reiniciará** en el último paso del Asistente inicial.

Si no se modifica la configuración de la zona horaria, el sistema no se reiniciará.

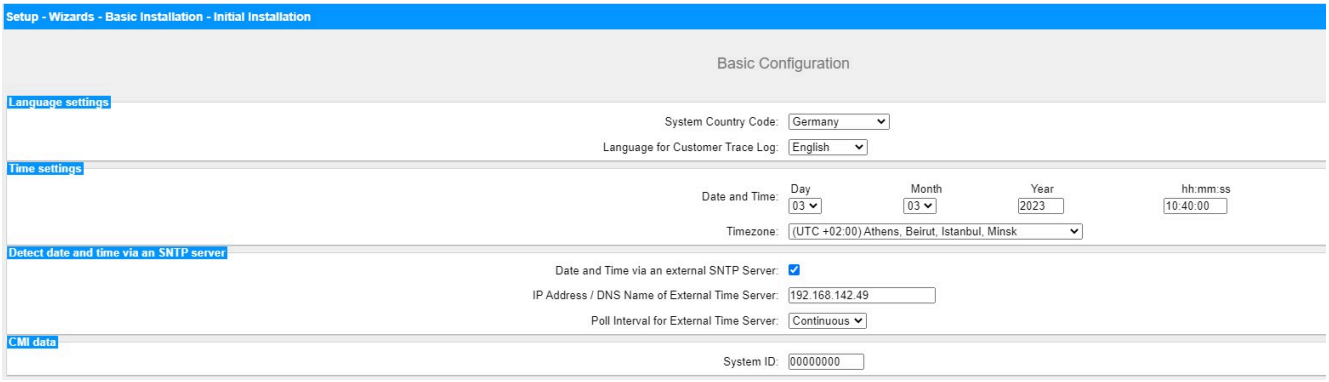
Pasos siguientes

Defina la Solución UC.

5.6.4.4 Obtención de la fecha y hora de un servidor SNTP

Requisitos previos

Se encuentra en la ventana **Configuración básica**.



Paso a paso

1) Active la casilla de verificación **Fecha y hora a través de un servidor SNTP externo**.

2) Introduzca la dirección IP o el nombre DNS del servidor SNTP (por ejemplo, `0.de.pool.ntp.org`) en el campo **Dirección IP / Nombre DNS del servidor horario externo**).
3) En la lista desplegable **Intervalo de sondeo para el servidor de hora externo**, seleccione después de cuántas horas deben sincronizarse la fecha y la hora mediante el servidor SNTP (valor recomendado: `4 h`).
4) Haga clic en **OK & Continuar**.

Pasos siguientes

Defina la Solución UC.

5.6.5 Solución UC

En la ventana **Modificar selección de aplicación** puede definir qué solución de UC utiliza.

Tiene las siguientes opciones:

- **Paquete con UC Smart**

  La solución de Comunicaciones Unificadas UC Smart está integrada en la placa base OpenScape Business X.
- **Paquete con UC Suite**

  La solución de Comunicaciones Unificadas UC Suite está integrada en la “UC Booster Card”, que se puede conectar internamente de forma opcional.
- **Paquete con UC Suite en OSBiz UC Booster Server**

  La solución de Comunicaciones Unificadas UC Smart está integrada en el servidor Linux externo "OpenScape Business UC Booster Server".
- **Paquete con UC Suite en OSBiz UC Booster Server**

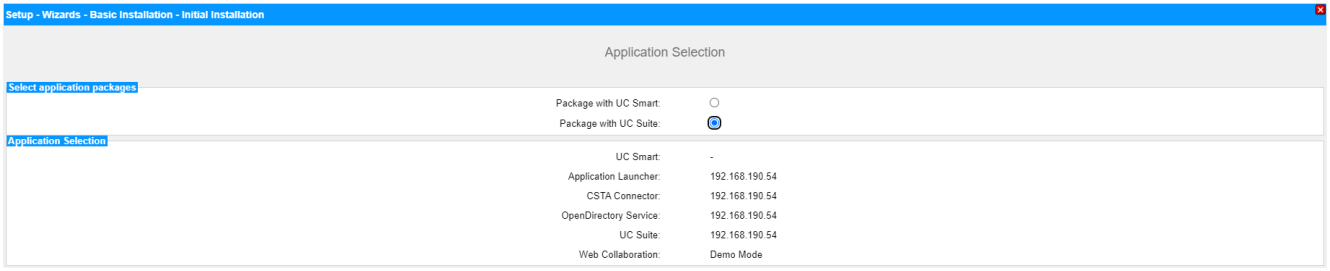
  La solución de Comunicaciones Unificadas UC Suite está integrada en el servidor Linux externo "OpenScape Business UC Booster Server".

5.6.5.1 Cómo establecer la solución UC

Requisitos previos

Ha adquirido licencias para la solución de Comunicaciones Unificadas UC Smart o para la solución de Comunicaciones Unificadas UC Suite.

Se encuentra en la ventana de **Selección de aplicación**.



Paso a paso

1) Si utiliza la solución de Comunicaciones Unificadas UC Smart sin un UC Booster Server, haga clic en **Paquete con UC Smart**.
2) Si utiliza la solución de Comunicaciones Unificadas UC Smart con UC Booster Server, haga clic en Paquete con **UC Smart en OSBiz UC Booster Server**. Además, introduzca la dirección IP del servidor Linux externo "OpenScape Business UC Booster Server" en el campo **Dirección IP del OSBiz UC Booster Servidor**.
3) Si quiere utilizar la solución de Comunicaciones Unificadas UC Suite con UC Booster Card, haga clic en **Paquete con UC Suite**.
4) Si utiliza la solución de Comunicaciones Unificadas UC Suite con UC Booster Server, haga clic en Paquete con **UC Suite en OSBiz UC Booster Server**. Además, introduzca la dirección IP del servidor Linux externo "OpenScape Business UC Booster Server" en el campo **Dirección IP del OSBiz UC Booster Servidor**.
5) Haga clic en **OK & Continuar**.
6) Se ha completado el asistente **Instalación inicial**. Haga clic en **Salir**.
7) Cierre la Gestión basada en Web (WBM), haciendo clic en el enlace **Finalizar sesión** y, a continuación, cerrando la ventana.

Nota: Si se han modificado direcciones IP o ajustes del servidor DHCP, el sistema de comunicación se reinicia. Puede durar algunos minutos.

Pasos siguientes

Conectar el sistema de comunicación con la LAN de clientes.

5.6.6 Conexión del sistema de comunicación en la LAN de clientes

Una vez finalizada la instalación inicial, el sistema de comunicación se conecta con la LAN de clientes existente.

5.6.6.1 Cómo conectar el sistema de comunicación en la LAN de clientes

Requisitos previos

El sistema de comunicación está operativo.

Paso a paso

1) Retire el cable LAN del PC de administración de la interfaz LAN central "LAN" e integre el PC de administración en la LAN de clientes conectándolo con un conmutador, por ejemplo.
2) Conecte un cable LAN con la interfaz LAN central "LAN" del sistema de comunicación.
3) Integre el sistema de comunicación mediante este cable LAN en la LAN de clientes conectándolo con un conmutador, por ejemplo.
4) Si hay insertada una tarjeta UC Booster Card (Tablero de aplicaciones), conecte otro cable LAN con la interfaz LAN "LAN2" de la UC Booster Card (la interfaz LAN de abajo a la derecha) e integre la UC Booster Card

mediante este cable LAN en la LAN de clientes. Para ello, por ejemplo, conéctelo con un conmutador.

Pasos siguientes

Iniciar la configuración básica.

5.7 Configuración básica

La configuración básica se realiza con el asistente **Instalación básica** de la Gestión basada en Web (WBM). Se definen los ajustes más importantes para el funcionamiento del sistema de comunicación.

El asistente de Instalación básica incluye un indicador de progreso con el paso actual y una indicación de los pasos siguientes.

5.7.1 Cómo iniciar el Asistente Configuración básica

Requisitos previos

Se ha completado el asistente **Instalación inicial**.

El sistema de comunicación está integrado en la LAN de clientes.

El sistema de comunicación está operativo. El LED "Run" de la placa base parpadea en verde a intervalos de 1 Hz 0,5 s encendido/ 0,5 s apagado).

Paso a paso

1) En el navegador Web del PC de administración, abra la página de registro de Gestión basada en Web (WBM), en la dirección:

   `https://<Dirección IP de OpenScape Business>`

   La dirección IP estándar de OpenScape Business es `192.168.1.2`, por tanto, por ejemplo, `https://192.168.1.2`
2) En el campo **Nombre de usuario**, introduzca el nombre de usuario estándar `administrador@sistema` para acceder como administrador.
3) En el campo **Contraseña**, indique la contraseña que haya definido durante la puesta en servicio inicial.
4) Haga clic en **Iniciar sesión**.
5) En la barra de navegación, haga clic en **Configuración**.
6) Haga clic en **Editar** para iniciar el asistente **Configuración básica**.

Pasos siguientes

Realice la Configuración básica tal y como se describe a continuación, paso a paso. Los campos que no se describen aquí están preestablecidos de acuerdo al caso estándar y solo hay que modificarlos cuando no coincidan con sus datos de red. Encontrará información detallada en la descripción de los distintos asistentes de la documentación del administrador.

5.7.2 Números de teléfono del sistema e interconexión

En la ventana **Resumen**, indique los números de teléfono del sistema (número de teléfonos del sistema, prefijo nacional y local, prefijo internacional) y establezca si desea interconectar OpenScape Business con otros sistemas OpenScape Business.

Para ello, siga este procedimiento:

1) Introducir números de teléfono del sistema

- Introducir números de teléfono del sistema para una conexión de centralita

  Aquí se indica el número de teléfono del sistema para su conexión de centralita y el prefijo nacional y local.

  Es imprescindible introducir el prefijo de país para la telefonía Internet y para las funciones de servidor de conferencias.

  El prefijo internacional está predefinido en función del código de país marcado antes.
- Introducir números de teléfono del sistema para acceso individual RDSI

  Aquí se indica el prefijo nacional y local para el acceso individual RDSI.

  Es imprescindible introducir el prefijo de país para la telefonía Internet y para las conferencias MeetMe.

  El prefijo internacional está predefinido en función del código de país marcado antes.

2) Activar y desactivar Interconexión.

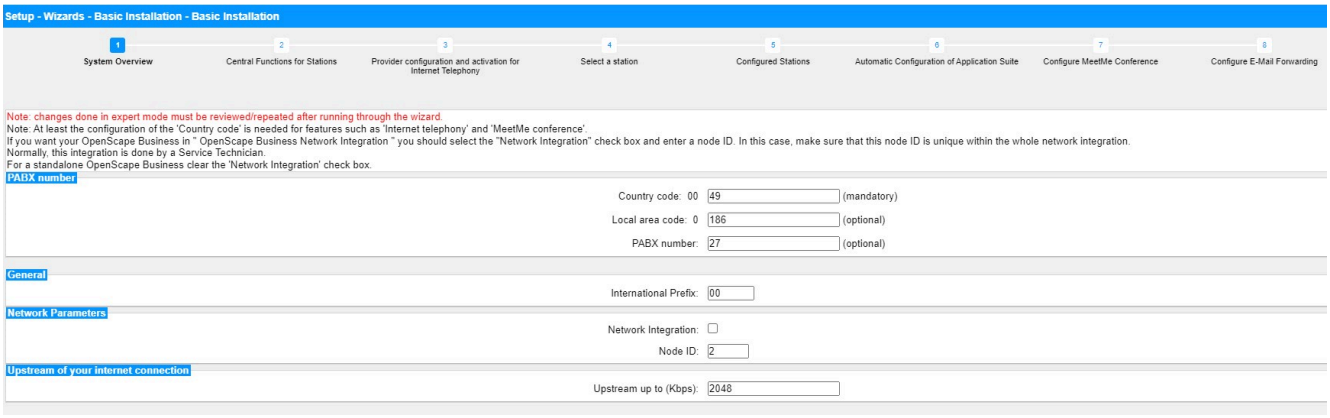
Si desea interconectar OpenScape Business con otros sistemas OpenScape Business, hay que activar Interconexión y hay que asignar un ID de nodo a OpenScape Business. Cada OpenScape Business debe tener un ID de nodo único en la interred.

5.7.2.1 Cómo introducir el número de teléfono del sistema para una conexión de centralita

Requisitos previos

Tiene una conexión de centralita.

Se encuentra en la ventana **Resumen** del asistente **Configuración básica**.



Paso a paso

1) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo `49` para Alemania o `1` para EE. UU.
2) En el campo **Código de red local**, indique el prefijo local, por ejemplo `89` para Múnich.
3) En **Nº tel. sistema**, indique el número del sistema de conexión urbana, p. ej. `7007` (su número de conexión).
4) Solo debe cambiar el campo **Prefijo internacional** cuando sea necesario. Para Alemania se usa `00` y para EE. UU. `011`).

   En las llamadas al extranjero, delante del número de teléfono se pone el prefijo internacional y el prefijo del país. Por ejemplo, de Alemania a EE.UU "00-1-..." y de EE. UU. a Alemania "011-49-...".

Pasos siguientes

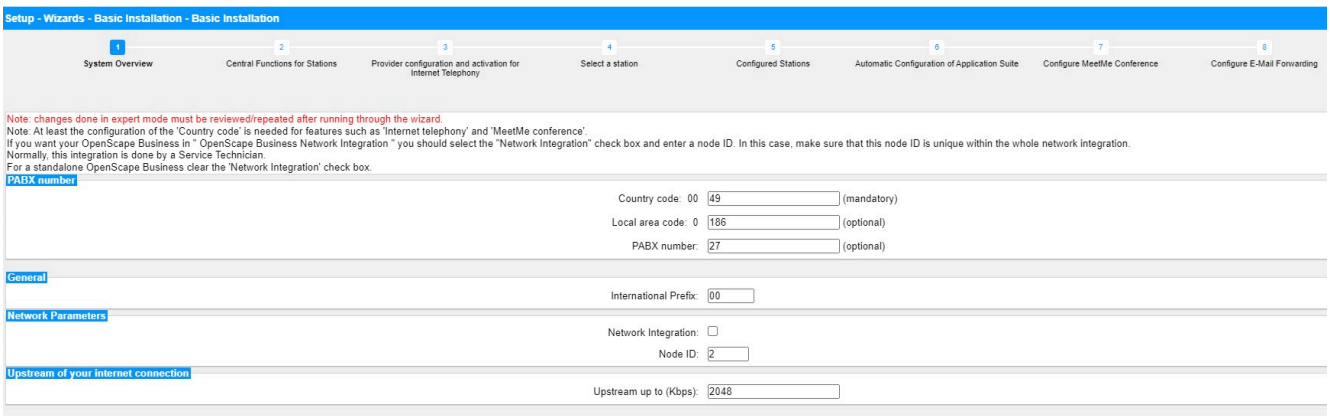
Activar y desactivar Interconexión.

5.7.2.2 Cómo introducir los números de teléfono del sistema para un acceso individual

Requisitos previos

Tiene un acceso individual.

Se encuentra en la ventana **Resumen** del asistente **Configuración básica**.



Paso a paso

1) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo `49` para Alemania o `1` para EE. UU.
2) En el campo **Código de red local**, indique el prefijo local, por ejemplo `89` para Múnich.
3) Deje vacío el campo **Nº teléfono del sistema**.
4) Solo debe cambiar el campo **Prefijo internacional** cuando sea necesario. Para Alemania se usa `00` y para EE. UU. `011`).

   En las llamadas al extranjero, delante del número de teléfono se pone el prefijo internacional y el prefijo del país. Por ejemplo, de Alemania a EE.UU "00-1-..." y de EE. UU. a Alemania "011-49-...".

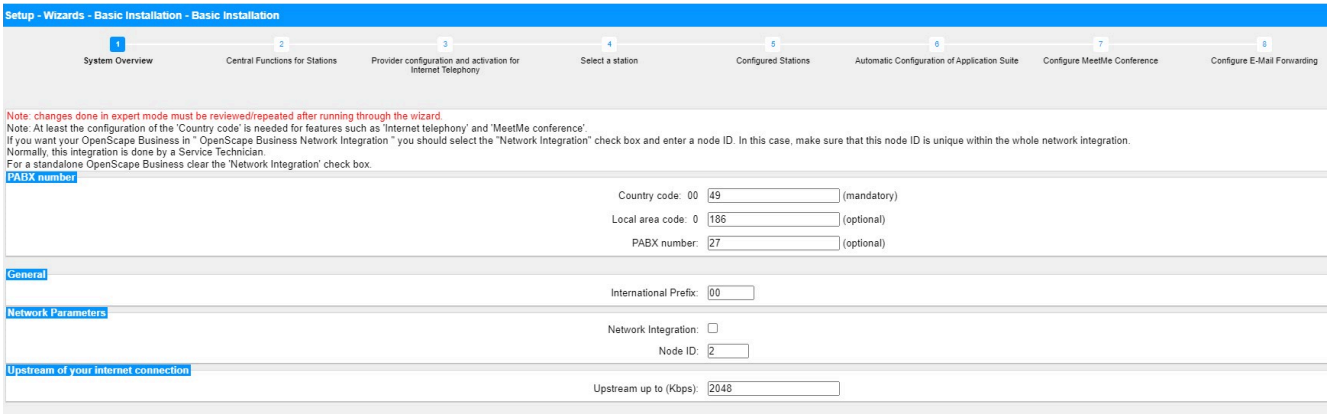
Pasos siguientes

Activar y desactivar Interconexión.

5.7.2.3 Cómo activar o desactivar la interconexión

Requisitos previos

Se encuentra en la ventana **Resumen** del asistente **Configuración básica**.



Paso a paso

1) Si se quiere interconectar el sistema de comunicación con otros sistemas de comunicación:
   a) Active **Integración de red**.
   b) En el campo **ID de nodo** para el sistema de comunicación asigne un ID de nodo único en la interred (se pueden usar cifras del `1` al `100`).
2) Si no se quiere interconectar el sistema de comunicación con otros sistemas de comunicación, deje desactivada la casilla de verificación **Integración de red**.

Pasos siguientes

Configure el flujo ascendente de su conexión a Internet.

5.7.3 Datos de extensión

Si es necesario, en la ventana **Funciones centrales para extensiones** puede configurar su plan de numeración individual en lugar del plan de numeración estándar predefinido e importar más datos de extensión. En la interred hay que ajustar el plan de numeración estándar al plan de numeración de la interred.

El plan de numeración estándar incluye números de teléfono predefinidos para distintos tipos de extensión (teléfonos IP, teléfonos analógicos...) y para funciones especiales (telefonía Internet, buzón de voz, AutoAttendant...).

Los datos de extensión incluyen, entre otros, los números de teléfono internos, los números de marcación directa y los nombres de las extensiones. Estos datos y otros datos de extensión se pueden importar en el sistema de comunicación durante la configuración básica mediante un archivo XML en formato UTF-8.

Nota:

Puede consultar una plantilla XML con la correspondiente explicación en la Gestión basada en Web (WBM), en **Centro de servicios** > **Documentos** > **Plantillas CSV**. En esta plantilla puede introducir sus datos, por ejemplo con Microsoft Excel.

Tiene las siguientes opciones:

- **Configurar datos de extensión sin interred**

  Para ello, siga este procedimiento:

  1) Mostrar datos de extensión

  Puede mostrar todos los datos de extensión y los números de teléfono preconfigurados.

  2) Borrar todos los números de llamada de extensión (opcional)

  Si utiliza un plan de numeración individual hay que borrar todos los números de teléfono preconfigurados.

  3) Ajustar números de teléfono preconfigurados al plan de numeración individual (opcional)

  Si utiliza un plan de numeración individual, puede ajustar los números de teléfono preconfigurados al plan de numeración propio.

  Nota:

  Si el usuario pasa por **Cambiar números de función y de llamada preconfigurados,** debe revisarse o repetirse todas las configuraciones personalizadas existentes realizadas en UC Suite (por ejemplo, colas piloto).

  ---

  4) Importar datos de extensión mediante un archivo XML (opcional)

  Puede importar sus números de teléfono individuales (con los datos de extensión adicionales) cómodamente durante la configuración básica mediante un archivo XML.

- **Configurar datos de extensión con interred**

  Para ello, siga este procedimiento:

  1) Borrar todos los números de llamada de extensión.

  Si en la interred se utiliza la UC Suite, hay que usar un plan de numeración cerrado, es decir: todos los números de teléfono de la interred deben ser únicos. Por ello, hay que borrar los números de teléfono preconfigurados y utilizar números adecuados para la interred.

  2) Importar datos de extensión mediante un archivo XML

  Los números de teléfono adaptados a la interred se deben importar junto con los datos de extensión adicionales durante la configuración básica mediante un archivo XML. El proceso es muy sencillo. Este archivo puede incluir todas las extensiones de la interred. En la importación se aplican únicamente los números de teléfono y los datos de extensión asignados previamente a los ID de nodo del sistema de comunicación.

Tareas relacionadas

Cómo mostrar datos masivos en la página 166
Cómo restablecer las entradas LCR en la página 1442

Referencia relacionada

LCR > Flags LCR en la página 1641

5.7.3.1 Cómo mostrar los datos de extensión

Requisitos previos

Se encuentra en la ventana **Funciones centrales para extensiones** del asistente **Configuración básica**.

Paso a paso

1) Active campo opción **Mostrar configuración extensiones**.

2) Clic en **Ejecutar función**. Aparece una lista de las extensiones con números de teléfono preconfigurados (Plan de numeración estándar).

3) Clic **Acept**. Regresa a la ventana **Funciones centrales para extensiones**.

4) Si no quiere modificar ningún dato de extensión, haga clic en **OK & Continuar**.

5.7.3.2 Cómo borrar todos los números de llamada

Requisitos previos

Se encuentra en la ventana **Funciones centrales para extensiones** del asistente **Configuración básica**.

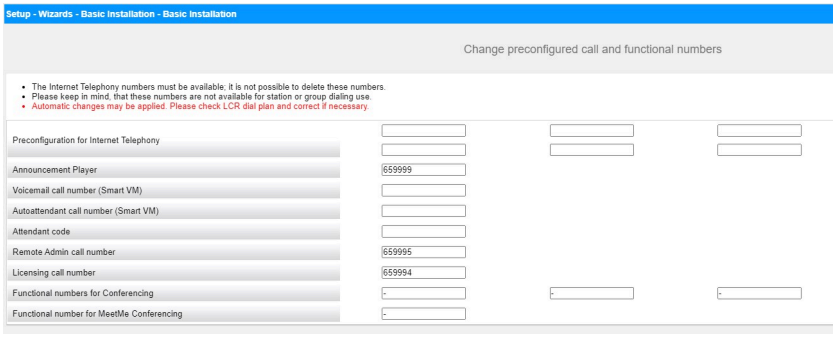
Paso a paso

1) Active la opción **Borrar todos nos. llamada**.

2) Active la casilla de verificación **Borrar todos nos. llamada**.

3) Haga clic en **Ejecutar función**. Todos los números de teléfono preasignados se aliminan excepto **Reproductor de anuncios, Núm. llam. de administración remota** y **Núm. llam. de registro de licencia**.

A continuación aparece la ventana **Cambiar números de función y de llamada preconfigurados**.



4) Ajuste los códigos y los números de teléfono especiales a sus necesidades y a continuación haga clic en **Aceptar**. Regresa a la ventana **Funciones centrales para extensiones**.
5) Si no desea modificar más datos de extensión, haga clic en **OK & Continuar**.

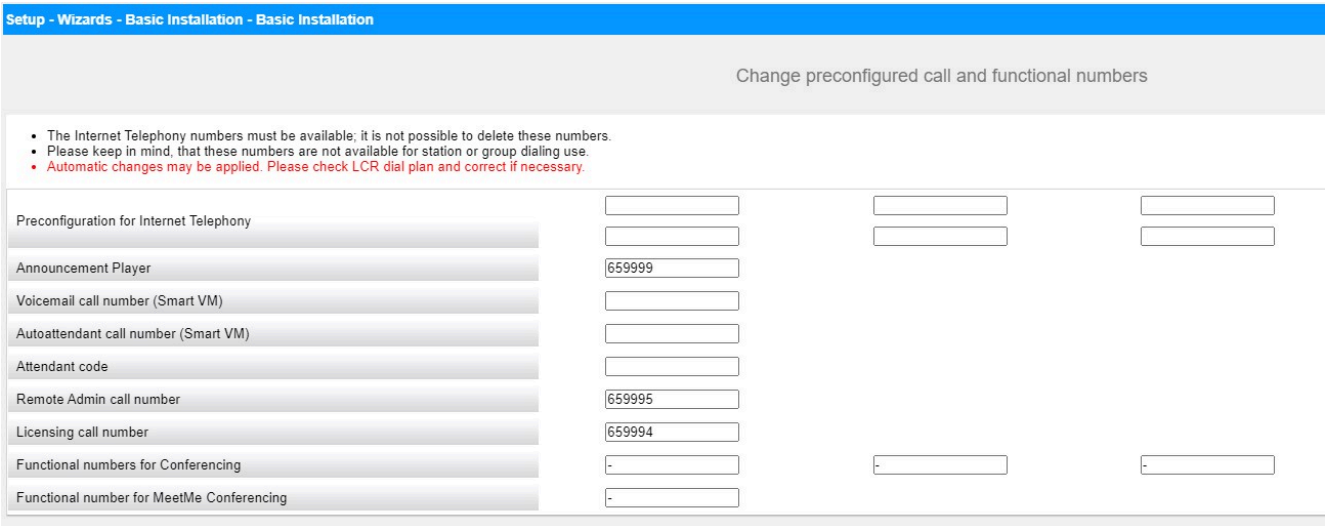
5.7.3.3 Adaptar los números de teléfono preconfigurados al plan de numeración individual

Requisitos previos

Se encuentra en la ventana **Funciones centrales para extensiones** del asistente **Configuración básica**.

Paso a paso

1) Active el campo de opción **Cambiar números de función y de llamada preconfigurados**.
2) Haga clic en **Ejecutar función**. Se abre la ventana **Cambiar números de función y de llamada preconfigurados**.



3) Adapte los números de teléfono preconfigurados a sus necesidades y a continuación haga clic en **Aceptar**. Regresa a la ventana **Funciones centrales para extensiones**.

4) Si no desea modificar más datos de extensión, haga clic en **OK & Continuar**.

5.7.3.4 Cómo importar los datos de extensión mediante un archivo XML

Requisitos previos

Se encuentra en la ventana **Funciones centrales para extensiones** del asistente **Configuración básica**.

Hay disponible archivo XML UTF-8 con los datos registrados. Puede consultar una plantilla XML en **Centro de servicios** > **Documentos** > **Plantillas CSV**.

Paso a paso

1) Active la opción **Importar archivo CSV/XML con datos de extensión**.
2) Haga clic en **Ejecutar función**.
3) Mediante **Examinar**, seleccione el archivo XML deseado y haga clic en **Abrir**.
4) Luego, haga clic en **OK**. Se importan los datos de extensión.
5) Haga clic en **OK y Continuar**.

5.7.3.5 Cómo mostrar datos masivos

Requisitos previos

- Se encuentra en la ventana **Funciones centrales para extensiones** del asistente **Configuración básica**.
- También puede acceder al **Asistente de datos masivos** desde **Asistentes** > **de instalación**.

Paso a paso

1) Active el botón **Asistente de datos masivos**.
2) Haga clic en **Ejecutar función**.
3) En la ventana **Asistente de datos masivos**, puede hacer clic en **Validar** para validar las entradas del sistema. Hay dos tipos de validación: la prueba de coherencia de front-end y la prueba de coherencia de back-end.
   En el campo de validación, solo se indican con color verde las acciones validadas recientemente. La validación de datos no se guarda, por lo que se debe realizar nuevamente si se cambian los valores.
4) Durante la prueba de coherencia de back-end y después de validar los datos correctamente, no se pueden hacer cambios en la ventana **Asistente de datos masivos**. Una vez hecha la validación, estará disponible la opción **OK y Continuar** en el modo de edición restringida. Al hacer clic en **Atrás**, el modo de edición pasa a estar disponible pero la opción **OK y Continuar** desaparece. Si la validación no es correcta, el modo de edición se mantiene y la opción **OK y Continuar** sigue oculta.

Nota: El usuario puede hacer clic en **Atrás** para volver a editar los datos; la ventana volverá al modo de edición. El usuario de edición restringida se asegura de que el usuario

no pueda hacer clic en OK y Continuar y enviar cambios que no estén validados.

5) Si el **Asistente de datos masivos** se configura correctamente, haga clic en **Finalizar**. En la página Finalizar aparece un resumen de todos los cambios.

   Los campos que no se pueden modificar ya incluyen los valores correspondientes recuperados de la base de datos. En consecuencia, la función de copiar y pegar no se puede usar en los datos.

   El campo Tipo es un menú desplegable seleccionable que permite editar. Sin embargo, las únicas opciones aceptadas son Libre, Cliente sist., Cliente SIP, Usuario Deskshare y, en su caso, un valor predefinido basado en la placa a la que pertenece. El usuario no podrá introducir un valor diferente y, si lo intenta, el menú desplegable no desaparecerá y seguirá ofreciendo una entrada adecuada.

   Otra restricción es que algunos puertos no se pueden modificar (por ejemplo, en los puertos que pertenecen a una tarjeta analógica, el tipo no se puede modificar y debe ser Ext. analógica). Todas las restricciones se aplican si el usuario intenta hacer copiar y pegar sobre la columna Tipo. Si el usuario intenta copiar datos no pertinentes que no cumplen las reglas anteriores, la acción no se llevará acabo.

   Copiar y pegar se puede aplicar a toda la tabla y a partes concretas de ella.

   Nota: Al seleccionar dos celdas adyacentes con un valor numérico y arrastrar los campos, las columnas siguientes no se rellenarán con números ascendentes sino con una copia de las celdas seleccionadas.

Conceptos relacionados

Datos de extensión en la página 163

5.7.4 Configuración RDSI

En la ventana **Configuración RDSI**, establezca si desea conectar extensiones RDSI y si la conexión de línea urbana se debe realizar mediante RDSI. La conexión urbana RDSI se puede configurar como conexión de centralita RDSI o como acceso individual RDSI. En función del sistema de comunicación y de los módulos utilizados, en su caso, hay disponibles diferentes interfaces S_0.

Tiene las siguientes opciones:

- Activar la configuración RDSI:

  1) Configurar la conexión de centralita RDSI

  Puede configurar una conexión de línea urbana RDSI como conexión de centralita RDSI con números de marcación directa.

  2) Configurar acceso individual RDSI

  Puede configurar una conexión de línea urbana RDSI como acceso individual RDSI con MSN.

  3) Configurar conexión de extensiones RDSI (opcional)

  Se pueden configurar una o varias interfaces S_0 como conexiones S_0 internas para conectar en ellas extensiones RDSI (teléfono RDSI o fax RDSI). Por cada extensión RDSI necesita una licencia de extensión.
- Desactivar la configuración RDSI

  Si no tiene ninguna conexión de línea urbana RDSI, debe desactivar la configuración RDSI. Todas las interfaces S_0 se configuran automáticamente como puertos S_0 internos.

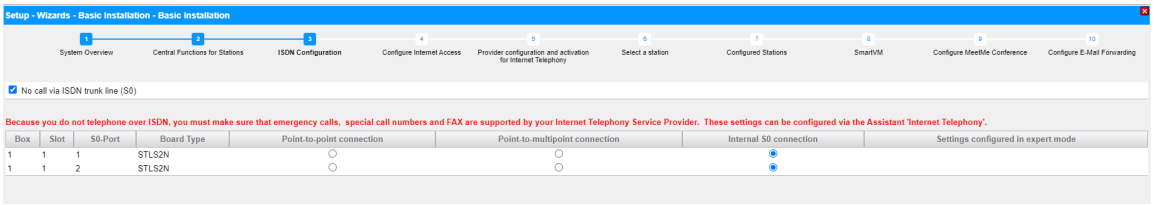
Opciones adicionales para una conexión de línea urbana

En lugar de una conexión de línea urbana RDSI, también puede configurar una conexión de línea urbana analógica o una conexión de línea urbana a través de un ITSP (Internet Telephony Service Provider). La conexión urbana analógica solo se puede configurar una vez finalizada la instalación básica.

5.7.4.1 Cómo configurar la conexión de extensiones RDSI

Requisitos previos

Se encuentra en la ventana **Configuración RDSI** del asistente **Configuración básica**.



Paso a paso

1) Desactive **Sin comun. a través lín. urbana RDSI (S0)**.

2) En la interfaz S_0 deseada, active el campo de opción **Conexión S0 interna**.

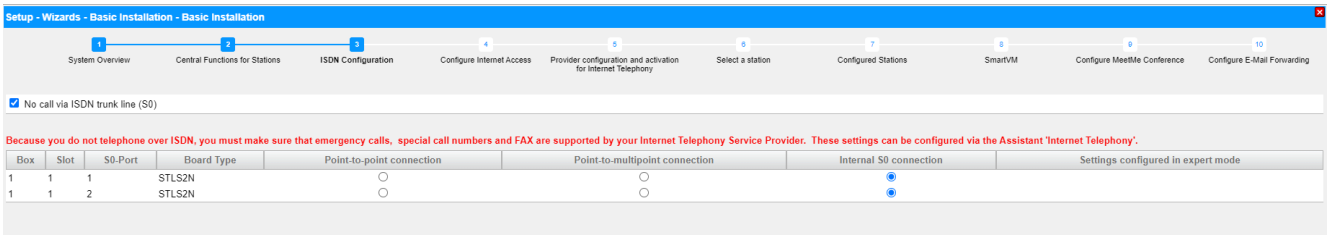
Pasos siguientes

Configure la conexión de centralita RDSI o el acceso individual RDSI.

5.7.4.2 Cómo configurar la conexión de centralita RDSI

Requisitos previos

Se encuentra en la ventana **Configuración RDSI** del asistente **Configuración básica**.



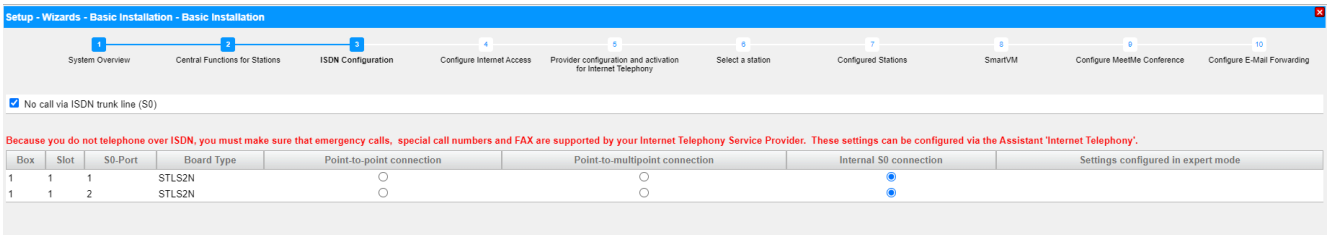
Paso a paso

1) Para la conexión urbana RDSI, desmarque **Sin comunicación a través de lín. urbana RDSI (S0)**.
2) En la conexión S_0 deseada, active el campo de opción **Conexión de centralita**.
3) Haga clic en **OK & Continuar**.

5.7.4.3 Cómo configurar el acceso individual RDSI

Requisitos previos

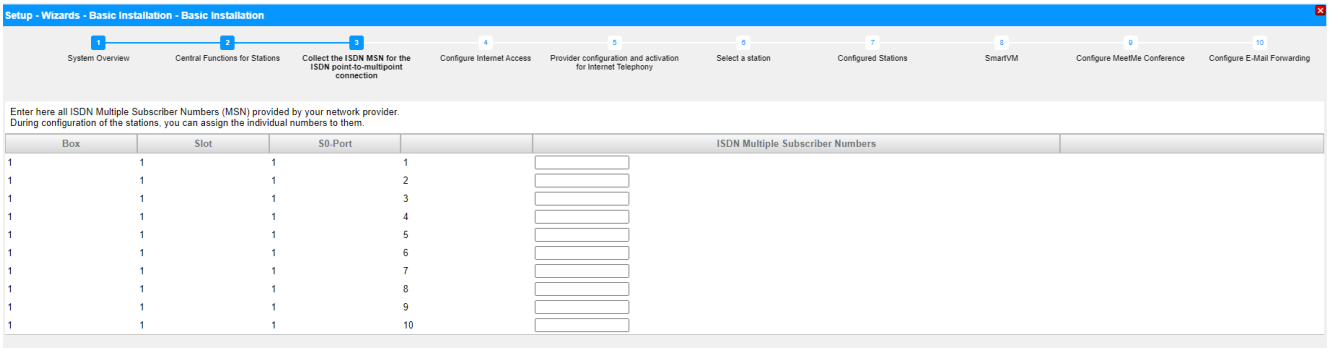
Se encuentra en la ventana **Configuración RDSI** del asistente **Configuración básica**.



Paso a paso

1) Para la conexión urbana RDSI, desmarque **Sin comunicación a través de lín. urbana RDSI (S0)**.
2) Junto a la conexión S**0** deseada, active el campo de opción **Acceso individual RDSI**.

3) Haga clic en **OK & Continuar**.



4) En la columna **Números de llamada múltiple RDSI** indique todos los números de teléfono (MSN) suministrados por su proveedor de red. Por cada conexión S_0 indique hasta 10 MSN. El número de conexiones S_0 depende del sistema de comunicación y de los módulos utilizados, en su caso.
5) Haga clic en **OK & Continuar**.

5.7.4.4 Cómo desactivar la configuración RDSI

Requisitos previos

Se encuentra en la ventana **Configuración RDSI** del asistente **Configuración básica**.

Paso a paso

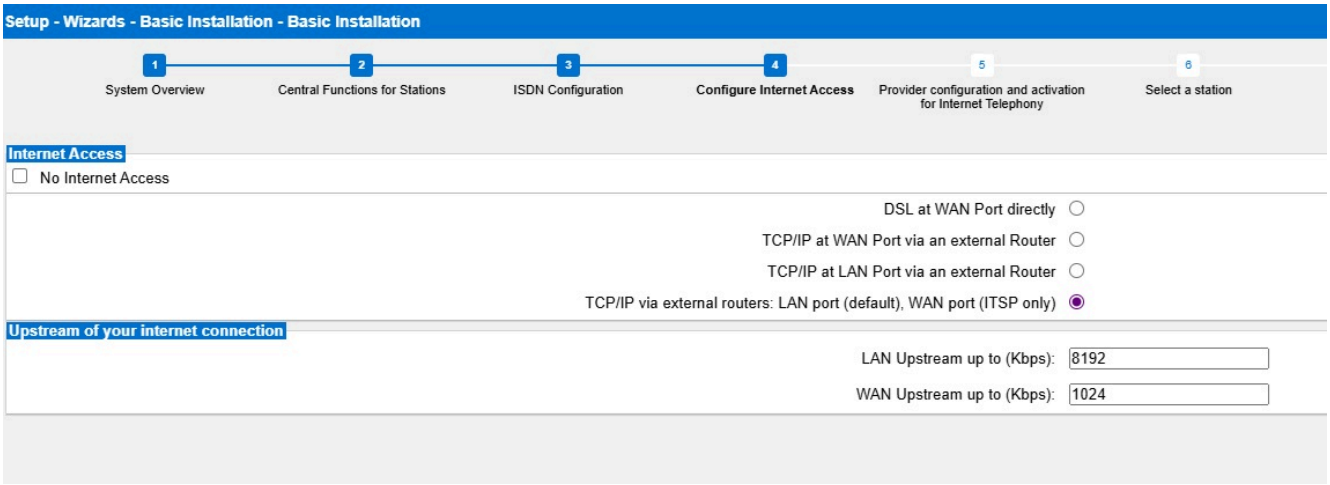
1) Desactive **Sin telefonía lín. urbana RDSI (S0)**.

> **Nota:** También se pueden realizar llamadas a través de un ITSP (Internet Telephony Service Provider), véase Telefonía Internet.

2) Clic **OK & Cont**.

5.7.5 Acceso a Internet

La ventana **Configurar acceso a Internet** se puede utilizar para configurar el acceso a Internet.



La configuración del acceso a Internet en el WBM depende de si la conexión a Internet ya se ha configurado en un enrutador externo o si se produce a través de un módem de Internet y, por lo tanto, debe configurarse en el WBM.

Sólo se puede seleccionar una de las opciones enumeradas aquí.

- Acceso a Internet a través de un módem de Internet (**DSL en el puerto WAN directamente**)

  Desea operar el sistema de comunicación directamente en un módem de Internet (DSL, cable, UMTS ...). OpenScape Business tiene el enrutador de Internet integrado. Introduzca los datos de acceso del proveedor de servicios de Internet (ISP) directamente en el sistema de comunicación y utilice el puerto WAN del sistema de comunicación.



Tiene las siguientes opciones:

– **Acceso a Internet a través de un ISP preconfigurado**
– **Acceso a Internet a través de PPPoE ISP estándar**
– **Acceso a Internet a través del estándar ISP PPTP**

Si su ISP no figura entre los ISPs preconfigurados, utilice el ISP predeterminado PPPoE o PPTP.

- Acceso a Internet a través de un enrutador de Internet externo

  Desea operar el sistema de comunicación en un enrutador de Internet externo. El proveedor de servicios de Internet ya está configurado en el enrutador de Internet.

  Tiene las siguientes opciones:

  – **Acceso a Internet a través de un enrutador de Internet externo en el puerto WAN**

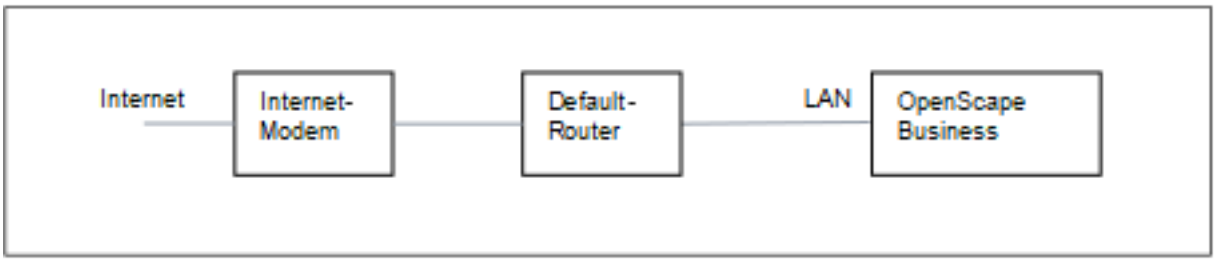
    (**TCP/IP en el puerto WAN a través de un enrutador externo**)



    Para ello, utilice el puerto WAN del sistema de comunicación. OpenScape Business conoce el enrutador de Internet o funciona como un cliente DHCP. Esta opción se puede utilizar si el enrutador de Internet está ubicado en otro segmento de red y tiene su propio servidor DHCP.

  – **Acceso a Internet a través de un enrutador de Internet externo en el puerto LAN**

    (**TCP/IP en el puerto LAN a través de un enrutador externo**)

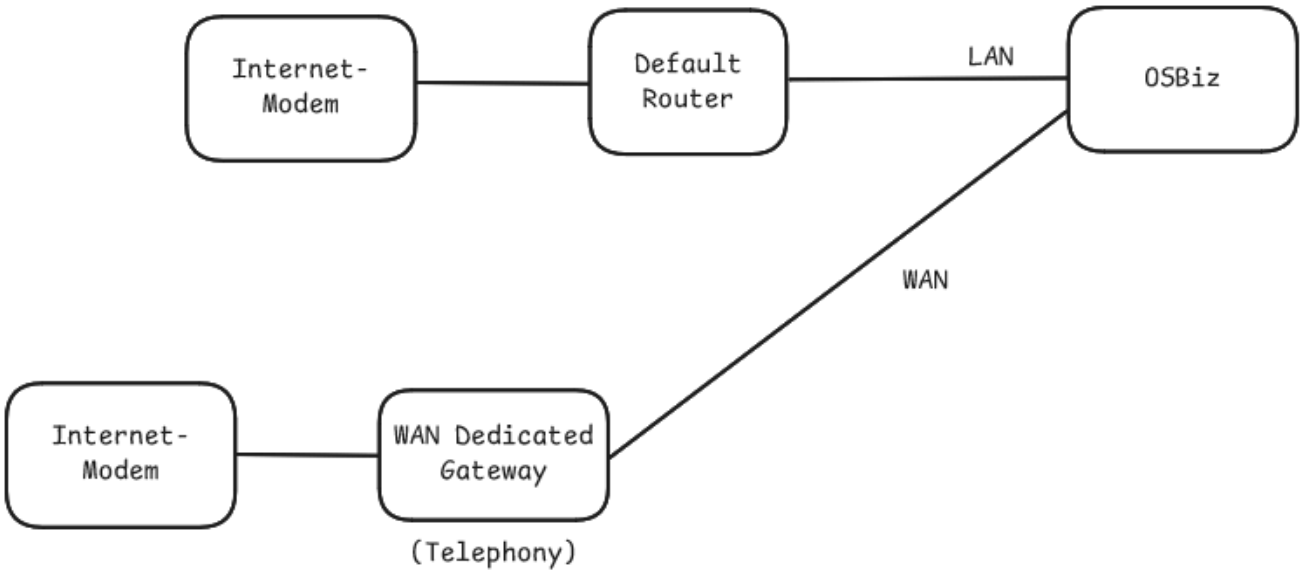


    Para ello, utilice el puerto LAN del sistema de comunicación. OpenScape Business solo conoce el enrutador predeterminado y no la infraestructura subyacente. Para activar la conexión al enrutador de Internet, es

necesario dar a conocer al sistema de comunicación la dirección IP del enrutador predeterminado y la del servidor DNS.

– **Acceso a Internet a través de un enrutador de Internet externo en el puerto LAN**

(**TCP/IP en el puerto LAN/WAN a través de un enrutador externo con puerto WAN dedicado a ITSP**)



Para ello, se utiliza el puerto LAN del sistema de comunicación, mientras que el puerto WAN está dedicado al ITSP. OpenScape Business solo conoce el enrutador predeterminado y no la infraestructura subyacente. Para activar la conexión al enrutador de Internet, es necesario dar a conocer al sistema de comunicación la dirección IP del enrutador predeterminado y la del servidor DNS.

- Desactivar el acceso a Internet (configuración predeterminada)

  No quiere utilizar Internet.

5.7.5.1 Cómo configurar el acceso a Internet a través de un router de Internet externo mediante la conexión LAN

Requisitos previos

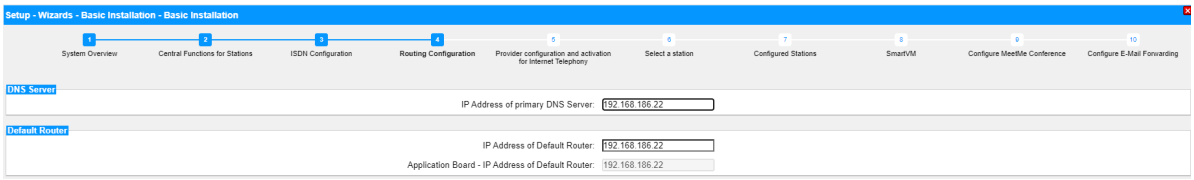
El sistema de comunicación debe conectarse con la LAN de clientes mediante la interfaz LAN "LAN". La conexión no se puede realizar a través de la conexión WAN porque está desactivada.

Se encuentra en la ventana **Configurar Acceso a Internet** del asistente **Configuración básica**.

Paso a paso

1) Desactive la casilla de verificación **Sin acceso a Internet**.

2) Active el botón de opción **TCP/IP en puerto LAN a través de un router externo**, introduzca una velocidad de subida para su conexión de Internet en el campo **Flujo saliente hasta (Kbit/s)** y haga clic en **OK y Continuar**.



3) En el campo **Dirección IP del servidor DNS**, introduzca la dirección IP del servidor DNS local (por ejemplo, router Internet) o del servidor DNS de Internet (por ejemplo, para Telefonía Internet).
4) En el campo **Dirección IP del router estándar** introduzca la dirección IP del router Internet externo.
5) Haga clic en **OK & Continuar**.

5.7.5.2 Cómo configurar el acceso a Internet a través de un router de Internet externo mediante la conexión WAN

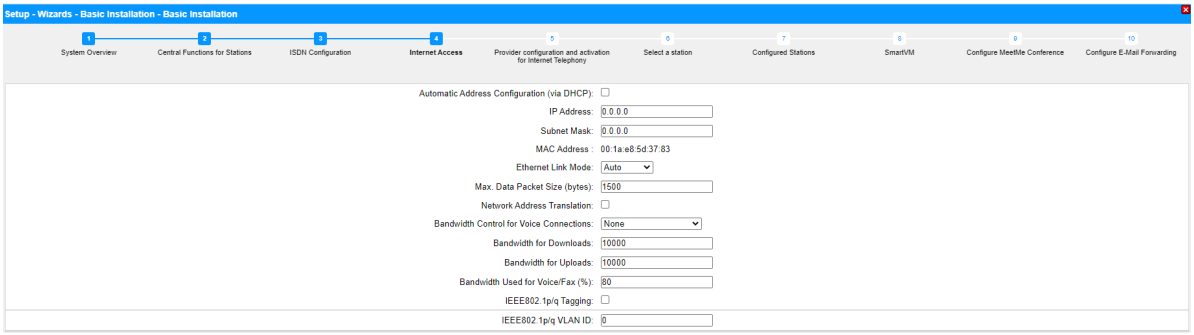
Requisitos previos

El sistema de comunicación tiene que estar conectado con el segmento de la LAN la LAN de clientes en el que se encuentra el router Internet mediante la interfaz LAN "WAN".

Se encuentra en la ventana **Configurar Acceso a Internet** del asistente **Configuración básica**.

Paso a paso

1) Desactive **Sin acceso a Internet**.
2) Active la opción **TCP/IP en interfaz WAN a través de un router externo** y haga clic en **OK & Continuar**.



3) Si los datos específicos de red de la interfaz WAN se deben obtener de un servidor DHCP ya activo:
   a) Active **Configuración de dirección automática (con DHCP)**.
   b) Active la casilla de verificación **Aceptar dirección IP del router estándar**.
   c) Si es necesario, active **Aceptar dirección IP del servidor DNS**.
   d) Si es necesario, active **Aceptar dirección IP del servidor SNTP**.

4) Si desea asignar a la interfaz WAN una dirección IP fija:
   a) Desactive la casilla de verificación **Configuración de dirección automática (con DHCP)**.
   b) Introduzca la **Dirección IP** y la **Máscara de red** deseadas de la interfaz WAN.
5) Activ **Trad dir red (NAT)**.
6) Si también quiere utilizar telefonía Internet, en la lista desplegable **Control ancho banda para conex. voz**, seleccione la entrada **Sólo carga** o **Carga y descarga**, según sus necesidades. Si el ancho de banda de la descarga es alto y el de carga es bajo, el control de ancho de banda sólo se debería activar para la dirección de carga, garantizando así que el ancho de banda de descarga reservado para la transmisión de voz no sea innecesariamente elevado.
7) En los campos **Ancho de banda para descargas** y **Ancho de banda para cargas**, seleccione el ancho de banda en Kbits/s para la descarga o para la carga. El valor le será suministrado por su ISP.
8) Clic **OK & Cont**.

5.7.5.3 Cómo configurar el acceso a Internet a través de un ISP preconfigurado

Requisitos previos

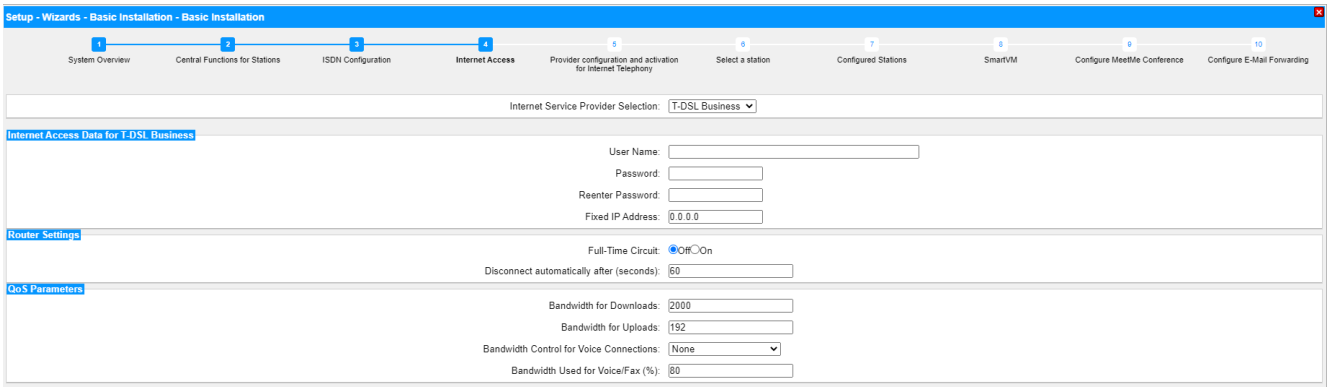
Se encuentra en la ventana **Configurar Acceso a Internet** del asistente **Configuración básica**.

Dispone de los datos de acceso a Internet de su ISP (p. ej. identificación de usuario, contraseña y ancho de banda de carga y descarga).

Opcional: Los datos de una cuenta DynDNS están a su disposición (nombre, contraseña, nombre de host, nombre de dominio del proveedor DynDNS)

Paso a paso

1) Deshabilite **Sin acceso a Internet** casilla de verificación.
2) Active el botón de radio **DSL directamente en el puerto WAN de la placa base** y haga clic en **Aceptar & Siguiente**.



3) En la lista desplegable **Selección de ISP**, seleccione su proveedor de servicios de Internet.
4) En la sección **Datos de acceso a Internet para**, indique los datos de acceso que le ha entregado su ISP. Los campos de este área dependen

del proveedor. Al introducir los datos, compruebe el uso de mayúsculas y minúsculas.

5) En la sección **Ajustes de router**, y en **Conexión permanente**, seleccione una de ambas opciones en función de su modelo de tarifas:

- Si tiene una tarifa plana como modelo de tarifas, active el campo de opción **Act.**. En el campo **Desconexión forzosa a las (hrs:min)**, establezca la hora en la que se desconectará la conexión a Internet (por ejemplo, 01:30). A esa hora no se deberían intercambiar datos con Internet (p. ej., descargas de software o telefonía por Internet).
- Si tiene un modelo de tarifa basado en tiempo, active la casilla de verificación **Desact.**. En el **Desconectarse automáticamente después de (segundos)**, ingrese la duración de la inactividad después de la cual se debe interrumpir la conexión (por ejemplo, 60 segundos).

6) En la sección **Parámetros QoS**, ajuste estos valores:

a) En los campos **Ancho de banda para descargas** y **Ancho de banda para cargas**, seleccione el ancho de banda en Kbit/s para la descarga o para la carga. El valor le será suministrado por su ISP.

b) Si también quiere utilizar telefonía Internet, en la lista desplegable **Control ancho banda para conex. voz**, seleccione la entrada **Solo carga** o **Carga y descarga**, según sus necesidades. En el campo **Ancho de banda utilizado para voz/fax (%)**, ingrese cuánto ancho de banda se reservará para las conexiones de voz y fax como valor porcentual (valor predeterminado: 80%).

7) Haga clic en **Aceptar & Siguiente**. Es conducido a la ventana **Configurar cuenta DynDNs**.

8) Si desea utilizar la red privada virtual o el acceso remoto y no tiene una dirección IP estática pública, debe haber solicitado y configurado una cuenta DynDNS (por ejemplo, en dyndns.org).

a) Si su proveedor DynDNS aparece en la lista desplegable **Nombre dominio**, selecciónelo (p.ej. dyndns.org).

b) Si su proveedor DynDNS no aparece en la lista desplegable **Nombre dominio**, active la casilla de verificación **Dominio definido por el usuario**. En el campo **Nombre dominio**, introduzca el proveedor DynDNS deseado y en el campo **URL de actualización**, la URL de actualización del proveedor DynDNS. La estructura de la URL depende del proveedor DynDNS. Además, hay que indicar parámetros específicos del cliente (en el ejemplo, marcados en *cursiva*).

```
http://www.anydns.info/update.php?
user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>
```

c) Introduzca el **Nombre de usuario** y **Contraseña** de su cuenta DynDNS.

d) En el campo **Nombre host**, indique el nombre de host suministrado por el proveedor DynDNS sin el nombre de dominio, por ejemplo, mihost. Su nombre de dominio completo será, por ejemplo, mihost.dyndns.org.

e) Compruebe la cuenta DynDNS con **Prueba de conexión**.

f) Si la comprobación termina con éxito, haga clic en **Aceptar**.

g) Haga clic en **Aceptar & Siguiente**.

9) Si tiene una dirección IP estática pública o desea utilizar la red privada virtual o el acceso remoto, haga clic en **Sin DynDNS**.

10) Haga clic en **Aceptar & Siguiente**.

5.7.5.4 Cómo configurar el acceso a Internet a través del PPPoE ISP estándar

Requisitos previos

Se encuentra en la ventana **Configurar Acceso a Internet** del asistente **Configuración básica**.

Dispone de estos datos de acceso a Internet de su ISP:

Campo	Descripción	Valor del ISP
Parámetros IP (solo con dirección IP fija)		
Dirección IP remota de la conexión PPP	Dirección IP del servidor de su ISP.	
Dirección IP local de la conexión PPP	Dirección IP suministrada por el proveedor de servicios de Internet.	
Autenticación (por PAP o CHAP). Hoy en día PAP a penas se utiliza porque la autenticación no está codificada.		
Nombre usuario PPP	Nombre de usuario para la conexión PPP, suministrado por el ISP.	
Modo autenticación PAP	Modo de autenticación para la conexión PPP sobre PAP: **Cliente PAP**, **Anfitrión PAP** o **No utilizado**.	
Clave PAP	Contraseña para la autenticación por PAP, suministrada por el ISP.	
Modo autentificación CHAP	Modo de autenticación para conexión PPP vía CHAP: **Cliente CHAP**, **Anfitrión CHAP**, **Cliente y host CHAP** o **No utilizado**.	
Clave CHAP	Contraseña para la autenticación por CHAP, suministrada por el ISP.	
Parámetros QoS de la interfaz		
Ancho de banda para descargas	Valora el ancho de banda en Kbit/seg para la descarga desde el ISP.	
Ancho de banda para cargas	Valora el ancho de banda en Kbit/seg para la carga al ISP.	

Opcional: Los datos de una cuenta DynDNS están a su disposición (nombre, contraseña, nombre de host, nombre de dominio del proveedor DynDNS)

Paso a paso

1) Deshabilite **Sin acceso a Internet** casilla de verificación.
2) Active el botón de opción **DSL en el puerto WAN directamente** y haga clic en **OK & Siguiente**.
3) En la lista desplegable **Selección de ISP** seleccione el tipo ISP estándar **PPPoE de proveedor**.
4) En el área **Parámetros IP** active la casilla de verificación **Parámetros IP** solamente si el ISP requiere un ajuste. En tal caso, en los campos **Dir. IP colateral de conex. PPP**, **Dirección IP local de conex. PPP** y **Long. máx. paquetes datos (bytes)** indique los valores que le hayan

sido suministrados por su ISP. En la lista desplegable **Negociación dir. IP** seleccione la entrada **Utilizar dirección IP config.**.

5) En la sección **Ajustes de router**, y en **Conexión permanente**, seleccione una de ambas opciones en función de su modelo de tarifas:

- Si tiene una tarifa plana como modelo de tarifas, active el campo de opción **Act.**. En el campo **Desconexión forzosa a las (hrs:min)**, establezca la hora en la que se desconectará la conexión a Internet (por ejemplo, 01:30). A esa hora no se deberían intercambiar datos con Internet (p. ej., descargas de software o telefonía por Internet).
- Si tiene un modelo de tarifa basado en tiempo, active la casilla de verificación **Desact.**. En el **Desconectarse automáticamente después de (segundos)**, ingrese la duración de la inactividad después de la cual se debe interrumpir la conexión (por ejemplo, 60 segundos).

6) Los ajustes de la sección **Autenticación** dependen de si su ISP exige o no una autenticación por PPP.

- Autenticación requerida por el ISP: Asegúrese de que la casilla de verificación **Autenticación PPP** está habilitada. Indique como nombre de usuario PPP el nombre de acceso a Internet del ISP. El estándar habitual es el modo de autenticación **Cliente CHAP**.
- Autenticación no requerida por el ISP: Asegúrese de que la casilla de verificación Autenticación PPP esté desactivada.

7) Si desea utilizar NAT, en la sección **Traduc. dirección**, active la casilla de verificación **NAT** (activada de forma predeterminada).

8) En la sección **Parámetros QoS de la interfaz** establezca estos valores:

a) En los campos **Ancho de banda para descargas** y **Ancho de banda para cargas**, seleccione el ancho de banda en Kbit/s para la descarga o para la carga. El valor le será suministrado por su ISP.

b) Si también quiere utilizar telefonía Internet, en la lista desplegable **Control ancho banda para conex. voz**, seleccione la entrada **Solo carga** o **Carga y descarga**, según sus necesidades. En el campo **Ancho de banda utilizado para voz/fax (%)**, ingrese cuánto ancho de banda se reservará para las conexiones de voz y fax como valor porcentual (valor predeterminado: 80%).

9) Haga clic en **Aceptar & Siguiente**. Es conducido a la ventana **Configurar cuenta DynDNs**.

10) Si desea utilizar la red privada virtual o el acceso remoto y no tiene una dirección IP estática pública, debe haber solicitado y configurado una cuenta DynDNS (por ejemplo, en dyndns.org).

a) Si su proveedor DynDNS aparece en la lista desplegable **Nombre dominio**, selecciónelo (p.ej. dyndns.org).

b) Si su proveedor DynDNS no aparece en la lista desplegable **Nombre dominio**, active la casilla de verificación **Dominio definido por el usuario**. En el campo **Nombre dominio**, introduzca el proveedor DynDNS deseado y en el campo **URL de actualización**, la URL de actualización del proveedor DynDNS. La estructura de la URL depende del proveedor DynDNS. Además, hay que indicar parámetros específicos del cliente (en el ejemplo, marcados en *cursiva*).

```
http://www.anydns.info/update.php?
user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>
```

c) Introduzca el **Nombre de usuario** y **Contraseña** de su cuenta DynDNS.

d) En el campo **Nombre host**, indique el nombre de host suministrado por el proveedor DynDNS sin el nombre de dominio, por ejemplo, mihost. Su nombre de dominio completo será, por ejemplo, mihost.dyndns.org.
e) Compruebe la cuenta DynDNS con **Prueba de conexión**.
f) Si la comprobación termina con éxito, haga clic en **Aceptar**.
g) Haga clic en **Aceptar & Siguiente**.

11) Si tiene una dirección IP estática pública o desea utilizar la red privada virtual o el acceso remoto, haga clic en **Sin DynDNS**.

12) Haga clic en **Aceptar & Siguiente**.

5.7.5.5 Cómo configurar el acceso a Internet a través de un PPTP ISP estándar

Requisitos previos

Se encuentra en la ventana **Configurar Acceso a Internet** del asistente **Configuración básica**.

Dispone de estos datos de acceso a Internet de su ISP:

Campo	Descripción	Valor del ISP
Parámetros IP (solo con dirección IP fija)		
Dir. IP colateral de conex. PPP	Dirección IP del servidor de su ISP.	
Dirección IP local de conex. PPP	Dirección IP suministrada por el proveedor de servicios de Internet.	
Parámetros PPTP		
Dirección IP local de conex. control	Dirección IP suministrada por el proveedor de servicios de Internet para la conexión PPTP. El valor preestablecido es 10.0.0.140.	
Dirección IP colateral de conex. control	Dirección IP del servidor ISP para la conexión PPTP. El valor preestablecido es 10.0.0.138.	
Másc. red colateral para conex. control	Máscara de red suministrada por el proveedor de servicios de Internet para la conexión PPTP. El valor preestablecido es 255.255.255.248.	
Autenticación (por PAP o CHAP). Hoy en día PAP a penas se utiliza porque la autenticación no está codificada.		
Nombre usuario PPP	Nombre de usuario para la conexión PPP, suministrado por el ISP.	
Modo autenticación PAP	Modo de autenticación para la conexión PPP por PAP: **Cliente PAP**, **Host PAP** o **Sin utilizar**.	
Clave PAP	Contraseña para la autenticación por PAP, suministrada por el ISP.	

Campo	Descripción	Valor del ISP
Modo autentificación CHAP	Modo de autenticación para la conexión PPP por CHAP: **Cliente CHAP**, **Host CHAP**, **Cliente y host CHAP** o **Sin utilizar**.	
Clave CHAP	Contraseña para la autenticación por CHAP, suministrada por el ISP.	
Parámetros QoS de la interfaz		
Ancho de banda para descargas	Valora el ancho de banda en Kbit/seg para la descarga desde el ISP.	
Ancho de banda para cargas	Valora el ancho de banda en Kbit/seg para la carga al ISP.	

Opcional: Conoce los datos de una cuenta DynDNS (nombre, contraseña, nombre host, nombre de dominio del proveedor DynDNS)

Paso a paso

1) Desactive **Sin acceso a Internet**.
2) Active la opción **DSL directamente a interfaz WAN** y haga clic en **OK & Continuar**.
3) En la lista desplegable **Selección de ISP**, seleccione el tipo ISP estándar **PPTP de proveedor**.
4) En el área **Parámetros IP** active la casilla de verificación **Parámetros IP** solamente si el ISP requiere un ajuste. En tal caso, en los campos **Dir. IP colateral de conex. PPP**, **Dirección IP local de conex. PPP** y **Long. máx. paquetes datos (bytes)** indique los valores que le hayan sido suministrados por su ISP. En la lista desplegable **Negociación dir. IP** seleccione la entrada **Utilizar dirección IP config.**.
5) En la sección **Parámetros PPTP**, indique los valores suministrados por su ISP.
6) Si tiene un modelo de tarifa basado en tiempo, active la casilla de verificación **Modo reten. breve**. En el campo **Tiempo reten. breve (s)**, indique el tiempo de inactividad tras el cual deberá interrumpirse la conexión (por ejemplo, 60 segundos).
7) Los ajustes de la sección **Autenticación** dependen de si su ISP exige o no una autenticación por PPP.
   - El ISP solicita autenticación: asegúrese de que la casilla de verificación **Autenticación PPP** está activada. Indique como nombre de usuario PPP el nombre de acceso a Internet del ISP. Establezca la configuración PAP y CHAP siguiendo los ajustes suministrados por su ISP.
   - El ISP no solicita autenticación: asegúrese de que la casilla de verificación Autenticación PPP está desactivada.
8) Si desea utilizar NAT, en la sección **Traduc. dirección**, active la casilla de verificación **NAT** (activada de forma predeterminada).

9) En la sección **Parámetros QoS de la interfaz** establezca estos valores:

a) En los campos **Ancho de banda para descargas** y **Ancho de banda para cargas**, seleccione el ancho de banda en Kbit/s para la descarga o para la carga. El valor le será suministrado por su ISP.

b) Si también quiere utilizar telefonía Internet, en la lista desplegable **Control ancho banda para conex. voz**, seleccione la entrada **Solo carga** o **Carga y descarga**, según sus necesidades. En el campo **Ancho banda para conex. voz/fax (%)** indique, en valores porcentuales, cuánto ancho de banda va a reservarse para las conexiones de voz y fax (valor estándar: 80%).

10) Haga clic en **OK & Continuar**. Es conducido a la ventana **Configurar cuenta DynDNs**.

11) Si desea utilizar la red privada virtual o el acceso remoto y no tiene una dirección IP estática pública, debe haber solicitado y configurado una cuenta DynDNS (por ejemplo, en dyndns.org).

a) Si su proveedor DynDNS aparece en la lista desplegable **Nombre dominio**, selecciónelo (p.ej. dyndns.org).

b) Si su proveedor DynDNS no aparece en la lista desplegable **Nombre dominio**, active la casilla de verificación **Dominio definido por el usuario**. En el campo **Nombre dominio**, introduzca el proveedor DynDNS deseado y en el campo **URL de actualización**, la URL de actualización del proveedor DynDNS. La estructura de la URL depende del proveedor DynDNS. Además, hay que indicar parámetros específicos del cliente (en el ejemplo, marcados en *cursiva*).

`http://www.anydns.info/update.php?user=<`*`nombre usuario`*`>&password=<`*`contraseña`*`>&host=<`*`dominio`*`>&ip=<`*`dir ip`*`>`

c) Introduzca el **Nombre de usuario** y **Contraseña** de su cuenta DynDNS.

d) En el campo **Nombre host**, indique el nombre de host suministrado por el proveedor DynDNS sin el nombre de dominio, por ejemplo, mihost. Su nombre de dominio completo será, por ejemplo, mihost.dyndns.org.

e) Compruebe la cuenta DynDNS con **Prueba de conexión**.

f) Si la comprobación termina con éxito, haga clic en **Aceptar**.

g) Haga clic en **OK & Continuar**.

12) Si tiene una dirección IP estática pública o desea utilizar la red privada virtual o el acceso remoto, haga clic en **Sin DynDNS**.

13) Clic **OK & Cont**.

5.7.5.6 Cómo configurar el acceso a Internet a través de un enrutador de Internet externo sobre la LAN con un puerto WAN dedicado a ITSP

Requisitos previos

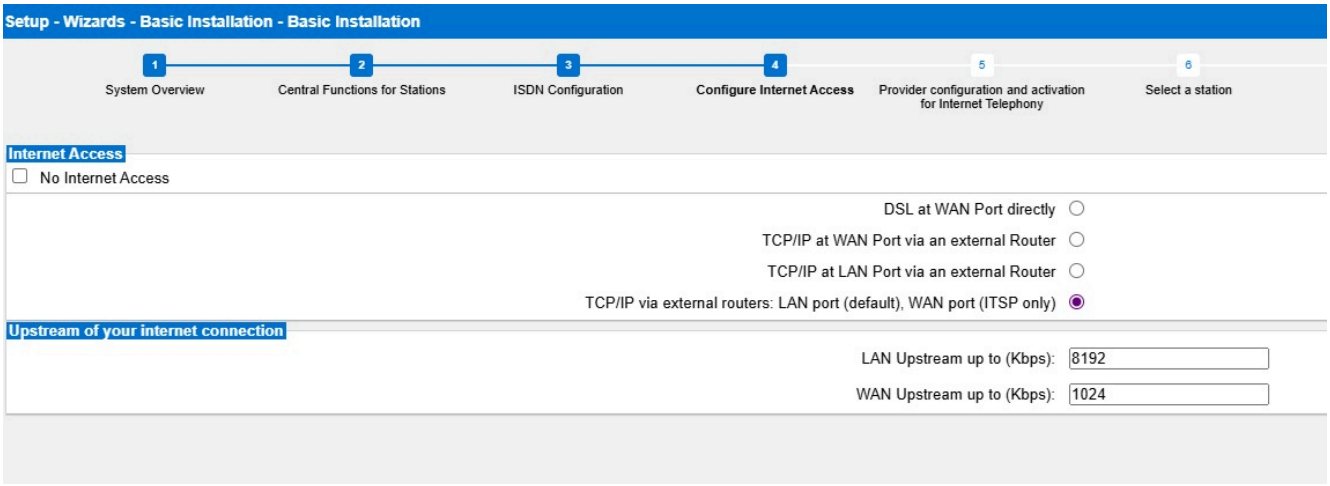
Se encuentra en la ventana **Configurar acceso a Internet** del asistente de **instalación básica.**

Esta función solo es aplicable a los ITSP que no requieren el uso de STUN en la configuración del proveedor.

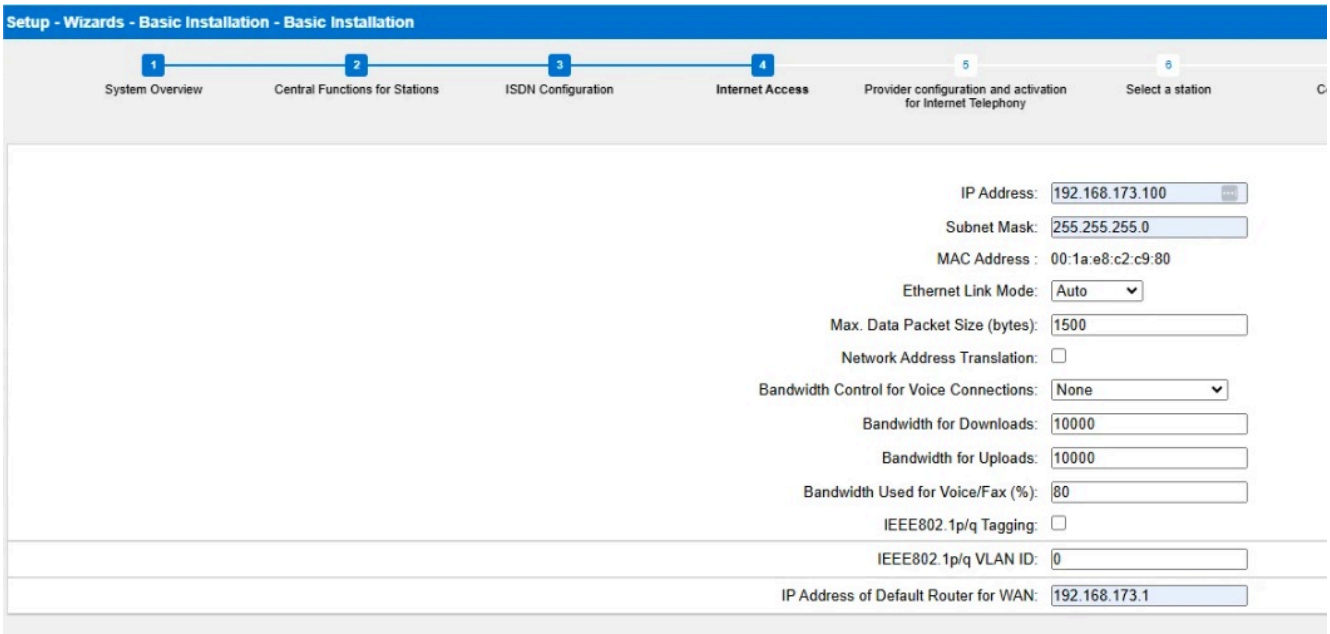
No es posible conectar dos ITSP idénticos (con el mismo registrador/proxy) simultáneamente a través de LAN y WAN.

Paso a paso

1) Deshabilite **Sin acceso a Internet** casilla de verificación.
2) Active el botón de opción **TCP/IP a través de enrutadores externos: Puerto LAN (predeterminado), puerto WAN solo para ITSP**.



3) Configure el valor máximo de Kbps de subida para cada interfaz en **LAN de Subida hasta (Kbps)** y **WAN de subida hasta (Kbps)**.
4) Haga clic en **Aceptar & Siguiente**.
5) Ingrese la configuración IP del puerto WAN y además la dirección IP del enrutador predeterminado para el puerto WAN.



6) Haga clic en **Aceptar & Siguiente**.

5.7.5.7 Cómo desactivar el acceso a Internet

Requisitos previos

Se encuentra en la ventana **Configurar Acceso a Internet** del asistente **Configuración básica**.

Paso a paso

1) Desactive la casilla de verificación **Sin acceso a Internet**.
2) Clic **OK & Cont**.

5.7.6 Telefonía Internet

En la ventana **Configuración y activación de proveedor para telefonía Internet** puede configurar la Telefonía Internet. Puede configurar ITSP (Internet Telephony Service Providers) nuevos o preconfigurados. Por cada ITSP se pueden configurar una o varias cuentas. Puede haber activos hasta 8 ITSP de manera simultánea.

Tiene las siguientes opciones:

- **Configurar ITSP preconfigurados**

  Puede utilizar plantillas de ITSP predefinidas. En estas plantillas se registran los números de acceso y los números de teléfono propios y, a continuación, se activan.
- **Configurar ITSP nuevos**

  También puede añadir y activar ITSP nuevos.

  Configurar un nuevo ITSP solo es necesario en contadas ocasiones y es un proceso complejo. Por ello, esta opción no se describe en la instalación inicial. Encontrará información más precisa en el capítulo Configuración de un ITSP.
- **Desactivar telefonía Internet**

  Puede desactivar la telefonía Internet.

Nota:

En Internet, en la **wiki para expertos en Internet** (*OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*, puede consultar ejemplos de configuración.

Asignación de los números de teléfono de ITSP

- En las **conexiones de extensión de telefonía por Internet**, el ITSP proporciona números de teléfono individuales (p.ej. 70005555, 70005556, etc.). Estos números se asignan de forma manual a los números de teléfono internos de las extensiones.
- En las **conexiones de centralita de telefonía por Internet**, el ITSP proporciona un área de números de teléfono (p.ej. de (+49) 89 7007-100 a (+49) 89 7007-147). Los números de teléfono del área se asignan de forma manual a los números de teléfono internos de las extensiones.

Los dos tipos de conexión se pueden combinar.

Como alternativa, para ambos tipos de conexión, en la configuración de las extensiones se pueden registrar los números de teléfono del ITSP como números de marcación directa de las extensiones.

Número de llamada Interno	Nombre	Marcación directa
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

Los números de teléfono del ITSP resultan del número de teléfono de centralita configurado (p.ej. código de país 49) y de los números de marcación directa registrados en formato largo. Esto supone ciertas ventajas en la evaluación de la marcación y la gestión de llamadas, también en una interred. Así, por ejemplo, la conexión ITSP tiene capacidad de marcación directa a otro nodo.

En este caso, solo se puede establecer otra conexión de línea urbana mediante RDSI con restricciones (útil por ejemplo para llamadas de emergencia).

5.7.6.1 Cómo configurar un ITSP predefinido

Requisitos previos

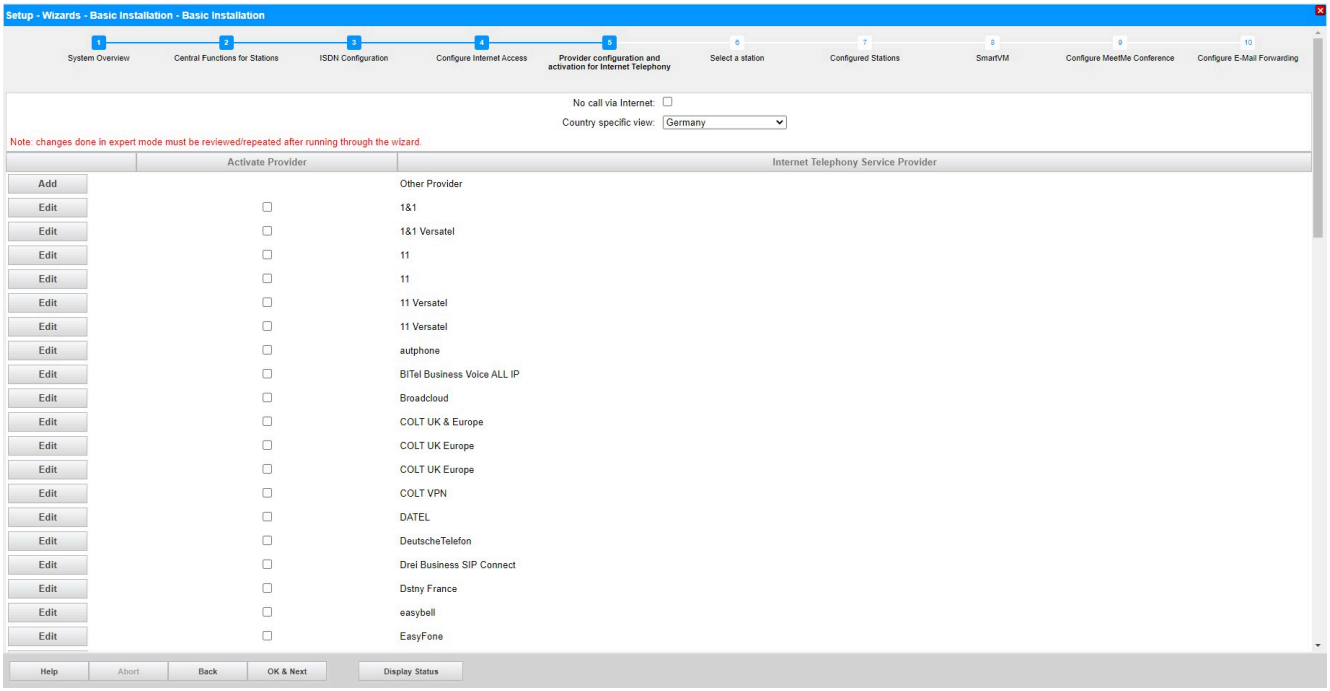
Se encuentra en la ventana **Configuración y activación de proveedor para telefonía Internet** del asistente **Configuración básica**.

La conexión a Internet está lista para el servicio.

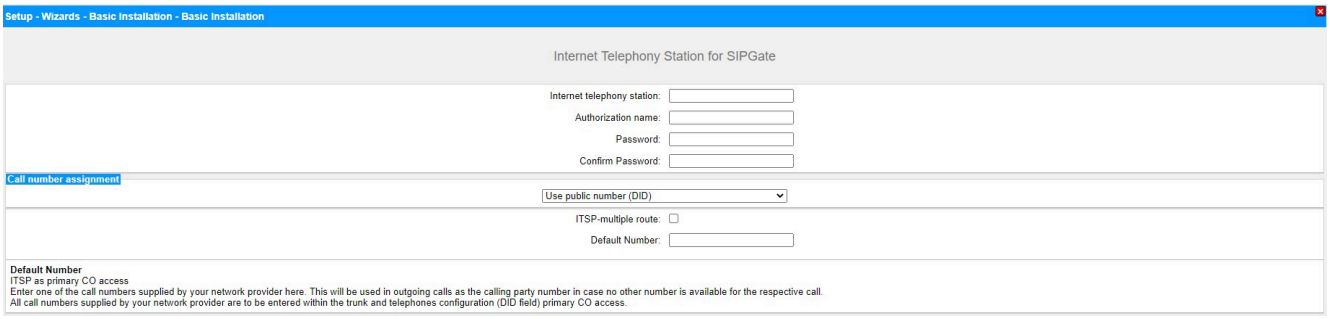
Dispone de los datos de acceso a Internet de su ITSP (p. ej. identificación de usuario, contraseña, números de teléfono de las extensiones de telefonía Internet).

Paso a paso

1) Borre la casilla de verificación **No hay llamada vía Internet**. Se muestra una lista de los ITSP disponibles en función del país. La lista contiene el ITSP predefinido para el país seleccionado y el ITSP ya creado (si lo hay).



2) Si desea modificar el país preestablecido, en la lista desplegable **Vista específica de país** seleccione el país deseado. Se muestran los ITSP disponibles para el país seleccionado.
3) Si es necesario, haga clic en **Mostrar estado**, para consultar qué ITSP están ya activados y qué extensiones de telefonía Internet están configuradas para cada uno de los ITSP. Se pueden activar, como máximo, 8 ITSP. Haga clic en **Aceptar** cuando esté terminado.
4) En la línea del ITSP correspondiente, haga clic en **Editar** para configurar un ITSP predefinido.
5) Active la casilla de verificación **Activar proveedor**.
6) Haga clic en **Aceptar & Siguiente**.
7) Haga clic en **Agregar** para configurar sus cuentas ITSP con los números de telefonía Internet correspondientes. Los campos que aparecen dependen del proveedor.



8) En el campo **Extensión de telefonía por Internet**, introduzca los datos de acceso de su cuenta. Los datos le son suministrados por su ITSP. En

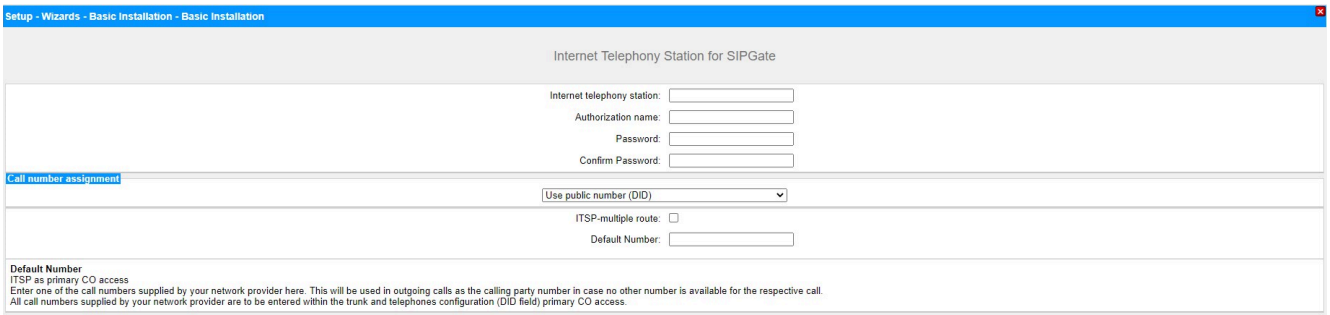
función del ITSP se utilizarán aquí distintas denominaciones (por ejemplo, Usuario SIP, ID SIP, etc.

9) En el campo **Nombre de autorización**, introduzca el nombre de autorización. Los datos le son suministrados por su ITSP. Si no ha recibido ningún nombre de autorización, indique los mismos datos en **Extensión de telefonía por Internet**.

10) En los campos **Nueva contraseña** y **Repetir clave** introduzca la contraseña que le ha suministrado el ITSP. En función del ITSP se utilizarán aquí distintas denominaciones (por ejemplo, Contraseña, Contraseña SIP, etc.)

11) Asignación de números de teléfono de telefonía por Internet - Opción 1:

Número de teléfono público (DuWa): los números de telefonía por Internet de su conexión de extensión de telefonía por Internet o de la conexión de sistema de telefonía por Internet no se registran aquí con la configuración de ITSP, sino en la configuración de extensión, en los campos **Marc. dir.**.



a) En el área **Asignación de números de teléfono**, seleccione el campo de opción **Número de teléfono público (DuWa)**.

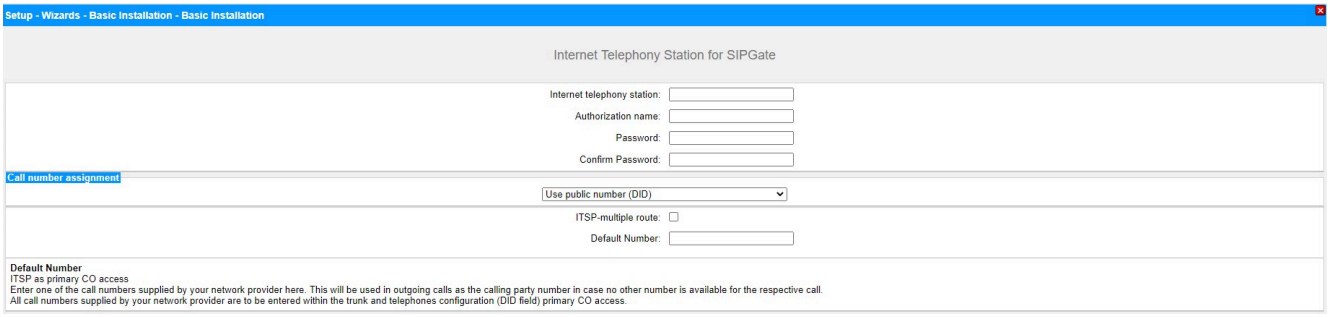
b) En **Número predeterminado**, ingrese el número de teléfono que se utilizará para las llamadas salientes cuando no haya ningún número DID de la persona que llama disponible.

c) Si su ITSP admite la prestación "Mobile Extension (MEX)", en **Número MEX** introduzca el número MEX que le haya proporcionado el ITSP (8 posiciones, solo números).

12) Asignación de números de teléfono de telefonía por Internet - Opción 2:

Usar número interno (CalIno) / Entradas individuales: Tiene una conexión a una estación de telefonía por Internet y ha recibido números de llamada individuales como números de teléfono de telefonía por Internet

(p. ej. 70005555, 70005556,...). A continuación, asigne estos números a los números de teléfono internos de las extensiones.



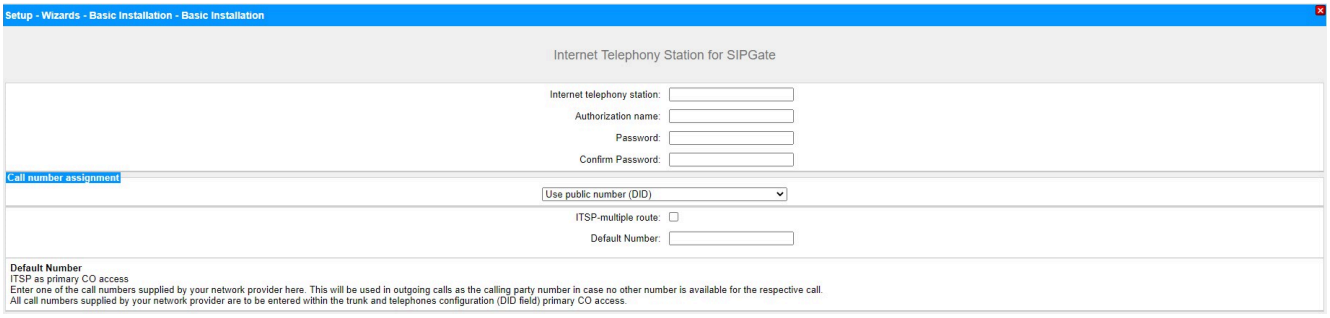
a) En el área **Asignación de números de teléfono**, seleccione el campo de opción **Utilizar número interno (n.º llamada)/Entradas individuales**.

b) En el área **Números de llamada de extensión de telefonía DSL**, y en el campo junto al botón **Agregar**, introduzca un número de teléfono de telefonía Internet que le haya sido comunicado por el proveedor de servicios de telefonía por Internet y haga clic en **Agregar**.

c) Si desea asignar a la cuenta más números de telefonía Internet, repita el paso b).

13) Asignación de números de teléfono de telefonía por Internet - Opción 3:

Usar número interno (CalIno) / Entrada de rango: Tiene una conexión de centralita de telefonía por Internet y ha recibido un intervalo de números de teléfono como números de teléfono de telefonía Internet, por ejemplo (+49) 89 7007-100 a (+49) 89 7007-147. A continuación, asigne los números de llamada del intervalo de números de llamada a los números de llamadas internas de los suscriptores.



a) En el área **Asignación de números de teléfono**, seleccione el campo de opción **Utilizar número interno (n.º llamada)/Intervalo**.

b) En **Número de llamada del sistema (prefijo)** introduzca el número de teléfono del sistema.

c) En los campos **Rango de marcación directa de** y **hasta** indique el rango de marcación directa deseado para la extensión de telefonía por Internet. Por defecto están registrados los valores 100 - 147.

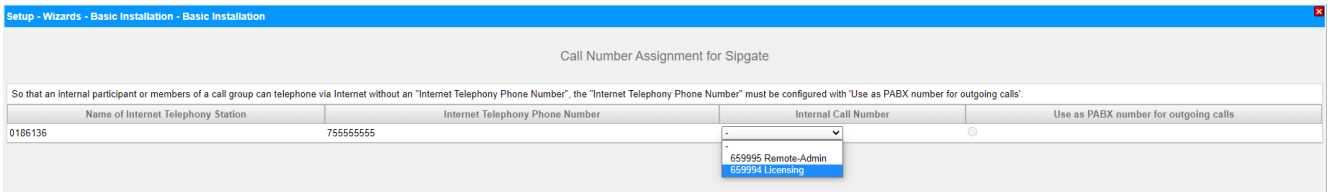
14) Haga clic en **Aceptar & Siguiente**.

15) Si desea configurar más cuentas con los números de telefonía Internet correspondientes, repita los pasos del 7 al 14.

16) Haga clic en **Aceptar & Siguiente**. Verá un resumen con los números de teléfono de telefonía Internet asignados y a qué cuentas lo están.

17) Asigna todos los números de telefonía por Internet a un número de teléfono interno de una extensión.

No es necesario dar este paso si para asignar los números de telefonía por Internet ha seleccionado la opción 1. En este caso, la asignación se realiza en la configuración de las extensiones, en el campo **DuWa**.



a) En la línea correspondiente de la lista desplegable **N.° llam. interno** seleccione un número de teléfono interno.

b) Si desea permitir que extensiones sin número de telefonía Internet o que los miembros de un grupo de llamadas realicen llamadas telefónicas externas por Internet, active el campo de opción **Utilizar como número de llamada del sistema saliente**. El campo de opción solo puede estar activado en un único número de telefonía Internet.

18) Haga clic en **Aceptar & Siguiente**. Aquí verá de nuevo la lista de los ITSP predefinidos y añadidos. Los ITSP activados aparecen marcados en la columna **Activar proveedor** con un signo de verificación. Con **Reiniciar ITSP** puede registrar de nuevo ITSP ya activado si hay problemas de conexión

19) Haga clic en **Aceptar & Siguiente**.

20) En el campo **Flujo saliente hasta (kbps)**, introduzca el valor de la velocidad de carga de su conexión a Internet. No debe confundirse con la velocidad de descarga.

Nota: En el campo **Cantidad de llamadas telefónicas Internet simultáneas** se indica el número de llamadas telefónicas Internet que puede realizar simultáneamente. Si la carga de red tiene efectos negativos en la calidad de las llamadas, reduzca el número.

Para obtener más información sobre la cantidad de llamadas simultáneas por Internet, consulte Restricción del número de llamadas simultáneas por ITSP en la página 842.

---

21) Haga clic en **Aceptar & Siguiente**.

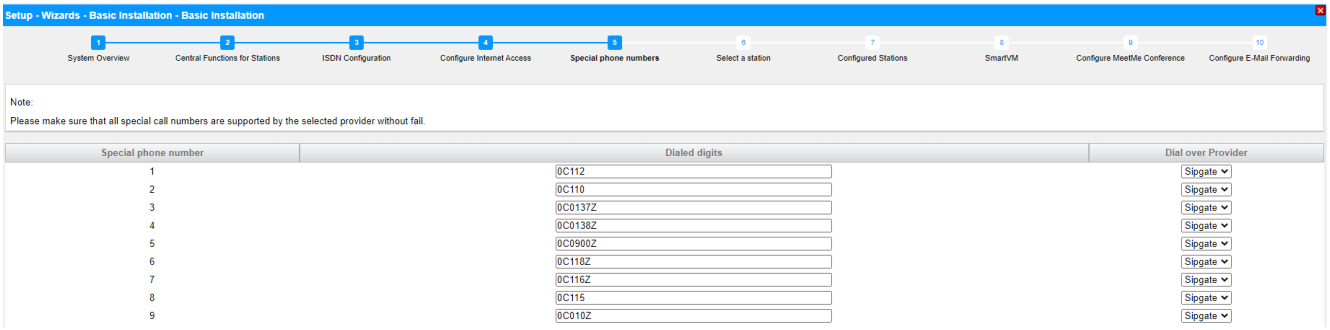
22) Si en la configuración de su acceso a Internet todavía no ha activado la conexión permanente, podrá hacerlo aquí. Sin conexión permanente no se pueden recibir llamadas a través de Internet. Si la conexión permanente ya está configurada, no aparecerán los campos descritos en los puntos de a) a c).

a) En **Conexión permanente**, active el campo de opción **Activado**.

b) En el campo **Desconexión Forzada a las (hora:min)**, introduzca la hora a la que se desactivará la conexión a Internet (p. ej., 04:59).

c) Haga clic en **Aceptar & Siguiente**.

23) En la columna **Cifras marcadas** introduzca los números de teléfono especiales deseados.



Son válidas estas entradas de número de teléfono:

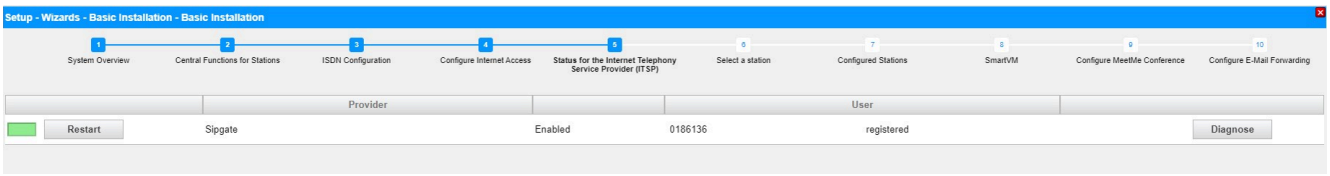
- 0 a 9: dígitos permitidos
- -: Separador de campos
- X: Cualquier dígito del 0 al 9
- N: Cualquier dígito del 2 al 9
- Z: Siguen, hasta el final de la marcación, uno o varios dígitos
- C: Tono de marcado simulado (se puede ingresar hasta tres veces)

24) En la columna **Marcar a través de proveedor** seleccione si el número de teléfono especial se marcará a través de RDSI o a través de un ITSP. Solo aparecen los ITSP activos.

Nota: Asegúrese de que siempre se pueden marcar los números de teléfono de emergencia. Si desea que los números de teléfono de emergencia se marquen a través de un ITSP, el proveedor debe admitir la función.

---

25) Haga clic en **Aceptar & Siguiente**. Se muestra el estado de los ITSP.



Aparecen marcados en verde los ITSP configurados y en los que ya está registrado.

Aparecen marcados en naranja los ITSP configurados y en los que todavía no está registrado.

26) Haga clic en **Siguiente** seguido de **Finalizar**.

5.7.6.2 Cómo desactivar telefonía Internet

Requisitos previos

Se encuentra en la ventana **Configuración y activación de proveedor para telefonía Internet** del asistente **Configuración básica**.

Paso a paso

1) Deje activada **Sin telefonía a través de Internet**.

2) Haga clic **OK & Cont**.

5.7.7 Extensiones

En las ventanas **Seleccionar extensión - ...** configure las extensiones conectadas con el sistema de comunicación.

Para ello, siga este procedimiento:

1) Configurar extensiones RDSI

   Son extensiones RDSI, por ejemplo, teléfonos RDSI y equipos de fax RDSI. Solo puede configurar extensiones RDSI si ha configurado una interfaz S_0 como conexión S_0 interna.

2) Configurar extensiones analógicas

   Son extensiones analógicas, por ejemplo, teléfonos analógicos y equipos de fax analógicos.

3) Configurar extensiones UP0

   Extensiones UP0 son teléfonos del sistema como los OpenStage 60 T.

4) Configurar extensiones DECT

   Extensiones DECT son teléfonos DECT/Cordless. Solo puede configurar extensiones DECT si hay conectadas una o varias extensiones base Cordless y los teléfonos DECT están registrados en ella. La configuración de las extensiones base se realiza con el Manager E. Para obtener más información sobre la configuración de Cordless, véase Configuración de la solución Cordless integrada

5) Configurar extensiones IP y SIP

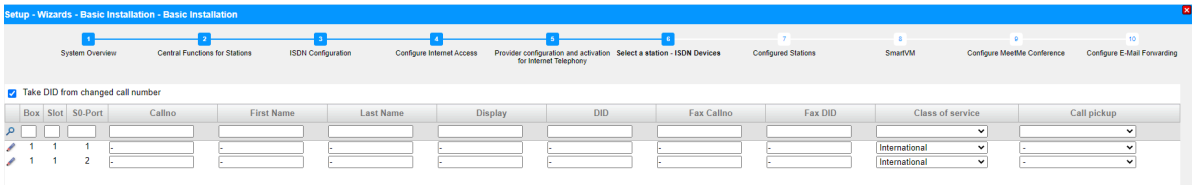
   Son extensiones IP y SIP, por ejemplo, teléfonos LAN y teléfonos WLAN.

5.7.7.1 Cómo configurar extensiones RDSI

Requisitos previos

Se encuentra en la ventana **Seleccionar extensión - Terminales RDSI** del asistente **Configuración básica**.

Las conexiones S_0 a las que están conectados los teléfonos RDSI, deben estar configuradas como conexiones S_0 internas.



Paso a paso

1) Si desea que el número de marcación directa de la extensión sea diferente al número de teléfono, en la línea de la extensión deseada, introduzca

el número de marcación directa de la extensión en el campo **Marcación directa**:

- Solo con conexión de centralita:

  Haga clic en el campo deseado e indique el número de marcación directa a través del teclado. El número de marcación directa puede ser idéntico al número de teléfono interno.
- Solo con acceso individual:

  Seleccione un MSN a través de la lista de selección. La extensión puede configurarse, por ejemplo, de forma interna a través de un número de teléfono interno 101 o de forma externa a través del MSN 654321.
- en una conexión de centralita y acceso individual:

  En el campo deseado, y a través de la lista desplegable, seleccione la entrada **xxx - editable** (xxx es el número de teléfono interno) e indique el número de marcación directa a través del teclado o seleccione un MSN a través de la lista desplegable.

2) En la línea de la extensión deseada, en **N.º llam**, indique el número de teléfono interno de la extensión. Puede utilizar el número de teléfono preestablecido o asignar otro todavía no ocupado.

3) En la línea de la extensión deseada, y en **Nombre**, introduzca un nombre con el formato `Apellidos, Nombre` o `Nombre Apellidos`.

Nota: El nombre puede incluir hasta 16 caracteres como máximo, pero no puede incluir diéresis ni caracteres especiales.

---

4) Si desea configurar un buzón de fax para la extensión (que se pueda utilizar, por ejemplo, con los clientes de UC **myPortal for Desktop** o **myPortal for Outlook**), siga este procedimiento:

a) En la línea de la extensión deseada, en el campo **Fax N.° llam**, introduzca el número de fax interno deseado con el que el usuario podrá recibir mensajes de fax internos.

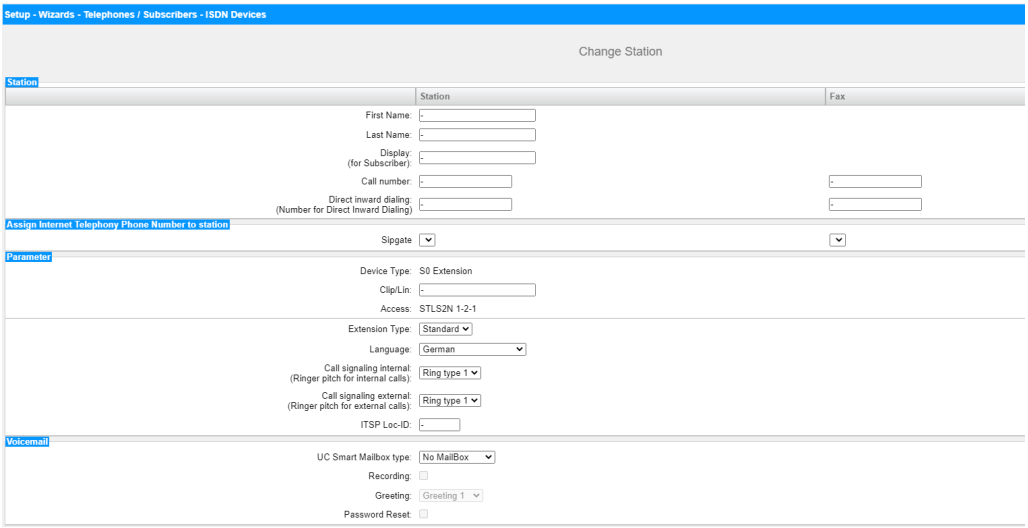
b) Si desea configurar un número de marcación directa para el buzón de fax, introduzca en la línea de la extensión deseada (en el campo **Marcación directa de fax**) el número de teléfono de fax externo deseado con el que la extensión podrá recibir mensajes de fax del exterior.

5) En la línea de la extensión deseada y utilizando la lista desplegable **Clase de servicio**, seleccione el grupo de clase de servicio deseado.

6) Para incluir las extensiones de un grupo de telecaptura, en la línea de la extensión deseada de la lista desplegable **Telecaptura de llamadas**, seleccione un grupo de telecaptura.

7) Los ajustes descritos en este paso solo se deben realizar si es necesario:

a) En la línea de la extensión RDSI deseada, haga clic en el símbolo en forma de lápiz **Editar**.



b) En **Clip/Lin** indique número teléfono (número de marcación directa o MSN) que aparecerá en el display del usuario llamado en lugar del número de teléfono en caso de llamada externa.

Nota: Esta prestación debe estar activada por el proveedor de red.

Nota: Se debe configurar al menos un número de marcación directa. De lo contrario, el sistema no tiene en cuenta el número CLIP del llamante, y el número de la llamada interna se formatea y se envía como número de llamante para la llamada externa.

---

c) En la lista desplegable **Tipo de ext.**, haga clic en el tipo de terminal RDSI.

d) En la sección **Mar. dir. para telefonía Internet**, utilice la lista desplegable para seleccionar un número de marcación directa. Por cada ITSP activo aparece una lista desplegable.

Nota: No se puede ver el campo **Marc. dir. para telefonía Internet** si la telefonía Internet no está configurada o no hay activado ningún ITSP.

---

e) En la lista desplegable **Señalización de llamadas internas**, asigne a la extensión una de las ocho señalizaciones de llamada acústicas para llamadas internas posibles. De esta forma, la extensión enviará a otras

extensiones internas un tono de llamada modificado que le permite ser reconocida por dichas extensiones (Estándar: Tipo de llamada 1).

f) En la lista desplegable **Señalización de llamadas externas**, asigne a la extensión una de las tres señalizaciones de llamada para llamadas externas posibles (Estándar: Tipo de llamada 1).

g) Haga clic en **OK & Continuar**.

h) Si es necesario, modifique los flags de extensión. Para consultar una descripción de los flags de extensión, véase Extensión > Extensión > Parámetros de extensión.

i) Haga clic en **OK & Continuar**.

8) Si desea configurar más extensiones RDSI, haga clic en **Guardar datos** y repita los pasos 1 a 7.

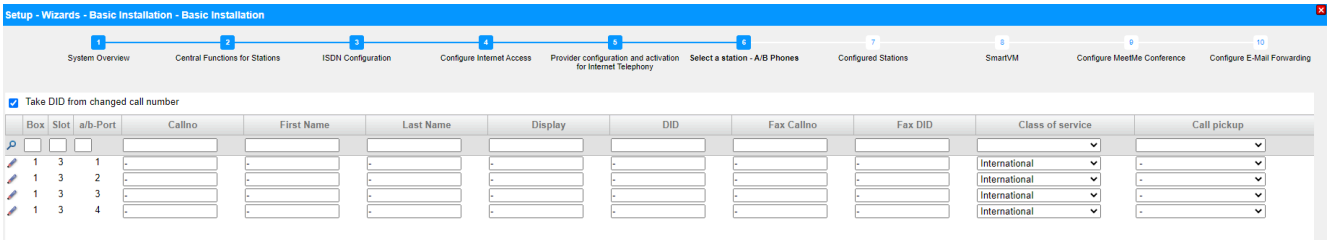
9) Haga clic en **OK & Continuar**.

5.7.7.2 Cómo configurar extensiones analógicas

Requisitos previos

Se encuentra en la ventana **Seleccionar extensión - Terminales A/B** del asistente **Configuración básica**.

Hay una placa base o un módulo con interfaces analógicas.



Paso a paso

1) Si desea que el número de marcación directa de la extensión sea diferente al número de teléfono, en la línea de la extensión deseada, introduzca el número de marcación directa de la extensión en el campo **Marcación directa**:

- Solo con conexión de centralita:

  Haga clic en el campo deseado e indique el número de marcación directa a través del teclado. El número de marcación directa puede ser idéntico al número de teléfono interno.
- Solo con acceso individual:

  Seleccione un MSN a través de la lista de selección. La extensión puede configurarse, por ejemplo, de forma interna a través de un número de teléfono interno 101 o de forma externa a través del MSN 654321.
- en una conexión de centralita y acceso individual:

  En el campo deseado, y a través de la lista desplegable, seleccione la entrada **xxx - editable** (xxx es el número de teléfono interno) e indique el número de marcación directa a través del teclado o seleccione un MSN a través de la lista desplegable.

2) En la línea de la extensión deseada, en **N.º llam**, indique el número de teléfono interno de la extensión. Puede utilizar el número de teléfono preestablecido o asignar otro todavía no ocupado.
3) En la línea de la extensión deseada, y en **Nombre**, introduzca un nombre con el formato `Apellidos, Nombre` o `Nombre Apellidos`.

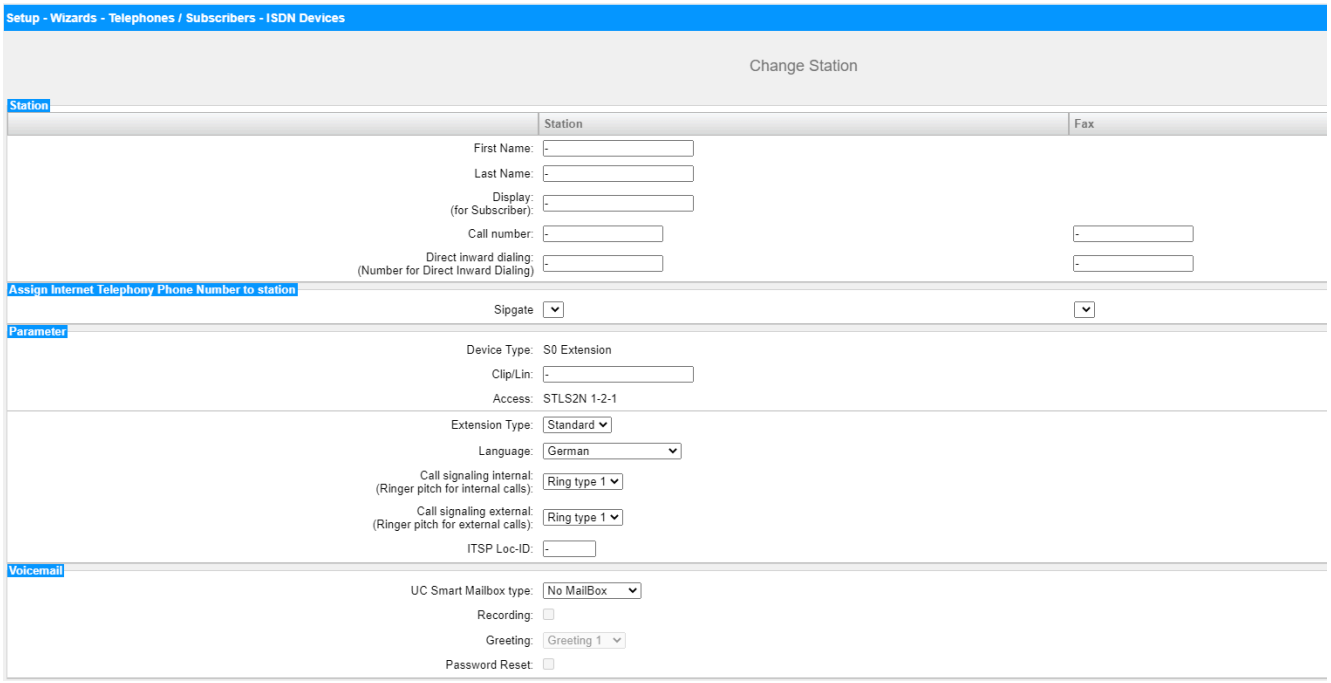
Nota: El nombre puede incluir hasta 16 caracteres como máximo, pero no puede incluir diéresis ni caracteres especiales.

---

4) Si desea configurar un buzón de fax para la extensión (que se pueda utilizar, por ejemplo, con los clientes de UC **myPortal for Desktop** o **myPortal for Outlook**), siga este procedimiento:
   a) En la línea de la extensión deseada, en el campo **Fax N.° llam**, introduzca el número de fax interno deseado con el que el usuario podrá recibir mensajes de fax internos.
   b) Si desea configurar un número de marcación directa para el buzón de fax, en la línea de la extensión deseada (en el campo **Marcación directa de fax**) introduzca el número de teléfono de fax externo deseado con el que la extensión podrá recibir mensajes de fax del exterior.
5) En la línea de la extensión deseada y utilizando la lista desplegable **Clase de servicio**, seleccione el grupo de clase de servicio deseado.
6) Para incluir las extensiones de un grupo de telecaptura, en la línea de la extensión deseada de la lista desplegable **Telecaptura de llamadas**, seleccione un grupo de telecaptura.

7) Los ajustes descritos en este paso solo se deben realizar si es necesario:

a) En la línea de la extensión analógica deseada, haga clic en el símbolo en forma de lápiz **Editar**.



b) En **Clip/Lin** indique número teléfono (número de marcación directa o MSN) que aparecerá en el display del usuario llamado en lugar del número de teléfono en caso de llamada externa.

Nota: Esta prestación debe estar activada por el proveedor de red.

Nota: Se debe configurar al menos un número de marcación directa. De lo contrario, el sistema no tiene en cuenta el número CLIP del llamante, y el número de la llamada interna se formatea y se envía como número de llamante para la llamada externa.

---

c) En la lista desplegable **Tipo de ext.** seleccione el tipo del terminal analógico (p. ej. Fax).

d) En la sección **Mar. dir. para telefonía Internet**, utilice la lista desplegable para seleccionar un número de marcación directa. Por cada ITSP activo aparece una lista desplegable.

Nota: No se puede ver el campo **Marc. dir. para telefonía Internet** si la telefonía Internet no está configurada o no hay activado ningún ITSP.

---

e) En la lista desplegable **Señalización de llamadas internas**, asigne a la extensión una de las ocho señalizaciones de llamada acústicas para llamadas internas posibles. De esta forma, la extensión enviará a otras

extensiones internas un tono de llamada modificado que le permite ser reconocida por dichas extensiones (Estándar: Tipo de llamada 1).

f) En la lista desplegable **Señalización de llamadas externas**, asigne a la extensión una de las tres señalizaciones de llamada para llamadas externas posibles (Estándar: Tipo de llamada 1).

g) Haga clic en **OK & Continuar**.

h) Si es necesario, modifique los flags de extensión. Para consultar una descripción de los flags de extensión, véase Extensión > Extensión > Parámetros de extensión.

i) Haga clic en **OK & Continuar**.

8) Si desea configurar otra extensión analógica más, haga clic en **Guardar datos** y repita los pasos 1 a 7.

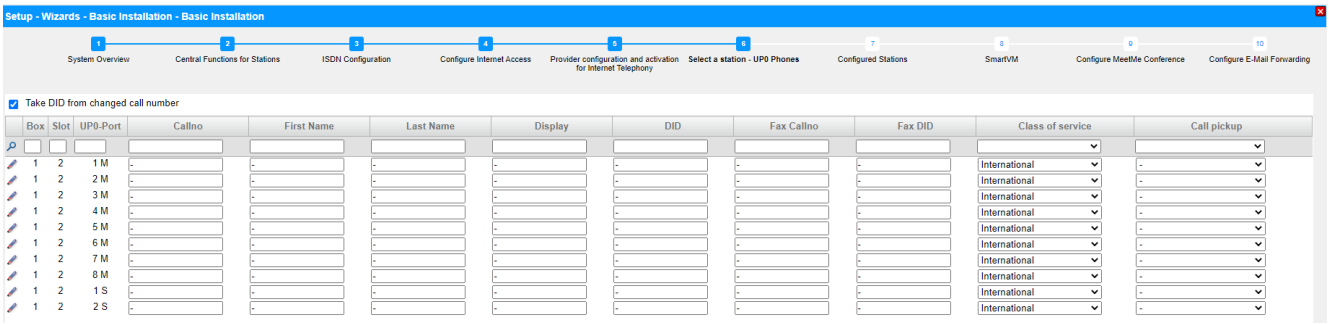
9) Haga clic en **OK & Continuar**.

5.7.7.3 Cómo configurar extensiones UP0

Requisitos previos

Se encuentra en la ventana **Seleccionar extensión - UP0 Telephones** del asistente **Configuración básica**.

Hay una placa base o un módulo con interfaces UP0.



Paso a paso

1) Si desea que el número de marcación directa de la extensión sea diferente al número de teléfono, en la línea de la extensión deseada, introduzca el número de marcación directa de la extensión en el campo **Marcación directa**:

- Solo con conexión de centralita:

  Haga clic en el campo deseado e indique el número de marcación directa a través del teclado. El número de marcación directa puede ser idéntico al número de teléfono interno.

- Solo con acceso individual:

  Seleccione un MSN a través de la lista de selección. La extensión puede configurarse, por ejemplo, de forma interna a través de un número de teléfono interno 101 o de forma externa a través del MSN 654321.

- en una conexión de centralita y acceso individual:

  En el campo deseado, y a través de la lista desplegable, seleccione la entrada **xxx - editable** (xxx es el número de teléfono interno) e indique el

número de marcación directa a través del teclado o seleccione un MSN a través de la lista desplegable.

2) En la línea de la extensión deseada, en **N.º llam**, indique el número de teléfono interno de la extensión. Puede utilizar el número de teléfono preestablecido o asignar otro todavía no ocupado.
3) En la línea de la extensión deseada, y en **Nombre**, introduzca un nombre con el formato `Apellidos, Nombre` o `Nombre Apellidos`.

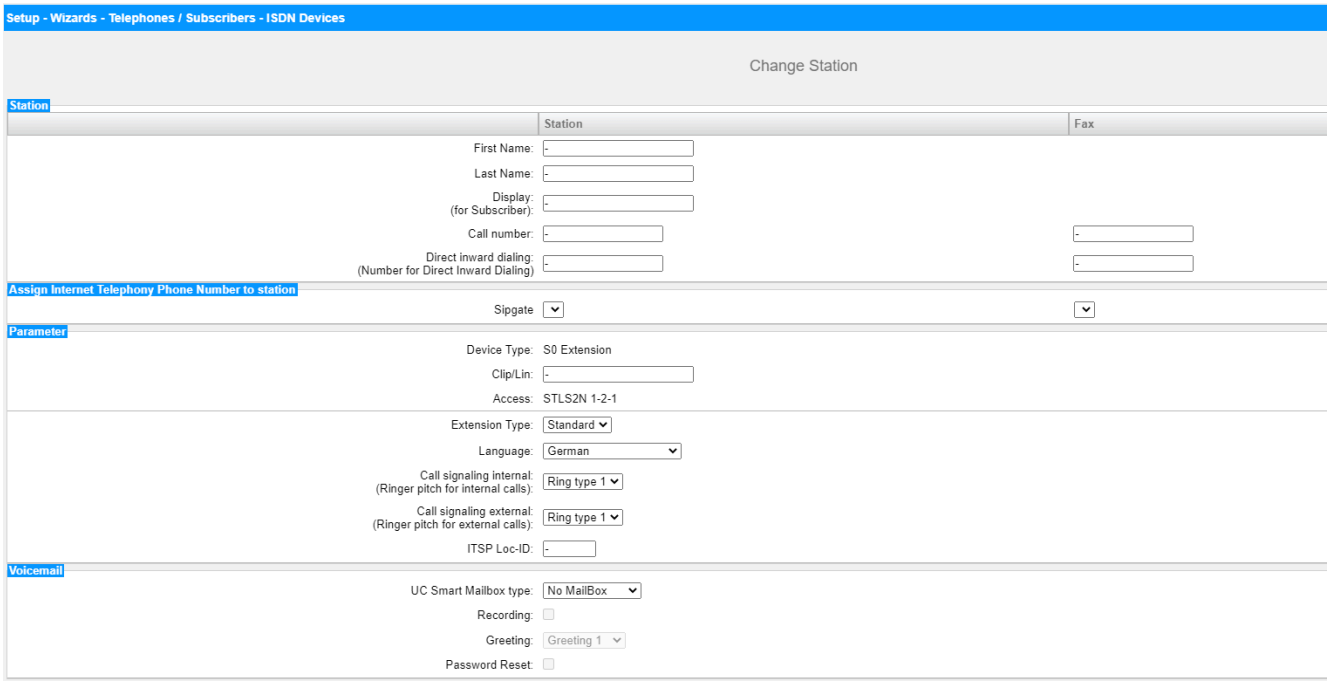
Nota: El nombre puede incluir hasta 16 caracteres como máximo, pero no puede incluir diéresis ni caracteres especiales.

---

4) Si desea configurar un buzón de fax para la extensión (que se pueda utilizar, por ejemplo, con los clientes de UC **myPortal for Desktop** o **myPortal for Outlook**), siga este procedimiento:
   a) En la línea de la extensión deseada, en el campo **Fax N.° llam**, introduzca el número de fax interno deseado con el que el usuario podrá recibir mensajes de fax internos.
   b) Si desea configurar un número de marcación directa para el buzón de fax, introduzca en la línea de la extensión deseada (en el campo **Marcación directa de fax**) el número de teléfono de fax externo deseado con el que la extensión podrá recibir mensajes de fax del exterior.
5) En la línea de la extensión deseada y utilizando la lista desplegable **Clase de servicio**, seleccione el grupo de clase de servicio deseado.
6) Para incluir las extensiones de un grupo de telecaptura, en la línea de la extensión deseada de la lista desplegable **Telecaptura de llamadas**, seleccione un grupo de telecaptura.

7) Los ajustes descritos en este paso solo se deben realizar si es necesario:

a) En la línea de la extensión deseada, haga clic en el símbolo en forma de lápiz **Editar**.



b) En **Clip/Lin** indique número teléfono (número de marcación directa o MSN) que aparecerá en el display del usuario llamado en lugar del número de teléfono en caso de llamada externa.

Nota: Esta prestación debe estar activada por el proveedor de red.

Nota: Se debe configurar al menos un número de marcación directa. De lo contrario, el sistema no tiene en cuenta el número CLIP del llamante, y el número de la llamada interna se formatea y se envía como número de llamante para la llamada externa.

---

c) En la lista desplegable **Tipo de ext.**, haga clic en el tipo de terminal TDM.

d) En la lista desplegable **Idioma** deje la selección predeterminada. Esta configuración no es relevante para los terminales TDM

e) En la sección **Mar. dir. para telefonía Internet**, utilice la lista desplegable para seleccionar un número de marcación directa. Por cada ITSP activo aparece una lista desplegable.

Nota: No se puede ver el campo **Marc. dir. para telefonía Internet** si la telefonía Internet no está configurada o no hay activado ningún ITSP.

---

f) En la lista desplegable **Señalización de llamadas internas**, asigne a la extensión una de las ocho señalizaciones de llamada acústicas para llamadas internas posibles. De esta forma, la extensión enviará a otras

extensiones internas un tono de llamada modificado que le permite ser reconocida por dichas extensiones (Estándar: Tipo de llamada 1).

g) En la lista desplegable **Señalización de llamadas externas**, asigne a la extensión una de las tres señalizaciones de llamada para llamadas externas posibles (Estándar: Tipo de llamada 1).

h) Haga clic en **OK & Continuar**.

i) Si es necesario, modifique los flags de extensión. Para consultar una descripción de los flags de extensión, véase Extensión > Extensión > Parámetros de extensión.

j) Haga clic en **OK & Continuar**.

8) Si quiere configurar otra extensión UP0, haga clic en **Guardar datos** y repita los pasos 1 a 7.

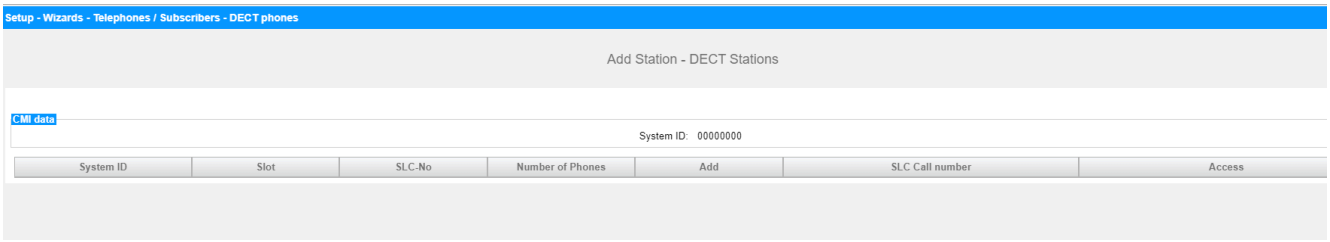
9) Haga clic en **OK & Continuar**.

5.7.7.4 Cómo configurar extensiones DECT

Requisitos previos

Se encuentra en la ventana **Seleccionar extensión - Extensiones DECT** del asistente **Configuración básica**.

Para configurar extensiones DECT debe haber conectada una extensión base y los teléfonos DECT tienen que haber iniciado sesión en ella. Si no es así, omita esta ventana. También puede configurar las extensiones DECT más adelante (véase , Configuración de extensiones).



Paso a paso

1) Si desea que el número de marcación directa de la extensión sea diferente al número de teléfono, en la línea de la extensión deseada, introduzca el número de marcación directa de la extensión en el campo **Marcación directa**:

- Solo con conexión de centralita:

  Haga clic en el campo deseado e indique el número de marcación directa a través del teclado. El número de marcación directa puede ser idéntico al número de teléfono interno.

- Solo con acceso individual:

  Seleccione un MSN a través de la lista de selección. La extensión puede configurarse, por ejemplo, de forma interna a través de un

número de teléfono interno 101 o de forma externa a través del MSN 654321.

- en una conexión de centralita y acceso individual:

  En el campo deseado, y a través de la lista desplegable, seleccione la entrada **xxx - editable** (xxx es el número de teléfono interno) e indique el número de marcación directa a través del teclado o seleccione un MSN a través de la lista desplegable.

2) En la línea de la extensión deseada, en **N.º llam**, indique el número de teléfono interno de la extensión. Puede utilizar el número de teléfono preestablecido o asignar otro todavía no ocupado.

3) Si desea configurar un buzón de fax para la extensión (que se pueda utilizar, por ejemplo, con los clientes de UC **myPortal for Desktop** o **myPortal for Outlook**), siga este procedimiento:

a) En la línea de la extensión deseada, en el campo **Fax N.° llam**, introduzca el número de fax interno deseado con el que el usuario podrá recibir mensajes de fax internos.

b) Si desea configurar un número de marcación directa para el buzón de fax, introduzca en la línea de la extensión deseada (en el campo **Marcación directa de fax**) el número de teléfono de fax externo deseado con el que la extensión podrá recibir mensajes de fax del exterior.

4) En la línea de la extensión deseada, y en **Nombre**, introduzca un nombre con el formato `Apellidos, Nombre` o `Nombre Apellidos`.

Nota: El nombre puede incluir hasta 16 caracteres como máximo, pero no puede incluir diéresis ni caracteres especiales.

---

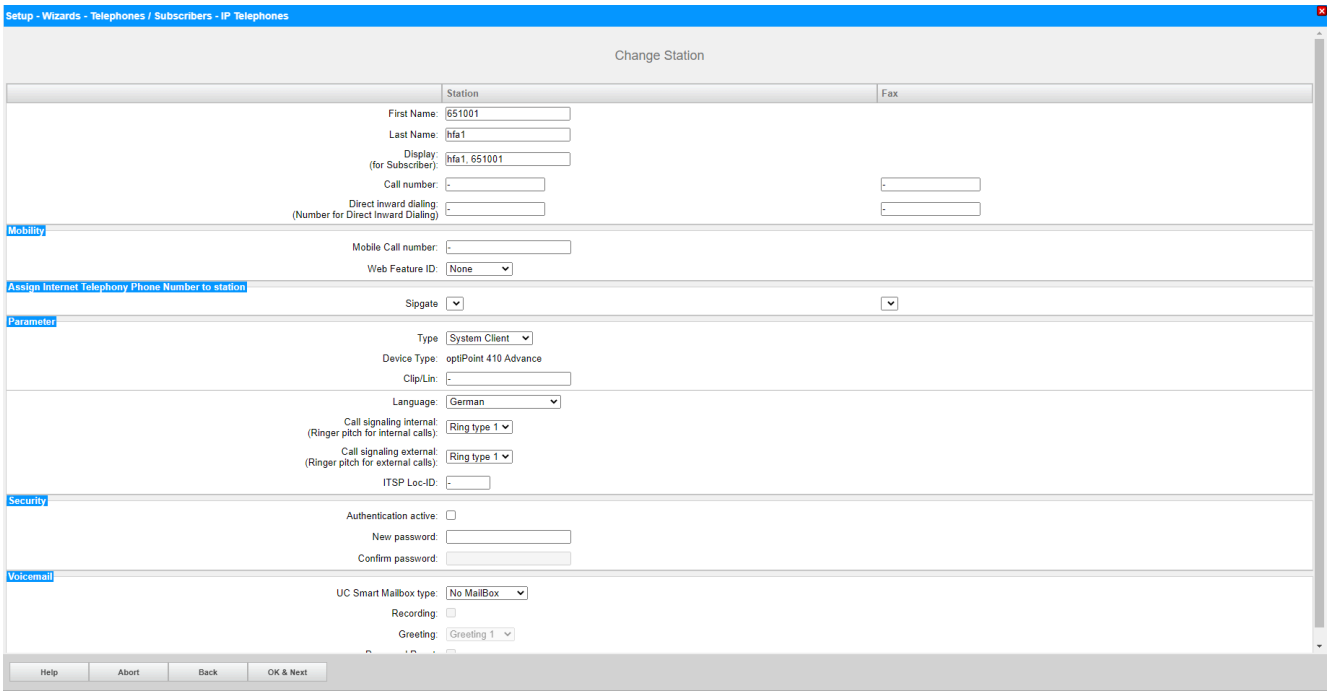
5) En la línea de la extensión deseada y utilizando la lista desplegable **Clase de servicio**, seleccione el grupo de clase de servicio deseado.

6) Para incluir las extensiones de un grupo de telecaptura, en la línea de la extensión deseada de la lista desplegable **Telecaptura de llamadas**, seleccione un grupo de telecaptura.

7) Si desea modificar el código telefónico DECT (PIN), en el campo **Código móvil** de la línea de la extensión deseada introduzca el código nuevo. La extensión DECT debe registrarse de nuevo en la extensión base con este código.

8) Los ajustes descritos en este paso solo se deben realizar si es necesario:

a) En la línea de la extensión deseada, haga clic en el símbolo en forma de lápiz **Editar**.



b) En **Clip/Lin** indique número teléfono (número de marcación directa o MSN) que aparecerá en el display del usuario llamado en lugar del número de teléfono en caso de llamada externa.

Nota: Esta prestación debe estar activada por el proveedor de red.

Nota: Se debe configurar al menos un número de marcación directa. De lo contrario, el sistema no tiene en cuenta el número CLIP del llamante, y el número de la llamada interna se formatea y se envía como número de llamante para la llamada externa.

---

c) En la lista desplegable **Tipo de ext.**, haga clic en el tipo de terminal inalámbrico.

d) En la lista desplegable **Idioma** deje la selección predeterminada. Esta configuración no es importante para los terminales inalámbricos.

e) En la sección **Mar. dir. para telefonía Internet**, utilice la lista desplegable para seleccionar un número de marcación directa. Por cada ITSP activo aparece una lista desplegable.

Nota: No se puede ver el campo **Marc. dir. para telefonía Internet** si la telefonía Internet no está configurada o no hay activado ningún ITSP.

---

f) En la lista desplegable **Señalización de llamadas internas**, asigne a la extensión una de las ocho señalizaciones de llamada acústicas para llamadas internas posibles. De esta forma, la extensión enviará a otras

extensiones internas un tono de llamada modificado que le permite ser reconocida por dichas extensiones (Estándar: Tipo de llamada 1).

g) En la lista desplegable **Señalización de llamadas externas**, asigne a la extensión una de las tres señalizaciones de llamada para llamadas externas posibles (Estándar: Tipo de llamada 1).

h) Haga clic en **OK & Continuar**.

i) Si es necesario, modifique los flags de extensión. Para consultar una descripción de los flags de extensión, véase Extensión > Extensión > Parámetros de extensión.

j) Haga clic en **OK & Continuar**.

9) Si desea configurar otra extensión, haga clic en **Guardar datos** y repita los pasos 1 a 8.

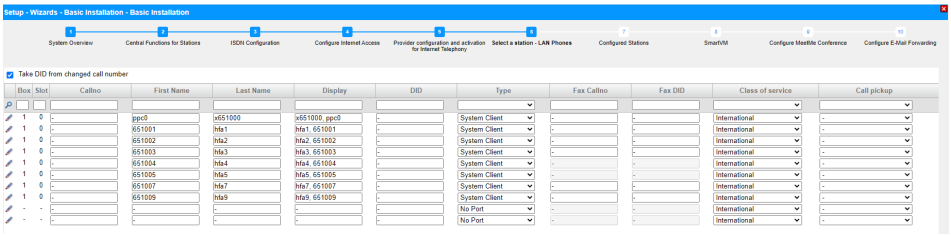
10) Haga clic en **OK & Continuar**.

5.7.7.5 Cómo configurar extensiones IP y SIP

Requisitos previos

Se encuentra en la ventana **Seleccionar extensión - Teléfonos LAN** del asistente **Configuración básica**.

Para poder poner en servicio los teléfonos WLAN necesita una red LAN inalámbrica operativa.



Paso a paso

1) Si desea que el número de marcación directa de la extensión sea diferente al número de teléfono, en la línea de la extensión deseada, introduzca el número de marcación directa de la extensión en el campo **Marcación directa**:

- Solo con conexión de centralita:

  Haga clic en el campo deseado e indique el número de marcación directa a través del teclado. El número de marcación directa puede ser idéntico al número de teléfono interno.
- Solo con acceso individual:

  Seleccione un MSN a través de la lista de selección. La extensión puede configurarse, por ejemplo, de forma interna a través de un número de teléfono interno 101 o de forma externa a través del MSN 654321.
- en una conexión de centralita y acceso individual:

  En el campo deseado, y a través de la lista desplegable, seleccione la entrada **xxx - editable** (xxx es el número de teléfono interno) e indique

el número de marcación directa a través del teclado o seleccione un MSN a través de la lista desplegable.

2) En la línea de la extensión deseada, en **N.º llam**, indique el número de teléfono interno de la extensión. Puede utilizar el número de teléfono preestablecido o asignar otro todavía no ocupado.

3) En la línea de la extensión deseada, y en **Nombre**, introduzca un nombre con el formato `Apellidos, Nombre`.

Nota: El nombre puede incluir hasta 16 caracteres como máximo, pero no puede incluir diéresis ni caracteres especiales. En los clientes de UC el nombre se registra como apellido tal y como esté aquí indicado (pero se puede modificar).

---

4) En la línea de la extensión deseada, y en la lista desplegable **Tipo**, seleccione el tipo de la extensión IP (p. ej., "Cliente de sistema" o "Cliente SIP").

5) Si desea configurar un buzón de fax para la extensión (que se pueda utilizar, por ejemplo, con los clientes de UC **myPortal for Desktop** o **myPortal for Outlook**), siga este procedimiento:

a) En la línea de la extensión deseada, en el campo **Fax N.° llam**, introduzca el número de fax interno deseado con el que el usuario podrá recibir mensajes de fax internos.

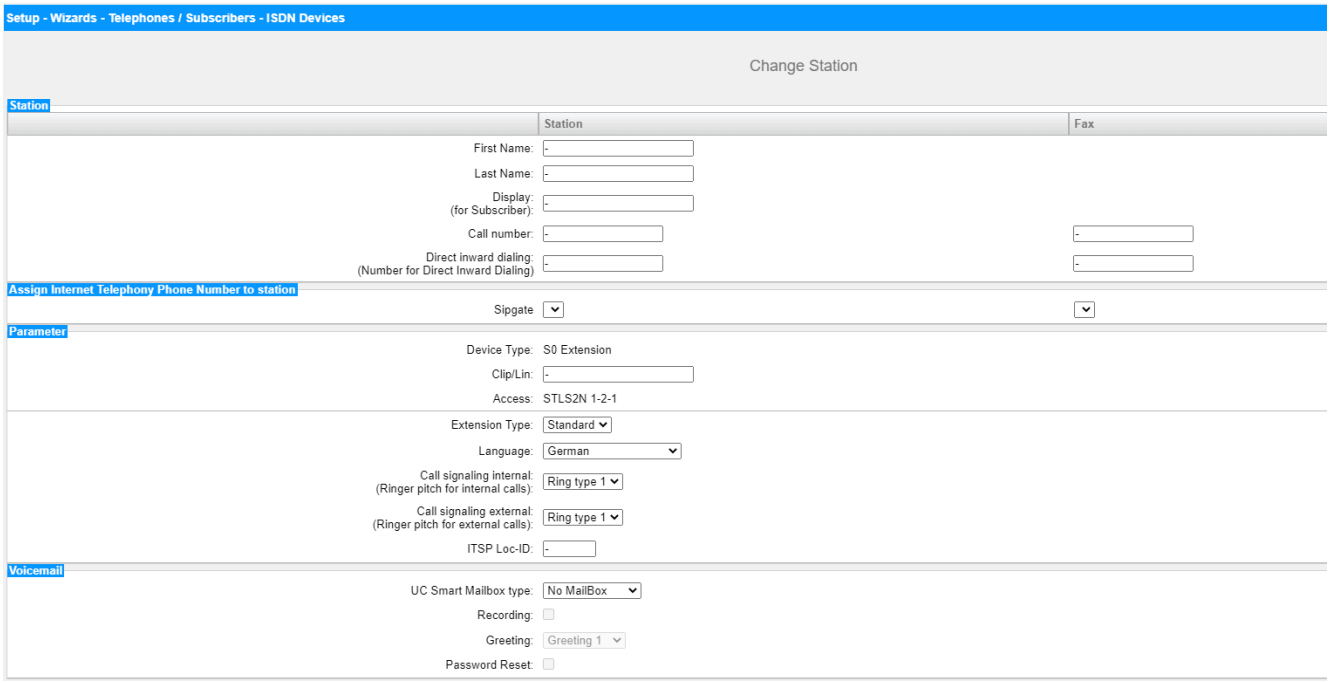
b) Si desea configurar un número de marcación directa para el buzón de fax, introduzca en la línea de la extensión deseada (en el campo **Marcación directa de fax**) el número de teléfono de fax externo deseado con el que la extensión podrá recibir mensajes de fax del exterior.

6) En la línea de la extensión deseada y utilizando la lista desplegable **Clase de servicio**, seleccione el grupo de clase de servicio deseado.

7) Para incluir las extensiones de un grupo de telecaptura, en la línea de la extensión deseada de la lista desplegable **Telecaptura de llamadas**, seleccione un grupo de telecaptura.

8) Solo debe realizar los ajustes descritos en este paso si es necesario o en los teléfonos SIP:

a) En la línea de la extensión deseada, haga clic en el símbolo en forma de lápiz **Editar**.



b) Para teléfonos SIP: Si el teléfono SIP se tiene que operar junto con un teléfono móvil Dual-Mode, en el área **Mobility**, en `Número de teléfono móvil`, indique el código urbano seguido por el número del teléfono móvil (p. ej., **0016012345678**). Además, en la lista desplegable **Web Feature ID**, seleccione este cliente SIP. (véase Telefonía Dual-Mode).

c) En **Clip/Lin** indique número teléfono (número de marcación directa o MSN) que aparecerá en el display del usuario llamado en lugar del número de teléfono en caso de llamada externa.

Nota: Esta prestación debe estar activada por el proveedor de red.

Nota: Se debe configurar al menos un número de marcación directa. De lo contrario, el sistema no tiene en cuenta el número CLIP del llamante, y el número de la llamada interna se formatea y se envía como número de llamante para la llamada externa.

---

d) En la lista desplegable **Idioma** seleccione el idioma para el control de menús del teléfono.

e) En la lista desplegable **Señalización de llamadas internas**, asigne a la extensión una de las ocho señalizaciones de llamada acústicas para llamadas internas posibles. De esta forma, la extensión enviará a otras extensiones internas un tono de llamada modificado que le permite ser reconocida por dichas extensiones (Estándar: Tipo de llamada 1).

f) En la lista desplegable **Señalización de llamadas externas**, asigne a la extensión una de las tres señalizaciones de llamada para llamadas externas posibles (Estándar: Tipo de llamada 1).
g) Solo para teléfonos SIP: Introduzca la contraseña de autenticación en los campos **Contraseña** y **Confirmar contraseña**.
h) Solo para teléfonos SIP: en el campo **ID de usuario SIP / Nombre usuario**, indique la identificación de usuario para la autenticación.
i) Solo para teléfonos SIP: en el campo **Ámbito**, indique la zona correspondiente a la autenticación.
j) Haga clic en **OK & Continuar**.
k) Si es necesario, modifique los flags de extensión. Para consultar una descripción de los flags de extensión, véase Extensión > Extensión > Parámetros de extensión.
l) Haga clic en **OK & Continuar**.

9) Si desea configurar otra extensión IP, haga clic en **Guardar datos** y repita los pasos 1 a 8.

10) Haga clic en **OK & Continuar**. Verá una lista de todas las extensiones configuradas. La lista se corresponde con un plan de numeración.

11) Si es necesario, haga clic en **Imprimir**, para imprimir los datos de las extensiones configuradas.

12) A continuación, haga clic en **OK y Continuar**.

Conceptos relacionados

Salida de texto multilingüe en la página 1256

5.7.8 Configuración de UC Suite

En la ventana **Configuración automática de la suite de aplicaciones** se puede hacer la configuración automática de la solución de Comunicaciones Unificadas UC Suite.

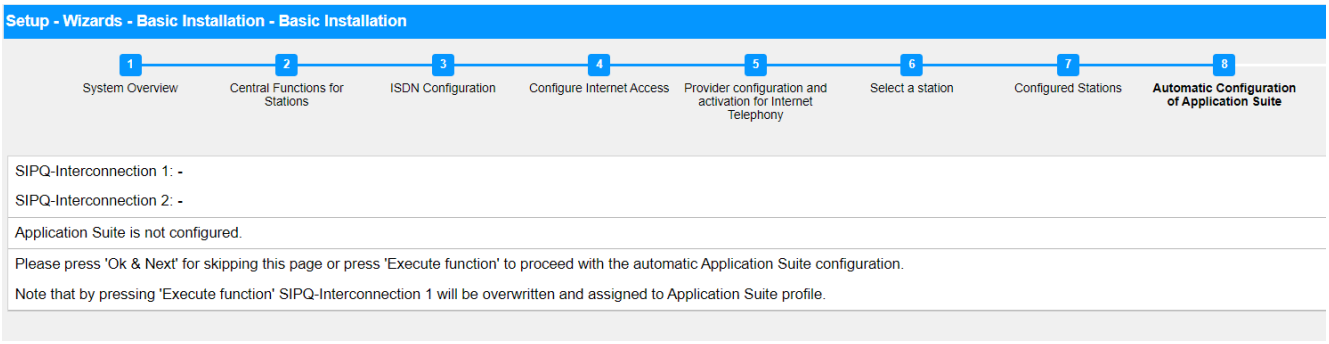
Nota: Esta ventana solo aparece si en el asistente **Instalación inicial** se ha seleccionado **Paquete con UC Suite** en la selección de aplicación.

La configuración automática de la solución UC Suite requiere un número de líneas urbanas libres que se ocuparán estáticamente para la aplicación. Este número depende de las capacidades de especificación del sistema y se enumera en la sección Valores máximos para líneas en la página 1469 (ver *Canales urbanos MEB para UC Suite* en las tablas). En caso de que se supere el límite global de 250 líneas urbanas, no será posible la configuración de UC Suite.

5.7.8.1 Cómo configurar la Suite UC

Requisitos previos

Se encuentra en la ventana **Configuración automática del conjunto de aplicaciones** del asistente de **instalación básica.**



Paso a paso

1) Si no hay ninguna tarjeta UC Booster integrada en el sistema de comunicación, haga clic en **Aceptar & Siguiente**. Se omitirá la configuración.
2) Si la tarjeta UC Booster está integrada en el sistema de comunicación, haga clic en **Ejecutar función**. La UC Suite se configura automáticamente. Cuando llegue al 100%, haga clic en **OK & Siguiente**.

Nota:

Para OpenScape Business X, el asistente genera automáticamente 76 canales multimedia.

5.7.9 Configuración de los buzones de voz de UC Smart

En la ventana **Configuración automática del Smart VM** puede hacer la configuración automática de los buzones de voz de UC Smart (Smart VM, Smart VoiceMail) si utiliza la solución de Comunicaciones Unificadas UC Smart.

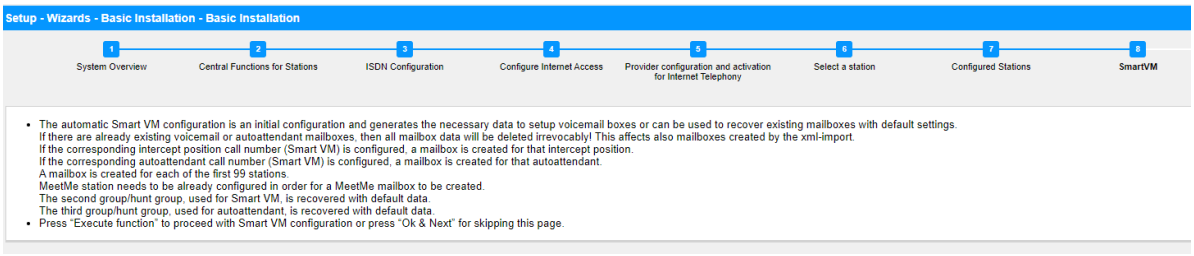
Nota:

Esta ventana solo aparece si en el asistente **Instalación inicial** se ha seleccionado **Paquete con UC Smart** en la selección de aplicación.

5.7.9.1 Cómo configurar los buzones de voz de UC Smart

Requisitos previos

Se encuentra en la ventana de **Configuración automática del Smart VM** del asistente **Configuración básica** .



Paso a paso

1) Si no desea utilizar los buzones de voz de UC Smart, haga clic en **OK & Continuar**. De esta forma se omite la configuración de los buzones de voz.
2) Si desea utilizar los buzones de voz de UC Smart, haga clic en **Ejecutar función**. Se configuran automáticamente buzones de voz para las 100 primeras extensiones. Cuando llegue al 100%, haga clic en **OK & Continuar**.

Nota: Los buzones de voz de UC Smart o los buzones de voz de UC Smart AutoAttendant presentes se borran y no se pueden recuperar.

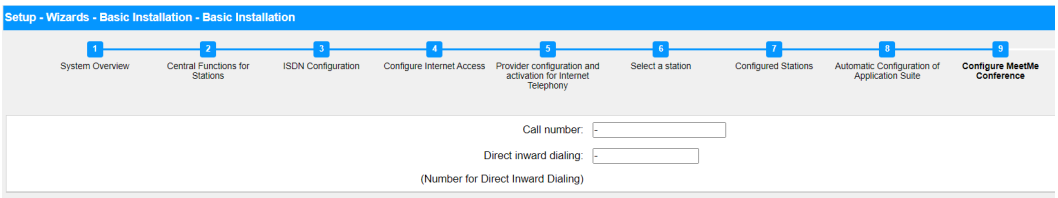
5.7.10 Ajustes del servidor de conferencias

En la ventana **Editar ajustes de conferencia Meet Me** puede establecer el número de teléfono y el número de acceso telefónico para las conferencias.

5.7.10.1 Cómo modificar los ajustes del servidor de conferencias

Requisitos previos

Se encuentra en la ventana **Configurar conferencia Meet-Me** del asistente **Configuración básica**.



Paso a paso

1) En el campo **Número de teléfono**, indique un número de teléfono para la conferencia.
2) En **Marcación directa**, establezca núm. acceso telef. conferencia (Nº llam. marc. dir. de conferencia). Con él, los participantes podrán acceder a una conf.
3) Clic **OK & Cont**.

5.7.11 Envío de correo electrónico (opcional)

En la ventana **Configurar transferencia de correos electrónicos** se puede configurar el envío de correo electrónico. Con ello, se notifica a las extensiones sobre nuevos mensajes de fax y voz, y el administrador recibe mensajes del sistema.

Tiene las siguientes opciones:

- Configurar el envío de correo electrónico

  Puede definir un servidor de correo electrónico externo que utilizará OpenScape Business para enviar los correos electrónicos. Los mensajes de voz y fax o mensajes internos del sistema se envían a través de este servidor de correo electrónico a una o varias direcciones de email configurables.

Nota: Es importante indicar un servidor de correo electrónico si desea enviar automáticamente por correo electrónico un enlace al archivo de instalación a los usuarios de la UC Suite.

5.7.11.1 Cómo configurar el envío de correo electrónico

Requisitos previos

Si el servidor de correo electrónico externo se ha configurado para utilizar la autenticación básica, asegúrese de que existe una cuenta de correo electrónico con contraseña en un proveedor de correo electrónico y de que conoce los datos de acceso de esta cuenta.

Si el servidor de correo electrónico externo se ha configurado para utilizar autenticación moderna (autorización basada en token Microsoft OAuth 2.0), como en el caso de Exchange Online, asegúrese de que:

- La cuenta de correo electrónico del remitente debe tener permiso para utilizar SMTP autenticado (por defecto, esta opción está inactiva en la tenencia de Microsoft 365). Una vez activado el SMTP autenticado, el reenvío de correo electrónico OAUTH 2.0 funciona normalmente con todas las placas base OpenScape Business.
- Se ha registrado una aplicación con los permisos necesarios en Microsoft Azure Active Directory (Azure AD) para que su sistema OpenScape Business envíe correos electrónicos.
- Usted conoce el ID de la aplicación (cliente) y el ID del directorio (inquilino) de la aplicación registrada.

  Pida a su administrador de Azure AD que le proporcione estos valores, si es necesario.
- La dirección de correo electrónico que aparecerá como remitente de los mensajes pertenece al mismo Azure AD o inquilino que la aplicación registrada.

Se encuentra en la ventana **Editar transferencia de correos electrónicos** del asistente **Configuración básica**.

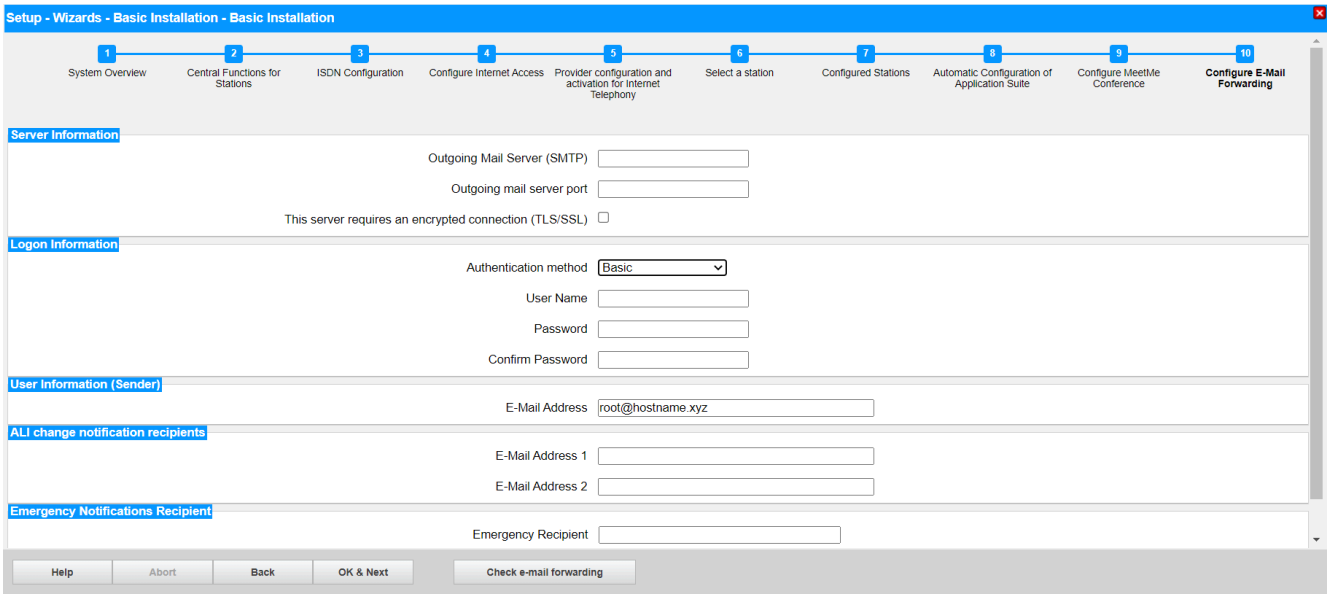


Figura 6: Opciones de reenvío de correo electrónico cuando se selecciona el método de autenticación básica

Paso a paso

1) Indique **servidor band. salida (SMTP)** del servidor correo para envío correo (p. ej., `smtp.web.es`). Si es necesario, consulte servidor band. salida proveedor correo.

   Nota: Compruebe que el nombre del servidor de salida de correo se puede resolver. Si no es así, inicie el asistente para el envío de correos electrónicos a través de **Centro de servicios** > **Transferencia de correos electrónicos** e introduzca la dirección IP del servidor de salida en lugar del nombre.

2) Complete el **Puerto del servidor de correo saliente** con el puerto del servidor que se deberá usar para el envío de correos electrónicos. Si es necesario, consulte servidor band. salida proveedor correo.
3) Si se requiere una conexión segura, active la casilla de verificación **Este servidor requiere una conexión cifrada (TLS/SSL)**. Si es necesario, consulte a su proveedor de correo electrónico si es necesario activar esta opción.
4) Si el servidor de correo electrónico externo se ha configurado para utilizar la autenticación básica, proceda como se indica a continuación:
   a) En la lista desplegable **Método de autenticación**, seleccione **Básico**.
   b) Indique **Nombre de usuario** cuenta correo, p. ej. `pepe.ejemplo`.
   c) En **Contraseña** y **Confirmar contraseña**, introduzca la contraseña de la cuenta de correo.

5) Si el servidor de correo electrónico externo se ha configurado para utilizar la autenticación moderna, proceda como se indica a continuación:

a) En la lista desplegable **Método de autenticación**, seleccione **Microsoft OAuth 2.0**.

b) Introduzca el ID de aplicación (cliente) obtenido del portal de Microsoft Azure en el campo **ID de aplicación**.

c) Introduzca el ID de directorio (inquilino) obtenido del portal de Microsoft Azure en el campo **Tenant**.

6) Introduzca la **Dirección de correo electrónico** que aparecerá como remitente de los mensajes, por ejemplo: `john.doe@web.de`.

7) Introduzca **Dir correo 1** para recibir notific. cuando se haya utilizado tolerancia ALI. También puede introducir una segunda dirección de correo electrónico en el campo **Dirección de correo electrónico 2**.

8) En el campo **Destinatario de emergencia**, indique la dirección de correo electrónico de un responsable de seguridad *in situ* a quien se le enviará un correo electrónico al marcar un número de emergencias.

El asunto del correo electrónico será "Nueva llamada de emergencia". El número de llamada y el nombre del llamante, de estar configurados, se incluyen en el correo electrónico recuperándose de la base de datos del sistema.

9) Si ha seleccionado **Microsoft OAuth 2.0** como método de autenticación, proceda como se indica a continuación:

a) Haga clic en **OK & Continuar**.

b) Espere a que aparezca un enlace de autorización y un código de usuario.

El código de autorización caduca al cabo de unos minutos.

c) Abra el enlace de autorización e introduzca el código de usuario en la ventana emergente.

d) Inicie sesión con la dirección de correo electrónico que ha introducido en el paso 6 en la página 210 **(Dirección de correo electrónico)**.

La dirección de correo electrónico debe estar en el mismo Azure AD o inquilino que la aplicación registrada.

e) Tras autenticarse correctamente, la ventana emergente muestra un mensaje como el siguiente:

`Ha iniciado sesión en <nombre-de-la-aplicación> en su dispositivo. Ahora puede cerrar esta ventana.`

f) Cierre la ventana emergente y vuelva a WBM. Si la autenticación se ha realizado correctamente, aparecerá el mensaje `La autenticación se ha realizado correctamente.`

10) Si desea comprobar los ajustes de correo electrónico, siga este procedimiento:

a) Haga clic en **Probar transferencia de correo electrónico**.
b) En **Enviar a correo**, indique dir. correo de buzón al que tenga acceso. El correo electrónico de prueba se envía a esa dirección.
c) En **Asunto correo electrónico**, introduzca descripción para identificar correo en buzón entrada.
d) Clic **Enviar correo prueba**. Se comprueban los ajustes de correo electrónico y el correo electrónico se envía al buzón de correo electrónico indicado.
e) Compruebe si correo electrónico ha llegado al buzón entr.
f) Si el correo electrónico se ha enviado correctamente, haga clic en **Atrás** y continúe al paso siguiente.
g) Si envío de correo es incorrecto, clic en **Volver** y compr. ajustes correo.

11) Haga clic en**OK & Continuar** y, a continuación, en **Salir**. La instalación básica ha finalizado. Antes de realizar la copia de seguridad de datos en el asistente, debería activar las licencias.

5.8 Tareas finales

Una vez finalizada la instalación inicial y la instalación básica con Gestión basada en Web (WBM), es necesario realizar algunos ajustes de configuración importantes para el servicio de OpenScape Business.

Para ello, siga este procedimiento:

1) Active y asigne licencias

Las licencias adquiridas con OpenScape Business se deben activar en un plazo de 30 días. El periodo de tiempo comienza al iniciar sesión por primera vez en la Gestión basada en Web (WBM). Terminado ese tiempo, el sistema de comunicación solo se puede utilizar con restricciones. Una vez terminada la activación, hay que asignar las licencias a extensiones y líneas. En un sistema independiente, las funciones en el ámbito del sistema están habilitadas desde el momento de la activación.

2) Aprovisionamiento del cliente de UC Smart para la instalación (solo para UC Smart)

3) Cómo preparar los clientes de UC Suite para la instalación (solo para UC Suite)

Los clientes de UC Suite forman parte de la UC Suite. La Gestión basada en Web (WBM) puede acceder a los archivos de instalación de los clientes de UC, que se pueden aprovisionar a las extensiones IP tanto de forma automática como manual.

Además, el administrador tiene la opción de realizar una instalación silenciosa. Se trata de un método basado en líneas de comandos para la instalación, desinstalación o modificación automáticas de clientes de la UC Suite presentes en un PC sin tener que hacer ningún tipo de entrada adicional. Para más información, consulte Instalación / desinstalación silenciosa para clientes de PC de la UC Suite.

4) Realizar un almacenamiento de datos

Hay que guardar los cambios realizados previamente en OpenScape Business. La copia de seguridad se puede guardar como conjunto de copias de seguridad en un soporte USB o en la red interna.

5.8.1 Cómo activar y asignar las licencias

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Conoce el LAC (código de autorización de licencia) para el registro de licencia y tiene un nombre de usuario y una contraseña para acceder al servidor de licencias.

Para establecer conexión con el servidor de licencias necesita un acceso a Internet.

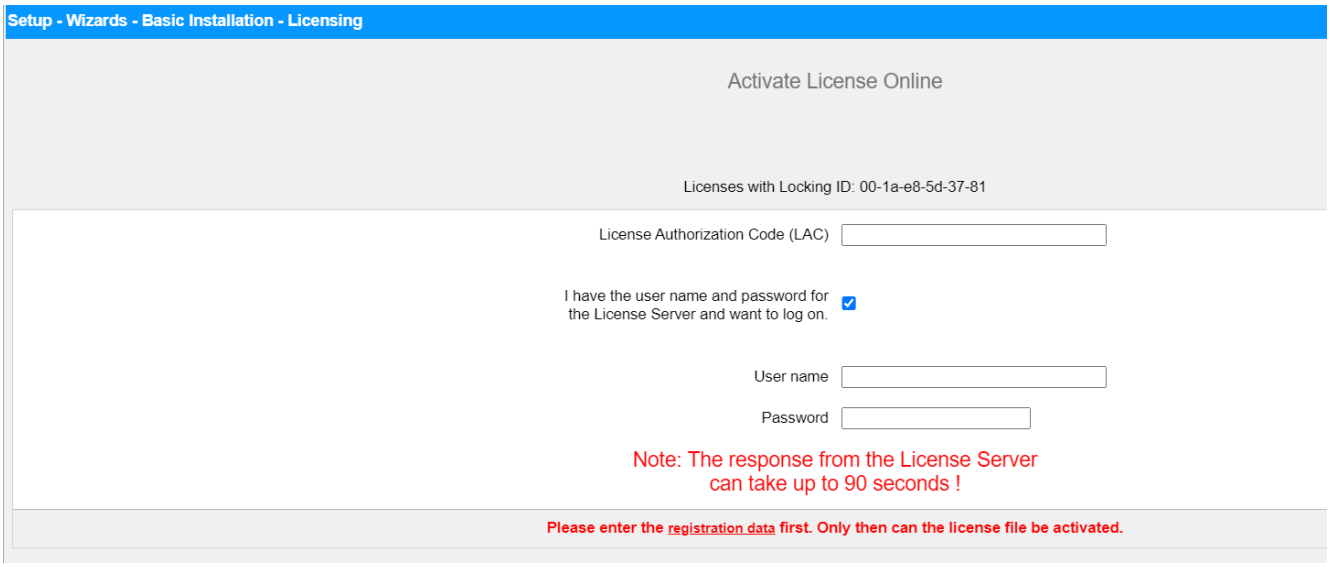
Paso a paso

1) Activar licencia online:

a) En la barra de navegación, haga clic en **Configuración**.

b) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.

c) Haga clic en **Editar** para iniciar el asistente **Registro de licencia**.



d) En el campo **Código de autorización de licencia (LAC)** indique el LAC.

e) Active la casilla de verificación **Tengo el nombre de usuario y la contraseña para el servidor de licencias y quiero iniciar sesión**.

f) Introduzca el **Nombre de usuario** y la **Contraseña** para iniciar sesión en el servidor de licencia.

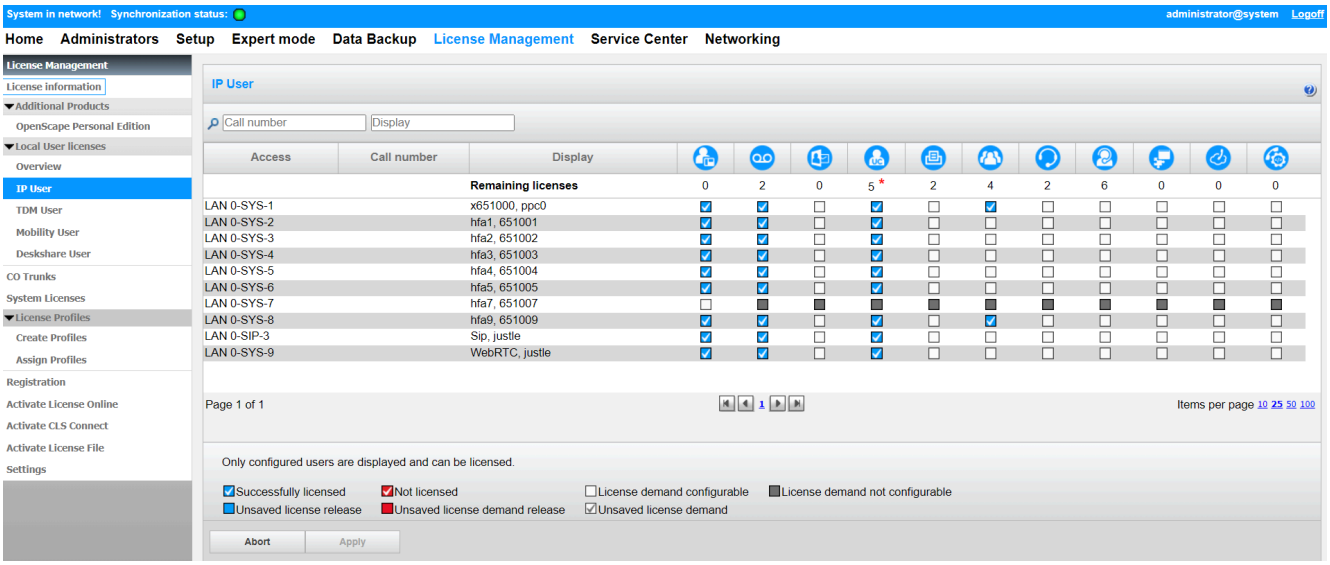
g) Haga clic en **OK y Continuar**. Se establece conexión con el servidor de licencias y se liberan las licencias.

2) Asignar licencias a las extensiones:

a) En la barra de navegación, haga clic en **Administración de licencias**.

b) En el árbol de navegación, en **Licencias de usuario local** > **...**, desplácese hasta el tipo de suscriptor deseado. Aparece una lista de todos los suscriptores del tipo seleccionado.

c) En la línea de la extensión deseada, active la casilla de verificación de la columna **Licencia de usuario** (primera columna con casillas de verificación).



d) En la línea del suscriptor deseado, active las licencias orientadas a usuarios. Para ello, active las casillas de verificación pertinentes.

Nota: Las licencias orientadas a usuarios (User) solo se pueden asignar a una extensión si antes se le ha asignado una licencia de extensión (licencia de usuario) (paso c).

---

e) Haga clic en **OK y Continuar**. Se comprueba si hay suficientes licencias para la asignación.

Si hay suficientes licencias, ha finalizado el registro de licencia de las extensiones.

f) Si faltan licencias, las casillas de verificación tendrán fondo rojo. Corrija los fallos y repita el paso e.

3) Asignar licencias a las líneas:

a) En el árbol de navegación, haga clic en **Líneas urbanas**. En el área **Líneas urbanas** aparece el número de licencias de línea adquiridas.

b) Para las líneas SIP: en el área **Demanda de licencias para el número de llamadas de Internet simultáneas en este nodo** indique el número

de llamadas de Internet que se pueden realizar al mismo tiempo mediante un ITSP.

c) Para las líneas S_{2M}: en el área **S2M** de la línea del slot deseado, seleccione el número de canales B deseado en la columna **Demandas**.
d) Para la líneas T1 (solo para EE. UU.): en el área **T1** de la línea del slot deseado, seleccione el número de canales B deseado en la columna **Demandas**.
e) Haga clic en **OK y Continuar**.

Nota: El número de líneas SIP con licencia y el número de líneas S_{2M}/T1 con licencia no puede ser superior al número de licencias de línea adquiridas.

5.8.2 Cómo proporcionar el cliente UC Smart para la instalación

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Está disponible el hardware y el software para usar la UC @work.

Nota: Para utilizar el cliente myPortal @work de UC Smart se requieren licencias.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Software**.
3) Haga clic en el icono de descarga de **myPortal @work** y guarde el archivo de instalación en una unidad de red habilitada.
4) Envíe a los usuarios de myPortal @Work los dos archivos de instalación.
5) Como alternativa, también puede enviar el enlace a los usuarios de myPortal @work para que puedan acceder directamente al archivo de instalación:

```
https://<Dirección IP del sistema de comunicación>/
management/downloads/myPortalAtWorkSetup.exe
```

5.8.3 Cómo preparar los clientes de UC Suite para la instalación

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Está disponible el hardware y el software para usar la UC Suite.

Nota: Para usar los clientes de UC Suite se necesitan licencias.

Paso a paso

1) Para poder ofrecer los archivos de instalación a una extensión de forma automática, compruebe que se han realizado los siguientes pasos:

a) Las direcciones de correo electrónico de las extensiones deben importarse junto con los datos de extensión a través de un archivo XML o se deben registrar en **Configuración** > **UC Suite** > **Directorio de usuario**.

b) Debe haber registrado un servidor de correo electrónico.

Nota: También puede introducir con posterioridad un servidor de correo electrónico en **Centro de servicios** > **Transferencia de correos electrónicos**.

Todas las extensiones con direcciones de correo electrónico conocidas recibirán un mensaje de correo electrónico con el enlace hacia el directorio de instalación de los clientes UC y una indicación de los primeros pasos. En el directorio de instalación encontrará, además, un archivo Léame con información sobre la instalación del software en los PC cliente.

2) Si no se han realizado los pasos necesarios para proceder a la notificación automática, también puede ofrecer los archivos de instalación de forma manual. Para ello, siga este procedimiento:

a) En la barra de navegación, haga clic en **Centro de servicios**.

b) En el árbol de navegación, haga clic en **Software**.

c) Haga clic en el cliente de UC deseado y guarde el archivo de instalación comprimido en una unidad de red compartida.

d) En el árbol de navegación, haga clic en **Documentos** y seleccione la lista desplegable **Instrucciones de uso**.

e) Haga clic en la documentación relativa al cliente de UC deseado y guarde el archivo de documentación en una unidad de red habilitada.

f) Envíe a los usuarios de los clientes UC el archivo de instalación comprimido y el archivo de documentación a través de un correo electrónico, o comunique a los usuarios la ubicación de los archivos.

g) El archivo comprimido ZIP con los archivos de instalación incluye también un archivo Readme. Indique a los usuarios que la instalación de los clientes de UC se debe realizar siguiendo las indicaciones de instalación del archivo Léame.

3) Como alternativa, también puede enviar enlaces a los usuarios de UC para que puedan acceder directamente a los archivos de instalación de los clientes de UC.

a) En la barra de navegación, haga clic en **Centro de servicios**.

b) En el árbol de navegación, haga clic en **Software**.

c) Haga clic en el botón **Mostrar enlaces de aplicación**. Se muestran varios enlaces, en función del sistema operativo utilizado y del cliente de UC deseado. Por ejemplo:

```
https://<Dirección IP del sistema de comunicación>/
management/downloads/install-common.zip
```

5.8.4 Cómo realizar la copia de seguridad

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Para hacer una copia de seguridad de los datos en un soporte USB (stick USB o disco duro USB), el soporte USB debe estar conectado con la interfaz de servidor USB.

Nota: Para obtener más información sobre la copia de seguridad, consulte Almacenamiento inmediato .

Paso a paso

1) En la barra de navegación, haga clic en **Almacenamiento de datos**.
2) En el árbol de navegación, haga clic en **Guardar - inmediatamente**.
3) En el área **Nombre**, y en el campo **Comentario**, introduzca un comentario para el conjunto de copias de seguridad. Este comentario permitirá identificar con mayor facilidad el conjunto de copias de seguridad en caso de que sea necesaria una recuperación. Al hacer la entrada evite el uso de diéresis y caracteres especiales.
4) En el área **Equipo**, active la unidad de destino en la que desea guardar el conjunto de copias de seguridad.
5) Haga clic en **OK & Continuar**. Se abrirá una nueva ventana con el progreso del proceso de guardado.
6) El mensaje **Guardar en orden indica que la copia se ha realizado con éxito.** aparece. Haga clic en **Salir**.
7) Si utiliza como soporte de copia de seguridad un stick USB, espere hasta que el LED del stick USB deje de parpadear. Solo entonces habrá finalizado la copia de seguridad en el stick USB. A continuación, extraiga el stick USB.
8) Concluye la puesta en servicio inicial con Gestión basada en Web (WBM). Cierre la Gestión basada en Web (WBM), haciendo clic en el enlace **Finalizar sesión** y, a continuación, cerrando la ventana.

Nota: Si hay disponible una nueva versión de software, le será comunicado en la página de inicio de Gestión basada en Web (WBM) (siempre que la conexión a Internet esté bien configurada). Si hay disponible una nueva versión de software, realice una actualización (véase Actualización del sistema de comunicación).

5.9 Puesta en servicio de los teléfonos IP

Para la puesta en servicio de los teléfonos IP se requiere un servidor DHCP que suministre al teléfono IP los datos importantes para iniciar sesión en el sistema de comunicación (datos específicos de red).

Datos específicos de red

Para iniciar sesión en el sistema de comunicación, los teléfonos IP necesitan datos específicos de red. Estos datos pueden estar memorizados en el servidor DHCP o se pueden introducir directamente en el teléfono IP. La ventaja de contar con un servidor DHCP es que todos los teléfonos IP conectados reciben los datos automáticamente.

El teléfono IP necesita los siguientes datos:

- Dirección IP del sistema de comunicación
- Dirección IP del servidor DLS

Además, el teléfono IP también necesita el número de teléfono propio. En el inicio de sesión, hay que introducir este número de forma manual en el teléfono.

Registro de teléfonos SIP

Por motivos de seguridad es recomendable registrar los teléfonos SIP en el sistema de comunicación. Para ello, los datos de registro del teléfono SIP y del sistema de comunicación tienen que coincidir.

Para el inicio de sesión se necesitan estos datos:

- ID de usuario SIP
- Contraseña SIP
- Ámbito SIP (opcional)

Utilice una contraseña compleja que cumpla estas normas:

- Al menos 8 posiciones
- Al menos una letra mayúscula (A - Z)
- Al menos una letra minúscula (a - z)
- Al menos un número (0-9)
- Al menos un carácter especial

Utilice un ID de usuario SIP que no incluya el número de teléfono.

Nota: Encontrará más información sobre la configuración de teléfonos SIP en `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Uso del servidor DHCP interno

Si se utiliza el servidor DHCP del sistema de comunicación, los datos específicos de red ya están depositados en él. Para que un teléfono IP se pueda registrar en el sistema de comunicación, solo hay que registrar en él el número de teléfono establecido. En los teléfonos SIP, además, los datos del registro SIP del teléfono SIP y del sistema de comunicación deben coincidir.

Uso de un servidor DHCP externo con datos específicos de red

Si se utiliza un servidor DHCP externo, los datos específicos de red deben depositarse ahí. Para que un teléfono IP se pueda registrar en el sistema de comunicación, solo hay que registrar en él el número de teléfono establecido. En los teléfonos SIP, además, los datos del registro SIP del teléfono SIP y del sistema de comunicación deben coincidir.

Uso de un servidor DHCP externo sin datos específicos de red

Si se utiliza un servidor DHCP externo en el que no se pueden depositar los datos específicos de red, hay que introducir esos datos en el teléfono IP. Para que un teléfono IP pueda registrarse en el sistema de comunicación, hay que introducir en él el número de teléfono establecido y la dirección IP del sistema de comunicación y, si es necesario, modificar la configuración del servicio de implementación (Deployment Service). En los teléfonos SIP, además, los datos del registro SIP del teléfono SIP y del sistema de comunicación deben coincidir.

5.9.1 Cómo configurar teléfono IP

Requisitos previos

El teléfono IP está conectado a la red interna y está operativo.

Nota: Aquí se describe la configuración tomando como ejemplo un teléfono de sistema OpenStage 40/60/80 IP. Hay que realizar ajustes análogos para todos los demás teléfonos IP. Para hacerlo, consulte las instrucciones de su teléfono IP.

Paso a paso

1) Para acceder al modo de administración del teléfono IP de sistema, en el teléfono pulse la tecla del menú de configuración/aplicaciones.

2) En la pestaña de `Configuración`, desplácese hasta `Admin` y confirme la acción con la tecla de verificación.

3) Introduzca la contraseña de administrador(valor estándar: `123456`) y confirme la entrada con la tecla de verificación.

4) Si en la red interna se utiliza el servidor DHCP del sistema de comunicación, omita el paso siguiente.

5) Si en la red interna no se utiliza el servidor DHCP del sistema de comunicación, hay que introducir la dirección IP del servidor servidor de despliegue (DLS) y del sistema de comunicación para poder actualizar el software del teléfono del sistema de forma automática. Esto solo se aplica a teléfonos IP del sistema. Para hacerlo, siga estos pasos:

a) Desplácese hasta `Network` (Red) y confirme la acción con la tecla de verificación.

b) Desplácese hasta `Update service (DLS)` (Servicio de actualización, DLS) y confirme la acción con la tecla de verificación.

c) Desplácese hasta `DLS address` (Dirección DLS) y confirme la acción con la tecla de verificación.

d) Introduzca como servidor de despliegue la dirección IP del sistema de comunicación (valor estándar: `192.168.1.2`) y confirme la acción con la tecla de verificación.

e) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.

f) Desplácese hasta `IPv4 configuration` (Configuración IPv4) y confirme la acción con la tecla de verificación.

g) Desplácese hasta `Route (default)` (Ruta, estándar) y confirme la acción con la tecla de verificación.

h) Introduzca la dirección IP del sistema de comunicación (valor estándar `192.168.1.2`) y confirme la entrada con la tecla de verificación.
i) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.
j) Desplácese atrás un nivel de menú con la tecla de retorno.

6) Defina el número de llamada del teléfono:
a) Desplácese hasta `System` (Sistema) y confirme la acción con la tecla de verificación.
b) Desplácese hasta `Identity` (Identidad) y confirme la acción con la tecla de verificación.
c) Desplácese hasta `Terminal number` (Número de terminal) y confirme la acción con la tecla de verificación.
d) Indique el número de teléfono establecido (p. ej., `120`y confirme la entrada con la tecla de verificación.
e) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.

7) Desplácese atrás un nivel de menú con la tecla de retorno.

8) Si es necesario reiniciar el teléfono de sistema para aplicar los cambios, en el menú `Admin` aparecerá la opción de menú `Restart` (Reiniciar). Confirme el `reinicio` con la tecla de verificación y, a continuación, pulse `Yes` (Sí) y la tecla de verificación. El teléfono de sistema se reinicia e inicia sesión en el sistema de comunicación.

5.9.2 Cómo configurar un teléfono SIP

Requisitos previos

El teléfono SIP está conectado con la LAN de clientes y está operativo.

Nota: Aquí se describe la configuración tomando como ejemplo un teléfono de sistema OpenStage 40/60/80 SIP. Los ajustes son análogos para otros teléfonos SIP. Para hacerlo, consulte las instrucciones del teléfono SIP.

Paso a paso

1) Para acceder al modo de administración del teléfono SIP de sistema, en el teléfono pulse la tecla del menú de configuración/aplicaciones.

2) En la pestaña de `Configuración`, desplácese hasta `Administrador (Admin)` y confirme la acción con la tecla de verificación.

3) Introduzca la contraseña de administrador(valor estándar: `123456`) y confirme la entrada con la tecla de verificación.

4) Si en la red interna se utiliza el servidor DHCP del sistema de comunicación, omita el paso siguiente.

5) Si en la red interna no se utiliza el servidor DHCP del sistema de comunicación, hay que introducir la dirección IP del servidor de despliegue (DLS) y del sistema de comunicación para poder actualizar el software

del teléfono del sistema SIP de forma automática. Esto solo se aplica a teléfonos del sistema SIP. Para hacerlo, siga estos pasos:

a) Desplácese hasta `Network` (Red) y confirme la acción con la tecla de verificación.
b) Desplácese hasta `Update service (DLS)` (Servicio de actualización, DLS) y confirme la acción con la tecla de verificación.
c) Desplácese hasta `DLS address` (Dirección DLS) y confirme la acción con la tecla de verificación.
d) Introduzca como servidor de despliegue la dirección IP del sistema de comunicación (valor estándar: `192.168.1.2`) y confirme la acción con la tecla de verificación.
e) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.
f) Desplácese hasta `IPv4 configuration` (Configuración IPv4) y confirme la acción con la tecla de verificación.
g) Desplácese hasta `Route (default)` (Ruta, estándar) y confirme la acción con la tecla de verificación.
h) Introduzca la dirección IP del sistema de comunicación (valor estándar `192.168.1.2`) y confirme la entrada con la tecla de verificación.
i) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.
j) Desplácese atrás un nivel de menú con la tecla de retorno.

6) Defina los ajustes horarios de SNTP:

a) Desplácese hasta `Date and time` (Fecha y hora) y confirme la acción con la tecla de verificación.
b) Desplácese hasta `Time source` (Fuente para la hora) y confirme la acción con la tecla de verificación.
c) Desplácese hasta `SNTP IP address` (Dirección IP de SNTP) y confirme la acción con la tecla de verificación.
d) Introduzca la dirección IP del sistema de comunicación (valor estándar `192.168.1.2`) y confirme la entrada con la tecla de verificación.
e) Desplácese hasta `Timezone offset` (Desfase de zona horaria) y confirme la acción con la tecla de verificación.
f) Introduzca el desfase de la hora local respecto a la hora UTC (Universal Time Coordinated) en horas (España/CES: `2`) y confirme la acción con la tecla de verificación.
g) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.
h) Desplácese atrás un nivel de menú con la tecla de retorno.

7) Defina el número de llamada del teléfono:

a) Desplácese hasta `System` (Sistema) y confirme la acción con la tecla de verificación.
b) Desplácese hasta `Identity` (Identidad) y confirme la acción con la tecla de verificación.
c) Desplácese hasta `Terminal number` (Número de terminal) y confirme la acción con la tecla de verificación.
d) Indique el número de teléfono establecido (p. ej., `120`y confirme la entrada con la tecla de verificación.
e) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.

8) Defina los datos de autenticación SIP:

a) Desplácese hasta `Registration` (Registro) y confirme la acción con la tecla de verificación.

b) Desplácese hasta `SIP session` (Sesión SIP) y confirme la acción con la tecla de verificación.

c) Ante el `Ámbito` o indique uno nuevo (p. ej. `OSBIZ-SIP`) en caso necesario.

d) Anote el `ID usuario` o indique uno nuevo (p. ej. `SIP-120`) en caso necesario.

e) Asigne una `Contraseña` para el registro en el servidor SIP.

f) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.

9) Con la tecla Volver, desplácese hasta el menú `Administrador`.

10) Si es necesario reiniciar el teléfono de sistema para aplicar los cambios, en el menú `Admin` aparecerá la opción de menú `Restart` (Reiniciar). Confirme el `reinicio` con la tecla de verificación y, a continuación, pulse `Yes` (Sí) y la tecla de verificación. El teléfono de sistema se reinicia e inicia sesión en el sistema de comunicación.

5.10 Cómo recopilar seguimientos de diagnóstico para incidentes de error

Puede recopilar automáticamente los datos de seguimientos (traces) de diagnóstico de un incidente de error. El **asistente de gestión de errores** le guiará durante todo el proceso.

Debe ejecutar el asistente de **gestión de errores** dos veces: antes y después de la ejecución del escenario problemático. Durante la primera ejecución (Fase 1), se activa la recogida de trazas de diagnóstico. Después de la ejecución del escenario problemático, ejecute de nuevo el asistente para recoger los datos de la traza de diagnóstico (Fase 2). Una vez completada la Fase 2, puede descargar el archivo de seguimiento para incluirlo en el sistema de tickets.

Para recopilar los datos de seguimiento de diagnóstico del incidente de error, siga estos pasos:

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) Haga clic en **Editar** junto a **Administración de errores**.

3) Haga clic en **OK y Continuar**.

4) Si desea recopilar los rastros por defecto, haga clic en la casilla **Rastros por defecto** .

5) Si desea especificar los tipos de trazas que se van a recoger, seleccione las que desee de la lista de trazas. Es posible realizar más de una selección.

Para obtener más información sobre los traces, véase la guía Resolución de problemas.

6) Haga clic en **OK y Continuar**.

7) Se mostrará una lista con información adicional, documentación relevante y recomendaciones. Haga clic en **OK y Continuar**.

8) Se mostrarán los escenarios y el tipo de traces que se van a recopilar. Haga clic en **Salir**.

9) Proceda a ejecutar el escenario problemático.

10) Una vez que haya completado el escenario, vuelva a desplazarse a **Configuración > Administración de errores** y haga clic en **Editar**.

Se le redirigirá al paso 2 de la recopilación de traces de diagnóstico. Si desea detener el proceso y volver a iniciarlo, puede hacer clic en el botón **Anular**.

11) Haga clic en **OK y Continuar**.

12) Introduzca la información necesaria y haga clic en **OK y Continuar**.

13) Se mostrará una lista con la información necesaria y algunas acciones adicionales.

14) Haga clic en **OK y Continuar**.

15) Haga clic en **Finalizar** para empezar a descargar los datos de traces de diagnóstico.

5.11 Reflashing

Siguiendo los pasos a continuación, podrá cambiar fácilmente el tipo de software de un dispositivo.

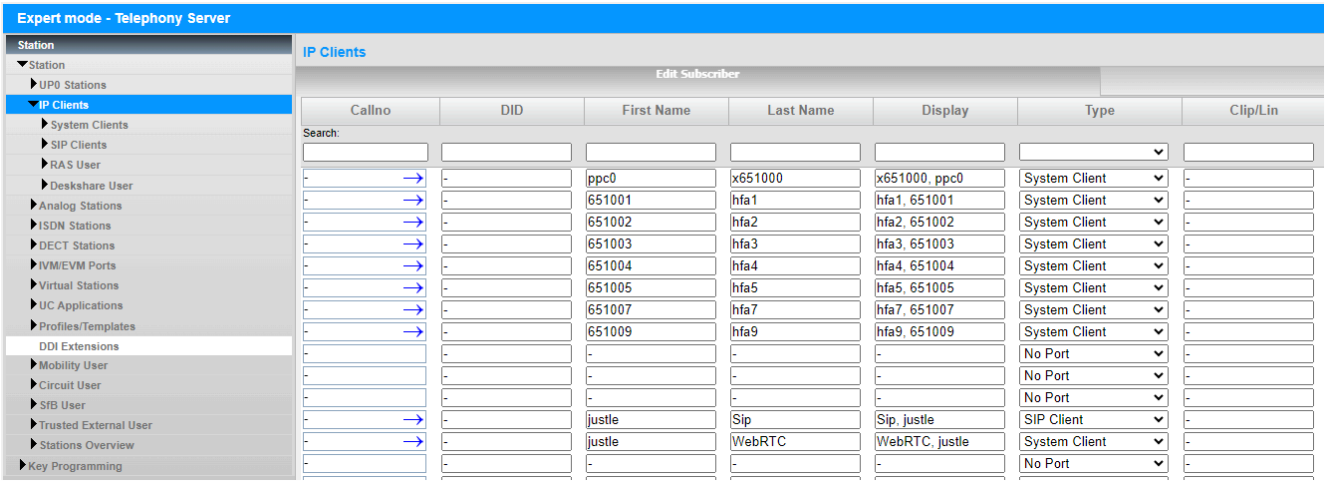
El concepto detrás de esta característica es simplificar la forma de obtener un dispositivo SIP (listo para usar) y registrarlo en el sistema OSBiz como un dispositivo HFA. Los únicos requisitos son:

- el teléfono debe obtener la dirección DLI (ya sea del servidor DHCP o manualmente)
- el administrador debe ingresar el número de teléfono (el cual debe estar preconfigurado como Cliente del Sistema)

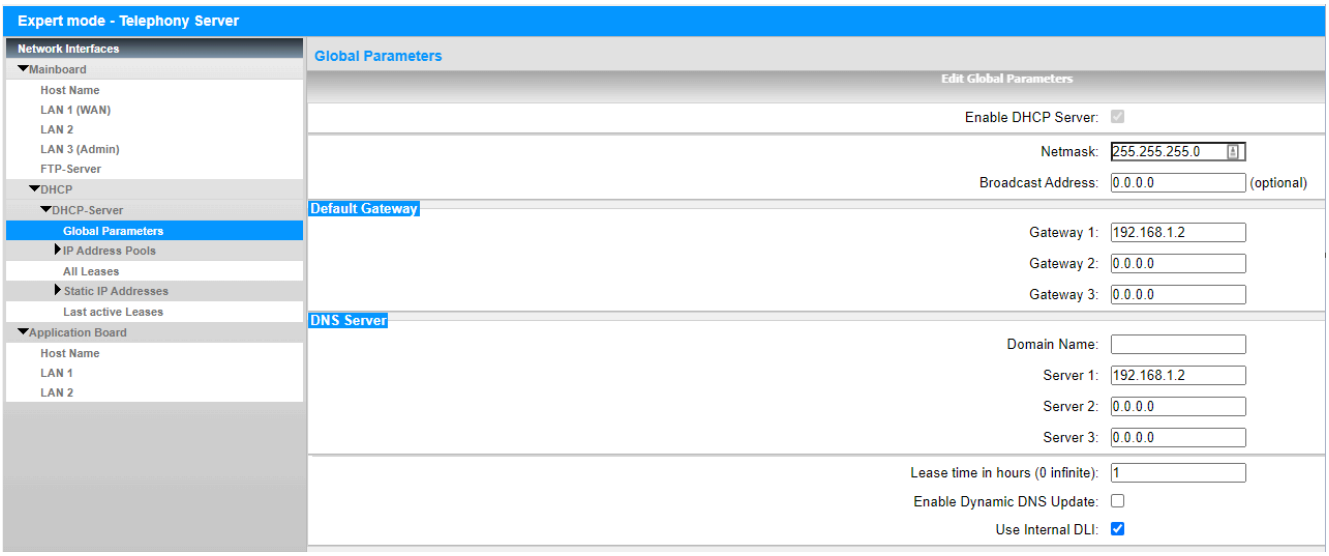
Una vez que el cliente obtenga un nuevo dispositivo, se preconfigurará como dispositivo SIP (configuración de fábrica). Los pasos para actualizar este dispositivo a un dispositivo HFA son los siguientes:

Paso a paso

1) Configure en la base de datos OSBIZ el número de teléfono deseado como Cliente del Sistema (HFA).



2) Configure el servidor DHCP para enviar la dirección IP de DLI. Esto se puede hacer en el servidor DHCP externo o en el servidor DHCP interno.



3) Si no se utiliza ningún servidor DHCP, debe configurar la IP DLI en el teléfono manualmente.

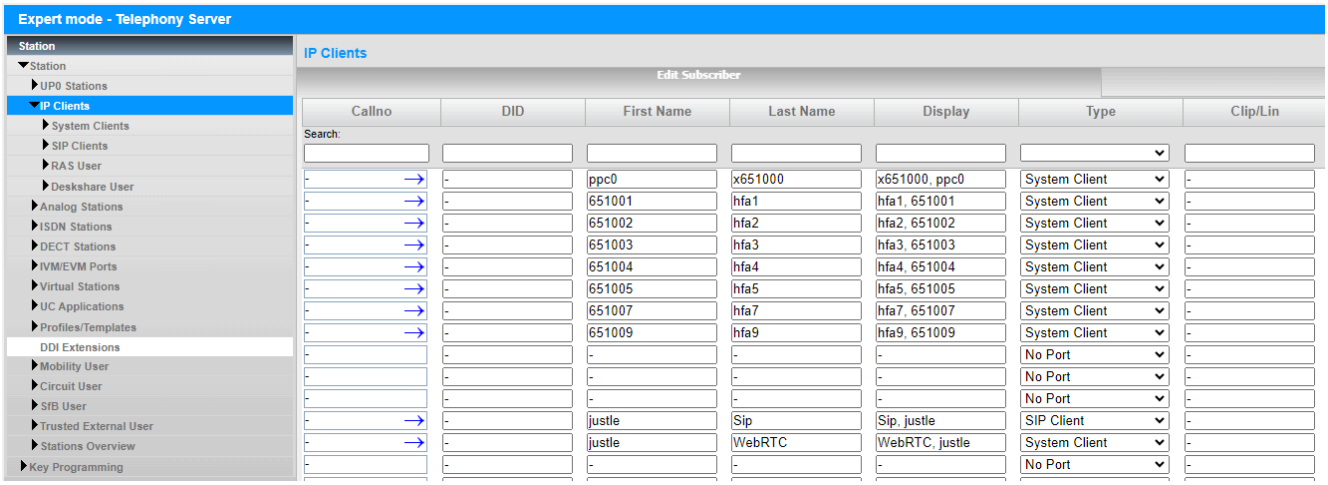
4) Una vez que el teléfono SIP obtenga una IP y una IP DLI, el dispositivo telefónico se registrará en la base de datos DLI y se mostrará un mensaje para ingresar el número de extensión.

5) Ingrese el número de terminal en el teléfono (el número debe ser el mismo configurado en el primer paso, por ejemplo, 4111).

6) Se iniciará la actualización y la nueva imagen HFA se descargará en el teléfono. Cuando el teléfono se reinicie, se registrará como un teléfono HFA y el sistema enviará los datos plug and play al teléfono.

7) **Para actualizar un teléfono SIP ya registrado:**

8) Cambie el dispositivo SIP que funciona a "Cliente del sistema".



9) Reinicia el teléfono

10) Se iniciará la actualización y la nueva imagen HFA se descargará en el teléfono. Cuando el teléfono se reinicie, se registrará como un teléfono HFA y el sistema enviará los datos plug and play al teléfono.

6 Puesta en servicio inicial por OpenScape Business S

Aquí se describe la configuración inicial de OpenScape Business S (también denominado “softswitch”, de forma abreviada). El softswitch y los componentes correspondientes están integrados en la LAN de clientes existente. Se configuran el acceso a Internet para la telefonía Internet y las extensiones conectadas.

Para OpenScape Business S, el software de comunicación OpenScape Business está instalado en el sistema operativo Linux SLES 12 SP5 de 64 bits o SLES 15 SP6 de 64 bits. El software de comunicación puede operar directamente con un servidor Linux o en un entorno virtual con VMware vSphere o Microsoft Hyper-V. La instalación del sistema operativo Linux se describe en la guía de instalación *OpenScape Business, Instalación del servidor Linux*.

La puesta en servicio inicial de OpenScape Business S se realiza con el programa de administración OpenScape Business Assistant (la "Gestión basada en Web" o"WBM").

Se describe la configuración de los componentes más utilizados. Usted no utilizará todos los componentes. Durante la configuración inicial, puede que tenga que elegir entre varias opciones en algunos puntos u omitir ajustes por completo, en función de los componentes que utilice.

En los siguientes capítulos encontrará información detallada sobre la administración de las prestaciones no incluidas en la configuración inicial.

Para realizar la puesta en servicio inicial hay que crear un esquema de direcciones IP y un plan de numeración.

Vista general de los pasos de instalación más importantes:

- Configuración de sistema
- Números de teléfono del sistema e interconexión
- Telefonía Internet
- Configuración de extensiones
- Registro de licencia
- Endurecimiento del sistema
- Almacenamiento de datos

6.1 Requisitos para la puesta en servicio inicial

El cumplimiento de los requisitos previos para la configuración inicial garantiza el correcto funcionamiento de OpenScape Business S.

General

En función del material utilizado (teléfonos...) y de la infraestructura existente, se aplicarán las siguientes condiciones generales:

- La infraestructura LAN (enrutadores de Internet, conmutadores, etc.) está presente y se puede utilizar.
- Los teléfonos IP están conectados a la LAN del cliente.
- El servidor Linux necesario para OpenScape Business S se instaló siguiendo las instrucciones de la *Guía de instalación del servidor Linux de*

OpenScape Business, se integró en la LAN del cliente y está listo para su uso.
- Todas las licencias necesarias para OpenScape Business S están presentes (por ejemplo, clientes UC, servicios de directorio, etc.).
- Existe un esquema de direcciones IP conocido.
- Existe y se conoce un plan de marcación (también llamado plan de numeración).

Software

El siguiente programa es necesario para instalar OpenScape Business S:

- DVD o imagen .ISO con el programa de comunicación OpenScape Business

  Contiene el programa de comunicación OpenScape Business. Este DVD o imagen .ISO está incluido en el paquete de entrega.
- DVD o memoria USB con sistema operativo Linux SLES 12 SP5 o SLES 15 SP6.

  Es posible que se necesite el DVD de Linux durante la instalación del software de comunicación OpenScape Business, ya que puede que algunos paquetes de software (RPM) necesarios para el software de comunicación deban instalarse posteriormente desde este DVD o imagen .ISO.

Administración

Para la configuración inicial de OpenScape Business S con OpenScape Business Assistant (WBM), se puede utilizar el servidor Linux o el PC de administración. El WBM se basa en el navegador y, por tanto, es independiente del sistema operativo.

- Navegadores web:

  Se admiten los siguientes navegadores web compatibles con HTML 5:

  – Microsoft Internet Explorer versión 11 y posteriores (PC administrador).
  – Microsoft Edge
  – Mozilla Firefox versiones 37.x y 38.x
  – Mozilla Firefox ESR versiones 24.x y 31.x
  – Google Chrome

  Si tiene instalada una versión antigua del navegador web, deberá instalar una versión actualizada antes de iniciar la configuración inicial del sistema.
- Java:

  Debe estar instalado Oracle Java 8 o superior o, en su defecto, OpenJDK 8. Si tiene instalada una versión anterior, deberá actualizarla a la última versión antes de empezar a configurar el sistema por primera vez.

- Resolución de pantalla: 1024x768 o superior

Cortafuegos

cuando se conecta a Internet, el servidor Linux necesita un cortafuegos para evitar accesos no autorizados desde el exterior. Después de instalar Linux, el cortafuegos de Linux está activado. El instalador del programa de comunicación ajusta la configuración del cortafuegos para que el programa de comunicación pueda funcionar de forma adecuada. Se abren los puertos para el programa de comunicación y se cierran todos los demás puertos.

Si se utiliza un cortafuegos externo en la red, debe desactivarse el cortafuegos de Linux y deben abrirse las direcciones y los puertos necesarios para el software de comunicación (véase Puertos utilizados).

Acceso a Internet

El PC servidor debe tener acceso a Internet de banda ancha para:

- Parches de seguridad y actualizaciones generales del software de Linux

OpenScape Business necesita una conexión a Internet para:

- Actualizaciones del programa OpenScape Business
- Funciones de OpenScape Business como la telefonía por Internet, por ejemplo
- OpenScape Business Mobility Clients como myPortal to go, por ejemplo.
- Servicio a distancia

Servidor de correo electrónico (opcional)

OpenScape Business requiere acceso a un servidor de correo electrónico para poder enviar mensajes. Para ello, los datos de acceso al servidor de correo electrónico deben introducirse en OpenScape Business y las cuentas correspondientes (dirección IP, URL, datos de inicio de sesión del servidor de correo electrónico) deben configurarse en el servidor de correo electrónico.

Si no se utiliza la función de correo electrónico en OpenScape Business, no es necesario introducir estos datos.

Telefonía por Internet, VoIP (opcional)

Si se utiliza la telefonía por Internet en OpenScape Business, OpenScape Business necesitará acceso de banda ancha a Internet y a un proveedor de servicios de telefonía por Internet (ITSP, proveedor SIP) para la telefonía SIP por Internet. Para ello, deben obtenerse las cuentas adecuadas del ITSP y deben configurarse en OpenScape Business los datos de acceso para el ITSP (dirección IP, URL, datos de inicio de sesión del proveedor SIP).

Segundo puerto LAN

Si OpenScape Business S (o el servidor Linux) tiene un segundo puerto LAN, puede utilizarlo como interfaz WAN para el acceso a Internet y telefonía Internet mediante un ITSP. El primer puerto LAN se utiliza como interfaz LAN para los PC y los teléfonos internos. La configuración del acceso a Internet se produce en el router de Internet externo de la LAN del cliente. La configuración del segundo puerto LAN se realiza durante la configuración inicial de Linux o puede realizarse más tarde mediante YaST. En el WBM, sólo es necesario activar el segundo puerto LAN como interfaz WAN.

Fax como PDF

Si los faxes deben guardarse en formato PDF, el PC servidor necesita al menos 4 GB de RAM. Si OpenScape Business S se utiliza en un entorno virtual, la máquina virtual también debe tener asignados 4 GB de RAM.

6.2 Componentes

A continuación se describen y resumen los componentes del ejemplo de instalación.

El ejemplo de instalación incluye estos componentes:

- OpenScape Business S

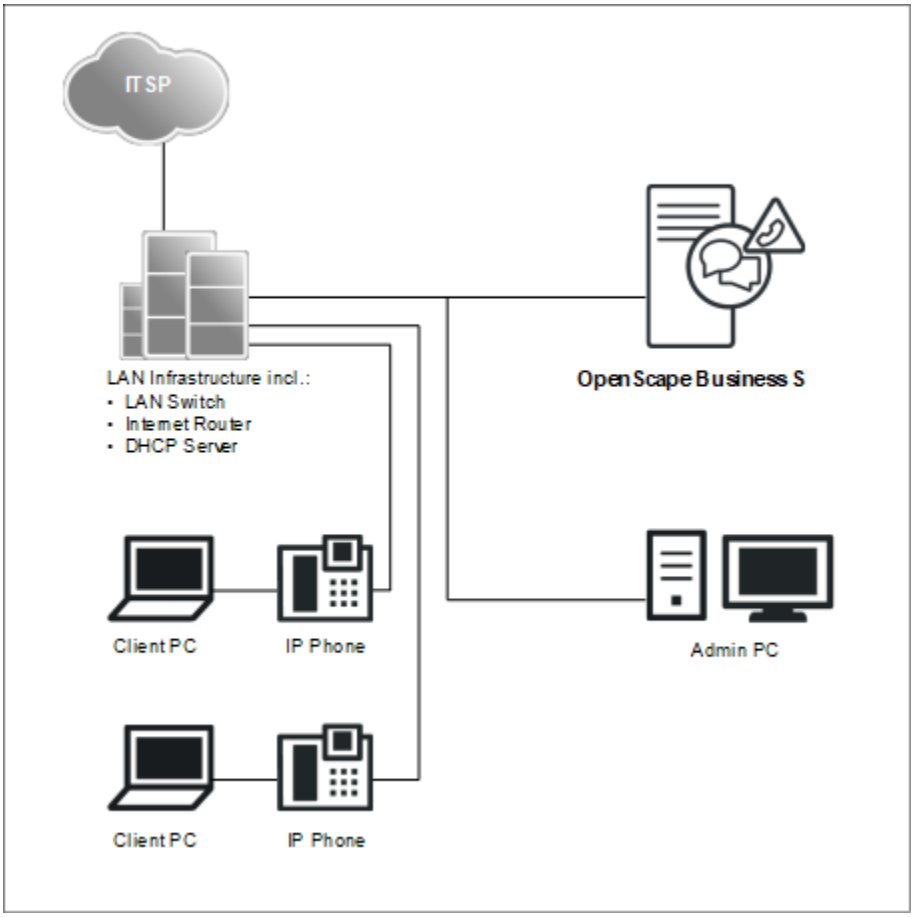
  El servidor Linux con el software de comunicación OpenScape Business S está integrado en la LAN de clientes existente a través de su interfaz LAN.
- PC de administración

  El PC de administración también se integra en la LAN de clientes existente a través de su interfaz LAN.
- Extensiones IP (Clientes IP)

  Las extensiones IP (teléfonos IP del sistema, PC de cliente, puntos de acceso WLAN...) se integran en la LAN a través de uno o varios conmutadores.

Un servidor DHCP interno (servidor DHCP del servidor Linux) o un servidor DHCP externo (servidor DHCP del router Internet) asigna dinámicamente las direcciones IP a los clientes IP.

El acceso a Internet está configurado en el router Internet.



6.3 Esquema de direcciones IP

Un esquema de direcciones IP define cómo se asignan las direcciones IP de la LAN de clientes. Incluye las direcciones IP de los PC, servidores, routers de Internet, teléfonos IP, etc.

Para conseguir una mejor visión general en la asignación de direcciones IP, es conveniente crear un esquema de direcciones IP.

Ejemplo de un esquema de direcciones IP con un rango de direcciones IP `192.168.5.x`:

Área direcc. IP	**Clientes**
hasta **192.168.5.1**	Clientes con dirección IP fija
192.168.5.1	Router interno (Gateway)
192.168.5.10	PC de servidor (OpenScape Business S)
192.168.5.20	Servidor de correo electrónico
192.168.5.100 hasta **192.168.5.254**	Clientes de PC y teléfonos IP, al mismo tiempo rango de dirección IP del servidor DHCP, la asignación de las direcciones IP a los clientes se realiza dinámicamente

6.4 Plan de numeración

Un plan de numeración es una lista de todos los números de teléfono disponibles en el sistema de comunicación. Contiene números de teléfono internos, números de marcación directa y números de llamada de grupo.

Plan de numeración estándar

Los números de teléfono internos tienen preasignados valores estándar. Si es necesario, puede ajustar estos valores a sus necesidades (plan de numeración individual).

Extracto del plan de numeración estándar:

Tipo de los números de teléfono	Números de teléfono estándar
Números de teléfono de extensión internos	100-349, 500-709
Números de marcación directa de extensión	100-349, 500-709
Número de llamada de grupos	350-439
Número del buzón de voz	71
Número de teléfono del Announcement Player	72
Códigos de ruta (códigos externos): ITSP de línea urbana	855-858

Tipo de los números de teléfono	Números de teléfono estándar
Número de teléfono para conferencias	7400-7404
Número de teléfono de aparcamiento	7405
Número de teléfono para AutoAttendant	7410-7429
Número de teléfono para conferencia Meet-Me	7430

Plan de numeración individual

Se puede importar un plan de numeración individual en la Gestión basada en Web (WBM) durante la configuración básica a través de un archivo XML.

El archivo XML incluye varios pestañas. La pestaña "Cliente" incluye además del nombre y del número de teléfono de la extensión otros datos como, por ejemplo, los tipos de extensiones y las direcciones de correo electrónico.

Puede consultar un ejemplo de archivo XML con la correspondiente explicación en la Gestión basada en Web (WBM), en **Centro de servicios** > **Documentos** > **Plantillas** > **Plantillas CSV**. El archivo XML ahí guardado también se puede utilizar como plantilla para sus datos. Se puede editar, por ejemplo, con Microsoft Excel.

6.5 Instalación del software de comunicación

El software de comunicación OpenScape Business S está instalado en el servidor Linux.

Asegúrese de que las direcciones IP y las máscaras de red que se configurarán sean adecuadas para la LAN del cliente.

Servidor DHCP

Un servidor DHCP asigna automáticamente una dirección IP única a cada estación IP (teléfonos IP, PC, etc.) y proporciona a las estaciones IP datos específicos de la red, como por ejemplo la dirección IP de la puerta de enlace predeterminada.

Se puede utilizar como servidor DHCP un servidor DHCP externo (por ejemplo, el servidor DHCP del enrutador de Internet o del sistema de comunicación) o el servidor DHCP del servidor Linux. Si se utiliza el servidor DHCP del servidor Linux, se debe deshabilitar el servidor DHCP externo. La configuración del servidor DHCP de Linux se puede realizar durante la instalación del software de comunicación OpenScape Business.

Nota: Debe activar DHCP desde yast o desde WBM, pero no desde ambos. Si activa el DHCP durante la instalación inicial de OpenScape Business S, es equivalente a activar el DHCP a través de yast. Si desea activar DHCP en OpenScape Business S desde WBM, entonces el DHCP no debe activarse durante la instalación inicial del software de comunicación.

Ambiente virtual

El software de comunicación puede ejecutarse en un entorno virtual. Hay dos formas de realizar la instalación:

- Instalación separada de Linux y el software de comunicación

  Para ello es necesario primero instalar y configurar el software de virtualización (sistema operativo del host) en el PC servidor. Linux se instala en el entorno virtual como sistema operativo invitado. Dentro del sistema operativo Linux, el software de comunicación se instala en último lugar con la ayuda del DVD de OpenScape Business o el archivo .ISO (consulte *OpenScape Business Linux Server, Guía de instalación* para más detalles).
- Instalación combinada de Linux y el software de comunicación (sólo VMWare)

  Para ello es necesario primero instalar y configurar el software de virtualización (sistema operativo del host) en el PC servidor. Se instala en el entorno virtual una imagen OVA (Open Virtualization Appliance), que incluye Linux y el software de comunicación. La imagen OVA se proporciona a través del servidor de suministro de software (SWS).

  Para más de 50 usuarios, la partición de inicio debe redimensionarse después de la instalación a 100 GB (para 50 a 100 usuarios) o 200 GB (para hasta 500 usuarios o para OpenScape Business Contact Center) o 500 GB (para más de 500 usuarios).

  Para las actualizaciones de Linux, también necesitará la clave de actualización de OpenScape Business SLES para poder registrarse en Linux.

Uso de instantáneas en máquinas virtuales (VM):

Las instantáneas pueden ser un mecanismo de mantenimiento valioso, por ejemplo, para realizar una reversión rápida a un estado operativo predefinido de la máquina virtual después de que falla un script de distribución masiva.

- No se pueden crear instantáneas durante el funcionamiento normal. El estado operativo actual de la máquina virtual está congelado mientras se toma una instantánea. En consecuencia, los terminales y aplicaciones conectados, como los teléfonos IP o los clientes UC, pueden perder la conexión con el servidor.
- Las instantáneas pueden provocar que los procesos internos del servidor pierdan su sincronización, lo que significa que ya no se puede garantizar el funcionamiento estable del sistema de comunicación. Por lo tanto, también se debe planificar un reinicio del servidor después de la instantánea dentro del período de mantenimiento.
- Las instantáneas anteriores no deben permanecer en el entorno de producción durante el funcionamiento normal.
- Se pueden tomar instantáneas durante una ventana de mantenimiento planificada o en el marco de la instalación.
- Las instantáneas se utilizan internamente mediante herramientas de respaldo como VDP o VDR. Se debe garantizar que estas operaciones de respaldo se programen fuera del horario comercial y que las instantáneas generadas por estas herramientas se eliminen al finalizar la operación.

Puede encontrar más información sobre las instantáneas en la base de conocimientos de VMware (KB). Un buen punto de partida es el artículo de Knowledge Base 1025279: Mejores prácticas para instantáneas de máquinas virtuales en el entorno VMware (`http://kb.vmware.com/kb/1025279`).

Toda la información sobre las instantáneas en Microsoft Hyper-V se puede encontrar en la biblioteca de TechNet en technet.microsoft.com dentro del capítulo Hyper-V.

6.5.1 Cómo instalar el software de comunicación

Requisitos previos

- El sistema operativo SLES 12 SP5 o SLES 15 SP6 se ha instalado e iniciado correctamente en el servidor Linux.
- DVD o archivo .ISO con el software de comunicación OpenScape Business.
- DVD o archivo .ISO o memoria USB con el sistema operativo Linux SLES 12 SP5 de 64 bits o SLES 15 SP6 de 64 bits, para cualquier instalación posterior de paquetes de software (RPM) que pueda ser necesaria.
- Los datos de acceso root (nombre de usuario y contraseña) para iniciar sesión en el servidor Linux están disponibles.

Importante: El software de comunicación OpenScape Business sobrescribe cualquier archivo de configuración existente (por ejemplo, para DHCP, FTP, Postfix, etc.) durante la instalación.

Paso a paso

1) Inicie sesión en el servidor Linux con privilegios de root.

2) Inserte el DVD de OpenScape Business o el archivo .ISO en la unidad de DVD.

3) Confirme el mensaje con **Ejecutar**. Se muestra la ventana "Welcome" (Bienvenido).

4) Seleccione el idioma de configuración deseado (por ejemplo, **inglés**) y haga clic en **Iniciar**. El resto de la instalación se describe aquí para el idioma inglés.

5) Elija el producto que desee de la lista y haga clic en **Seleccionar**. Se realiza una comprobación para determinar si el hardware cumple con todos los requisitos para la instalación. Se muestra una advertencia para deficiencias menores en el cumplimiento de los requisitos. Después de la confirmación, se puede continuar con la instalación. En el caso de deficiencias graves, la instalación se cancela automáticamente.

6) Se realiza una comprobación para determinar si es necesario instalar paquetes RPM adicionales. En caso afirmativo, confírmelo con **Confirmar**. Si esto ocurre, deberá volver a cambiar a SLES 12 o SLES 15, DVD o archivo .ISO más adelante.

7) Aparecerá una ventana con los términos de la licencia (es decir, el Acuerdo de licencia de usuario final o EULA). Lea los términos de la licencia y acepte el acuerdo de licencia con **Sí**.

8) Si ya hay un servidor DHCP en la LAN del cliente (por ejemplo, el servidor DHCP del router de Internet), detenga la configuración del servidor DHCP de Linux aquí con **No** y proceda al paso 12 para continuar.

Nota: Para garantizar que el software de los teléfonos del sistema se pueda actualizar automáticamente incluso

cuando se utiliza un servidor DHCP externo, tiene dos opciones:

a) La dirección IP del servidor Linux debe introducirse como dirección DLS en cada teléfono del sistema.

b) Los datos específicos de la red deben introducirse en el servidor DHCP externo. Los parámetros para esto se pueden encontrar en `/var/registro/OPTI.txt`.

---

9) Si desea utilizar el servidor DHCP de Linux, haga clic en **Sí** para habilitar y configurar el servidor DHCP de Linux.

10) Introduzca los siguientes valores (preestablecidos con valores predeterminados):

- **Ruta predeterminada**: dirección IP de la puerta de enlace predeterminada; por regla general, la dirección IP del router de Internet, p. ej., `192.168.5.1`.
- **Dominio** (opcional): el dominio especificado durante la instalación de Linux, p. ej., `<customer>.COM</customer>`
- **Servidor DNS** (Opcional): Dirección IP del servidor DNS especificado durante la instalación de Linux. Si no hay ningún servidor DNS disponible en la red interna, puede introducir la dirección IP del router de Internet (p. ej., `192.168.5.1`) aquí.
- **Servidor SNTP**: Dirección IP del servidor NTP interno o externo.
- **Servidor DLS/DLI**: Dirección IP del servidor DLS, es decir, la dirección IP del servidor Linux (p. ej.: `192.168.5.10`).
- **Subred**: subred apropiada para el rango de direcciones IP, p. ej.: `192.168.5.0`.
- **Netmask**: Máscara de subred del servidor Linux que se especificó durante la instalación de Linux, por ejemplo: `255.255.255.0`.
- **Comienza el rango de IP** y **Fin del rango IP**: Rango de direcciones IP desde el cual el servidor DHCP puede asignar direcciones IP, por ejemplo: `192.168.5.100` Para `192.168.5.254`.

11) Haga clic en **Continuar**.

12) Después de la instalación, es necesario reiniciar el sistema operativo Linux. Seleccione la casilla de verificación **Reinicio de PC** y confirme con **Continuar**.

13) Si es necesario instalar paquetes RPM adicionales, se le pedirá que inserte el DVD SLES 12 o la memoria USB SLES 15. Inserte el DVD o la memoria USB y confirme con **Continuar**. Después de instalar exitosamente los paquetes RPM, vuelva a insertar el DVD de OpenScape Business o el archivo .ISO y confírmelo con **Continuar**, seguido de **Ejecutar**.

14) Se ha instalado el software de comunicación OpenScape Business. A continuación, el sistema operativo realiza automáticamente un reinicio.

15) Después del reinicio, inicie sesión con la cuenta de usuario que se configuró anteriormente durante la instalación de Linux.

16) Haga clic con el botón derecho en el icono de la unidad de DVD en el escritorio y seleccione el elemento de menú **Expulsar**. Retire el DVD de OpenScape Business de la unidad de DVD.

Nota: Se tarda unos minutos en activar todos los componentes del software de comunicación OpenScape Business.

6.6 Puesta en servicio

Con el asistente **Instalación inicial** de la Gestión basada en Web (WBM) se realizan los ajustes de configuración básicos.

6.6.1 Cómo iniciar el asistente de instalación inicial

Requisitos previos

Se ha iniciado la Gestión basada en Web.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) Haga clic en **Editar** para iniciar el asistente **Instalación inicial**.

Nota: Si el tamaño de la ventana del navegador no puede mostrar el área de trabajo completa a bajas resoluciones de pantalla, aparecerá a los lados una barra de deslizamiento horizontal o vertical para desplazarse hasta la sección deseada.

Pasos siguientes

Realice la instalación inicial tal y como se describe a continuación, paso a paso. Los campos que no se describen aquí están preestablecidos de acuerdo al caso estándar y solo hay que modificarlos cuando no coincidan con sus datos de red. Encontrará información detallada en la descripción de los distintos asistentes de la documentación del administrador.

6.6.2 Configuración de sistema

En la ventana **Configuración de sistema**, configure los ajustes del sistema de comunicación.

Proceder de la siguiente manera:

1) Defina el logotipo en pantalla y la denominación de producto

Puede definir un texto que se mostrará en el display de los teléfonos el sistema. También puede seleccionar la denominación de producto.

2) Seleccionar el distintivo de país y el idioma para los registros de sucesos

Para que la inicialización del país sea correcta, debe seleccionar el idioma en el que estará en servicio el sistema de comunicación. Además, puede

seleccionar el idioma en el que se guardarán los registros de sucesos (protocolos de eventos del sistema, errores, etc).

3) Solo en caso necesario: active otro puerto LAN como interfaz WAN

   Si OpenScape Business S (o el servidor Linux) tiene un segundo puerto LAN, puede utilizarlo como interfaz WAN para el acceso a Internet y telefonía Internet mediante un ITSP. El primer puerto LAN se utiliza como interfaz LAN para los PC y los teléfonos internos.

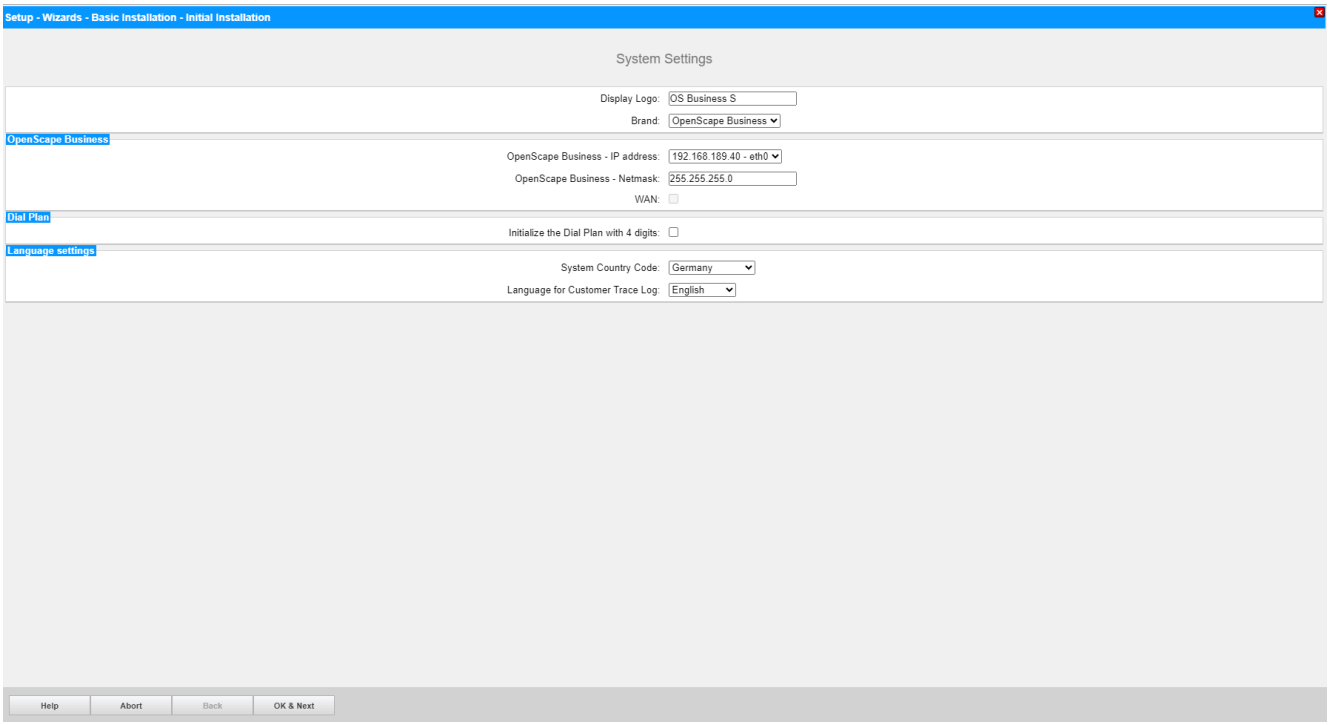
4) Cambie el plan de marcado predeterminado a números de 4 dígitos (disponible solo para OSBiz S)

   En una instalación nueva del sistema, puede inicializar el plan de marcado con 4 dígitos, en lugar de 3. Al hacerlo, se cambian los números predeterminados del sistema de 100, 101, 102, ... a 1000, 1001, 1002, etc. Esto permite la asignación automática de números de llamada para un gran número de estaciones de usuario. Tenga en cuenta que después de habilitar este indicador, el sistema se reinicia.

6.6.2.1 Cómo definir el logotipo de pantalla y la designación de producto

Requisitos previos

Se encuentra en la ventana **Configuración de sistema**.



Paso a paso

1) En el campo **Mostrar logotipo** introduzca el texto que usted elija (p. ej. OS Business S). El texto puede tener como máximo 16 caracteres. Evite el uso de diéresis y caracteres especiales.
2) En la lista desplegable **Marca**, seleccione la denominación del producto.

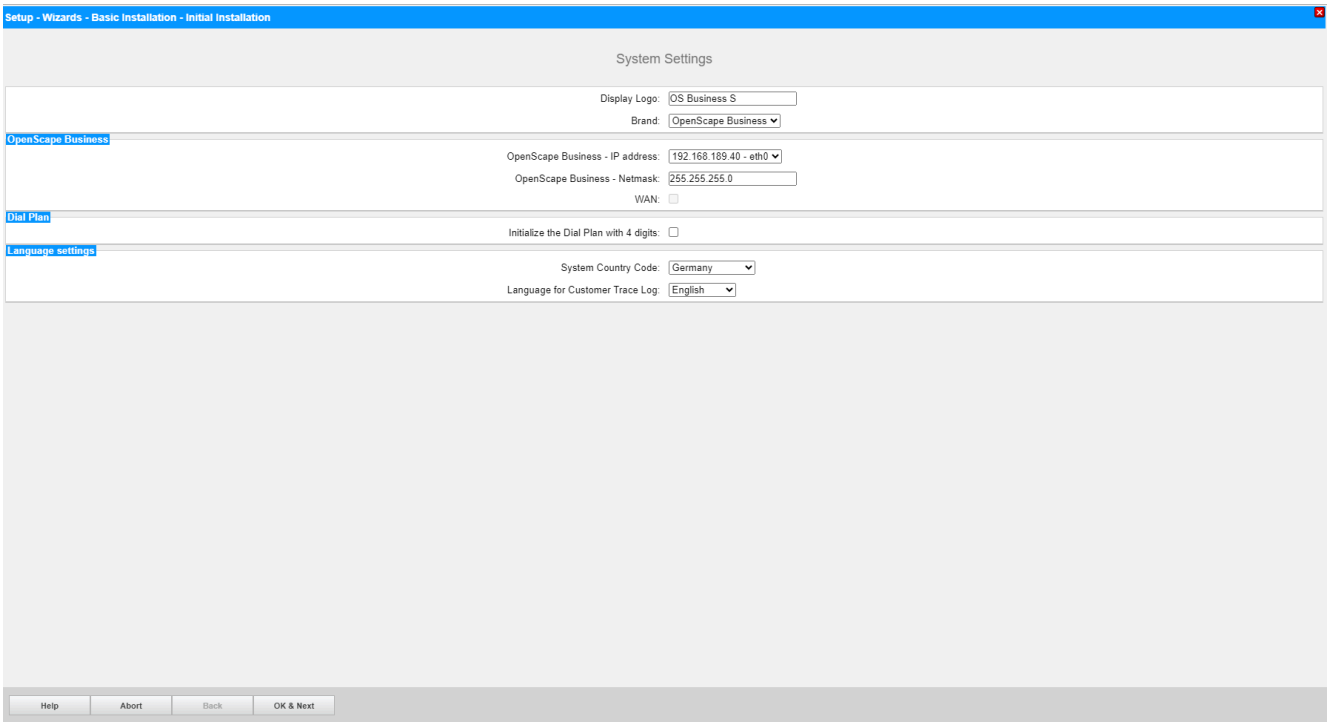
Pasos siguientes

Seleccione el código de país y el idioma que se utilizarán para los registros de seguimiento.

6.6.2.2 Cómo seleccionar el código de país y el idioma para los registros de seguimiento

Requisitos previos

Se encuentra en la ventana **Configuración de sistema**.



Paso a paso

1) En la lista desplegable **Código de país del sistema** seleccione el país en el que estará en funcionamiento el sistema de comunicación.
2) En el campo **Idioma para el registro de seguimiento del cliente**, ingrese el idioma en el que se generarán los registros de eventos (registros de eventos del sistema, registros de errores, etc.).

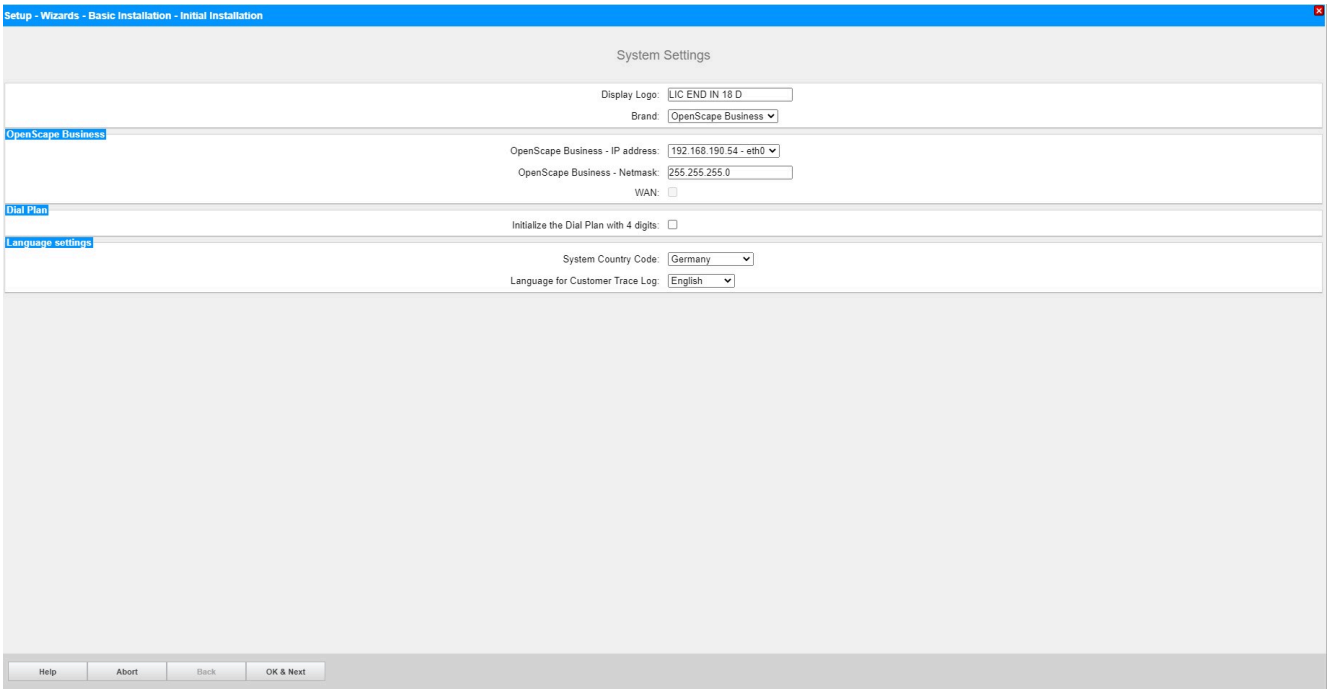
Pasos siguientes

Iniciar la configuración básica.

6.6.2.3 Cómo activar un puerto LAN adicional como interfaz WAN

Requisitos previos

Se encuentra en la ventana **Configuración de sistema**.



Paso a paso

1) Seleccione la casilla de verificación **WAN**.
2) Seleccione el puerto LAN deseado (por ejemplo, `eth1` o `eth2`) de la lista desplegable **OpenScape Business - Dirección IP (WAN)**. Si solo hay dos puertos LAN disponibles, el segundo puerto LAN `eth1` se activa automáticamente.

Importante: Asegúrese de seleccionar la interfaz de red real, en lugar del host local.

Nota: La asignación de direcciones IP y máscaras de subred a los puertos LAN se realiza durante la instalación inicial de Linux o posteriormente a través de YaST.

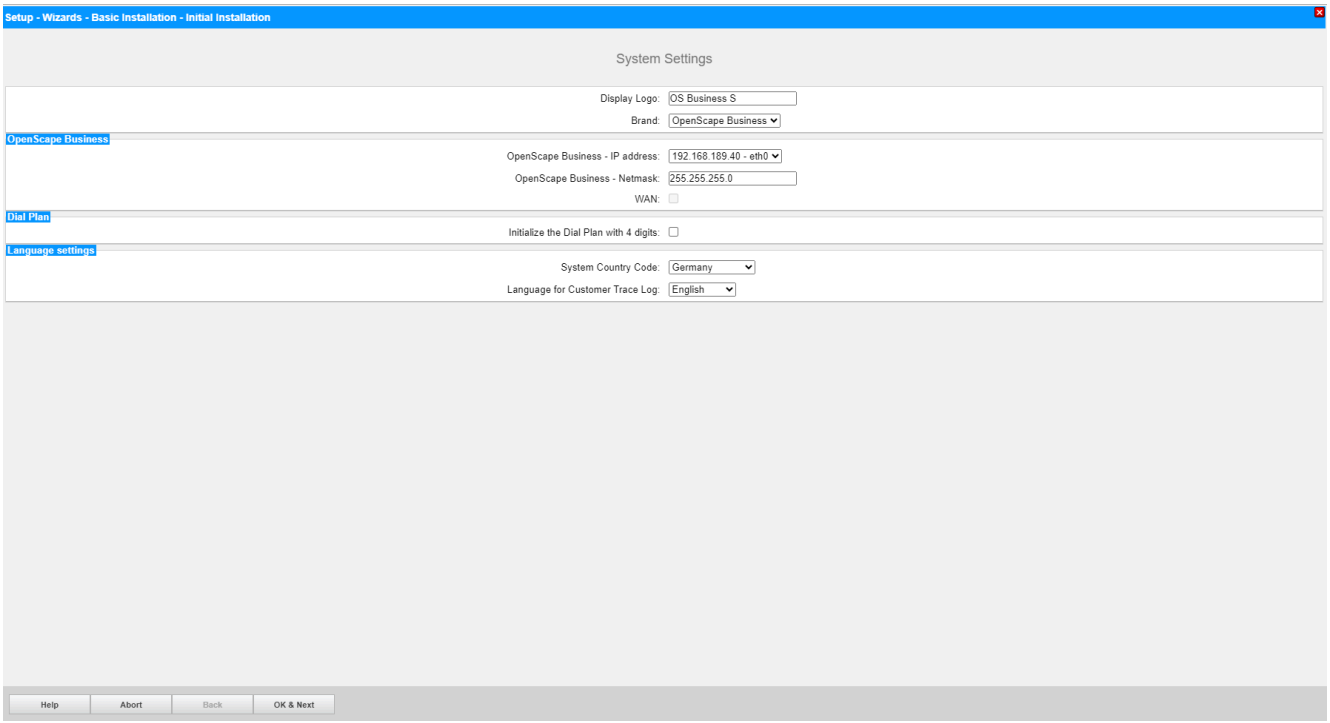
Pasos siguientes

Especifique la solución UC.

6.6.2.4 Cómo cambiar el plan de marcado a 4 dígitos

Requisitos previos

Se encuentra en la ventana **Configuración de sistema**.



Paso a paso

Haga clic en la casilla de verificación del campo **Inicializar el plan de marcado con 4 dígitos.**

Pasos siguientes

El sistema se reinicia

6.6.3 Solución UC

En la ventana **Modificar selección de aplicación** puede definir qué solución de UC utiliza.

Tiene las siguientes opciones:

- **Paquete con UC Smart**

  La solución de Comunicaciones Unificadas UC Smart está integrada en OpenScape Business S.
- **Paquete con UC Suite**

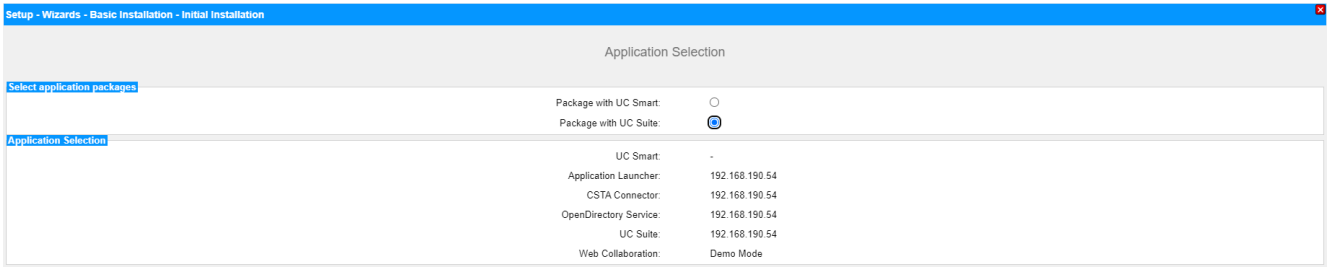
  La solución de Comunicaciones Unificadas UC Suite está integrada en OpenScape Business S.

6.6.3.1 Cómo establecer la solución UC

Requisitos previos

Ha adquirido licencias para la solución de Comunicaciones Unificadas UC Smart o para la solución de Comunicaciones Unificadas UC Suite.

Se encuentra en la ventana de **Selección de aplicación**.



Paso a paso

1) Si utiliza la solución de Comunicaciones Unificadas UC Smart, haga clic en **Paquete con UC Smart**.
2) Si utiliza la solución de Comunicaciones Unificadas UC Suite, haga clic en **Paquete con UC Suite**.
3) Haga clic en **OK & Continuar**.
4) Se ha completado el asistente **Instalación inicial**. Haga clic en **Finalizar**.

Pasos siguientes

Iniciar la configuración básica.

6.7 Configuración básica

La configuración básica se realiza con el asistente **Instalación básica** de la Gestión basada en Web (WBM). Se definen los ajustes más importantes para el funcionamiento del sistema de comunicación.

El asistente de Instalación básica incluye un indicador de progreso con el paso actual y una indicación de los pasos siguientes.

6.7.1 Cómo iniciar el Asistente Configuración básica

Requisitos previos

Se ha completado el asistente **Instalación inicial**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) Haga clic en **Editar** para iniciar el asistente **Configuración básica**.

Pasos siguientes

Realice la Configuración básica tal y como se describe a continuación, paso a paso. Los campos que no se describen aquí están preestablecidos de acuerdo al caso estándar y solo hay que modificarlos cuando no coincidan con sus datos de red. Encontrará información detallada en la descripción de los distintos asistentes de la documentación del administrador.

6.7.2 Números de teléfono del sistema e interconexión

En la ventana **Resumen**, indique los números de teléfono del sistema (número de teléfonos del sistema, prefijo nacional y local, prefijo internacional) y establezca si desea interconectar OpenScape Business con otros sistemas OpenScape Business.

Para ello, siga este procedimiento:

1) Introducir números de teléfono del sistema

- Introducir números de teléfono del sistema para una conexión de centralita

  Aquí se indica el número de teléfono del sistema para su conexión de centralita y el prefijo nacional y local.

  Es imprescindible introducir el prefijo de país para la telefonía Internet y para las funciones de servidor de conferencias.

  El prefijo internacional está predefinido en función del código de país marcado antes.
- Introducir números de teléfono del sistema para acceso individual RDSI

  Aquí se indica el prefijo nacional y local para el acceso individual RDSI.

  Es imprescindible introducir el prefijo de país para la telefonía Internet y para las conferencias MeetMe.

  El prefijo internacional está predefinido en función del código de país marcado antes.

2) Activar y desactivar Interconexión.

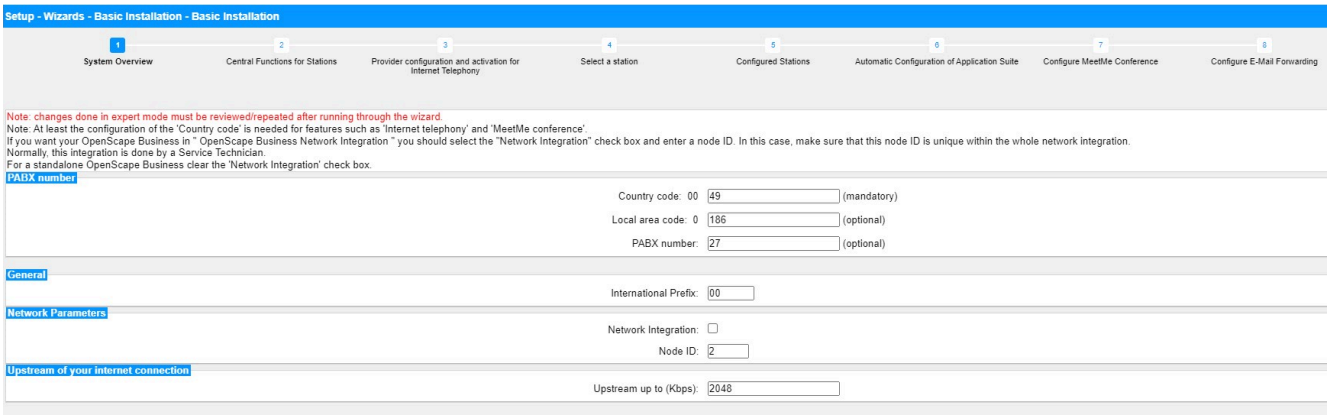
Si desea interconectar OpenScape Business con otros sistemas OpenScape Business, hay que activar Interconexión y hay que asignar un ID de nodo a OpenScape Business. Cada OpenScape Business debe tener un ID de nodo único en la interred.

6.7.2.1 Cómo introducir el número de teléfono del sistema para una conexión de centralita

Requisitos previos

Tiene una conexión de centralita.

Se encuentra en la ventana **Resumen** del asistente **Configuración básica**.



Paso a paso

1) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo `49` para Alemania o `1` para EE. UU.
2) En el campo **Código de red local**, indique el prefijo local, por ejemplo `89` para Múnich.
3) En **Nº tel. sistema**, indique el número del sistema de conexión urbana, p. ej. `7007` (su número de conexión).
4) Solo debe cambiar el campo **Prefijo internacional** cuando sea necesario. Para Alemania se usa `00` y para EE. UU. `011`).

   En las llamadas al extranjero, delante del número de teléfono se pone el prefijo internacional y el prefijo del país. Por ejemplo, de Alemania a EE.UU "00-1-..." y de EE. UU. a Alemania "011-49-...".

Pasos siguientes

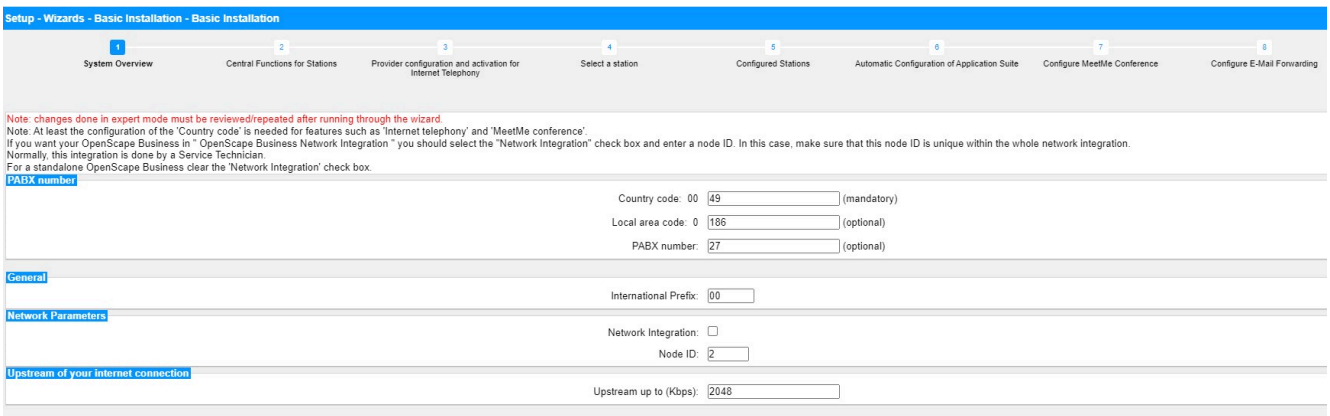
Activar y desactivar Interconexión.

6.7.2.2 Cómo introducir los números de teléfono del sistema para un acceso individual

Requisitos previos

Tiene un acceso individual.

Se encuentra en la ventana **Resumen** del asistente **Configuración básica**.



Paso a paso

1) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo `49` para Alemania o `1` para EE. UU.
2) En el campo **Código de red local**, indique el prefijo local, por ejemplo `89` para Múnich.
3) Deje vacío el campo **Nº teléfono del sistema**.
4) Solo debe cambiar el campo **Prefijo internacional** cuando sea necesario. Para Alemania se usa `00` y para EE. UU. `011`).

   En las llamadas al extranjero, delante del número de teléfono se pone el prefijo internacional y el prefijo del país. Por ejemplo, de Alemania a EE.UU "00-1-..." y de EE. UU. a Alemania "011-49-...".

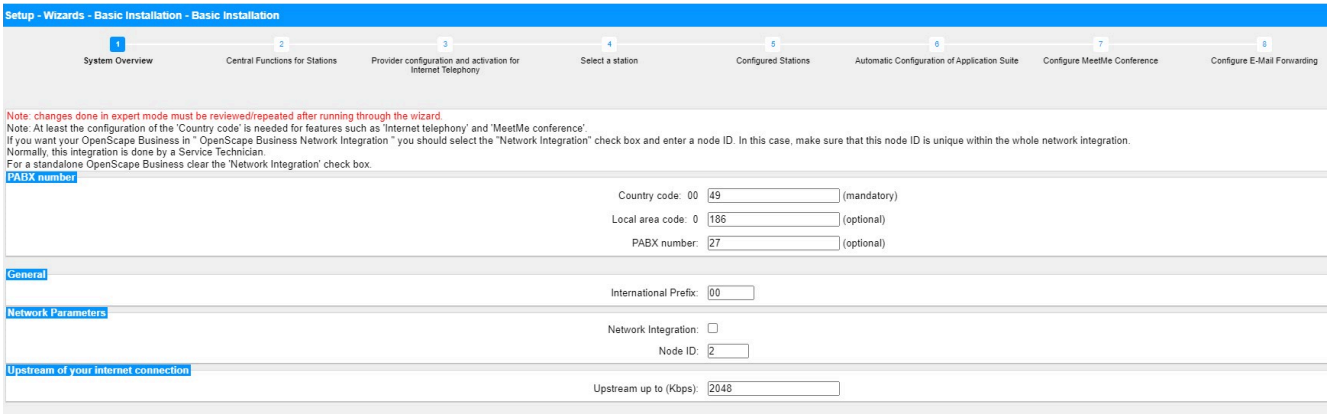
Pasos siguientes

Activar y desactivar Interconexión.

6.7.2.3 Cómo activar o desactivar la interconexión

Requisitos previos

Se encuentra en la ventana **Resumen** del asistente **Configuración básica**.



Paso a paso

1) Si se quiere interconectar el sistema de comunicación con otros sistemas de comunicación:
   a) Active **Integración de red**.
   b) En el campo **ID de nodo** para el sistema de comunicación asigne un ID de nodo único en la interred (se pueden usar cifras del `1` al `100`).
2) Si no se quiere interconectar el sistema de comunicación con otros sistemas de comunicación, deje desactivada la casilla de verificación **Integración de red**.

Pasos siguientes

Configure el flujo ascendente de su conexión a Internet.

6.7.2.4 Cómo configurar el flujo ascendente de su conexión a Internet

Requisitos previos

Se encuentra en la ventana **Resumen**.

Paso a paso

1) En el campo **Flujo saliente hasta (Kbit/s)**, introduzca la velocidad de su conexión a Internet.
2) Haga clic en **OK & Continuar**.

Pasos siguientes

Configurar datos de extensión.

6.7.3 Datos de extensión

Si es necesario, en la ventana **Funciones centrales para extensiones** puede configurar su plan de numeración individual en lugar del plan de numeración estándar predefinido e importar más datos de extensión. En la interred hay que ajustar el plan de numeración estándar al plan de numeración de la interred.

El plan de numeración estándar incluye números de teléfono predefinidos para distintos tipos de extensión (teléfonos IP, teléfonos analógicos...) y para funciones especiales (telefonía Internet, buzón de voz, AutoAttendant...).

Los datos de extensión incluyen, entre otros, los números de teléfono internos, los números de marcación directa y los nombres de las extensiones. Estos datos y otros datos de extensión se pueden importar en el sistema de comunicación durante la configuración básica mediante un archivo XML en formato UTF-8.

Nota:

Puede consultar una plantilla XML con la correspondiente explicación en la Gestión basada en Web (WBM), en **Centro de servicios** > **Documentos** > **Plantillas CSV**. En esta plantilla puede introducir sus datos, por ejemplo con Microsoft Excel.

Tiene las siguientes opciones:

- **Configurar datos de extensión sin interred**

  Para ello, siga este procedimiento:

  1) Mostrar datos de extensión

  Puede mostrar todos los datos de extensión y los números de teléfono preconfigurados.

  2) Borrar todos los números de llamada de extensión (opcional)

  Si utiliza un plan de numeración individual hay que borrar todos los números de teléfono preconfigurados.

  3) Ajustar números de teléfono preconfigurados al plan de numeración individual (opcional)

  Si utiliza un plan de numeración individual, puede ajustar los números de teléfono preconfigurados al plan de numeración propio.

  Nota:

  Si el usuario pasa por **Cambiar números de función y de llamada preconfigurados,** debe revisarse o repetirse todas las configuraciones personalizadas existentes realizadas en UC Suite (por ejemplo, colas piloto).

  ---

  4) Importar datos de extensión mediante un archivo XML (opcional)

  Puede importar sus números de teléfono individuales (con los datos de extensión adicionales) cómodamente durante la configuración básica mediante un archivo XML.

- **Configurar datos de extensión con interred**

  Para ello, siga este procedimiento:

  1) Borrar todos los números de llamada de extensión.

  Si en la interred se utiliza la UC Suite, hay que usar un plan de numeración cerrado, es decir: todos los números de teléfono de la interred deben ser únicos. Por ello, hay que borrar los números de teléfono preconfigurados y utilizar números adecuados para la interred.

  2) Importar datos de extensión mediante un archivo XML

  Los números de teléfono adaptados a la interred se deben importar junto con los datos de extensión adicionales durante la configuración básica mediante un archivo XML. El proceso es muy sencillo. Este archivo puede incluir todas las extensiones de la interred. En la importación se aplican únicamente los números de teléfono y los datos de extensión asignados previamente a los ID de nodo del sistema de comunicación.

Tareas relacionadas

Cómo mostrar datos masivos en la página 166

Cómo restablecer las entradas LCR en la página 1442

Referencia relacionada

LCR > Flags LCR en la página 1641

6.7.3.1 Cómo mostrar los datos de extensión

Requisitos previos

Se encuentra en la ventana **Funciones centrales para extensiones** del asistente **Configuración básica**.

Paso a paso

1) Active campo opción **Mostrar configuración extensiones**.
2) Clic en **Ejecutar función**. Aparece una lista de las extensiones con números de teléfono preconfigurados (Plan de numeración estándar).
3) Clic **Acept**. Regresa a la ventana **Funciones centrales para extensiones**.
4) Si no quiere modificar ningún dato de extensión, haga clic en **OK & Continuar**.

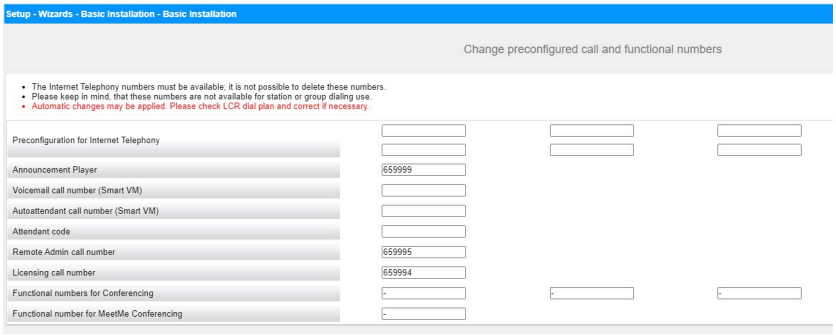
6.7.3.2 Cómo borrar todos los números de llamada

Requisitos previos

Se encuentra en la ventana **Funciones centrales para extensiones** del asistente **Configuración básica**.

Paso a paso

1) Active la opción **Borrar todos nos. llamada**.
2) Active la casilla de verificación **Borrar todos nos. llamada**.
3) Haga clic en **Ejecutar función**. Todos los números de teléfono preasignados se aliminan excepto **Reproductor de anuncios, Núm. llam. de administración remota** y **Núm. llam. de registro de licencia**. A continuación aparece la ventana **Cambiar números de función y de llamada preconfigurados**.



4) Ajuste los códigos y los números de teléfono especiales a sus necesidades y a continuación haga clic en **Aceptar**. Regresa a la ventana **Funciones centrales para extensiones**.
5) Si no desea modificar más datos de extensión, haga clic en **OK & Continuar**.

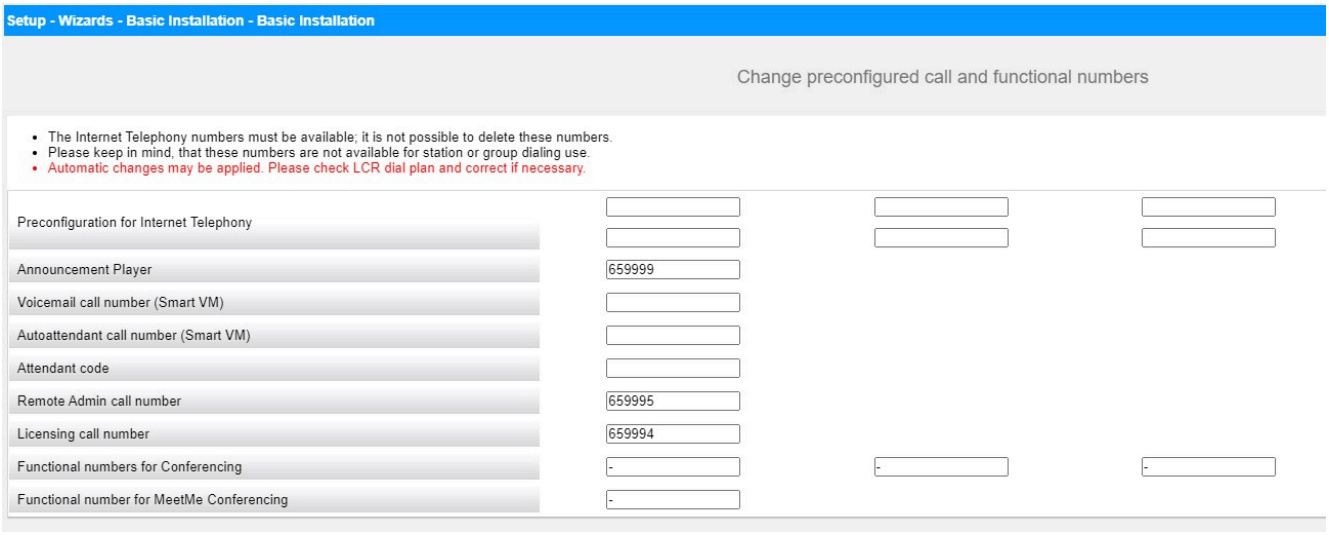
6.7.3.3 Adaptar los números de teléfono preconfigurados al plan de numeración individual

Requisitos previos

Se encuentra en la ventana **Funciones centrales para extensiones** del asistente **Configuración básica**.

Paso a paso

1) Active el campo de opción **Cambiar números de función y de llamada preconfigurados**.
2) Haga clic en **Ejecutar función**. Se abre la ventana **Cambiar números de función y de llamada preconfigurados**.



3) Adapte los números de teléfono preconfigurados a sus necesidades y a continuación haga clic en **Aceptar**. Regresa a la ventana **Funciones centrales para extensiones**.
4) Si no desea modificar más datos de extensión, haga clic en **OK & Continuar**.

6.7.3.4 Cómo importar los datos de extensión mediante un archivo XML

Requisitos previos

Se encuentra en la ventana **Funciones centrales para extensiones** del asistente **Configuración básica**.

Hay disponible archivo XML UTF-8 con los datos registrados. Puede consultar una plantilla XML en **Centro de servicios** > **Documentos** > **Plantillas CSV**.

Paso a paso

1) Active la opción **Importar archivo CSV/XML con datos de extensión**.
2) Haga clic en **Ejecutar función**.
3) Mediante **Examinar**, seleccione el archivo XML deseado y haga clic en **Abrir**.
4) Luego, haga clic en **OK**. Se importan los datos de extensión.

5) Haga clic en **OK y Continuar**.

6.7.4 Acceso a Internet

6.7.4.1 Cómo configurar el acceso a Internet a través de un enrutador de Internet externo sobre la LAN con un puerto WAN dedicado a ITSP

Requisitos previos

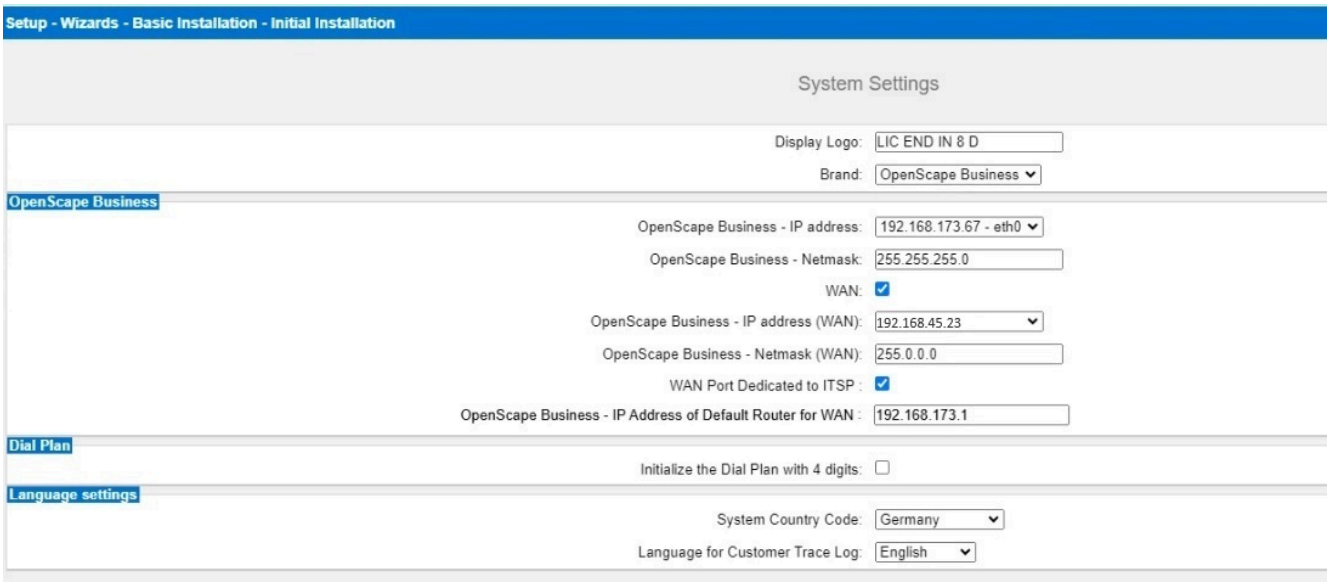
Ha creado una nueva interfaz de red en SLES.

Se encuentra en la ventana **Configuración del sistema** del asistente de **instalación inicial**.

Tenga en cuenta que esta función solo se aplica a los ITSP que no requieren el uso de STUN en la configuración del proveedor.

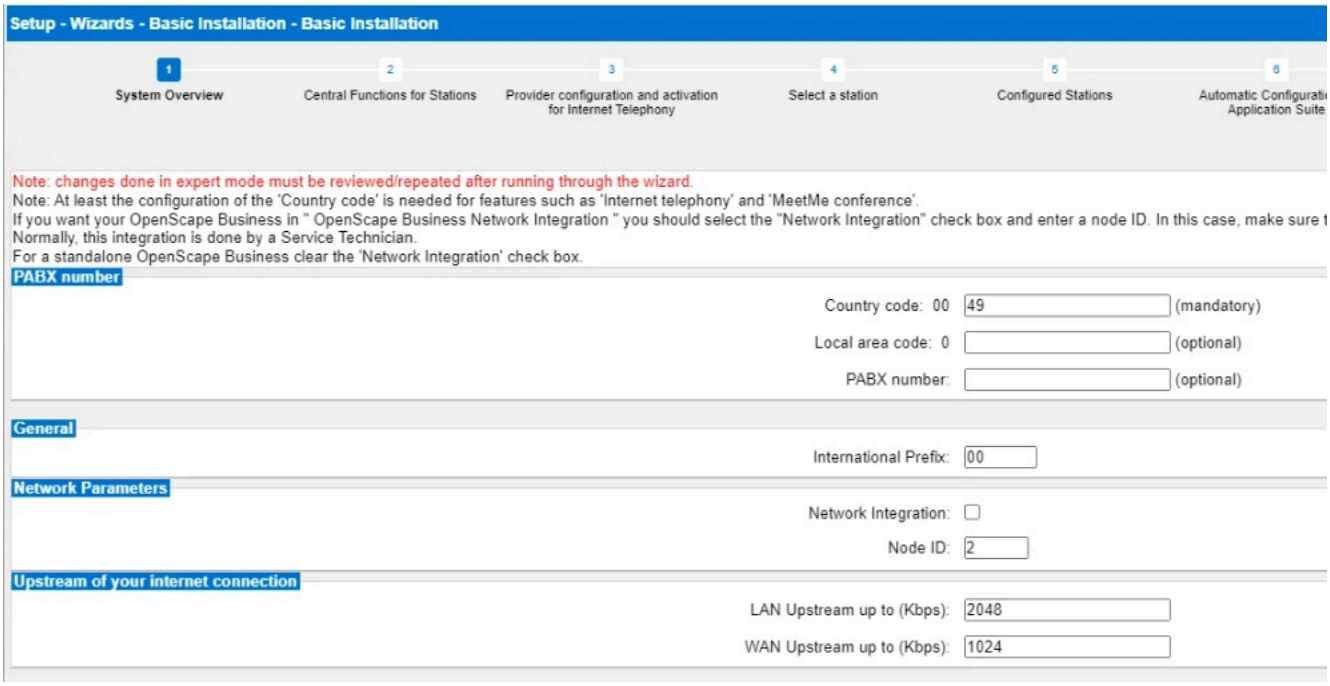
Paso a paso

1) Habilite la casilla de verificación **WAN** y seleccione la interfaz de red adecuada.
   La opción **Interfaz WAN dedicada a ITSP** se hace disponible.
2) Haga clic para habilitar la casilla de verificación **Interfaz WAN dedicada a ITSP.**



3) Haga clic en **Aceptar & Siguiente**.
4) Vaya a **Configuración > Instalación básica** y ejecute el asistente **Instalación básica**.

5) Configure los valores máximos de subida en los campos correspondientes **Subida de LAN hasta (Kbps)** y **Subida de WAN hasta (Kbps).**



6) Haga clic en **Aceptar & Siguiente**.

7) Después de aplicar la configuración, es necesario reiniciar el sistema.

6.7.5 Telefonía Internet

En la ventana **Configuración y activación de proveedor para telefonía Internet** puede configurar la Telefonía Internet. Puede configurar ITSP (Internet Telephony Service Providers) nuevos o preconfigurados. Por cada ITSP se pueden configurar una o varias cuentas. Puede haber activos hasta 8 ITSP de manera simultánea.

Tiene las siguientes opciones:

- **Configurar ITSP preconfigurados**

  Puede utilizar plantillas de ITSP predefinidas. En estas plantillas se registran los números de acceso y los números de teléfono propios y, a continuación, se activan.
- **Configurar ITSP nuevos**

  También puede añadir y activar ITSP nuevos.

  Configurar un nuevo ITSP solo es necesario en contadas ocasiones y es un proceso complejo. Por ello, esta opción no se describe en la instalación inicial. Encontrará información más precisa en el capítulo Configuración de un ITSP.
- **Desactivar telefonía Internet**

  Puede desactivar la telefonía Internet.

Nota:

En Internet, en la **wiki para expertos en Internet** (*OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*, puede consultar ejemplos de configuración.

Asignación de los números de teléfono de ITSP

- En las **conexiones de extensión de telefonía por Internet**, el ITSP proporciona números de teléfono individuales (p.ej. 70005555, 70005556, etc.). Estos números se asignan de forma manual a los números de teléfono internos de las extensiones.
- En las **conexiones de centralita de telefonía por Internet**, el ITSP proporciona un área de números de teléfono (p.ej. de (+49) 89 7007-100 a (+49) 89 7007-147). Los números de teléfono del área se asignan de forma manual a los números de teléfono internos de las extensiones.

Los dos tipos de conexión se pueden combinar.

Como alternativa, para ambos tipos de conexión, en la configuración de las extensiones se pueden registrar los números de teléfono del ITSP como números de marcación directa de las extensiones.

Número de llamada Interno	Nombre	Marcación directa
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

Los números de teléfono del ITSP resultan del número de teléfono de centralita configurado (p.ej. código de país 49) y de los números de marcación directa registrados en formato largo. Esto supone ciertas ventajas en la evaluación de la marcación y la gestión de llamadas, también en una interred. Así, por ejemplo, la conexión ITSP tiene capacidad de marcación directa a otro nodo.

En este caso, solo se puede establecer otra conexión de línea urbana mediante RDSI con restricciones (útil por ejemplo para llamadas de emergencia).

6.7.5.1 Cómo configurar un ITSP predefinido

Requisitos previos

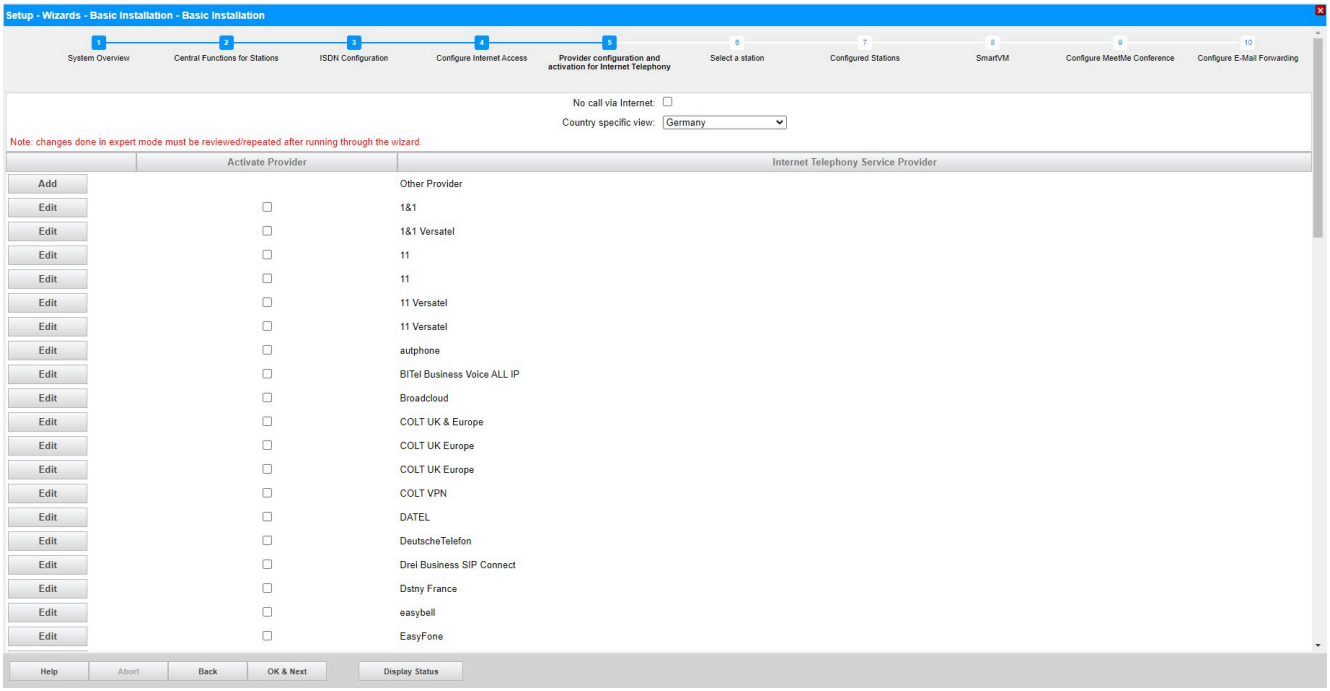
Se encuentra en la ventana **Configuración y activación de proveedor para telefonía Internet** del asistente **Configuración básica**.

La conexión a Internet está lista para el servicio.

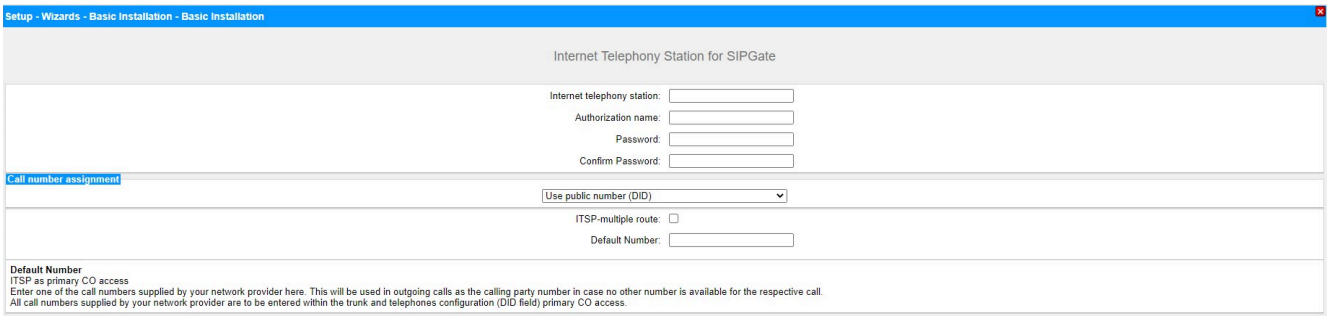
Dispone de los datos de acceso a Internet de su ITSP (p. ej. identificación de usuario, contraseña, números de teléfono de las extensiones de telefonía Internet).

Paso a paso

1) Borre la casilla de verificación **No hay llamada vía Internet**. Se muestra una lista de los ITSP disponibles en función del país. La lista contiene el ITSP predefinido para el país seleccionado y el ITSP ya creado (si lo hay).



2) Si desea modificar el país preestablecido, en la lista desplegable **Vista específica de país** seleccione el país deseado. Se muestran los ITSP disponibles para el país seleccionado.
3) Si es necesario, haga clic en **Mostrar estado**, para consultar qué ITSP están ya activados y qué extensiones de telefonía Internet están configuradas para cada uno de los ITSP. Se pueden activar, como máximo, 8 ITSP. Haga clic en **Aceptar** cuando esté terminado.
4) En la línea del ITSP correspondiente, haga clic en **Editar** para configurar un ITSP predefinido.
5) Active la casilla de verificación **Activar proveedor**.
6) Haga clic en **Aceptar & Siguiente**.
7) Haga clic en **Agregar** para configurar sus cuentas ITSP con los números de telefonía Internet correspondientes. Los campos que aparecen dependen del proveedor.



8) En el campo **Extensión de telefonía por Internet**, introduzca los datos de acceso de su cuenta. Los datos le son suministrados por su ITSP. En

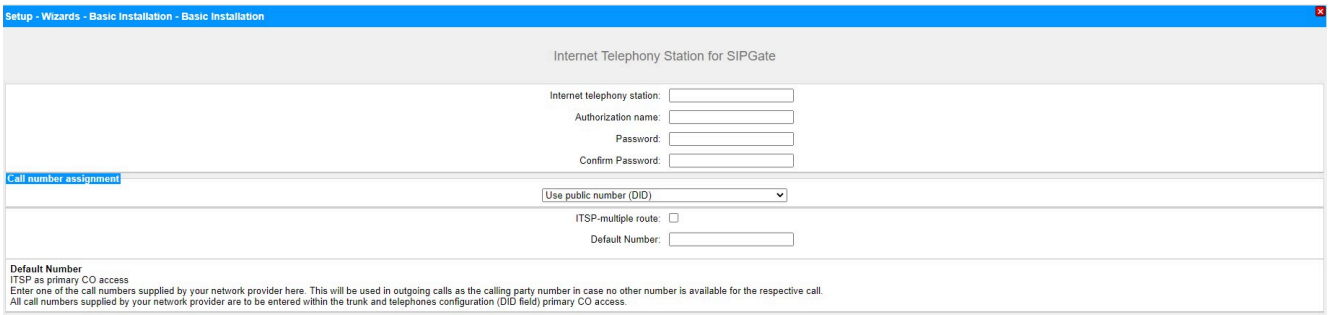
función del ITSP se utilizarán aquí distintas denominaciones (por ejemplo, Usuario SIP, ID SIP, etc.

9) En el campo **Nombre de autorización**, introduzca el nombre de autorización. Los datos le son suministrados por su ITSP. Si no ha recibido ningún nombre de autorización, indique los mismos datos en **Extensión de telefonía por Internet**.

10) En los campos **Nueva contraseña** y **Repetir clave** introduzca la contraseña que le ha suministrado el ITSP. En función del ITSP se utilizarán aquí distintas denominaciones (por ejemplo, Contraseña, Contraseña SIP, etc.)

11) Asignación de números de teléfono de telefonía por Internet - Opción 1:

Número de teléfono público (DuWa): los números de telefonía por Internet de su conexión de extensión de telefonía por Internet o de la conexión de sistema de telefonía por Internet no se registran aquí con la configuración de ITSP, sino en la configuración de extensión, en los campos **Marc. dir.**.



a) En el área **Asignación de números de teléfono**, seleccione el campo de opción **Número de teléfono público (DuWa)**.

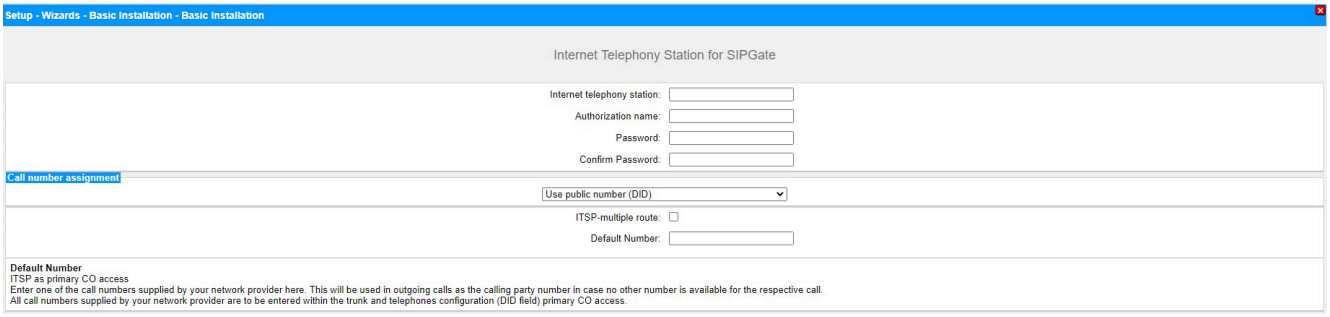
b) En **Número predeterminado**, ingrese el número de teléfono que se utilizará para las llamadas salientes cuando no haya ningún número DID de la persona que llama disponible.

c) Si su ITSP admite la prestación "Mobile Extension (MEX)", en **Número MEX** introduzca el número MEX que le haya proporcionado el ITSP (8 posiciones, solo números).

12) Asignación de números de teléfono de telefonía por Internet - Opción 2:

Usar número interno (CalIno) / Entradas individuales: Tiene una conexión a una estación de telefonía por Internet y ha recibido números de llamada individuales como números de teléfono de telefonía por Internet

(p. ej. 70005555, 70005556,...). A continuación, asigne estos números a los números de teléfono internos de las extensiones.



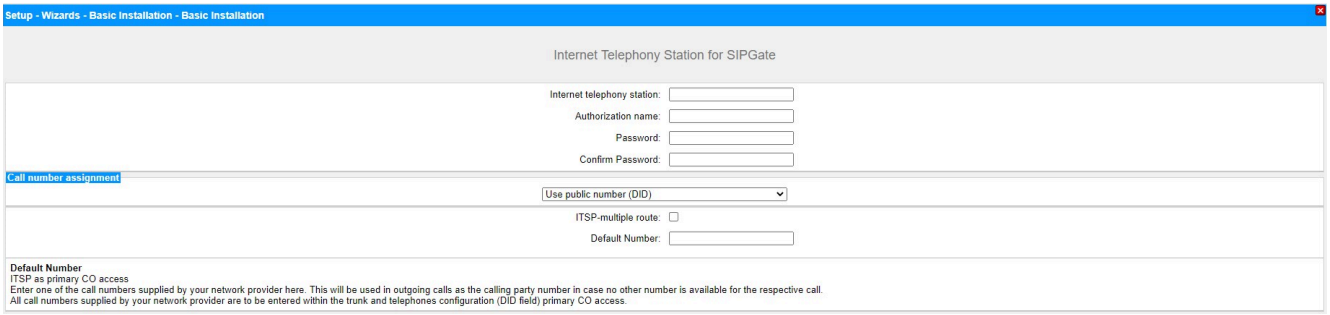
a) En el área **Asignación de números de teléfono**, seleccione el campo de opción **Utilizar número interno (n.º llamada)/Entradas individuales**.

b) En el área **Números de llamada de extensión de telefonía DSL**, y en el campo junto al botón **Agregar**, introduzca un número de teléfono de telefonía Internet que le haya sido comunicado por el proveedor de servicios de telefonía por Internet y haga clic en **Agregar**.

c) Si desea asignar a la cuenta más números de telefonía Internet, repita el paso b).

13) Asignación de números de teléfono de telefonía por Internet - Opción 3:

Usar número interno (CalIno) / Entrada de rango: Tiene una conexión de centralita de telefonía por Internet y ha recibido un intervalo de números de teléfono como números de teléfono de telefonía Internet, por ejemplo (+49) 89 7007-100 a (+49) 89 7007-147. A continuación, asigne los números de llamada del intervalo de números de llamada a los números de llamadas internas de los suscriptores.



a) En el área **Asignación de números de teléfono**, seleccione el campo de opción **Utilizar número interno (n.º llamada)/Intervalo**.

b) En **Número de llamada del sistema (prefijo)** introduzca el número de teléfono del sistema.

c) En los campos **Rango de marcación directa de** y **hasta** indique el rango de marcación directa deseado para la extensión de telefonía por Internet. Por defecto están registrados los valores 100 - 147.

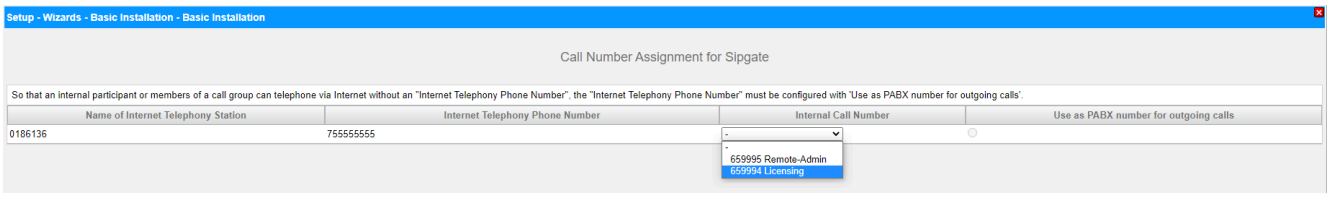
14) Haga clic en **Aceptar & Siguiente**.

15) Si desea configurar más cuentas con los números de telefonía Internet correspondientes, repita los pasos del 7 al 14.

16) Haga clic en **Aceptar & Siguiente**. Verá un resumen con los números de teléfono de telefonía Internet asignados y a qué cuentas lo están.

17) Asigna todos los números de telefonía por Internet a un número de teléfono interno de una extensión.

No es necesario dar este paso si para asignar los números de telefonía por Internet ha seleccionado la opción 1. En este caso, la asignación se realiza en la configuración de las extensiones, en el campo **DuWa**.



a) En la línea correspondiente de la lista desplegable **N.° llam. interno** seleccione un número de teléfono interno.

b) Si desea permitir que extensiones sin número de telefonía Internet o que los miembros de un grupo de llamadas realicen llamadas telefónicas externas por Internet, active el campo de opción **Utilizar como número de llamada del sistema saliente**. El campo de opción solo puede estar activado en un único número de telefonía Internet.

18) Haga clic en **Aceptar & Siguiente**. Aquí verá de nuevo la lista de los ITSP predefinidos y añadidos. Los ITSP activados aparecen marcados en la columna **Activar proveedor** con un signo de verificación. Con **Reiniciar ITSP** puede registrar de nuevo ITSP ya activado si hay problemas de conexión

19) Haga clic en **Aceptar & Siguiente**.

20) En el campo **Flujo saliente hasta (kbps)**, introduzca el valor de la velocidad de carga de su conexión a Internet. No debe confundirse con la velocidad de descarga.

Nota: En el campo **Cantidad de llamadas telefónicas Internet simultáneas** se indica el número de llamadas telefónicas Internet que puede realizar simultáneamente. Si la carga de red tiene efectos negativos en la calidad de las llamadas, reduzca el número.

Para obtener más información sobre la cantidad de llamadas simultáneas por Internet, consulte Restricción del número de llamadas simultáneas por ITSP en la página 842.

---

21) Haga clic en **Aceptar & Siguiente**.

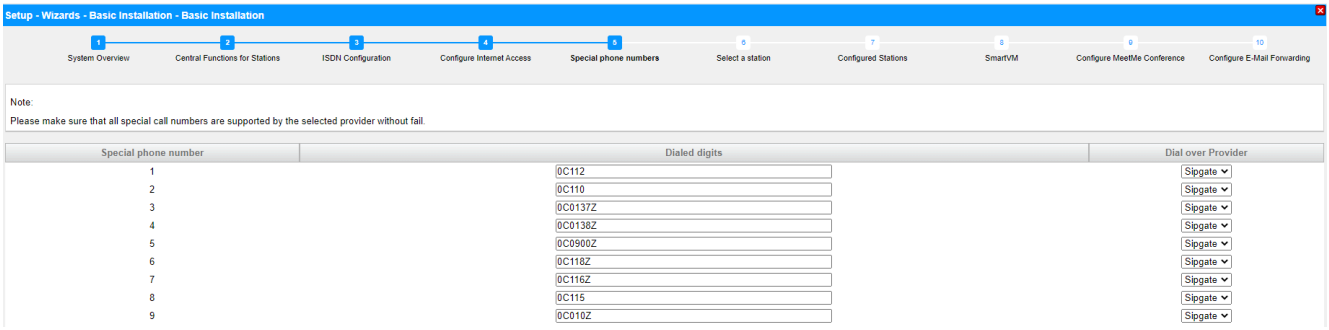
22) Si en la configuración de su acceso a Internet todavía no ha activado la conexión permanente, podrá hacerlo aquí. Sin conexión permanente no se pueden recibir llamadas a través de Internet. Si la conexión permanente ya está configurada, no aparecerán los campos descritos en los puntos de a) a c).

a) En **Conexión permanente**, active el campo de opción **Activado**.

b) En el campo **Desconexión Forzada a las (hora:min)**, introduzca la hora a la que se desactivará la conexión a Internet (p. ej., 04:59).

c) Haga clic en **Aceptar & Siguiente**.

23) En la columna **Cifras marcadas** introduzca los números de teléfono especiales deseados.



Son válidas estas entradas de número de teléfono:

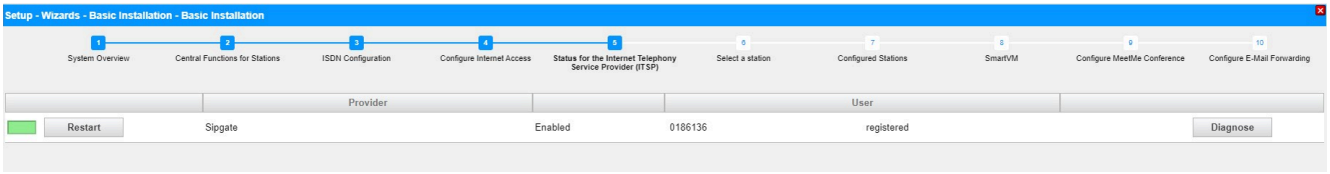
- 0 a 9: dígitos permitidos
- -: Separador de campos
- X: Cualquier dígito del 0 al 9
- N: Cualquier dígito del 2 al 9
- Z: Siguen, hasta el final de la marcación, uno o varios dígitos
- C: Tono de marcado simulado (se puede ingresar hasta tres veces)

24) En la columna **Marcar a través de proveedor** seleccione si el número de teléfono especial se marcará a través de RDSI o a través de un ITSP. Solo aparecen los ITSP activos.

Nota: Asegúrese de que siempre se pueden marcar los números de teléfono de emergencia. Si desea que los números de teléfono de emergencia se marquen a través de un ITSP, el proveedor debe admitir la función.

---

25) Haga clic en **Aceptar & Siguiente**. Se muestra el estado de los ITSP.



Aparecen marcados en verde los ITSP configurados y en los que ya está registrado.

Aparecen marcados en naranja los ITSP configurados y en los que todavía no está registrado.

26) Haga clic en **Siguiente** seguido de **Finalizar**.

6.7.5.2 Cómo desactivar telefonía Internet

Requisitos previos

Se encuentra en la ventana **Configuración y activación de proveedor para telefonía Internet** del asistente **Configuración básica**.

Paso a paso

1) Deje activada **Sin telefonía a través de Internet**.

2) Haga clic **OK & Cont**.

6.7.6 Extensiones

En las ventanas **Seleccionar extensión - ...** configure las extensiones conectadas con el sistema de comunicación.

Para ello, siga este procedimiento:

1) Configurar extensiones IP y SIP

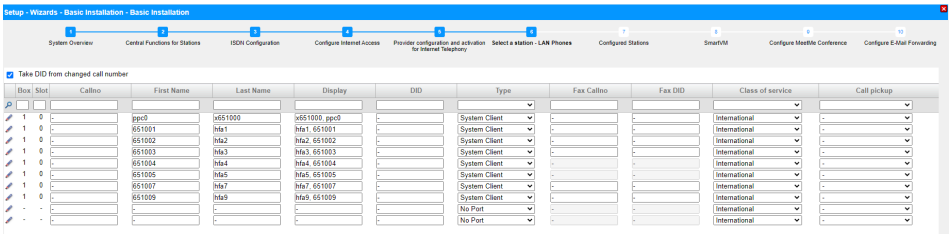
   Son extensiones IP y SIP, por ejemplo, teléfonos LAN y teléfonos WLAN.

6.7.6.1 Cómo configurar extensiones IP y SIP

Requisitos previos

Se encuentra en la ventana **Seleccionar extensión - Teléfonos LAN** del asistente **Configuración básica**.

Para poder poner en servicio los teléfonos WLAN necesita una red LAN inalámbrica operativa.



Paso a paso

1) Si desea que el número de marcación directa de la extensión sea diferente al número de teléfono, en la línea de la extensión deseada, introduzca el número de marcación directa de la extensión en el campo **Marcación directa**:

   - Solo con conexión de centralita:

     Haga clic en el campo deseado e indique el número de marcación directa a través del teclado. El número de marcación directa puede ser idéntico al número de teléfono interno.
   - Solo con acceso individual:

     Seleccione un MSN a través de la lista de selección. La extensión puede configurarse, por ejemplo, de forma interna a través de un número de teléfono interno 101 o de forma externa a través del MSN 654321.
   - en una conexión de centralita y acceso individual:

     En el campo deseado, y a través de la lista desplegable, seleccione la entrada **xxx - editable** (xxx es el número de teléfono interno) e indique el número de marcación directa a través del teclado o seleccione un MSN a través de la lista desplegable.

2) En la línea de la extensión deseada, en **N.º llam**, indique el número de teléfono interno de la extensión. Puede utilizar el número de teléfono preestablecido o asignar otro todavía no ocupado.

3) En la línea de la extensión deseada, y en **Nombre**, introduzca un nombre con el formato `Apellidos, Nombre`.

> **Nota:** El nombre puede incluir hasta 16 caracteres como máximo, pero no puede incluir diéresis ni caracteres especiales. En los clientes de UC el nombre se registra como apellido tal y como esté aquí indicado (pero se puede modificar).

4) En la línea de la extensión deseada, y en la lista desplegable **Tipo**, seleccione el tipo de la extensión IP (p. ej., "Cliente de sistema" o "Cliente SIP").

5) Si desea configurar un buzón de fax para la extensión (que se pueda utilizar, por ejemplo, con los clientes de UC **myPortal for Desktop** o **myPortal for Outlook**), siga este procedimiento:

a) En la línea de la extensión deseada, en el campo **Fax N.° llam**, introduzca el número de fax interno deseado con el que el usuario podrá recibir mensajes de fax internos.

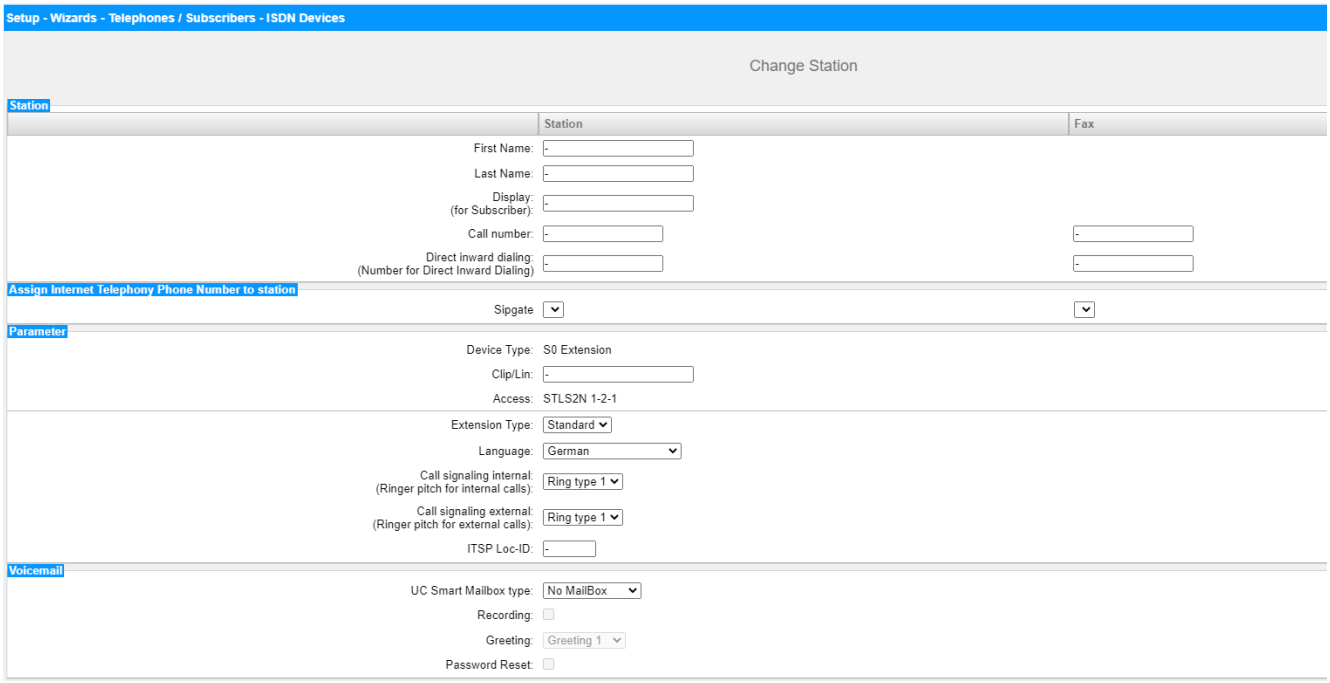
b) Si desea configurar un número de marcación directa para el buzón de fax, introduzca en la línea de la extensión deseada (en el campo **Marcación directa de fax**) el número de teléfono de fax externo deseado con el que la extensión podrá recibir mensajes de fax del exterior.

6) En la línea de la extensión deseada y utilizando la lista desplegable **Clase de servicio**, seleccione el grupo de clase de servicio deseado.

7) Para incluir las extensiones de un grupo de telecaptura, en la línea de la extensión deseada de la lista desplegable **Telecaptura de llamadas**, seleccione un grupo de telecaptura.

8) Solo debe realizar los ajustes descritos en este paso si es necesario o en los teléfonos SIP:

a) En la línea de la extensión deseada, haga clic en el símbolo en forma de lápiz **Editar**.



b) Para teléfonos SIP: Si el teléfono SIP se tiene que operar junto con un teléfono móvil Dual-Mode, en el área **Mobility**, en `Número de teléfono móvil`, indique el código urbano seguido por el número del teléfono móvil (p. ej., **0016012345678**). Además, en la lista desplegable **Web Feature ID**, seleccione este cliente SIP. (véase Telefonía Dual-Mode).

c) En **Clip/Lin** indique número teléfono (número de marcación directa o MSN) que aparecerá en el display del usuario llamado en lugar del número de teléfono en caso de llamada externa.

Nota: Esta prestación debe estar activada por el proveedor de red.

Nota: Se debe configurar al menos un número de marcación directa. De lo contrario, el sistema no tiene en cuenta el número CLIP del llamante, y el número de la llamada interna se formatea y se envía como número de llamante para la llamada externa.

---

d) En la lista desplegable **Idioma** seleccione el idioma para el control de menús del teléfono.

e) En la lista desplegable **Señalización de llamadas internas**, asigne a la extensión una de las ocho señalizaciones de llamada acústicas para llamadas internas posibles. De esta forma, la extensión enviará a otras extensiones internas un tono de llamada modificado que le permite ser reconocida por dichas extensiones (Estándar: Tipo de llamada 1).

f) En la lista desplegable **Señalización de llamadas externas**, asigne a la extensión una de las tres señalizaciones de llamada para llamadas externas posibles (Estándar: Tipo de llamada 1).
g) Solo para teléfonos SIP: Introduzca la contraseña de autenticación en los campos **Contraseña** y **Confirmar contraseña**.
h) Solo para teléfonos SIP: en el campo **ID de usuario SIP / Nombre usuario**, indique la identificación de usuario para la autenticación.
i) Solo para teléfonos SIP: en el campo **Ámbito**, indique la zona correspondiente a la autenticación.
j) Haga clic en **OK & Continuar**.
k) Si es necesario, modifique los flags de extensión. Para consultar una descripción de los flags de extensión, véase Extensión > Extensión > Parámetros de extensión.
l) Haga clic en **OK & Continuar**.

9) Si desea configurar otra extensión IP, haga clic en **Guardar datos** y repita los pasos 1 a 8.

10) Haga clic en **OK & Continuar**. Verá una lista de todas las extensiones configuradas. La lista se corresponde con un plan de numeración.

11) Si es necesario, haga clic en **Imprimir**, para imprimir los datos de las extensiones configuradas.

12) A continuación, haga clic en **OK y Continuar**.

Conceptos relacionados

Salida de texto multilingüe en la página 1256

6.7.7 Configuración de UC Suite

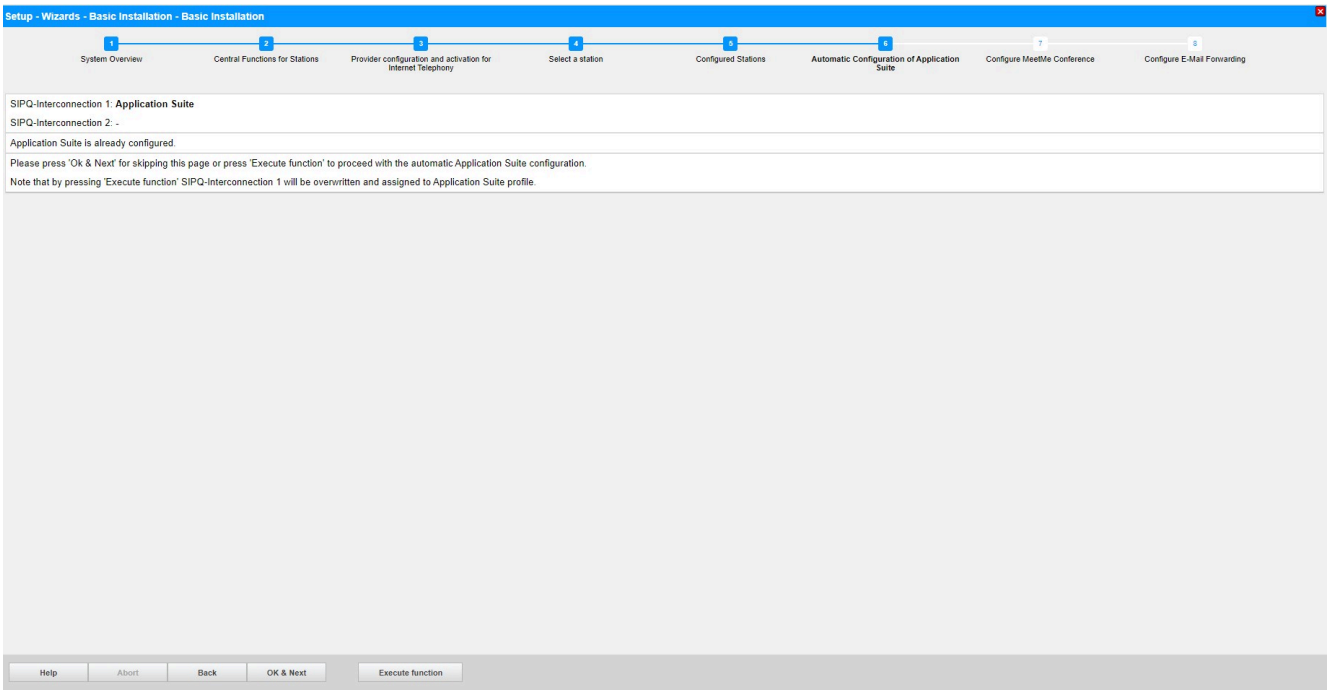
En la ventana **Configuración automática de la suite de aplicaciones** se puede hacer la configuración automática de la solución de Comunicaciones Unificadas UC Suite.

Nota: Esta ventana solo aparece si en el asistente **Instalación inicial** se ha seleccionado **Paquete con UC Suite** en la selección de aplicación.

6.7.7.1 Cómo configurar la Suite UC

Requisitos previos

Está en la ventana **Configuración automática del conjunto de aplicaciones**.



Paso a paso

Haga clic en **Ejecutar función**. La UC Suite se configura automáticamente. Cuando llegue al 100%, haga clic en **OK & Siguiente**.

Nota:

Para OpenScape Business S, el asistente genera automáticamente 60 canales multimedia en UC Suite. En paralelo, se pueden utilizar 16 canales para anuncios sin necesidad de configurar canales multimedia adicionales.

6.7.8 Configuración de los buzones de voz de UC Smart

En la ventana **Configuración automática del Smart VM** puede hacer la configuración automática de los buzones de voz de UC Smart (Smart VM, Smart VoiceMail) si utiliza la solución de Comunicaciones Unificadas UC Smart.

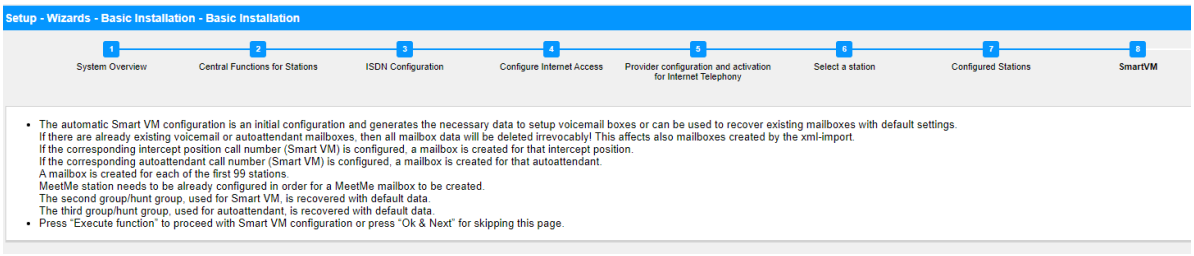
Nota:

Esta ventana solo aparece si en el asistente **Instalación inicial** se ha seleccionado **Paquete con UC Smart** en la selección de aplicación.

6.7.8.1 Cómo configurar los buzones de voz de UC Smart

Requisitos previos

Se encuentra en la ventana de **Configuración automática del Smart VM**.



Paso a paso

1) Si no desea utilizar los buzones de voz de UC Smart, haga clic en **OK & Continuar**. De esta forma se omite la configuración de los buzones de voz.
2) Si desea utilizar los buzones de voz de UC Smart, haga clic en **Ejecutar función**. Se configuran automáticamente buzones de voz para las 100 primeras extensiones. En cuanto la barra de progreso llegue al 100%, haga clic en **OK & Continuar**.

Nota: Los buzones de voz de UC Smart o los buzones de voz de UC Smart AutoAttendant presentes se borran y no se pueden recuperar.

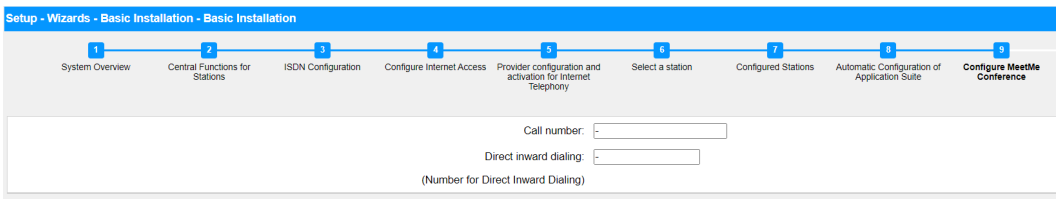
6.7.9 Ajustes del servidor de conferencias

En la ventana **Editar ajustes de conferencia Meet Me** puede establecer el número de teléfono y el número de acceso telefónico para las conferencias.

6.7.9.1 Cómo modificar los ajustes del servidor de conferencias

Requisitos previos

Se encuentra en la ventana **Configurar conferencia Meet-Me** del asistente **Configuración básica**.



Paso a paso

1) En el campo **Número de teléfono**, indique un número de teléfono para la conferencia.
2) En **Marcación directa**, establezca núm. acceso telef. conferencia (Nº llam. marc. dir. de conferencia). Con él, los participantes podrán acceder a una conf.
3) Clic **OK & Cont**.

6.7.10 Envío de correo electrónico (opcional)

En la ventana **Configurar transferencia de correos electrónicos** se puede configurar el envío de correo electrónico. Con ello, se notifica a las extensiones sobre nuevos mensajes de fax y voz, y el administrador recibe mensajes del sistema.

Tiene las siguientes opciones:

- Configurar el envío de correo electrónico

  Puede definir un servidor de correo electrónico externo que utilizará OpenScape Business para enviar los correos electrónicos. Los mensajes de voz y fax o mensajes internos del sistema se envían a través de este servidor de correo electrónico a una o varias direcciones de email configurables.

  Nota: Es importante indicar un servidor de correo electrónico si desea enviar automáticamente por correo electrónico un enlace al archivo de instalación a los usuarios de la UC Suite.

6.7.10.1 Cómo configurar el envío de correo electrónico

Requisitos previos

Si el servidor de correo electrónico externo se ha configurado para utilizar la autenticación básica, asegúrese de que existe una cuenta de correo electrónico con contraseña en un proveedor de correo electrónico y de que conoce los datos de acceso de esta cuenta.

Si el servidor de correo electrónico externo se ha configurado para utilizar autenticación moderna (autorización basada en token Microsoft OAuth 2.0), como en el caso de Exchange Online, asegúrese de que:

- La cuenta de correo electrónico del remitente debe tener permiso para utilizar SMTP autenticado (por defecto, esta opción está inactiva en la tenencia de Microsoft 365). Una vez activado el SMTP autenticado, el reenvío de correo electrónico OAUTH 2.0 funciona normalmente con todas las placas base OpenScape Business.
- Se ha registrado una aplicación con los permisos necesarios en Microsoft Azure Active Directory (Azure AD) para que su sistema OpenScape Business envíe correos electrónicos.
- Usted conoce el ID de la aplicación (cliente) y el ID del directorio (inquilino) de la aplicación registrada.

  Pida a su administrador de Azure AD que le proporcione estos valores, si es necesario.
- La dirección de correo electrónico que aparecerá como remitente de los mensajes pertenece al mismo Azure AD o inquilino que la aplicación registrada.

Se encuentra en la ventana **Editar transferencia de correos electrónicos** del asistente **Configuración básica**.

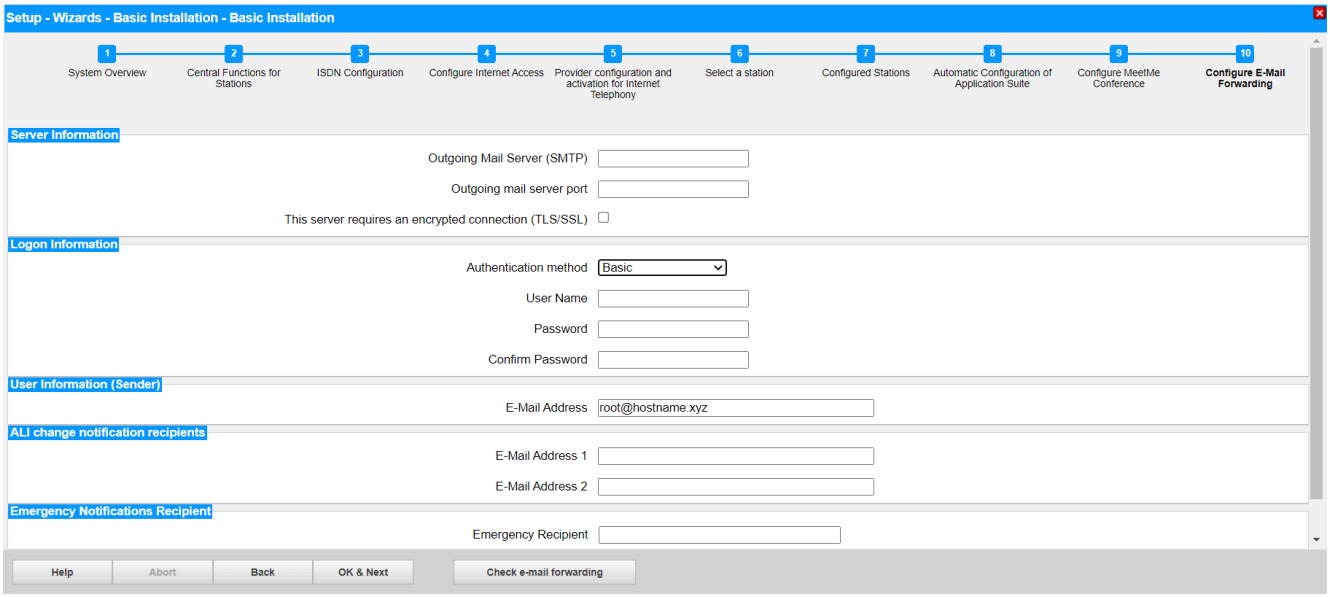


Figura 7: Opciones de reenvío de correo electrónico cuando se selecciona el método de autenticación básica

Paso a paso

1) Indique **servidor band. salida (SMTP)** del servidor correo para envío correo (p. ej., `smtp.web.es`). Si es necesario, consulte servidor band. salida proveedor correo.

> **Nota:** Compruebe que el nombre del servidor de salida de correo se puede resolver. Si no es así, inicie el asistente para el envío de correos electrónicos a través de **Centro de servicios** > **Transferencia de correos electrónicos** e introduzca la dirección IP del servidor de salida en lugar del nombre.

2) Complete el **Puerto del servidor de correo saliente** con el puerto del servidor que se deberá usar para el envío de correos electrónicos. Si es necesario, consulte servidor band. salida proveedor correo.

3) Si se requiere una conexión segura, active la casilla de verificación **Este servidor requiere una conexión cifrada (TLS/SSL)**. Si es necesario, consulte a su proveedor de correo electrónico si es necesario activar esta opción.

4) Si el servidor de correo electrónico externo se ha configurado para utilizar la autenticación básica, proceda como se indica a continuación:

a) En la lista desplegable **Método de autenticación**, seleccione **Básico**.

b) Indique **Nombre de usuario** cuenta correo, p. ej. `pepe.ejemplo`.

c) En **Contraseña** y **Confirmar contraseña**, introduzca la contraseña de la cuenta de correo.

5) Si el servidor de correo electrónico externo se ha configurado para utilizar la autenticación moderna, proceda como se indica a continuación:

a) En la lista desplegable **Método de autenticación**, seleccione **Microsoft OAuth 2.0**.

b) Introduzca el ID de aplicación (cliente) obtenido del portal de Microsoft Azure en el campo **ID de aplicación**.

c) Introduzca el ID de directorio (inquilino) obtenido del portal de Microsoft Azure en el campo **Tenant**.

6) Introduzca la **Dirección de correo electrónico** que aparecerá como remitente de los mensajes, por ejemplo: `john.doe@web.de`.

7) Introduzca **Dir correo 1** para recibir notific. cuando se haya utilizado tolerancia ALI. También puede introducir una segunda dirección de correo electrónico en el campo **Dirección de correo electrónico 2**.

8) En el campo **Destinatario de emergencia**, indique la dirección de correo electrónico de un responsable de seguridad *in situ* a quien se le enviará un correo electrónico al marcar un número de emergencias.

El asunto del correo electrónico será "Nueva llamada de emergencia". El número de llamada y el nombre del llamante, de estar configurados, se incluyen en el correo electrónico recuperándose de la base de datos del sistema.

9) Si ha seleccionado **Microsoft OAuth 2.0** como método de autenticación, proceda como se indica a continuación:

a) Haga clic en **OK & Continuar**.

b) Espere a que aparezca un enlace de autorización y un código de usuario.

El código de autorización caduca al cabo de unos minutos.

c) Abra el enlace de autorización e introduzca el código de usuario en la ventana emergente.

d) Inicie sesión con la dirección de correo electrónico que ha introducido en el paso 6 en la página 263 **(Dirección de correo electrónico)**.

La dirección de correo electrónico debe estar en el mismo Azure AD o inquilino que la aplicación registrada.

e) Tras autenticarse correctamente, la ventana emergente muestra un mensaje como el siguiente:

`Ha iniciado sesión en <nombre-de-la-aplicación> en su dispositivo. Ahora puede cerrar esta ventana.`

f) Cierre la ventana emergente y vuelva a WBM. Si la autenticación se ha realizado correctamente, aparecerá el mensaje `La autenticación se ha realizado correctamente.`

10) Si desea comprobar los ajustes de correo electrónico, siga este procedimiento:

a) Haga clic en **Probar transferencia de correo electrónico**.
b) En **Enviar a correo**, indique dir. correo de buzón al que tenga acceso. El correo electrónico de prueba se envía a esa dirección.
c) En **Asunto correo electrónico**, introduzca descripción para identificar correo en buzón entrada.
d) Clic **Enviar correo prueba**. Se comprueban los ajustes de correo electrónico y el correo electrónico se envía al buzón de correo electrónico indicado.
e) Compruebe si correo electrónico ha llegado al buzón entr.
f) Si el correo electrónico se ha enviado correctamente, haga clic en **Atrás** y continúe al paso siguiente.
g) Si envío de correo es incorrecto, clic en **Volver** y compr. ajustes correo.

11) Haga clic en**OK & Continuar** y, a continuación, en **Salir**. La instalación básica ha finalizado. Antes de realizar la copia de seguridad de datos en el asistente, debería activar las licencias.

6.8 Tareas finales

Una vez finalizada la instalación inicial y la instalación básica con Gestión basada en Web (WBM), es necesario realizar algunos ajustes de configuración importantes para el servicio de OpenScape Business.

Para ello, siga este procedimiento:

1) Active y asigne licencias

Las licencias adquiridas con OpenScape Business se deben activar en un plazo de 30 días. El periodo de tiempo comienza al iniciar sesión por primera vez en la Gestión basada en Web (WBM). Terminado ese tiempo, el sistema de comunicación solo se puede utilizar con restricciones. Una vez terminada la activación, hay que asignar las licencias a extensiones y líneas. Al hacer la activación se habilitan ya las prestaciones a nivel de sistema.

2) Aprovisionamiento del cliente de UC Smart para la instalación (solo para UC Smart)

3) Cómo preparar los clientes de UC para la instalación

Los clientes de UC forman parte de la UC Suite. La Gestión basada en Web (WBM) puede acceder a los archivos de instalación de los clientes de UC, que se pueden aprovisionar a las extensiones IP tanto de forma automática como manual.

Además, el administrador tiene la opción de realizar una instalación silenciosa. Se trata de un método basado en líneas de comandos para la instalación, desinstalación o modificación automáticas de clientes de la UC Suite presentes en un PC sin tener que hacer ningún tipo de entrada adicional. Para más información, consulte Instalación / desinstalación silenciosa para clientes de PC de la UC Suite.

4) Realizar un almacenamiento de datos

Hay que guardar los cambios realizados previamente en OpenScape Business. La copia de seguridad se puede guardar como conjunto de copias de seguridad, por ejemplo en la red interna.

6.8.1 Cómo activar y asignar las licencias

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Conoce el LAC (código de autorización de licencia) para el registro de licencia y tiene un nombre de usuario y una contraseña para acceder al servidor de licencias.

Para establecer conexión con el servidor de licencias necesita un acceso a Internet.

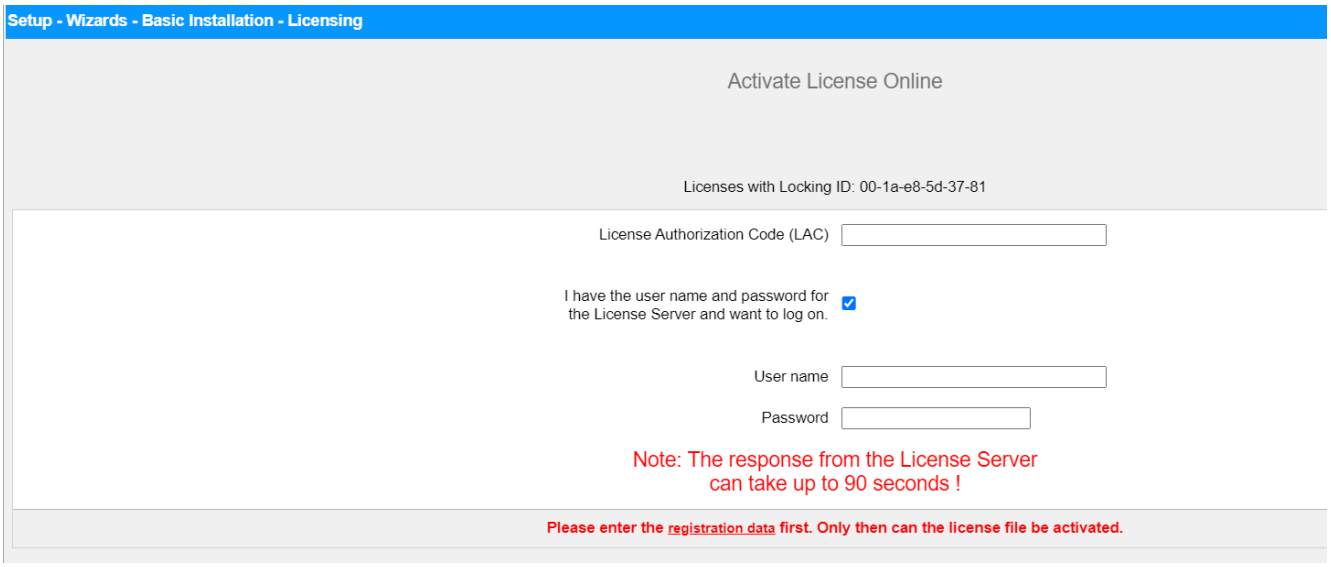
Paso a paso

1) Activar licencia online:

a) En la barra de navegación, haga clic en **Configuración**.

b) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.

c) Haga clic en **Editar** para iniciar el asistente **Registro de licencia**.



d) En el campo **Código de autorización de licencia (LAC)** indique el LAC.

e) Active la casilla de verificación **Tengo el nombre de usuario y la contraseña para el servidor de licencias y quiero iniciar sesión**.

f) Introduzca el **Nombre de usuario** y la **Contraseña** para iniciar sesión en el servidor de licencia.

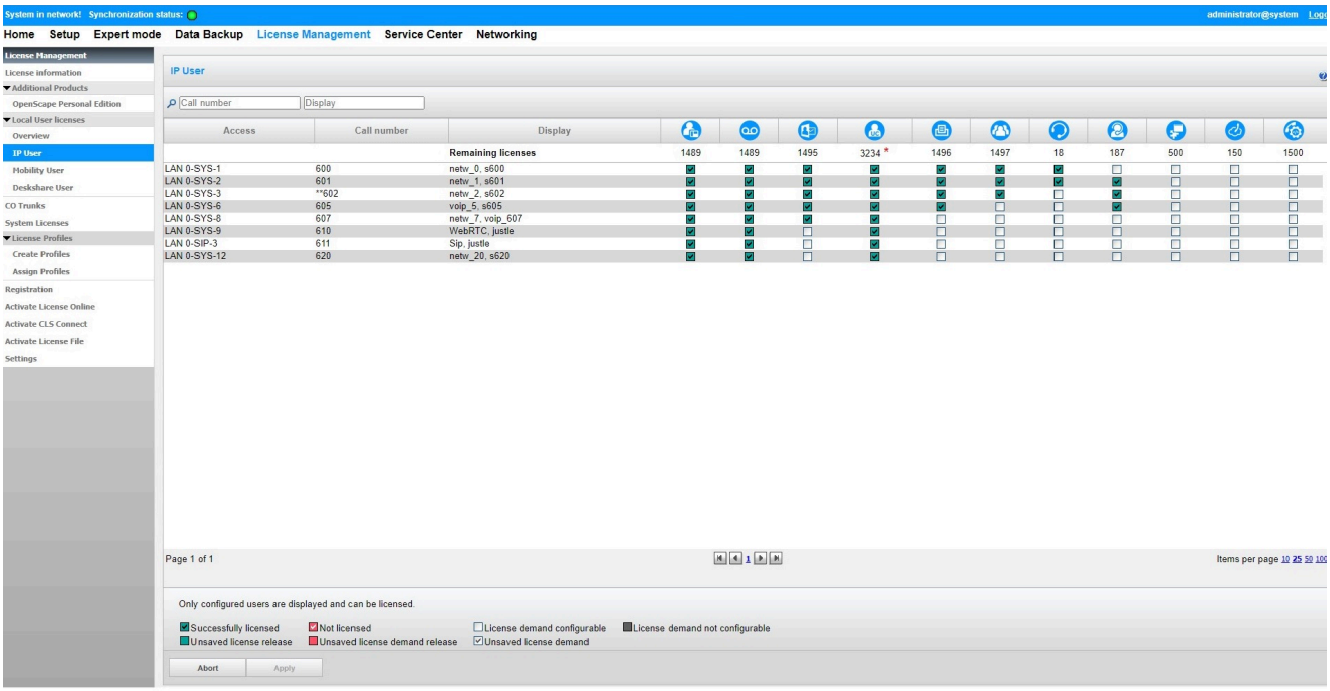
g) Haga clic en **OK y Continuar**. Se establece conexión con el servidor de licencias y se liberan las licencias.

2) Asignar licencias a las extensiones:

a) En la barra de navegación, haga clic en **Administración de licencias**.

b) En el árbol de navegación, en **Licencias de usuario local** > **...**, desplácese hasta el tipo de suscriptor deseado. Aparece una lista de todos los suscriptores del tipo seleccionado.

c) En la línea de la extensión deseada, active la casilla de verificación de la columna **Licencia de usuario** (primera columna con casillas de verificación).



d) En la línea del suscriptor deseado, active las licencias orientadas a usuarios. Para ello, active las casillas de verificación pertinentes.

Nota: Las licencias orientadas a usuarios (User) solo se pueden asignar a una extensión si antes se le ha asignado una licencia de extensión (licencia de usuario) (paso c).

---

e) Haga clic en **OK y Continuar**. Se comprueba si hay suficientes licencias para la asignación.

Si hay suficientes licencias, ha finalizado el registro de licencia de las extensiones.

f) Si faltan licencias, las casillas de verificación tendrán fondo rojo. Corrija los fallos y repita el paso e.

3) Asignar licencias a las líneas:

a) En el árbol de navegación, haga clic en **Líneas urbanas**. En el área **Líneas urbanas** aparece el número de licencias de línea adquiridas.

b) Para las líneas SIP: en el área **Demanda de licencias para el número de llamadas de Internet simultáneas en este nodo** indique el número de llamadas de Internet que se pueden realizar al mismo tiempo mediante un ITSP.

c) Haga clic en **OK y Continuar**.

6.8.2 Cómo proporcionar el cliente UC Smart para la instalación

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Está disponible el hardware y el software para usar la UC @work.

Nota: Para utilizar el cliente myPortal @work de UC Smart se requieren licencias.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Software**.
3) Haga clic en el icono de descarga de **myPortal @work** y guarde el archivo de instalación en una unidad de red habilitada.
4) Envíe a los usuarios de myPortal @Work los dos archivos de instalación.
5) Como alternativa, también puede enviar el enlace a los usuarios de myPortal @work para que puedan acceder directamente al archivo de instalación:

   `https://<Dirección IP del sistema de comunicación>/management/downloads/myPortalAtWorkSetup.exe`

6.8.3 Cómo preparar los clientes de UC Suite para la instalación

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Está disponible el hardware y el software para usar la UC Suite.

Nota: Para usar los clientes de UC Suite se necesitan licencias.

Paso a paso

1) Para poder ofrecer los archivos de instalación a una extensión de forma automática, compruebe que se han realizado los siguientes pasos:
   a) Las direcciones de correo electrónico de las extensiones deben importarse junto con los datos de extensión a través de un archivo XML o se deben registrar en **Configuración** > **UC Suite** > **Directorio de usuario**.
   b) Debe haber registrado un servidor de correo electrónico.

   Nota: También puede introducir con posterioridad un servidor de correo electrónico en **Centro de servicios** > **Transferencia de correos electrónicos**.

   Todas las extensiones con direcciones de correo electrónico conocidas recibirán un mensaje de correo electrónico con el enlace hacia el directorio de instalación de los clientes UC y una indicación de los primeros pasos.

En el directorio de instalación encontrará, además, un archivo Léame con información sobre la instalación del software en los PC cliente.

2) Si no se han realizado los pasos necesarios para proceder a la notificación automática, también puede ofrecer los archivos de instalación de forma manual. Para ello, siga este procedimiento:
   a) En la barra de navegación, haga clic en **Centro de servicios**.
   b) En el árbol de navegación, haga clic en **Software**.
   c) Haga clic en el cliente de UC deseado y guarde el archivo de instalación comprimido en una unidad de red compartida.
   d) En el árbol de navegación, haga clic en **Documentos** y seleccione la lista desplegable **Instrucciones de uso**.
   e) Haga clic en la documentación relativa al cliente de UC deseado y guarde el archivo de documentación en una unidad de red habilitada.
   f) Envíe a los usuarios de los clientes UC el archivo de instalación comprimido y el archivo de documentación a través de un correo electrónico, o comunique a los usuarios la ubicación de los archivos.
   g) El archivo comprimido ZIP con los archivos de instalación incluye también un archivo Readme. Indique a los usuarios que la instalación de los clientes de UC se debe realizar siguiendo las indicaciones de instalación del archivo Léame.
3) Como alternativa, también puede enviar enlaces a los usuarios de UC para que puedan acceder directamente a los archivos de instalación de los clientes de UC.
   a) En la barra de navegación, haga clic en **Centro de servicios**.
   b) En el árbol de navegación, haga clic en **Software**.
   c) Haga clic en el botón **Mostrar enlaces de aplicación**. Se muestran varios enlaces, en función del sistema operativo utilizado y del cliente de UC deseado. Por ejemplo:

   ```
   https://<Dirección IP del sistema de comunicación>/
   management/downloads/install-common.zip
   ```

6.8.4 Cómo realizar la copia de seguridad

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Nota: Para obtener más información sobre la copia de seguridad, consulte Almacenamiento inmediato .

Paso a paso

1) En la barra de navegación, haga clic en **Almacenamiento de datos**.
2) En el árbol de navegación, haga clic en **Guardar - inmediatamente**.
3) En el área **Nombre**, y en el campo **Comentario**, introduzca un comentario para el conjunto de copias de seguridad. Este comentario permitirá identificar con mayor facilidad el conjunto de copias de seguridad en caso de que sea necesaria una recuperación. Al hacer la entrada evite el uso de diéresis y caracteres especiales.

4) En el área **Equipo**, active la unidad de destino en la que desea guardar el conjunto de copias de seguridad (p.ej., en una unidad de red).
5) Haga clic en **OK & Continuar**. Se abrirá una nueva ventana con el progreso del proceso de guardado.
6) El mensaje **Guardar en orden indica que la copia se ha realizado con éxito.** aparece. Haga clic en **Salir**.
7) Concluye la puesta en servicio inicial con Gestión basada en Web (WBM). Cierre la Gestión basada en Web (WBM), haciendo clic en el enlace **Finalizar sesión** y, a continuación, cerrando la ventana.

6.9 Puesta en servicio de los teléfonos IP

Para la puesta en servicio de los teléfonos IP se requiere un servidor DHCP que suministre al teléfono IP los datos importantes para iniciar sesión en el sistema de comunicación (datos específicos de red).

Datos específicos de red

Para iniciar sesión en el sistema de comunicación, los teléfonos IP necesitan datos específicos de red. Estos datos pueden estar memorizados en el servidor DHCP o se pueden introducir directamente en el teléfono IP. La ventaja de contar con un servidor DHCP es que todos los teléfonos IP conectados reciben los datos automáticamente.

El teléfono IP necesita los siguientes datos:

- Dirección IP del sistema de comunicación
- Dirección IP del servidor DLS

Además, el teléfono IP también necesita el número de teléfono propio. En el inicio de sesión, hay que introducir este número de forma manual en el teléfono.

Registro de teléfonos SIP

Por motivos de seguridad es recomendable registrar los teléfonos SIP en el sistema de comunicación. Para ello, los datos de registro del teléfono SIP y del sistema de comunicación tienen que coincidir.

Para el inicio de sesión se necesitan estos datos:

- ID de usuario SIP
- Contraseña SIP
- Ámbito SIP (opcional)

Utilice una contraseña compleja que cumpla estas normas:

- Al menos 8 posiciones
- Al menos una letra mayúscula (A - Z)
- Al menos una letra minúscula (a - z)
- Al menos un número (0-9)
- Al menos un carácter especial

Utilice un ID de usuario SIP que no incluya el número de teléfono.

Nota: Encontrará más información sobre la configuración de teléfonos SIP en `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Uso del servidor DHCP interno

Si se utiliza el servidor DHCP del sistema de comunicación, los datos específicos de red ya están depositados en él. Para que un teléfono IP se pueda registrar en el sistema de comunicación, solo hay que registrar en él el número de teléfono establecido. En los teléfonos SIP, además, los datos del registro SIP del teléfono SIP y del sistema de comunicación deben coincidir.

Uso de un servidor DHCP externo con datos específicos de red

Si se utiliza un servidor DHCP externo, los datos específicos de red deben depositarse ahí. Para que un teléfono IP se pueda registrar en el sistema de comunicación, solo hay que registrar en él el número de teléfono establecido. En los teléfonos SIP, además, los datos del registro SIP del teléfono SIP y del sistema de comunicación deben coincidir.

Uso de un servidor DHCP externo sin datos específicos de red

Si se utiliza un servidor DHCP externo en el que no se pueden depositar los datos específicos de red, hay que introducir esos datos en el teléfono IP. Para que un teléfono IP pueda registrarse en el sistema de comunicación, hay que introducir en él el número de teléfono establecido y la dirección IP del sistema de comunicación y, si es necesario, modificar la configuración del servicio de implementación (Deployment Service). En los teléfonos SIP, además, los datos del registro SIP del teléfono SIP y del sistema de comunicación deben coincidir.

6.9.1 Cómo configurar teléfono IP

Requisitos previos

El teléfono IP está conectado a la red interna y está operativo.

Nota: Aquí se describe la configuración tomando como ejemplo un teléfono de sistema OpenStage 40/60/80 IP. Hay que realizar ajustes análogos para todos los demás teléfonos IP. Para hacerlo, consulte las instrucciones de su teléfono IP.

Paso a paso

1) Para acceder al modo de administración del teléfono IP de sistema, en el teléfono pulse la tecla del menú de configuración/aplicaciones.
2) En la pestaña de `Configuración`, desplácese hasta `Admin` y confirme la acción con la tecla de verificación.
3) Introduzca la contraseña de administrador(valor estándar: `123456`) y confirme la entrada con la tecla de verificación.
4) Si en la red interna se utiliza el servidor DHCP del sistema de comunicación, omita el paso siguiente.
5) Si en la red interna no se utiliza el servidor DHCP del sistema de comunicación, hay que introducir la dirección IP del servidor servidor de

despliegue (DLS) y del sistema de comunicación para poder actualizar el software del teléfono del sistema de forma automática. Esto solo se aplica a teléfonos IP del sistema. Para hacerlo, siga estos pasos:

a) Desplácese hasta `Network` (Red) y confirme la acción con la tecla de verificación.
b) Desplácese hasta `Update service (DLS)` (Servicio de actualización, DLS) y confirme la acción con la tecla de verificación.
c) Desplácese hasta `DLS address` (Dirección DLS) y confirme la acción con la tecla de verificación.
d) Introduzca como servidor de despliegue la dirección IP del sistema de comunicación (valor estándar: `192.168.1.2`) y confirme la acción con la tecla de verificación.
e) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.
f) Desplácese hasta `IPv4 configuration` (Configuración IPv4) y confirme la acción con la tecla de verificación.
g) Desplácese hasta `Route (default)` (Ruta, estándar) y confirme la acción con la tecla de verificación.
h) Introduzca la dirección IP del sistema de comunicación (valor estándar `192.168.1.2`) y confirme la entrada con la tecla de verificación.
i) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.
j) Desplácese atrás un nivel de menú con la tecla de retorno.

6) Defina el número de llamada del teléfono:

a) Desplácese hasta `System` (Sistema) y confirme la acción con la tecla de verificación.
b) Desplácese hasta `Identity` (Identidad) y confirme la acción con la tecla de verificación.
c) Desplácese hasta `Terminal number` (Número de terminal) y confirme la acción con la tecla de verificación.
d) Indique el número de teléfono establecido (p. ej., `120`y confirme la entrada con la tecla de verificación.
e) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.

7) Desplácese atrás un nivel de menú con la tecla de retorno.

8) Si es necesario reiniciar el teléfono de sistema para aplicar los cambios, en el menú `Admin` aparecerá la opción de menú `Restart` (Reiniciar). Confirme el `reinicio` con la tecla de verificación y, a continuación, pulse `Yes` (Sí) y la tecla de verificación. El teléfono de sistema se reinicia e inicia sesión en el sistema de comunicación.

6.9.2 Cómo configurar un teléfono SIP

Requisitos previos

El teléfono SIP está conectado con la LAN de clientes y está operativo.

Nota: Aquí se describe la configuración tomando como ejemplo un teléfono de sistema OpenStage 40/60/80 SIP. Los ajustes

son análogos para otros teléfonos SIP. Para hacerlo, consulte las instrucciones del teléfono SIP.

Paso a paso

1) Para acceder al modo de administración del teléfono SIP de sistema, en el teléfono pulse la tecla del menú de configuración/aplicaciones.

2) En la pestaña de `Configuración`, desplácese hasta `Administrador (Admin)` y confirme la acción con la tecla de verificación.

3) Introduzca la contraseña de administrador(valor estándar: `123456`) y confirme la entrada con la tecla de verificación.

4) Si en la red interna se utiliza el servidor DHCP del sistema de comunicación, omita el paso siguiente.

5) Si en la red interna no se utiliza el servidor DHCP del sistema de comunicación, hay que introducir la dirección IP del servidor de despliegue (DLS) y del sistema de comunicación para poder actualizar el software del teléfono del sistema SIP de forma automática. Esto solo se aplica a teléfonos del sistema SIP. Para hacerlo, siga estos pasos:

a) Desplácese hasta `Network` (Red) y confirme la acción con la tecla de verificación.

b) Desplácese hasta `Update service (DLS)` (Servicio de actualización, DLS) y confirme la acción con la tecla de verificación.

c) Desplácese hasta `DLS address` (Dirección DLS) y confirme la acción con la tecla de verificación.

d) Introduzca como servidor de despliegue la dirección IP del sistema de comunicación (valor estándar: `192.168.1.2`) y confirme la acción con la tecla de verificación.

e) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.

f) Desplácese hasta `IPv4 configuration` (Configuración IPv4) y confirme la acción con la tecla de verificación.

g) Desplácese hasta `Route (default)` (Ruta, estándar) y confirme la acción con la tecla de verificación.

h) Introduzca la dirección IP del sistema de comunicación (valor estándar `192.168.1.2`) y confirme la entrada con la tecla de verificación.

i) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.

j) Desplácese atrás un nivel de menú con la tecla de retorno.

6) Defina los ajustes horarios de SNTP:

a) Desplácese hasta `Date and time` (Fecha y hora) y confirme la acción con la tecla de verificación.

b) Desplácese hasta `Time source` (Fuente para la hora) y confirme la acción con la tecla de verificación.

c) Desplácese hasta `SNTP IP address` (Dirección IP de SNTP) y confirme la acción con la tecla de verificación.

d) Introduzca la dirección IP del sistema de comunicación (valor estándar `192.168.1.2`) y confirme la entrada con la tecla de verificación.

e) Desplácese hasta `Timezone offset` (Desfase de zona horaria) y confirme la acción con la tecla de verificación.

f) Introduzca el desfase de la hora local respecto a la hora UTC (Universal Time Coordinated) en horas (España/CES: `2`) y confirme la acción con la tecla de verificación.

g) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.

h) Desplácese atrás un nivel de menú con la tecla de retorno.

7) Defina el número de llamada del teléfono:

a) Desplácese hasta `System` (Sistema) y confirme la acción con la tecla de verificación.

b) Desplácese hasta `Identity` (Identidad) y confirme la acción con la tecla de verificación.

c) Desplácese hasta `Terminal number` (Número de terminal) y confirme la acción con la tecla de verificación.

d) Indique el número de teléfono establecido (p. ej., `120`y confirme la entrada con la tecla de verificación.

e) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.

8) Defina los datos de autenticación SIP:

a) Desplácese hasta `Registration` (Registro) y confirme la acción con la tecla de verificación.

b) Desplácese hasta `SIP session` (Sesión SIP) y confirme la acción con la tecla de verificación.

c) Ante el `Ámbito` o indique uno nuevo (p. ej. `OSBIZ-SIP`) en caso necesario.

d) Anote el `ID usuario` o indique uno nuevo (p. ej. `SIP-120`) en caso necesario.

e) Asigne una `Contraseña` para el registro en el servidor SIP.

f) Desplácese hasta `Save & Exit` (Guardar y salir) y confirme la acción con la tecla de verificación.

9) Con la tecla Volver, desplácese hasta el menú `Administrador`.

10) Si es necesario reiniciar el teléfono de sistema para aplicar los cambios, en el menú `Admin` aparecerá la opción de menú `Restart` (Reiniciar). Confirme el `reinicio` con la tecla de verificación y, a continuación, pulse `Yes` (Sí) y la tecla de verificación. El teléfono de sistema se reinicia e inicia sesión en el sistema de comunicación.

6.10 Desinstalación del software de comunicación

El software de comunicación se puede desinstalar mediante una consola de texto.

6.10.1 Cómo desinstalar el software de comunicación

Paso a paso

1) Abra un terminal (por ejemplo, el terminal GNOME).
2) En la interfaz Shell, introduzca el comando `su` (para superuser = root) y confirme la entrada con la tecla Intro.
3) En la interfaz Shell, introduzca la contraseña del usuario "root" y confirme la entrada con la tecla Intro.
4) En la interfaz Shell, introduzca el comando `oso_deinstall.sh` y confirme la entrada con la tecla Intro. Siga las indicaciones del programa de desinstalación.

6.11 Puertos utilizados

Los componentes del sistema OpenScape Business utilizan diferentes puertos; es posible que deba abrirlos en el firewall, en caso necesario. Para los puertos de los clientes basados en web (por ejemplo, myPortal to go), en el router debe configurarse el desvío de puertos.

Una lista real y completa de todos los puertos utilizados de OpenScape Business está disponible en la «Base de datos de gestión de interfaces» (IFMD) a la que se puede acceder a través del portal de socios de Unify (https://unify.com/en/partners/partner-portal.

Nota: Los puertos identificados con "O" en la lista siguiente son opcionales, es decir, no están abiertos permanentemente en el firewall.

Descripción	TCP	UDP	Número de puerto	OpenScape Business X	Tarjeta de refuerzo UC	OpenScape Business S	UC Booster Server
Componentes del sistema							
Portal de administración (https)	X		443	X	X	X	X
Controles CAR Alive	X		12062	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
CLS	X		7780, 7790 (hasta V3R3) 7780, 7791 (a partir de V3R3.1)	O		O	
Programa de instalación de clientes de comunicaciones	X		8101	X	X	X	X
Distribuidor de mensajes CSTA (CMD)	X		8900		X	X	X

Descripción	TCP	UDP	Número de puerto	OpenScape Business X	Tarjeta de refuerzo UC	OpenScape Business S	UC Booster Server
CSTA Protocol Handler (CPH)	X		7004	X		X	
Proveedor de servicios CSTA (CSP)	X		8800		X	X	X
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000-40040	O		O	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Mensajería instantánea (http)	X		8101	X	X	X	X
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS servicio cloud	X		8602	X			
Servidor LDAP	X		389		X	X	X
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
NAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
Openfire Admin (https)	X		9091		X	X	X
Servicio de actualización automática OpenScape Business (http)	X		8101	X	X	X	X
OpenScape Business Multisite	X		8778		X	X	X
OpenScape Business myReports (http)	X		8101		X	X	X
OpenScape Business Status Server	X		8808	X		X	X
OpenScape Business User Portal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (incrustado)		X	29100-30530	X	X	X	X
RTP (servidor)		X	29100-30888	X	X	X	X
SIP (servidor)	X	X	5060	X		X	

Descripción	TCP	UDP	Número de puerto	OpenScape Business X	Tarjeta de refuerzo UC	OpenScape Business S	UC Booster Server
SIP TLS SIPQ (servidor)	X		5061	X		X	
SIP TLS Subscriber (servidor)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (capturas)		X	162	X		X	
VSL	X		8770-8780		X	X	X
Webadmin para Clientes	X		8803	X	X	X	X
Clientes basados en Web							
Clientes basados en Web (http)	X		8801	X	X	X	X
Clientes basados en Web (https)	X		8802	X	X	X	X

Nota: Por motivos de seguridad, recomendamos utilizar únicamente https para los clientes basados en web y configurar el desvío de puertos desde el TCP/443 externo al TCP/8802 interno.

Certificado CLS

A partir de V3R3.1 se proporciona un nuevo certificado CLS con un nombre común (CN) actualizado mediante un puerto introducido recientemente. Esto ofrece un algoritmo de compendio mejorado y más sólido, así como entidades legales actualizadas. Los sistemas con licencia en línea a través del modo CLS Connect necesitan los siguientes dos requisitos previos:

- La dirección IP 188.64.16.4 está habilitada en el cortafuegos para el tráfico saliente.
- Los puertos 7780 y 7791 están habilitados en el cortafuegos para el tráfico saliente.

Para aumentar la seguridad el puerto 7790, utilizado anteriormente, puede eliminarse de la configuración del cortafuegos tras la actualización a V3R3.1.

6.12 Cómo recopilar seguimientos de diagnóstico para incidentes de error

Puede recopilar automáticamente los datos de seguimientos (traces) de diagnóstico de un incidente de error. El **asistente de gestión de errores** le guiará durante todo el proceso.

Debe ejecutar el asistente de **gestión de errores** dos veces: antes y después de la ejecución del escenario problemático. Durante la primera ejecución (Fase 1), se activa la recogida de trazas de diagnóstico. Después de la ejecución del escenario problemático, ejecute de nuevo el asistente para recoger los datos

de la traza de diagnóstico (Fase 2). Una vez completada la Fase 2, puede descargar el archivo de seguimiento para incluirlo en el sistema de tickets.

Para recopilar los datos de seguimiento de diagnóstico del incidente de error, siga estos pasos:

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) Haga clic en **Editar** junto a **Administración de errores**.
3) Haga clic en **OK y Continuar**.
4) Si desea recopilar los rastros por defecto, haga clic en la casilla **Rastros por defecto** .
5) Si desea especificar los tipos de trazas que se van a recoger, seleccione las que desee de la lista de trazas. Es posible realizar más de una selección.

   Para obtener más información sobre los traces, véase la guía Resolución de problemas.
6) Haga clic en **OK y Continuar**.
7) Se mostrará una lista con información adicional, documentación relevante y recomendaciones. Haga clic en **OK y Continuar**.
8) Se mostrarán los escenarios y el tipo de traces que se van a recopilar. Haga clic en **Salir**.
9) Proceda a ejecutar el escenario problemático.
10) Una vez que haya completado el escenario, vuelva a desplazarse a **Configuración > Administración de errores** y haga clic en **Editar**.

    Se le redirigirá al paso 2 de la recopilación de traces de diagnóstico. Si desea detener el proceso y volver a iniciarlo, puede hacer clic en el botón **Anular**.
11) Haga clic en **OK y Continuar**.
12) Introduzca la información necesaria y haga clic en **OK y Continuar**.
13) Se mostrará una lista con la información necesaria y algunas acciones adicionales.
14) Haga clic en **OK y Continuar**.
15) Haga clic en **Finalizar** para empezar a descargar los datos de traces de diagnóstico.

6.13 Reflashing

Siguiendo los pasos a continuación, podrá cambiar fácilmente el tipo de software de un dispositivo.

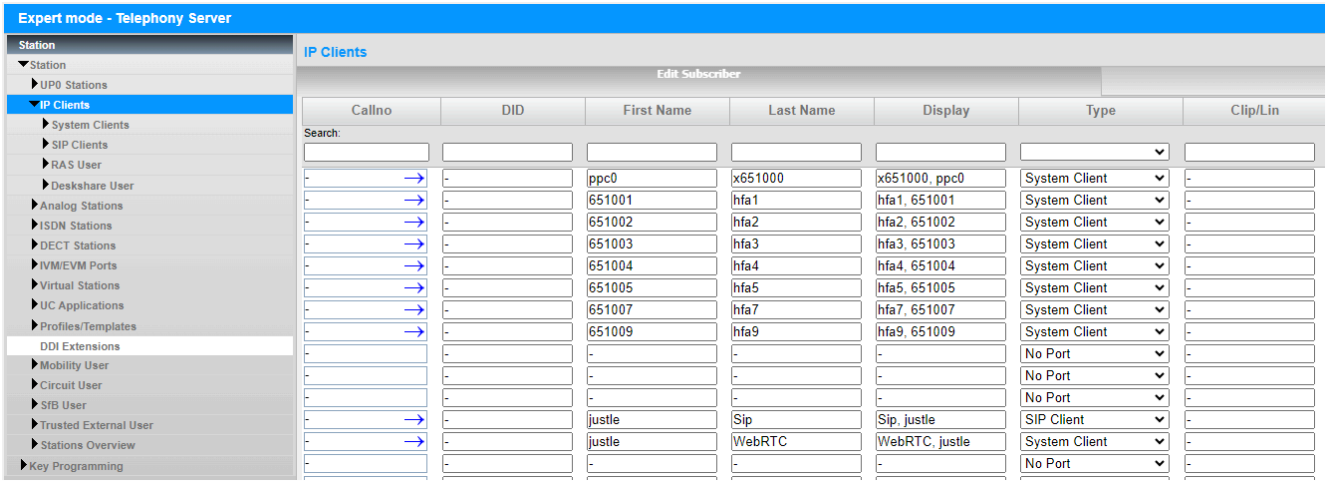
El concepto detrás de esta característica es simplificar la forma de obtener un dispositivo SIP (listo para usar) y registrarlo en el sistema OSBiz como un dispositivo HFA. Los únicos requisitos son:

- el teléfono debe obtener la dirección DLI (ya sea del servidor DHCP o manualmente)
- el administrador debe ingresar el número de teléfono (el cual debe estar preconfigurado como Cliente del Sistema)

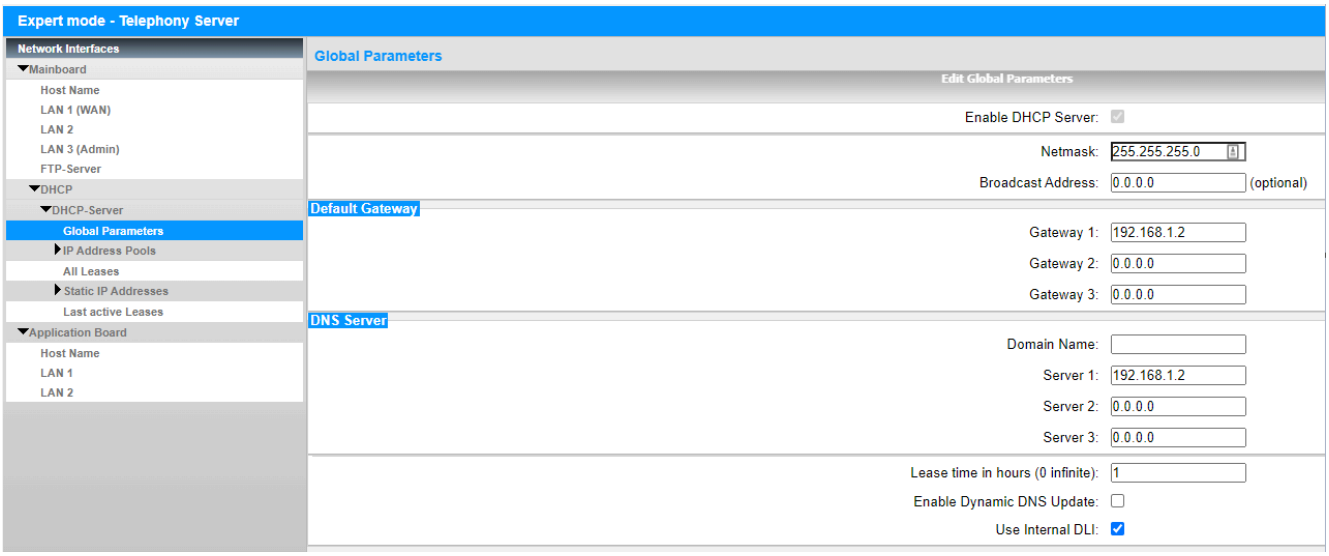
Una vez que el cliente obtenga un nuevo dispositivo, se preconfigurará como dispositivo SIP (configuración de fábrica). Los pasos para actualizar este dispositivo a un dispositivo HFA son los siguientes:

Paso a paso

1) Configure en la base de datos OSBIZ el número de teléfono deseado como Cliente del Sistema (HFA).

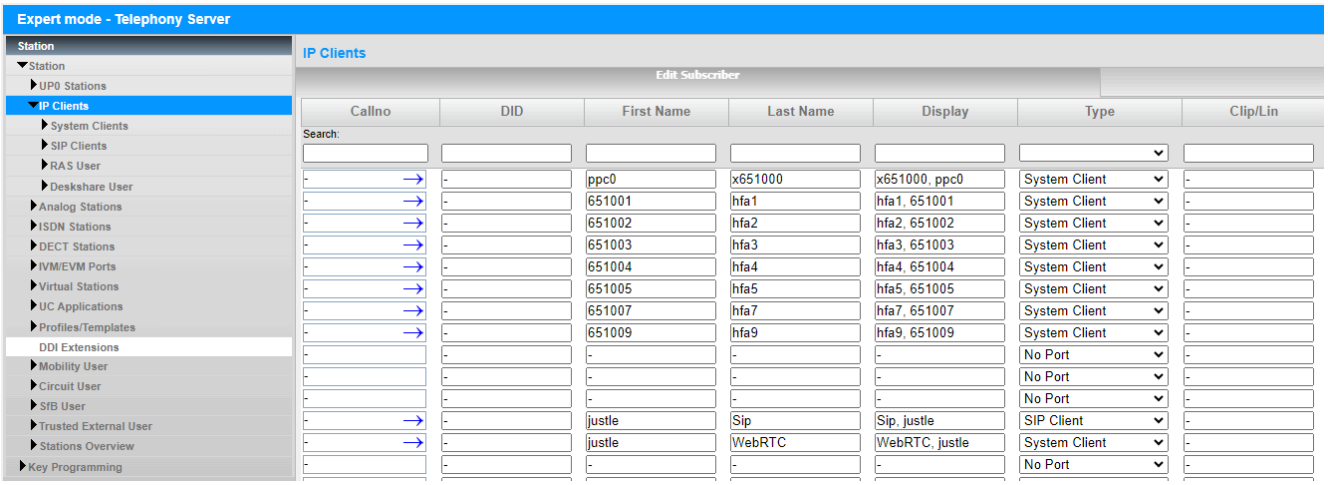


2) Configure el servidor DHCP para enviar la dirección IP de DLI. Esto se puede hacer en el servidor DHCP externo o en el servidor DHCP interno.



3) Si no se utiliza ningún servidor DHCP, debe configurar la IP DLI en el teléfono manualmente.
4) Una vez que el teléfono SIP obtenga una IP y una IP DLI, el dispositivo telefónico se registrará en la base de datos DLI y se mostrará un mensaje para ingresar el número de extensión.
5) Ingrese el número de terminal en el teléfono (el número debe ser el mismo configurado en el primer paso, por ejemplo, 4111).
6) Se iniciará la actualización y la nueva imagen HFA se descargará en el teléfono. Cuando el teléfono se reinicie, se registrará como un teléfono HFA y el sistema enviará los datos plug and play al teléfono.
7) **Para actualizar un teléfono SIP ya registrado:**

8) Cambie el tipo de dispositivo SIP en funcionamiento a "Cliente del sistema".



9) Reinicia el teléfono.

10) Se iniciará la actualización y la nueva imagen HFA se descargará en el teléfono. Cuando el teléfono se reinicie, se registrará como un teléfono HFA y el sistema enviará los datos plug and play al teléfono.

7 Configuración inicial de OpenScape Business UC Booster

Esta sección describe la instalación y configuración inicial del OpenScape Business UC Booster en el sistema de comunicación OpenScape Business X3/X5/X8. Tenga en cuenta que aquí se hace una distinción, dependiendo de si se va a utilizar la tarjeta OpenScape Business UC Booster o el servidor OpenScape Business UC Booster Server para la funcionalidad UC Booster.

La configuración inicial de OpenScape Business UC Booster se realiza mediante el programa de administración OpenScape Business Assistant (gestión basada en web, también denominada de forma abreviada WBM).

En los siguientes capítulos encontrará información detallada sobre la administración de las prestaciones no incluidas en la configuración inicial.

Configuración inicial de la tarjeta OpenScape Business UC Booster

La tarjeta OpenScape Business UC Booster se instala en el sistema de comunicación OpenScape Business X3/X5/X8 y se configura para su funcionamiento. A continuación, se configura la funcionalidad OpenScape Business UC Booster.

Los pasos necesarios específicos de instalación para la configuración inicial varían en función de si la tarjeta UC Booster funciona con el sistema de comunicación OpenScape Business X3/X5/X8 por primera vez o si se integra posteriormente en un sistema de comunicación OpenScape Business X3/X5/X8 existente y ya configurado.

Resumen de los pasos de instalación para ambas opciones:

Integración en un nuevo sistema de comunicación	Integración en un sistema de comunicación existente
	Copia de seguridad de los datos de configuración del sistema de comunicación
Instalación de la tarjeta UC Booster La tarjeta UC Booster se instala en el sistema de comunicación OpenScape Business X3/X5/X8. Para consultar su descripción, consulte la documentación de OpenScape Business Service, Instalación del hardware: descripción de las placas.	Instalación de la tarjeta UC Booster La tarjeta UC Booster se instala en el sistema de comunicación OpenScape Business X3/X5/X8. Para consultar su descripción, consulte la documentación de OpenScape Business Service, Instalación del hardware: descripción de las placas.
Configuración de la tarjeta UC Booster La configuración de la tarjeta UC Booster se realiza junto con la instalación inicial del sistema de comunicación OpenScape Business X3/X5/X8. Para una descripción, consulte Integración en la LAN del cliente.	Configuración de la tarjeta UC Booster La configuración de la tarjeta UC Booster se realiza posteriormente en un sistema de comunicación ya configurado OpenScape Business X3/X5/X8. Para una descripción, consulte Integración en la LAN del cliente. Para conocer los detalles de la configuración, consulte Configuración de la tarjeta UC Booster

Integración en un nuevo sistema de comunicación	Integración en un sistema de comunicación existente
Configuración básica La configuración básica se realiza junto con la instalación inicial del sistema de comunicación OpenScape Business X3/X5/X8. Para una descripción, véase Configuración básica.	Configuración básica La configuración básica se realiza posteriormente en un sistema de comunicación OpenScape Business X3/X5/X8 ya configurado. Para una descripción, véase Configuración básica. Para conocer las particularidades de la configuración básica, consulte Configuración básica
Actividades de cierre Las actividades de cierre (incluida la licencia de los clientes UC) se realizan junto con la instalación inicial del sistema de comunicaciones OpenScape Business X3/X5/X8. Para una descripción, consulte las Actividades de cierre.	Actividades de cierre Las actividades de cierre (incluida la licencia de los clientes UC) se realizan junto con la instalación inicial del sistema de comunicaciones OpenScape Business X3/X5/X8. Para una descripción, consulte las Actividades de cierre. Para conocer las particularidades de las actividades de cierre, véase Actividades de cierre.

Instalación inicial de OpenScape Business UC Booster Server

El OpenScape Business UC Booster Server se integra junto al sistema de comunicaciones OpenScape Business X3/X5/X8 en la LAN del cliente.

El software de comunicación OpenScape Business para OpenScape Business UC Booster Server, que da la funcionalidad OpenScape Business UC Booster, se instala en el sistema operativo Linux SLES 12 SP5 64 bits o SLES 15 SP6 64 bits. El software de comunicación puede funcionar directamente en un servidor Linux o en un entorno virtual con VMware vSphere. La instalación del sistema operativo Linux se describe en la guía de instalación *OpenScape Business, instalación del servidor Linux*.

OpenScape Business UC Booster Server tiene su propio WBM. Este WBM se utiliza para actualizaciones de software, copias de seguridad de los datos de configuración y diagnósticos del OpenScape Business UC Booster Server. La instalación inicial del servidor OpenScape Business UC Booster se realiza con el WBM del sistema de comunicación.

Los pasos específicos necesarios para las instalación inicial difieren en función de si el UC Booster Server se activa con el sistema de comunicación OpenScape Business X3/X5/X8 por primera vez o si se conecta posteriormente a un sistema de comunicación OpenScape Business X3/X5/X8 ya existente y configurado.

Resumen de los pasos de instalación para ambas opciones:

Integración en un nuevo sistema de comunicación	Integración en un sistema de comunicación existente
	Copia de seguridad de los datos de configuración del sistema de comunicación

Integración en un nuevo sistema de comunicación	Integración en un sistema de comunicación existente
Instalación del servidor Linux En la Guía de instalación de OpenScape Business Linux Server se describe la instalación del servidor Linux.	Instalación del servidor Linux En la Guía de instalación de OpenScape Business Linux Server se describe la instalación del servidor Linux.
Instalación del software de comunicación	Instalación del software de comunicación
Configuración del UC Booster Server La configuración del UC Booster Server se realiza junto con la instalación inicial del sistema de comunicación OpenScape Business X3/X5/X8. Para una descripción, consulte Integración en la LAN del cliente.	Configuración del UC Booster Server La configuración del UC Booster Server se realiza posteriormente en un sistema de comunicación OpenScape Business X3/X5/X8 ya configurado. Para una descripción, consulte Integración en la LAN del cliente. Para conocer los detalles de la configuración, consulte Configuración del UC Booster Server
Configuración básica La configuración básica se realiza junto con la instalación inicial del sistema de comunicación OpenScape Business X3/X5/X8. Para una descripción, véase Configuración básica.	Configuración básica La configuración básica se realiza posteriormente en un sistema de comunicación OpenScape Business X3/X5/X8 ya configurado. Para una descripción, véase Configuración básica. Para conocer las particularidades de la configuración básica, consulte Configuración básica
Actividades de cierre Las actividades de cierre (incluida la licencia de los clientes UC) se realizan junto con la instalación inicial del sistema de comunicaciones OpenScape Business X3/X5/X8. Para una descripción, consulte las Actividades de cierre.	Actividades de cierre Las actividades de cierre (incluida la licencia de los clientes UC) se realizan junto con la instalación inicial del sistema de comunicaciones OpenScape Business X3/X5/X8. Para una descripción, consulte las Actividades de cierre. Para conocer las particularidades de las actividades de cierre, véase Actividades de cierre.

7.1 Requisitos para la puesta en servicio inicial

El cumplimiento de los requisitos para la configuración inicial garantiza el correcto funcionamiento de OpenScape Business UC Booster.

General

En función del material utilizado (teléfonos...) y de la infraestructura existente, se aplicarán las siguientes condiciones generales:

- El sistema de comunicación OpenScape Business X3/X5/X8 está configurado y listo para su uso.
- La infraestructura LAN (enrutadores de Internet, conmutadores, etc.) está presente y se puede utilizar.

- Los teléfonos IP están conectados a la LAN del cliente.
- Se recomienda una conexión a Internet de banda ancha para las actualizaciones de software y el acceso remoto.
- Todas las licencias necesarias para OpenScape Business UC Booster están presentes (por ejemplo, clientes UC, servicios de directorio, etc.). Cuando se integra en un sistema de comunicación ya licenciado, no hay periodo de activación.
- Existe y se conoce un esquema de direcciones IP.
- Existe y se conoce un plan de marcación (también llamado plan de numeración).

Para la tarjeta UC Booster

Deben observarse los siguientes requisitos para el funcionamiento de la tarjeta UC Booster.

- Hardware OpenScape Business:

  La tarjeta UC Booster está instalada.
- Equipo de red:

  es obligatorio disponer de un equipo de red habilitado para IPv6 a través del cual la tarjeta UC Booster se conecte con el sistema de comunicaciones para que funcione correctamente. Esto hace que la tarjeta UC Booster reciba automáticamente una dirección IP durante la configuración inicial y después de cada reinicio del sistema.

  Si el equipo de red no está habilitado para IPv6, parpadeará el LED rojo del sistema de comunicación. En este caso, el puerto de administración del sistema debe conectarse al segundo puerto LAN de la tarjeta UC Booster mediante un cable Ethernet adicional. Esto hace que la tarjeta UC Booster reciba automáticamente una dirección IP IPv4 a través del protocolo IPv6. En cuanto la tarjeta UC Booster es accesible a través de IP, el LED rojo del sistema de comunicación se apaga. La dirección IP deseada para la tarjeta UC Booster puede introducirse durante la configuración inicial y después de cada reinicio del sistema. La comunicación entre el sistema y la tarjeta UC Booster se realiza ahora a través de la conexión IPv4 del conmutador.

  Nota: El cable Ethernet adicional debe dejarse conectado por si fuera necesario reiniciar o recargar.
- Kit ventilador:

  La tarjeta UC Booster requiere un ventilador adicional. El kit ventilador depende del sistema de comunicación.
- Tapa de la carcasa:

  Para el OpenScape Business X3W, se necesita una nueva tapa de carcasa para el kit de ventilador de la tarjeta UC Booster.

  Al migrar desde sistemas HiPath 3000, se necesitan nuevas tapas de carcasa para alojar el kit de ventilador de la tarjeta UC Booster para OpenScape Business X3W/X5W y X3R/X5R.
- Software de comunicación:

  el software del sistema de comunicación debe actualizarse a la última versión publicada. Tenga en cuenta que para ello debe utilizar la imagen que incluye el software de la tarjeta UC Booster.

- Navegadores web:

  el PC de administración se utiliza para la configuración inicial de la tarjeta UC Booster con OpenScape Business Assistant (WBM). El WBM se basa en el navegador y, por tanto, es independiente del sistema operativo. Se requiere una resolución de pantalla de 1024 x 768 o superior.

  Se admiten los siguientes navegadores web compatibles con HTML 5:

  – Microsoft Internet Explorer versión 10 y posteriores.
  – Microsoft Edge
  – Mozilla Firefox versión 17 y posteriores
  – Google Chrome

  Si tiene instalada una versión antigua del navegador web, deberá instalar una versión actualizada antes de iniciar la configuración inicial del sistema.

  Nota: Se necesita un acceso a la red sin restricciones entre OSCC y OCAB.

Para el UC Booster Server

Para el funcionamiento del UC Booster Server deben observarse los siguientes requisitos.

- Servidor Linux:

  El servidor Linux necesario para OpenScape Business S se instaló siguiendo las instrucciones de la *Guía de instalación del servidor Linux de OpenScape Business*, se integró en la LAN del cliente y está listo para su uso.
- Software de comunicación OpenScape Business:

  El DVD de instalación con el software de comunicación OpenScape Business está disponible. Tras la instalación del software, el software del sistema de comunicación y el software de comunicación del UC Booster Server deben actualizarse por separado a la misma versión de software más reciente.
- DVD o memoria USB con el sistema operativo Linux SLES 12 SP5 64 bits o SLES 15 SP6 64 bits.

  El DVD de Linux puede ser necesario durante la instalación del software de comunicación OpenScape Business, ya que algunos paquetes de software (RPM) necesarios para el software de comunicación pueden tener que instalarse posteriormente desde este DVD.
- Navegadores web:

  Para la configuración inicial de UC Booster Server con OpenScape Business Assistant (WBM), se puede utilizar el servidor Linux o el PC de administración. El WBM se basa en el navegador y, por tanto, es

independiente del sistema operativo. Se requiere una resolución de pantalla de 1024 x 768 o superior.

Se admiten los siguientes navegadores web compatibles con HTML 5:

– Microsoft Internet Explorer versión 10 y posterior (PC administrador).
– Microsoft Edge
– Mozilla Firefox versión 17 y posterior (servidor Linux / PC de administración)
– Google Chrome

Si tiene instalada una versión antigua del navegador web, deberá instalar una versión actualizada antes de iniciar la configuración inicial del sistema.

- Cortafuegos:

  cuando se conecta a Internet, el servidor Linux necesita un cortafuegos para evitar accesos no autorizados desde el exterior. El cortafuegos de Linux se activa tras instalar Linux. El instalador del software de comunicación ajusta la configuración del cortafuegos para que este pueda funcionar correctamente. Se abren los puertos para el software de comunicación y se cierran todos los demás puertos.

  Si se utiliza un cortafuegos externo en la red, debe desactivarse el cortafuegos de Linux y deben abrirse las direcciones y los puertos necesarios para el software de comunicación (véase Puertos utilizados).

7.2 Copia de seguridad de los datos de configuración del sistema de comunicación

Antes de instalar OpenScape Business UC Booster hay que hacer una copia de seguridad de los datos de configuración existentes del sistema de comunicación OpenScape Business.

La copia de seguridad se realiza en la Gestión basada en Web (WBM) del sistema de comunicación OpenScape Business.

Los datos se pueden almacenar en distintos medios de copia de seguridad (cono por ejemplo un soporte USB o una unidad de red).

7.2.1 Cómo realizar la copia de seguridad

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) del sistema de comunicación con el perfil **Avanzado**.

Para hacer una copia de seguridad de datos en un soporte USB, este debe estar conectado con la interfaz de servidor USB del sistema de comunicación.

Paso a paso

1) En la barra de navegación, haga clic en **Almacenamiento de datos**.
2) En el árbol de navegación, haga clic en **Guardar - inmediatamente**.
3) En el área **Nombre**, y en el campo **Comentario**, introduzca un comentario para el conjunto de copias de seguridad. Este comentario permitirá identificar con mayor facilidad el conjunto de copias de seguridad en caso

de que sea necesaria una recuperación. Al hacer la entrada evite el uso de diéresis y caracteres especiales.

4) En el área **Equipo**, active la unidad de destino en la que desea guardar el conjunto de copias de seguridad.
5) Haga clic en **OK & Continuar**. Se abrirá una nueva ventana con el progreso del proceso de guardado.
6) El mensaje **Guardar en orden indica que la copia se ha realizado con éxito.** aparece. Haga clic en **Salir**.
7) Si utiliza como soporte de copia de seguridad un stick USB, espere hasta que el LED del stick USB deje de parpadear. Solo entonces habrá finalizado la copia de seguridad en el stick USB. A continuación, extraiga el stick USB.
8) Ya ha finalizado la copia de seguridad de datos con la Gestión basada en Web (WBM). Cierre la Gestión basada en Web (WBM), haciendo clic en el enlace **Finalizar sesión** y, a continuación, cerrando la ventana.

7.3 Puesta en servicio de la UC Booster Card

La puesta en servicio de la UC Booster Card incluye el montaje en el sistema de comunicación OpenScape Business y la configuración inicial para el correcto funcionamiento.

Una vez finalizada correctamente la configuración, hay que hacer una actualización de software.

7.3.1 Montaje de la UC Booster Card

La UC Booster Card se integra en el sistema de comunicación OpenScape Business. El slot para la UC Booster Card depende del sistema de comunicación.

El montaje de la UC Booster Card se describe detalladamente en la Documentación de servicio, Montaje del hardware, capítulo "Descripción de los módulos".

La UC Booster Card se puede integrar en los siguientes sistemas de comunicación OpenScape Business:

- OpenScape Business X3R y X5R (OCCMR)

  UC Booster Card con kit de ventiladores adicional.
- OpenScape Business X3W y X5W (OCCM)

  UC Booster Card con kit de ventiladores adicional.

  Para OpenScape Business X3W, se requiere una nueva tapa de la carcasa para el kit de ventiladores.
- OpenScape Business X8 (OCCL)

  UC Booster Card con kit de ventiladores adicional.

7.3.2 Configuración de la UC Booster Card

Durante la configuración se definen todos los ajustes de configuración básicos para el servicio de la UC Booster Card.

La UC Booster Card se configura con el asistente **Instalación inicial** de la Gestión basada en Web (WBM) del sistema de comunicación. Encontrará la descripción de la configuración en el capítulo Instalación inicial de OpenScape Business X3/X5/X8.

El asistente **Instalación inicial** de la Gestión basada en Web (WBM) incluye la configuración inicial de todo el sistema de comunicación. Para operar la OpenScape Business UC Booster Card son importantes las siguientes configuraciones:

- Dirección IP de la UC Booster Card

  La UC Booster Card requiere una dirección IP propia del segmento de red del sistema de comunicación.
- Selección de la Solución UC

  Puede seleccionar la solución de Comunicaciones Unificadas UC Smart o UC Suite.

Al cambiar la dirección IP de la UC Booster Card o de la solución de Comunicaciones Unificadas se reinicia el sistema de comunicación.

7.3.3 Actualización de software para la UC Booster Card

Para que la UC Booster Card funcione correctamente hay que actualizar el software del sistema de comunicación. Al hacerlo, se instalan todos los componentes de software faltantes para la UC Booster Card.

Si el software del sistema de comunicación ya está actualizado, hay que volver a actualizar el sistema con el software actual para que todos los componentes necesarios para las funciones de UC Booster se instalen con posterioridad.

La actualización de software se puede realizar por Internet o a través de un archivo de imagen disponible en el Software Download Server. Al actualizar mediante el archivo de imagen hay que utilizar el archivo de imagen que incluya las partes de la UC Booster Card (osbiz..._ocab.tar).

7.3.3.1 Cómo ejecutar una actualización de software

Requisitos previos

Hay disponible un acceso a Internet.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Actualización de software** > **Actualización a través de Internet**. Se muestra la versión de software instalada actualmente.
3) Haga clic en **OK y Continuar**.
4) Lea el acuerdo de licencia (EULA) y, a continuación, active el campo de opción **Acepto del acuerdo de licencia**.
5) Haga clic en **OK y Continuar**.
6) Active el campo de opción **Iniciar acción - Inmediatamente / inmed. tras transmisión**.

7) Haga clic en **OK y Continuar**. La actualización de software se carga en el sistema de comunicación en segundo plano y se activa automáticamente después de la transferencia. Después de reiniciar dos veces, el software está actualizado.

Nota: Puede cerrar la ventana del navegador en cualquier momento.

---

8) Puede consultar el estado actual de la actualización con la Gestión basada en Web (WBM) en **Centro de servicios** > **Actualización de software** > **Estado**.

7.4 Puesta en servicio del UC Booster Server

La puesta en servicio del UC Booster Server incluye la instalación del software de comunicación OpenScape Business en el servidor Linux y la configuración inicial para el funcionamiento correcto.

Una vez finalizada correctamente la configuración, hay que hacer una actualización de software.

7.4.1 Instalación del software de comunicación

El software de comunicación OpenScape Business se instala en el servidor Linux mediante el DVD de OpenScape Business.

Tenga en cuenta que las direcciones IP y las máscaras de red que se van a configurar deben corresponderse con la LAN de clientes.

Servidor DHCP

Un servidor DHCP asigna automáticamente una dirección IP a las extensiones IP (teléfonos IP, PC, etc.) y les suministra datos específicos de red (como, por ejemplo, la dirección IP del gateway estándar).

Como servidor DHCP se puede utilizar un servidor DHCP externo (p.ej. el servidor DHCP del router Internet o del sistema de comunicación) o el servidor DHCP del servidor Linux. Si se va a utilizar el servidor DHCP del servidor Linux, hay que desactivar el servidor DHCP externo. El servidor DHCP Linux se puede configurar durante la instalación del software de comunicación OpenScape Business.

Entorno virtual

El software de comunicación se puede ejecutar en un entorno virtual. Para ello, en el PC de servidor se instala y configura previamente el software de virtualización (sistema operativo host). A continuación se instala Linux como sistema operativo invitado. En el sistema operativo Linux, el software de comunicación es lo último que se instala (véase *OpenScape Business, Linux Server, Instrucciones de instalación*).

Uso de snapshots en máquinas virtuales (VM):

Los snapshots pueden ser un mecanismo de mantenimiento muy útil, por ejemplo para realizar un rollback rápido a un estado operativo predefinido

de la máquina virtual después de que se produzca un fallo en un script de distribución en masa.

- Los snapshots no se pueden ejecutar durante el estado operativo. Mientras se recupera un snapshot, se bloquea el estado operativo de la máquina virtual. Por ello, los terminales y las aplicaciones conectados (teléfonos IP o clientes UC) pueden perder la conexión con el servidor.
- Los snapshots pueden ocasionar que los procesos internos del servidor pierdan sincronización y que no se pueda seguir garantizando la estabilidad del sistema de comunicación. Por ello, cada vez que se ejecute el snapshot hay que planificar un reinicio del servidor dentro de las tareas de mantenimiento.
- Durante el servicio normal, no pueden permanecer snapshots previos en el entorno de producción.
- Los snapshots se pueden recuperar durante unas tareas de mantenimiento programadas o en el marco de la instalación.
- Los snapshot son utilizados internamente por herramientas de copia de seguridad como VDP o VDR. Hay que asegurarse de que estos procesos de copia de seguridad estén planificados fuera de los horarios de trabajo y de que los snapshots que generan estas herramientas se borran al final del proceso.

Puede obtener más información sobre Snapshot en la Knowledge Base (KB) de VMware. Un buen punto de partida es el artículo 1025279 de la KB "Best Practices for virtual machine snapshots in the VMware environment" (Prácticas recomendadas para snapshots de máquina virtual en el entorno VMware) (`http://kb.vmware.com/kb/1025279`).

7.4.1.1 Cómo instalar el software de comunicación

Requisitos previos

- El sistema operativo SLES 12 SP5 o SLES 15 SP6 se ha instalado e iniciado correctamente en el servidor Linux.
- DVD o archivo .ISO con el software de comunicación OpenScape Business.
- DVD o archivo .ISO o memoria USB con el sistema operativo Linux SLES 12 SP5 de 64 bits o SLES 15 SP6 de 64 bits, para cualquier instalación posterior de paquetes de software (RPM) que pueda ser necesaria.
- Los datos de acceso root (nombre de usuario y contraseña) para iniciar sesión en el servidor Linux están disponibles.

Importante: El software de comunicación OpenScape Business sobrescribe cualquier archivo de configuración existente (por ejemplo, para DHCP, FTP, Postfix, etc.) durante la instalación.

Paso a paso

1) Inicie sesión en el servidor Linux con privilegios de root.

2) Inserte el DVD de OpenScape Business o el archivo .ISO en la unidad de DVD.

3) Confirme el mensaje con **Ejecutar**. Se muestra la ventana "Welcome" (Bienvenido).

4) Seleccione el idioma de configuración deseado (por ejemplo, **inglés**) y haga clic en **Iniciar**. El resto de la instalación se describe aquí para el idioma inglés.

5) Elija el producto que desee de la lista y haga clic en **Seleccionar**. Se realiza una comprobación para determinar si el hardware cumple con todos los requisitos para la instalación. Se muestra una advertencia para deficiencias menores en el cumplimiento de los requisitos. Después de la confirmación, se puede continuar con la instalación. En el caso de deficiencias graves, la instalación se cancela automáticamente.

6) Se realiza una comprobación para determinar si es necesario instalar paquetes RPM adicionales. En caso afirmativo, confírmelo con **Confirmar**. Si esto ocurre, deberá volver a cambiar a SLES 12 o SLES 15, DVD o archivo .ISO más adelante.

7) Aparecerá una ventana con los términos de la licencia (es decir, el Acuerdo de licencia de usuario final o EULA). Lea los términos de la licencia y acepte el acuerdo de licencia con **Sí**.

8) Si ya hay un servidor DHCP en la LAN del cliente (por ejemplo, el servidor DHCP del router de Internet), detenga la configuración del servidor DHCP de Linux aquí con **No** y proceda al paso 12 para continuar.

Nota: Para garantizar que el software de los teléfonos del sistema se pueda actualizar automáticamente incluso cuando se utiliza un servidor DHCP externo, tiene dos opciones:

a) La dirección IP del servidor Linux debe introducirse como dirección DLS en cada teléfono del sistema.

b) Los datos específicos de la red deben introducirse en el servidor DHCP externo. Los parámetros para esto se pueden encontrar en `/var/registro/OPTI.txt`.

---

9) Si desea utilizar el servidor DHCP de Linux, haga clic en **Sí** para habilitar y configurar el servidor DHCP de Linux.

10) Introduzca los siguientes valores (preestablecidos con valores predeterminados):

- **Ruta predeterminada**: dirección IP de la puerta de enlace predeterminada; por regla general, la dirección IP del router de Internet, p. ej., `192.168.5.1`.
- **Dominio** (opcional): el dominio especificado durante la instalación de Linux, p. ej., `<customer>.COM`</customer>
- **Servidor DNS** (Opcional): Dirección IP del servidor DNS especificado durante la instalación de Linux. Si no hay ningún servidor DNS

disponible en la red interna, puede introducir la dirección IP del router de Internet (p. ej., `192.168.5.1`) aquí.

- **Servidor SNTP**: Dirección IP del servidor NTP interno o externo.
- **Servidor DLS/DLI**: Dirección IP del servidor DLS, es decir, la dirección IP del servidor Linux (p. ej.: `192.168.5.10`).
- **Subred**: subred apropiada para el rango de direcciones IP, p. ej.: `192.168.5.0`.
- **Netmask**: Máscara de subred del servidor Linux que se especificó durante la instalación de Linux, por ejemplo: `255.255.255.0`.
- **Comienza el rango de IP** y **Fin del rango IP**: Rango de direcciones IP desde el cual el servidor DHCP puede asignar direcciones IP, por ejemplo: `192.168.5.100` Para `192.168.5.254`.

11) Haga clic en **Continuar**.

12) Después de la instalación, es necesario reiniciar el sistema operativo Linux. Seleccione la casilla de verificación **Reinicio de PC** y confirme con **Continuar**.

13) Si es necesario instalar paquetes RPM adicionales, se le pedirá que inserte el DVD SLES 12 o la memoria USB SLES 15. Inserte el DVD o la memoria USB y confirme con **Continuar**. Después de instalar exitosamente los paquetes RPM, vuelva a insertar el DVD de OpenScape Business o el archivo .ISO y confírmelo con **Continuar**, seguido de **Ejecutar**.

14) Se ha instalado el software de comunicación OpenScape Business. A continuación, el sistema operativo realiza automáticamente un reinicio.

15) Después del reinicio, inicie sesión con la cuenta de usuario que se configuró anteriormente durante la instalación de Linux.

16) Haga clic con el botón derecho en el icono de la unidad de DVD en el escritorio y seleccione el elemento de menú **Expulsar**. Retire el DVD de OpenScape Business de la unidad de DVD.

Nota: Se tarda unos minutos en activar todos los componentes del software de comunicación OpenScape Business.

7.4.2 Configuración del UC Booster Server

Durante la configuración se definen los ajustes de configuración básicos para el servicio del UC Booster Server.

El UC Booster Server se configura con el asistente **Instalación inicial** de la Gestión basada en Web (WBM) del sistema de comunicación. Encontrará la descripción de la configuración en el capítulo Instalación inicial de OpenScape Business X.

El asistente **Instalación inicial** de la Gestión basada en Web (WBM) incluye la configuración inicial de todo el sistema de comunicación. Para operar el OpenScape Business UC Booster Server son importantes estas configuraciones:

- Selección de la Solución UC

  Puede seleccionar la solución de Comunicaciones Unificadas UC Smart o UC Suite. Para ello también hay que registrar la dirección IP del servidor Linux.

  Al cambiar la solución de Comunicaciones Unificadas se reinicia el sistema de comunicación.

Además, en la Gestión basada en Web (WBM) del UC Booster Server hay que indicar la dirección IP del sistema de comunicación.

7.4.2.1 Comunicar la dirección IP del sistema de comunicación

Requisitos previos

El UC Booster Server está integrado en la LAN de clientes y está operativo.

El sistema de comunicación OpenScape Business está operativo.

Paso a paso

1) En el PC Linux, inicie el navegador Web y abra la Gestión basada en Web (WBM) del OpenScape Business Server con esta dirección:

`https://<Dirección IP del servidor Linux>`, por ejemplo, `https://192.168.1.10`

2) Si el navegador Web notifica un problema con un certificado de seguridad, instale el certificado (en el ejemplo se utiliza Internet Explorer V10).

a) Cierre el navegador Web.

b) Abra el navegador Web con derechos de administrador. Para ello, haga clic con el botón secundario del ratón en el símbolo del navegador

Web y en el menú contextual seleccione la entrada **Ejecutar como administrador**.

c) Autorice el control de cuentas de usuario.

d) Acceda a la Gestión basada en Web (WBM) del servidor OpenScape Business con la siguiente dirección:

`https://<Dirección IP del servidor Linux>`, por ejemplo, `https://192.168.1.10`

e) Haga clic en **Continuar cargando este sitio Web**.

f) Haga clic en el mensaje **Error de certificado** en la barra de navegación del navegador Web.

g) Haga clic en **Mostrar certificados**.

h) Haga clic en **Instalar certificado** (solo visible con derechos de administrador).

i) Seleccione la opción **Ordenador local** y confirme la acción con **Continuar**.

j) Seleccione la opción **Colocar todos los certificados en el siguiente almacén**, haga clic en **Examinar** e introduzca **Entidades emisoras raíz de confianza**.

k) Confirme con **Aceptar** y, a continuación, con **Continuar** y **Finalizar**.

l) Confirme el certificado de importación con **Aceptar** y cierre la ventana del certificado con **Aceptar**.

m) Cierre el navegador Web.

n) Inicie de nuevo el navegador Web (sin derechos de administrador) y acceda a la Gestión basada en Web (WBM) del servidor OpenScape Business con la siguiente dirección:

`https://<Dirección IP del servidor Linux>`, por ejemplo, `https://192.168.1.10`

3) Arriba a la derecha, haga clic en la abreviatura de idioma y en el menú seleccione el idioma para visualizar la interfaz de la Gestión basada en Web (WBM). La página de registro aparece en el idioma seleccionado.

4) En el primer campo en **Inicio de sesión**, introduzca el nombre de usuario estándar `administrador@sistema` para acceder como administrador.

Nota: Si después de introducir `Administrador` pasa al campo **Contraseña**, `@system` se añade automáticamente.

---

5) En el segundo campo en **Inicio de sesión**, indique la contraseña estándar `administrator` para acceder como administrador.

6) Haga clic en **Inicio de sesión**.

7) Estos pasos solo son necesarios una vez, al iniciar sesión por primera vez en la Gestión basada en Web (WBM):

a) En el campo **Contraseña**, vuelva a introducir la contraseña estándar `administrator`.

b) En los campos **Nueva contraseña** y **Confirmar nueva contraseña**, introduzca una nueva contraseña para proteger el sistema contra el uso indebido. Esta opción distingue entre mayúsculas y minúsculas;

compruebe también las teclas `Num` y `BloqMayús` (tecla de ajuste fijo). La contraseña aparece oculta con asteriscos (*).

Nota: La contraseña debe tener una extensión mínima de 8 caracteres e incluir una cifra. Recuerde exactamente cuál es esa contraseña.

---

c) Haga clic en **Inicio de sesión**.
d) Seleccione la fecha actual e introduzca la hora correctamente.
e) Haga clic en **OK & Continuar**. La sesión de Gestión basada en Web (WBM) finaliza automáticamente.
f) En el primer campo en **Inicio de sesión**, introduzca el nombre de usuario estándar `administrador@sistema` para acceder como administrador.

Nota: Si después de introducir `Administrador` pasa al campo **Contraseña**, `@system` se añade automáticamente.

---

g) En el segundo campo en **Inicio de sesión** introduzca la contraseña que acaba de definir para acceder como administrador.
h) Haga clic en **Inicio de sesión**. Se abre la página de inicio de la Gestión basada en Web (WBM).
i) En la barra de navegación, haga clic en **Administradores**.
j) En la **lista de administradores** active la casilla de verificación que hay delante de la entrada **Administrador**.
k) Haga clic en **Editar**.
l) En la lista desplegable **Rol de usuario**, seleccione el perfil de usuario **Experto**.
m) Haga clic en **OK & Continuar**.
n) Cierre sesión en la Gestión basada en Web (WBM) con el enlace **Finalizar sesión** de la esquina superior derecha.
o) Vuelva a iniciar sesión en la Gestión basada en Web (WBM) con el nombre de usuario estándar `administrator@system` y la nueva contraseña.

8) En la barra de navegación, haga clic en **Modo Experto**.
9) En el árbol de navegación, haga clic en **Mantenimiento** > **Configuración**.
10) En la pestaña **Modificar dirección IP de gateway**, en **Dirección IP del gateway**, introduzca la dirección IP del sistema de comunicación, por ejemplo, `192.168.1.2`.
11) Haga clic en **Aplicar**.

7.4.3 Actualización de software para el UC Booster Server

Para que el UC Booster Server funcione correctamente, hay que actualizar el software del sistema de comunicación y el software del sistema de comunicación del UC Booster Server con la misma versión de software.

Si el software del sistema de comunicación ya está actualizado, solo hay que actualizar el software del UC Booster Server.

La actualización de software se puede realizar por Internet o a través de un archivo de imagen disponible en el Software Download Server. Al actualizar

el UC Booster Server mediante el archivo de imagen hay que asegurarse de utilizar el archivo de imagen que incluya las partes del UC Booster Server (osbiz..._pcx.tar).

7.5 Configuración básica

Durante la configuración básica se definen los ajustes de configuración más importantes para el servicio de OpenScape Business UC Booster.

La configuración básica para la UC Booster Card y para el UC Booster Server se realiza con el asistente **Instalación básica** de la Gestión basada en Web (WBM) del sistema de comunicación. Encontrará la descripción de la configuración básica en el capítulo Instalación inicial de OpenScape Business X.

La configuración básica incluye la configuración de todo el sistema de comunicación. Para el servicio del OpenScape Business UC Booster son importantes las siguientes configuraciones:

- Datos de extensión

  Se pueden ajustar números de teléfono especiales necesarios para el servicio de OpenScape Business UC Booster. Aquí se puede indicar por ejemplo el número de teléfono del buzón de voz (Voicemail) de la UC Suite.
- Configuración de la UC Booster Card

  Si en el sistema de comunicación hay integrada una UC Booster Card, hay que iniciar la configuración automática de la UC Booster Card.
- Ajustes de conferencia Meet-Me

  Con OpenScape Business UC Booster está disponible la prestación de conferencia Meet-Me. El número de teléfono y el número de acceso telefónico preasignados para la conferencia Meet-Me se pueden modificar.

7.6 Tareas finales

Una vez finalizada la instalación inicial y la instalación básica con Gestión basada en Web (WBM), es necesario realizar algunos ajustes de configuración importantes para el servicio de OpenScape Business UC Booster.

Las tareas finales se hacen con la Gestión basada en Web (WBM) del sistema de comunicación, tanto para la UC Booster Card como para el UC Booster Server. Encontrará la descripción de las tareas finales en la ayuda online o en el capítulo Instalación inicial de OpenScape Business X de la documentación para el administrador de OpenScape Business.

Para el correcto funcionamiento del OpenScape Business UC Booster son importantes las siguientes tareas finales:

- Active y asigne licencias

  Para poder utilizar las funciones de OpenScape Business UC Booster, al hacer una integración en un sistema de comunicación ya registrado hay que activar inmediatamente las licencias. Al hacer una integración en un sistema de comunicación que todavía no esté registrado, las licencias se tienen que activar en un plazo de 30 días. Una vez terminada correctamente la activación, hay que asignar las licencias a extensiones. En un sistema

independiente, las licencias para las prestaciones a nivel de sistema se habilitan ya con la activación.

- Cómo preparar los clientes de UC para la instalación

  Los clientes de UC forman parte de la UC Suite. La Gestión basada en Web (WBM) puede acceder a los archivos de instalación de los clientes de UC, que se pueden aprovisionar a las extensiones IP tanto de forma automática como manual.
- Realizar un almacenamiento de datos

  Hay que guardar los cambios realizados previamente en OpenScape Business. La copia de seguridad se puede guardar como conjunto de copias de seguridad en un soporte USB o en la red interna.

  Con la UC Booster Card basta con hacer una copia de seguridad de datos del sistema de comunicación. Con el UC Booster Server hay que hacer una copia de seguridad de los datos del sistema de comunicación y también de los datos del software de comunicación del UC Booster Server.

7.7 Desinstalación del software de comunicación

El software de comunicación se puede desinstalar mediante una consola de texto.

7.7.1 Cómo desinstalar el software de comunicación

Paso a paso

1) Abra un terminal (por ejemplo, el terminal GNOME).
2) En la interfaz Shell, introduzca el comando `su` (para superuser = root) y confirme la entrada con la tecla Intro.
3) En la interfaz Shell, introduzca la contraseña del usuario "root" y confirme la entrada con la tecla Intro.
4) En la interfaz Shell, introduzca el comando `oso_deinstall.sh` y confirme la entrada con la tecla Intro. Siga las indicaciones del programa de desinstalación.

7.8 Actualización de UC Booster Card a UC Booster Server

Para actualizar un sistema de comunicación OpenScape Business con UC Booster Card integrada a un sistema de comunicación OpenScape Business con UC Booster Server conectado, hay que seguir los pasos descritos a continuación.

Pasos de actualización

Siga estos pasos en orden:

1) **Copia de seguridad de los datos de configuración**

   Haga una copia de seguridad de los datos de configuración del sistema de comunicación.

   Para una descripción de la copia de seguridad de datos, véase Copia de seguridad de los datos de configuración del sistema de comunicación.

2) **Cambio de la dirección IP de la UC Booster Card**

   En la Gestión basada en Web (WBM) del sistema de comunicación (con el asistente **Instalación inicial**) modifique la dirección IP de la UC Booster Card con una dirección IP que no esté en uso. Se interrumpe la conexión con los clientes de UC.

   Para una descripción del cambio de direcciones IP, véase Configuración de sistema .

3) **Cambio de la selección de aplicación**

   Con el asistente **Instalación inicial** de la administración basada en web (WBM) del sistema de comunicación, cambie la selección de aplicación de **Paquete con UC Suite** a **Paquete con UC Suite en OSBiz UC Booster Server** si desea utilizar UC Suite (o de **Paquete con UC Smart** a **Paquete con UC Smart en OSBiz UC Booster Server** si va a utilizar UC Smart) e introduzca la dirección IP anterior de la UC Booster Card como la dirección IP del UC Booster Server.

   Para una descripción de la selección de aplicación, véase Solución UC.

4) **Instalación del servidor Linux**

   En el servidor Linux hay que instalar el sistema operativo Linux habilitado para el UC Booster Server.

   Para una descripción de la instalación de Linux, véanse las instrucciones de instalación del servidor Linux de OpenScape Business.

5) **Cambio de la dirección IP del UC Booster Server**

   Para la dirección IP del UC Booster Server (= Dirección IP del servidor Linux) hay que indicar la antigua dirección IP de la UC Booster Card. Puede introducir la dirección IP del servidor Linux durante la instalación del sistema operativo Linux o modificar posteriormente mediante YaST.

   Para una descripción de la asignación de direcciones IP durante la instalación de Linux, véanse las instrucciones de instalación del servidor Linux de OpenScape Business.

6) **Instalación del software de comunicación**

   En el servidor Linux hay que instalar el software de comunicación OpenScape Business.

   Para una descripción de la instalación del software de comunicación, véase Instalación del software de comunicación.

7) **Configuración del UC Booster Server**

   En la Gestión basada en Web (WBM) del UC Booster Server, introduzca la dirección IP del sistema de comunicación.

   Para una descripción de la asignación de direcciones IP del sistema de comunicación, véase Configuración del UC Booster Server.

8) **Reinicio del software de comunicación**

   En la Gestión basada en Web (WBM) del UC Booster Server, reinicie el software de comunicación del UC Booster Server.

   Para una descripción del reinicio, véase Reinicio (Restart) de la aplicación de UC .

9) **Actualización del software**

   El software del sistema de comunicación y el del UC Booster Server deben tener la misma versión.

   Para una descripción de la actualización de software, véase Actualizaciones.

10) **Restauración de los datos de configuración**

    En la Gestión basada en Web (WBM) del sistema de comunicación, reproduzca la copia de seguridad de los datos de configuración del sistema de comunicación. El sistema de comunicación y el software de comunicación se reinician consecutivamente, y se restauran las conexiones con los clientes de la UC Suite.

    Para una descripción de la restauración de datos, véase Recuperación.

7.9 Puertos utilizados

Los componentes del sistema OpenScape Business utilizan diferentes puertos; es posible que deba abrirlos en el firewall, en caso necesario. Para los puertos de los clientes basados en web (por ejemplo, myPortal to go), en el router debe configurarse el desvío de puertos.

Una lista real y completa de todos los puertos utilizados de OpenScape Business está disponible en la «Base de datos de gestión de interfaces» (IFMD) a la que se puede acceder a través del portal de socios de Unify (https://unify.com/en/partners/partner-portal.

Nota: Los puertos identificados con "O" en la lista siguiente son opcionales, es decir, no están abiertos permanentemente en el firewall.

Descripción	TCP	UDP	Número de puerto	OpenScape Business X	Tarjeta de refuerzo UC	OpenScape Business S	UC Booster Server
Componentes del sistema							
Portal de administración (https)	X		443	X	X	X	X
Controles CAR Alive	X		12062	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
CLS	X		7780, 7790 (hasta V3R3) 7780, 7791 (a partir de V3R3.1)	O		O	

Descripción	TCP	UDP	Número de puerto	OpenScape Business X	Tarjeta de refuerzo UC	OpenScape Business S	UC Booster Server
Programa de instalación de clientes de comunicaciones	X		8101	X	X	X	X
Distribuidor de mensajes CSTA (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	
Proveedor de servicios CSTA (CSP)	X		8800		X	X	X
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000-40040	O		O	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Mensajería instantánea (http)	X		8101	X	X	X	X
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS servicio cloud	X		8602	X			
Servidor LDAP	X		389		X	X	X
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
NAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
Openfire Admin (https)	X		9091		X	X	X
Servicio de actualización automática OpenScape Business (http)	X		8101	X	X	X	X
OpenScape Business Multisite	X		8778		X	X	X
OpenScape Business myReports (http)	X		8101		X	X	X
OpenScape Business Status Server	X		8808	X		X	X
OpenScape Business User Portal	X	X	8779		X	X	X

Descripción	TCP	UDP	Número de puerto	OpenScape Business X	Tarjeta de refuerzo UC	OpenScape Business S	UC Booster Server
Postgres	X		5432	X	X	X	X
RTP (incrustado)		X	29100-30530	X	X	X	X
RTP (servidor)		X	29100-30888	X	X	X	X
SIP (servidor)	X	X	5060	X		X	
SIP TLS SIPQ (servidor)	X		5061	X		X	
SIP TLS Subscriber (servidor)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (capturas)		X	162	X		X	
VSL	X		8770-8780		X	X	X
Webadmin para Clientes	X		8803	X	X	X	X
Clientes basados en Web							
Clientes basados en Web (http)	X		8801	X	X	X	X
Clientes basados en Web (https)	X		8802	X	X	X	X

Nota: Por motivos de seguridad, recomendamos utilizar únicamente https para los clientes basados en web y configurar el desvío de puertos desde el TCP/443 externo al TCP/8802 interno.

Certificado CLS

A partir de V3R3.1 se proporciona un nuevo certificado CLS con un nombre común (CN) actualizado mediante un puerto introducido recientemente. Esto ofrece un algoritmo de compendio mejorado y más sólido, así como entidades legales actualizadas. Los sistemas con licencia en línea a través del modo CLS Connect necesitan los siguientes dos requisitos previos:

- La dirección IP 188.64.16.4 está habilitada en el cortafuegos para el tráfico saliente.
- Los puertos 7780 y 7791 están habilitados en el cortafuegos para el tráfico saliente.

Para aumentar la seguridad el puerto 7790, utilizado anteriormente, puede eliminarse de la configuración del cortafuegos tras la actualización a V3R3.1.

8 Registro de licencia

El concepto flexible de licencias de OpenScape Business permite a los clientes adaptar el abanico de funciones a sus requisitos a través de la adquisición de licencias. Todos los sistemas de comunicación OpenScape Business X y OpenScape Business S responden a este principio de licencia. De esta forma, los teléfonos, los clientes de CU, las funciones de CU y las prestaciones en todo el sistema se pueden habilitar de forma personalizada y de acuerdo con las necesidades del cliente. En todos los sistemas de comunicación OpenScape Business se utilizan licencias únicas.

Si más tarde hay que ampliar OpenScape Business o equiparlo con prestaciones adicionales, se puede hacer en cualquier momento mediante la compra de licencias adicionales.

Todas las licencias están vinculadas con la licencia básica del sistema de comunicación y permiten utilizar las prestaciones adquiridas para la versión correspondiente de OpenScape Business.

A fin de ofrecer al cliente prestaciones especiales para prueba o para su conocimiento, se pueden solicitar licencias de evaluación con una validez de 90 días.

Nota: Es recomendable no instalar archivos de licencia ni ejecutar ningún asistente si el sistema está activo, ya que las llamadas activas se pueden interrumpir.

Periodo de activación (Activation Period)

La licencia se debe activar dentro del periodo de activación (30 días). El periodo de activación comienza al introducir la fecha actual en la Gestión basada en Web (WBM). Se guarda la fecha de vencimiento del periodo de activación.

Durante el periodo de activación, el producto tiene todas sus funciones y se puede utilizar el número máximo de licencias.

Si el sistema pierde la fecha actual durante el periodo de activación (por ejemplo, porque se descarga la batería de la placa base), hay que actualizar la fecha lo antes posible en la Gestión basada en Web (WBM) para que el sistema se pueda utilizar sin restricciones durante dicho periodo.

Si una vez concluido el periodo de activación no se ha registrado ninguna licencia, el sistema de comunicación solo se puede seguir utilizando con muchas restricciones. Puede haber comunicación interna entre las extensiones, pero hacia el exterior (por ejemplo, para llamadas de emergencia) solo pueden telefonear los dos primeros teléfonos activos. Se puede seguir accediendo al sistema de comunicación mediante la administración remota (acceso remoto). El sistema también se encuentra en este estado de uso limitado si la instalación inicial solo se ha realizado con el Manager E, ya que con ello no se da comienzo al periodo de activación.

Estructura de las licencias

Las licencias del sistema de comunicación tienen esta estructura:

- Una licencia básica activa el software del sistema de comunicación de forma previa. y se necesita para activar todas las demás licencias.

- Licencias de extensión para activar los teléfonos para la comunicación de voz externa.
- Licencias orientadas a usuarios (Users) para habilitar prestaciones específicas para los usuarios.
- Licencias de sistema para habilitar prestaciones generales en todo el sistema.

Migración

Para los clientes de HiPath 3000 V9 se ofrece una migración de licencia mediante una licencia de actualización. La migración de licencia protege la inversión de los clientes, y les permite usar los teléfonos y las prestaciones de voz.

Nota: Para obtener información sobre licencias y actualización o migración de sistemas en una red, consulte la sección **Red - Licencias** en el capítulo Actualizaciones.

Conceptos relacionados

Estaciones en la página 432

8.1 Procedimiento de activación de licencia

La licencia se activa a través de un procedimiento centralizado de gestión de licencias (OpenScape License Management) para la activación y administración de licencias. Esto garantiza que los clientes siempre pueden usar la extensión del sistema o las prestaciones exactas para las que ha adquirido las licencias correspondientes (derechos de uso).

Las licencias de los sistemas de comunicación OpenScape Business se vinculan con el ID de bloqueo o el ID de bloqueo avanzado del sistema de comunicación (véase ID de bloqueo e ID de bloqueo avanzado).

El cliente solicita las prestaciones deseadas y recibe una clave de activación de licencia (LAC). Una vez finalizada la instalación inicial del sistema de comunicación, el cliente activa las licencias adquiridas con un archivo licencia. El archivo de licencia ofrece al sistema un pool o reserva con todas las licencias adquiridas para hacer a continuación la asignación de licencias.

La Gestión basada en Web (WBM) ofrece mediante asistentes las funciones de registro de clientes, activación de licencias y asignación de licencias para sistemas independientes y sistemas de una interred OpenScape Business. Con el Manager E no se puede hacer un registro de licencia.

Pasos para el registro de licencia

1) Configuración del sistema en el periodo de activación
2) Registro de los datos de cliente
3) Activación de licencia
4) Asignación de licencias

Registro de clientes

En el registro de licencia, es obligatorio introducir los datos del cliente en el sistema del cliente para que se pueda hacer el registro. Los datos de cliente

se utilizan para poder informar rápidamente si se produce algún tipo de evento relevante para seguridad (especialmente retiradas de productos). Además, los clientes reciben información para evitar el uso indebido de las licencias por parte de terceros (por ejemplo, reenlazando la información de licencia).

Activación de licencia

En la activación de licencia, las licencias adquiridas se vinculan con el sistema de comunicación mediante la administración de licencias de la Gestión basada en Web (WBM). Para ello hay 2 métodos disponibles:

- Activación en línea

  En la activación en línea, después de introducir la LAC a través de Internet se establece conexión con el servidor central de licencias (Central License Server, CLS) y el archivo de licencia se transfiere automáticamente al agente de licencias integrado en el sistema de comunicación (Customer License Agent, CLA). A continuación, las licencias se activan automáticamente.
- Activación sin conexión

  Si la activación se hace sin conexión (offline), el sistema de comunicación no establece conexión con el servidor de licencias central (Central License Server, CLS). Un socio autorizado genera el archivo de licencia en el CLS y durante la activación de licencia el archivo se tiene que transferir de forma manual al agente de licencia (Customer License Agent, CLA) integrado en el sistema de comunicación.

Asignación de licencias

Todas las licencias adquiridas se asignan de forma fija todas las licencias mediante la administración de licencias de la Gestión basada en Web (WBM).

Para asignar licencias a extensiones, antes hay que configurar las extensiones con la Gestión basada en Web (WBM), por ejemplo, en la instalación inicial. Se pueden configurar todas las configuraciones del sistema, con independencia de las licencias disponibles. No obstante, las prestaciones solo se pueden utilizar después de hacer la asignación de licencias.

Al hablar de asignación de licencias se distingue entre configuración y distribución de licencias. Para las licencias orientadas a usuarios (User) y extensiones se configuran solicitudes de licencia. Si se hace una solicitud de licencia y hay una licencia disponible en el pool, se habilita la prestación correspondiente. Si no hay ninguna licencia en el pool, se mantiene la solicitud de licencia correspondiente pero la prestación no se habilita. Si es necesario hay que comprar las licencias que falten.

Registro de licencia en la interred

Para las interredes OpenScape Business, un asociado autorizado genera un archivo de licencia (archivo de licencia de red) a nivel de red en el servidor de licencias central (CLS). El agente de licencias central (CLA) del nodo maestro administra este archivo de licencia a nivel de red y pone las licencias a disposición de los distintos nodos. La asignación de las licencias se realiza mediante la Gestión basada en Web (WBM) de cada nodo. Dentro de una interred, las licencias se pueden mover mediante la Gestión basada en Web (WBM).

Al hacer el registro de licencia de una interred no se puede hacer la activación en línea.

Pago por uso

Además del esquema de licencia tradicional, OpenScape Business admite el modelo de licencia por suscripción (Pago por uso). "Pago por uso" brinda la oportunidad de facturar solo las licencias usadas en cada período de facturación y usar licencias adicionales sin extender el archivo licencia. No es necesario decidir la cantidad de licencias de antemano

Se requiere una conexión permanente a Internet desde el sistema OpenScape Business al servidor central de licencias (CLS). Se puede activar en línea con un código de activación de licencia (LAC) o con la carga de archivos. Después de la instalación, configurar la solución según las necesidades personalizadas y activar "Pago por uso", se envía periódicamente un informe de las licencias utilizadas al Servidor Central de Licencias (CLS) y se evalúa. Una vez al mes, se crea un informe final en el sitio del producto Servidor central de licencias (CLS) y el contenido de las licencias utilizadas de este informe final se utiliza para la contabilidad de licencias.

Con la licencia de suscripción se introduce un nuevo período de tiempo, el período de calificación. El período de calificación comienza con el inicio del sistema o si se activa un archivo licencia de "Pago por uso". El período comienza consecutivamente y durante este período una configuración de licencia realizada en WBM no provocará la actualización del uso de la licencia. La duración máxima del período de calificación es de 2 horas.

Nota: Para que el firewall tenga acceso al CLS, se necesitan las siguientes acciones:

- Puerto 7790 para tráfico IP saliente liberado

- 188.64.16.4 liberada para tráfico IP saliente

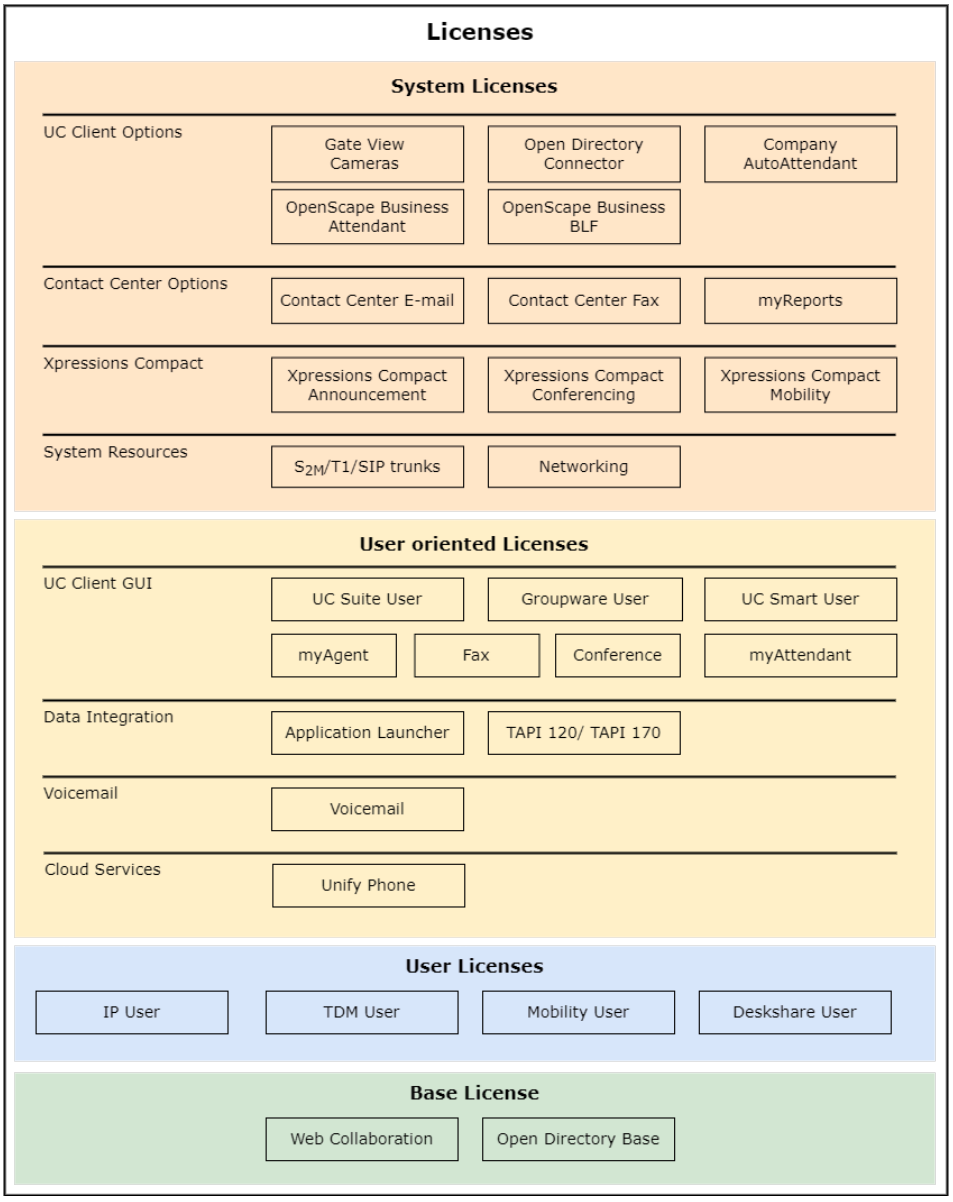
Los nuevos sistemas de software V3R3 utilizan el puerto 7791 para la activación de licencias en línea.

8.2 Licencias

Para poder usar las prestaciones del sistema de comunicación hay que adquirir licencias. En un tiempo determinado (periodo de activación) hay que activar las licencias adquiridas.

Las licencias se agrupan en licencias por temas. Hay disponibles los siguientes grupos de licencias:

- Licencias básicas
- Licencias de extensión
- Licencias orientadas a usuarios (User)
- Licencias de sistema



Las licencias detalladas arriba se pueden utilizar para OpenScape Business X, OpenScape Business S y OpenScape Business UC Booster Server. El servidor UC Booster Server no tiene licencia básica propia. Las licencias cubren todas las prestaciones y también se pueden combinar según las necesidades del cliente. Las opciones de combinación de las licencias se explican de forma más precisa en la sección sobre asignación de licencias y perfiles de licencia.

Las licencias de extensión y las licencias orientadas a usuario (User) se asignan de forma fija a las extensiones.

8.2.1 Licencia básica

La licencia básica permite el uso general del sistema de comunicación y es necesaria para activar todas las demás licencias.

Telefonía por Internet y Servicio de emergencia también están disponibles sin licencia básica.

Están disponibles las siguientes licencias básicas:

- **OpenScape Business V2 X1 Base**

  Para habilitar el conjunto de funciones V2 de

  – OpenScape Business X1

  La licencia básica incluye además, las licencias OpenDirectory Base, para el uso de Open Directory Service (ODS); y Web Collaboration, para iniciar una sesión de Web Collaboration. De esta forma se puede conectar la solución UC "UC Smart" con una base de datos externa.
- **OpenScape Business V2 Base**

  Para habilitar el conjunto de funciones V2 de

  – OpenScape Business X3/X5/X8 con o sin UC Booster (UC Booster Card o UC Booster Server) o
  – OpenScape Business S

  La licencia básica incluye además la licencia OpenDirectory Base, para el uso de Open Directory Service (ODS); y Web Collaboration para iniciar una sesión de Web Collaboration. De esta forma se puede conectar las soluciones de UC UC Suite o UC Smart con una base de datos externa.

8.2.2 Licencias de usuario

Todos los suscriptores conectados con el sistema de comunicación requieren una licencia de usuario para la telefonía externa. Esta licencia se asigna de forma fija al número de teléfono del suscriptor mediante WBM.

Las licencias de usuario incluyen las amplias funciones de voz de OpenScape Business. Para utilizar las soluciones de UC, UC Smart o UC Suite, se requieren licencias adicionales (véase Licencias orientadas a usuarios).

Están disponibles las siguientes licencias de extensión:

- **Usuario IP**

  Para utilizar teléfonos del sistema IP (HFA) y teléfonos SIP.
- **Usuario TDM**

  Para utilizar teléfonos del sistema UP0, teléfonos analógicos, faxes analógicos, teléfonos RDSI, faxes RDSI y teléfonos DECT.
- **Usuario Mobility**

  Para utilizar teléfonos GSM/móviles, smartphones y tabletas como extensiones del sistema de comunicación. Para utilizar myPortal to go y Mobility Entry. No es necesario asignar un teléfono de sobremesa adicional. Para el uso conjunto del cliente de Unify Phone con OpenScape Business.
- **Usuario de Deskshare**

  Para utilizar la prestación DeskSharing. Esta extensión solo tiene asignado de forma fija un número de teléfono, sin ningún teléfono físico. La extensión puede utilizar determinados teléfonos IP del sistema con su número de teléfono asignado y con los teléfonos puede acceder a su configuración telefónica personal.
- **Usuario de conm. reserva**

  Para uso de telefonía básica en caso de producirse un fallo de un nodo del sistema. La licencia es compatible con una licencia Pago por uso basada en

tiempo. El tiempo de uso se calcula en función de los días que el sistema hospede a usuarios de otros nodos. Las licencias solo son efectivas durante este tiempo de hospedaje. En un modo de operación normal, los usuarios en reserva son como usuarios sin licencia.

Registro flexible de licencias de extensión

El registro flexible de licencias de extensión permite registrar usuarios TDM, Mobility y DeskShare con licencias de usuario IP. Si todas las licencias de usuarios TDM, DeskShare y Mobility están ya asignadas a suscriptores y se requieren más usuarios TDM, DeskShare y Mobility, se pueden utilizar licencias de usuario IP restantes para cubrir la demanda.

Para utilizar el registro flexible de licencias de extensión se requiere la versión de software V1R3.3 y un archivo de licencia generado en el CLS, que se debe ejecutar y activar en OpenScape Business.

Registro flexible de licencias de extensión para UC Suite

El registro flexible de licencias de extensión para UC Suite permite registrar usuarios myPortal for Desktop con licencias de usuario myPortal for Outlook. Si todas las licencias myPortal for Desktop están asignadas y se requieren más usuarios, se pueden utilizar licencias de usuario myPortal for Outlook para cubrir esa necesidad.

Para utilizar el registro flexible de licencias de extensión se requiere la versión de software V2 y un archivo de licencia generado en el CLS, que se debe ejecutar y activar en el OpenScape Business.

8.2.3 Licencias orientadas a usuarios (User)

Las licencias orientadas a usuarios (User) están vinculadas a extensiones y autorizan el uso de prestaciones de Comunicaciones Unificadas y de las aplicaciones para la integración de datos. Las licencias orientadas a usuarios (User) presumen siempre la existencia de una licencia de extensión y están vinculadas de forma permanente con el número de teléfono de la extensión.

Están disponibles las siguientes licencias orientadas a usuarios:

Buzón de voz

- **Buzón de voz**

  Para usar un buzón de voz personal a través del teléfono (TUI) y de la interfaz de las soluciones de Comunicaciones Unificadas UC Smart o UC Suite.

  Nota: Si la solución de Comunicaciones Unificadas UC Smart se amplía a la UC Suite, se conservan las licencias de VoiceMail existentes y la asignación a las extensiones.

  Nota: Al asignar una licencia de Buzón de voz a una extensión, se crea un usuario de UC Suite y se restablecen todos los desvíos de llamadas activos.

Servicios en la nube

- **Unify Phone**

  Para el uso del cliente Unify Phone en combinación con OpenScape Business.

Interfaz de usuario del cliente de UC

- **Usuario UC Smart User**

  Para usar las funciones de UC Smart de los clientes de comunicaciones de myPortal @work, myPortal to go y otros clientes de Web Services.
- **Usuario UC Suite User**

  Para usar las funciones de UC Suite de los clientes de comunicaciones de myPortal @work, myPortal for Desktop, myPortal to go y otros clientes de Web Services.
- **Usuario groupware**

  Para usar las funciones de UC Suite de los clientes de comunicaciones de myPortal @work, myPortal for Outlook, myPortal to go y otros clientes de Web Services.
- **Fax**

  Para usar un buzón de fax en la UC Suite. Como requisito previo, se necesita además una licencia UC User o Groupware User.
- **Conferencia**

  Para usar la gestión de conferencias dentro de la UC Suite, por ejemplo, gestión e inicio de conferencias permanentes y recurrentes. Como requisito previo, se necesita además una licencia UC User o Groupware User.

  Para participar en conferencias no se requieren licencias.
- **myAttendant**

  Para usar las funciones de conmutación de la UC Suite.
- **myAgent**

  Para usar las funciones de Contact Center como, por ejemplo, información sobre colas, mensajes emergentes con información del cliente en caso de llamada entrante o acceso al historial de llamadas.

Nota: Para el cliente móvil myPortal to go, además de la licencia Mobility User, se requiere una licencia UC User o Groupware User para la solución de comunicaciones unificadas UC Smart o para la solución de comunicaciones unificadas UC Suite.

Integración de datos

- **Application Launcher**

  Para el control relativo a llamadas de aplicaciones en un PC cliente con llamadas entrantes y salientes, por ejemplo, abrir una aplicación o visualizar datos de llamante. Application Launcher se puede utilizar con UC Smart, UC Suite o myAgent, y requiere además una licencia UC User, una licencia Groupware o una licencia myAgent. De forma opcional puede utilizar el Open Directory Service.

- **OpenScape Business TAPI**

  Para usar las aplicaciones conformes con TAPI y telefonía por PC con programas propios del cliente de diferentes desarrolladores de software. Se requiere UC Booster (UC Booster Card o UC Booster Server).

8.2.4 Licencias de sistema

Las licencias de sistema no son relativas a extensiones y liberan prestaciones a nivel de sistema. Todas las extensiones del sistema de comunicación pueden usar estas prestaciones.

Descripción general de requisitos de licencias del sistema

Tipo de línea	Licencia SSP	Licencias/canal de línea	Licencia de red
ITSP	sí	sí	no
Línea de SIP nativo	sí	no	sí
Skype for Business	sí	sí	no
Unify Phone	sí	no	no
Interconexón-SIPQ	no	no	sí

Están disponibles las siguientes licencias de sistema.

Recursos del sistema

- **Líneas S_{2M}/T1/SIP**

  Para utilizar canales S_{2M}/T1 e ITSP. No hay que registrar la licencia de los canales S_0, se incluyen también conexiones con servidores de fax S_0 en el modo PP. En las conexiones múltiplex primarias S_{2M} o T1 (EE. UU.) los diferentes canales de voz se registran con licencia. En las conexiones ITSP se registra el número de conexiones simultáneas con uno o varios proveedores ITSP (proveedores SIP). El número de conexiones simultáneas posibles depende del ancho de banda de la conexión.
- **Redes**

  Para la interconexión IP mediante SIP-Q/native SIP o para la interconexión TDM mediante CorNet-NQ o QSIG. Para la interconexión de las aplicaciones de la UC Suite. Se requiere una licencia por cada nodo.

  Nota: La licencia de redes libera las líneas para la interconexión de voz y para la interconexión de la UC Suite para un nodo. Para las líneas de interconexión no se requieren licencias de línea S_{2M}/T1/SIP.

Tabla 3: Vista general de las licencias de recursos del sistema (S_{2M}/ITSP)

Protocolo	Licencias			
	Sin licencia	**OpenScape Business Networking (1x por sistema)**	**OpenScape Business S_{2M} / ITSP (1x por canal)**	**Usuario TDM**
S_0 interna				
Servidor de fax (DSS1/ QSIG)	X			
Euro-Bus				por cada estación S_0
Líneas S_0 - urbanas				
Euro-Línea urbana PP	X			
Euro-Línea urbana PMP	X			
Líneas S_{2M} - urbanas				
Euro-Línea urbana PP			X	
Proveedor ITSP				
ITSP 1 a 8			X	
Interconexión S_0				
QSIG		X		
CorNet-NQ		X		
Interconexión S_{2M}				
QSIG		X		
CorNet-NQ		X		
Interconexión SIP				
SIP-Q		X		
SIP nativo		X		

Opciones de Contact Center

- **Contact Center Mail**

  Para configurar uno o varios buzones de correo electrónico para la recepción y envío de correos electrónicos para los agentes de Contact Center. Se requiere una licencia de extensión y una licencia de myAgent. Se requiere una licencia por cada nodo.
- **Contact Center Fax**

  Para configurar uno o varios buzones de fax para la recepción y envío de faxes para los agentes de Contact Center. Se requiere una licencia de extensión y una licencia de myAgent. Se requiere una licencia por cada nodo.

- **myReports**

  Para generar estadísticas sobre la carga de los recursos del Contact Center según distintos criterios. El Administrador de plan horario (Schedule Manager) permite crear informes a partir de más de 100 plantillas de informe predefinidas para contactos de teléfono, fax y correo electrónico. Las plantillas de informe se administran mediante el Administrador de informes (Report Manager) que permite reagrupar, añadir y borrar nuevas plantillas de informe.

Opciones de cliente UC

- **Open Directory Connector**

  Para la conexión de Open Directory Service (ODS), para poder acceder a una base de datos externa o a un directorio externo. Por cada nodo se pueden conectar hasta cuatro bases de datos.
- **Company AutoAttendant**

  Para la utilización de un AutoAttendant central, basado en UC Smart o UC Suite para la conmutación automática de llamadas. Se requiere una licencia por cada nodo.

  Los anuncios grabados del tipo "Música en espera" (continua) solo se reproducen con esta licencia.
- **OpenScape Business Attendant**

  Para el uso del puesto de operadora de PC OpenScape Business Attendant. Por cada nodo se pueden registrar hasta 8 OpenScape Business Attendant.

  Si desea que OpenScape Business Attendant pueda acceder a información sobre el estado de presencia, se requiere una licencia UC User.
- **OpenScape Business BLF**

  Para la utilización del indicador adicional de campos de lámparas de ocupado OpenScape Business BLF. Por extensión se requiere una licencia BLF o una licencia UC User. Por cada nodo se pueden registrar hasta 50 OpenScape Business BLF.

8.2.5 Licencias de evaluación

Una licencia de evaluación permite probar ciertas aplicaciones durante un determinado tiempo (periodo de evaluación) con todo su abanico de prestaciones de forma gratuita. Si durante el periodo de evaluación se activa una licencia regular para la prestación se activa la licencia de evaluación.

Están disponibles las siguientes licencias de evaluación:

- **Evaluación de OpenScape Business V3 Service**

  Esta licencia de evaluación está destinada a socios de sistema que preconfiguren el sistema de comunicación en su empresa y lo quieran poner en servicio en el cliente. El periodo de activación de 30 días comienza durante la preconfiguración. Para que el periodo de activación se reinicie

después de la puesta en servicio del sistema, la licencia de evaluación se debe activar después de la puesta en servicio en el cliente.#

La activación solamente se puede realizar una vez por sistema y dentro del periodo de activación. Si el periodo de activación ha terminado, hay que registrar el sistema con licencias permanentes.

Nota: Cuando la Evaluación de Servicio está activada, CLS connect no puede activarse.

- **Evaluación de OpenScape Business V3 UC Smart**

  Esta licencia de evaluación es para clientes que desean probar las funciones de UC Smart. Con la licencia de evaluación se pueden usar todas las prestaciones de UC Smart.

  Nota: Esta licencia de evaluación no se puede utilizar si el sistema de comunicación está en una interred y la licencia "Networking" está activa. Si ya hay disponibles licencias de buzón de voz se utilizan junto con las nuevas licencias de evaluación de UC.

- **Evaluación de OpenScape Business V3 UC Suite**

  Esta licencia de evaluación es para clientes que desean probar las funciones de UC Suite. Con la licencia de evaluación se pueden usar todas las prestaciones de UC Suite.

  Nota: Esta licencia de evaluación no se puede utilizar si el sistema de comunicación está en una interred y la licencia "Networking" está activa. Si ya hay disponibles licencias de buzón de voz se utilizan junto con las nuevas licencias de evaluación de UC.

- **Evaluación de OpenScape Business V3 UC Suite Contact Center**

  Esta licencia de evaluación es para clientes que desean probar el Multimedia Contact Center. Esta licencia de evaluación permite utilizar todas las prestaciones del Multimedia Contact Center.

  Nota: Si durante el periodo de evaluación no se registra la licencia del Multimedia Contact Center, el administrador debe deshacer los ajustes realizados en el Contact Center antes del final de la licencia de evaluación (por ejemplo: borrar planes horarios y colas de espera, desactivar agentes, etc.). De lo contrario, pueden producirse errores de funcionamiento de OpenScape Business.

- **Evaluación de OpenScape Business V3 CRM**

  Esta licencia de evaluación es para clientes que desean probar Application Launcher, Open Directory Service y TAPI.

- **Evaluación de OpenScape Business V3 Attendant**

  Esta licencia de evaluación es para clientes que desean probar la aplicación OpenScape Business Attendant.

- **Evaluación de OpenScape Business V3 BLF**

  Esta licencia de evaluación está destinada a clientes que quieren probar la aplicación OpenScape Business BLF, por ejemplo, para la indicación propia de campos de lámparas de ocupado e información de presencia.

Reglas

- La licencia de evaluación se activa en el CLS (Servidor de licencias de cliente o "Customer License Server") y solo se puede activar una vez.
- El periodo de evaluación es de 90 días. Después de 60 días, en la pantalla de los teléfonos de sistema se muestra el tiempo restante en días, a modo de cuenta atrás.
- Una vez finalizado el periodo de evaluación la prestación se desactiva automáticamente.
- Puede haber distintas licencias de evaluación activas al mismo tiempo en el sistema, pero finalizan en momentos diferentes.
- Si hay activa una licencia sin límite temporal, no se inicia la licencia de evaluación o, si la hay, se detiene.

8.2.6 Licencias de upgrade

Para actualizar los sistemas HiPath 3000 V9, OpenScape Office V3 y OpenScape Business V1 a OpenScape Business V2 se requieren licencias de upgrade.

La migración de licencia de sistemas HiPath 3000 requiere un sistema HiPath 3000 V9 operativo y, en su caso, con registro de licencia. Hay que seguir cuidadosamente los pasos para la migración de hardware y de licencia (véase Migración). Los sistemas HiPath 3000 TDM puros sin licencias se deben actualizar primero a la versión 9. A continuación se pueden actualizar a OpenScape Business con una licencia de upgrade.

Están disponibles las siguientes licencias de Upgrade:

- **Upgrade de HiPath 3000 V9 a OpenScape Business V2**

  Para la migración de HiPath 3000 V9 a OpenScape Business V2 X3/X5/X8.
- **Upgrade de HiPath 3000 V8 a OpenScape Business V2**

  Para la migración de HiPath 3000 V8 a HiPath 3000 V9 y, a continuación, a OpenScape Business V2 X3/X5/X8.
- **Upgrade de HiPath 3000 V7 a OpenScape Business V2**

  Para la migración de HiPath 3000 V7 a HiPath 3000 V9 y, a continuación, a OpenScape Business V2 X3/X5/X8.
- **Upgrade de OpenScape Office V3 MX/LX a OpenScape Business V2**

  Para la migración de OpenScape Office V3 MX/LX a OpenScape Business V2.

8.2.7 Combinaciones de licencias posibles

Las licencias se pueden combinar de cualquier forma. A continuación se enumeran algunas propuestas para combinar las licencias y utilizar las funciones deseadas.

Téngase en cuenta que algunas funciones requieren varias licencias.

Telefonía

- Necesario: licencia de extensión de usuario IP, usuario TDM o usuario Deskshare

  Nota: Sin una licencia válida, el teléfono solo está habilitado para conexiones internas.

Telefonía con UC Smart

- Telefonía con buzón de voz (UC Smart)
  - Necesario: licencia de extensión de usuario IP, usuario TDM o usuario Deskshare
  - Requiere: licencia de buzón de voz orientada a usuarios
- Telefonía con Mobility Entry (movilidad basada en DISA)
  - Necesario: licencia de extensión de usuario Mobility
- Telefonía con myPortal to go
  - Necesario: licencia de extensión de usuario Mobility

    En el modo de servicio **Teléfono de sobremesa** (control del teléfono de oficina) no se requiere ninguna licencia Usuario Mobility.
  - Necesario: licencia UC User orientada a usuarios
  - Opcional: licencia de buzón de voz orientada a usuarios
- Telefonía con myPortal Smart @work
  - Necesario: Usuario IP
  - Necesario: licencia UC User orientada a usuarios
  - Opcional: licencia de buzón de voz orientada a usuarios
  - Opcional: licencia de conferencia orientada a usuarios
- Telefonía con myPortal @work VoIP
  - Necesario: Usuario IP
  - Necesario: licencia UC User orientada a usuarios
  - Opcional: licencia de buzón de voz orientada a usuarios
  - Opcional: licencia de conferencia orientada a usuarios
- Telefonía con optClient Attendant
  - Necesario: licencia de extensión de usuario IP, usuario TDM o usuario Deskshare
  - Necesario: licencia de sistema OpenScape Business Attendant
  - Opcional: licencia de buzón de voz orientada a usuarios
  - Opcional: licencia UC User orientada a usuarios (para indicación de presencia)

Telefonía con UC Suite

- Telefonía con buzón de voz (UC Suite)
  - Necesario: licencia de extensión de usuario IP, usuario TDM o usuario Deskshare
  - Requiere: licencia de buzón de voz orientada a usuarios
- Telefonía con myPortal for Desktop
  - Necesario: licencia de extensión de usuario IP, usuario TDM o usuario Deskshare
  - Necesario: licencia UC User orientada a usuarios
  - Opcional: licencia de buzón de voz orientada a usuarios
  - Opcional: licencia de fax orientada a usuarios
  - Opcional: licencia de conferencia orientada a usuarios
- Telefonía con myPortal for Outlook
  - Necesario: licencia de extensión de usuario IP, usuario TDM o usuario Deskshare
  - Requiere: licencia de Usuario groupware orientada a usuarios
  - Opcional: licencia de buzón de voz orientada a usuarios
  - Opcional: licencia de fax orientada a usuarios
  - Opcional: licencia de conferencia orientada a usuarios
- Telefonía con myPortal to go
  - Necesario: licencia de extensión de usuario Mobility

    En el modo de servicio **Teléfono de sobremesa** (control del teléfono de oficina) no se requiere ninguna licencia Usuario Mobility.
  - Necesario: licencia Groupware User orientada a usuarios o licencia UC User orientada a usuarios
  - Opcional: licencia de buzón de voz orientada a usuarios
- Telefonía con myPortal Smart @work
  - Necesario: Usuario IP
  - Necesario: licencia Groupware User orientada a usuarios o licencia UC User orientada a usuarios
  - Opcional: licencia de buzón de voz orientada a usuarios
  - Opcional: licencia de conferencia orientada a usuarios
- Telefonía con myPortal @work VoIP
  - Necesario: Usuario IP
  - Necesario: licencia Groupware User orientada a usuarios o licencia UC User orientada a usuarios
  - Opcional: licencia de buzón de voz orientada a usuarios
  - Opcional: licencia de conferencia orientada a usuarios
- Telefonía con myAttendant
  - Necesario: licencia de extensión de usuario IP, usuario TDM o usuario Deskshare
  - Requiere: licencia myAttendant orientada a usuarios
  - Opcional: licencia de buzón de voz orientada a usuarios

Telefonía con Unify Phone

- Necesario: Usuario IP
- Necesario: licencia de Unify Phone orientada a usuarios
- Opcional: licencia de VoiceMail orientada a usuarios y licencia de IP User adicional para la configuración del equipo

Uso del Centro de contactos

- Necesario: licencia de extensión de usuario IP, usuario TDM, usuario Deskshare o usuario Mobility
- Requiere: licencia myAgent orientada a usuarios

  Al menos una licencia de myAgent debe estar activa para que el sistema pueda enrutar y atender las llamadas del Contact Center.
- Opcional: licencia de sistema de correo de centro de Contact Center
- Opcional: licencia de sistema de fax de Contact Center
- Opcional: licencia de sistema myReports

Uso de Company AutoAttendant

- Necesario: licencia de sistema de Company AutoAttendant

  La licencia del sistema Company AutoAttendant debe estar activa para que el sistema pueda enrutar y dirigir las llamadas de AutoAttendant.

8.3 Registro de licencia de un sistema de comunicación (independiente)

El registro de licencia de un sistema independiente debe seguir siempre un orden determinado. Mostramos este orden tomando como ejemplo uno de los sistemas de comunicación OpenScape Business X.

La ejecución de los pasos 3 y 4 mediante la Gestión basada en Web (WBM) se detalla en los siguientes capítulos secundarios.

1) **Código de autorización de licencia (LAC)**

   Al comprar licencias el cliente recibe un código de autorización de licencia (LAC). Los datos acerca de las licencias adquiridas se almacenen an la base de datos del servidor de licencias central (CLS).
2) **Instalación y configuración**

   El cliente o el técnico de servicio instala y configura el sistema de comunicación mediante los asistentes de la Gestión basada en Web (WBM) (entre ellos, Extensiones y líneas). Al iniciar por primera vez la Gestión basada en Web (WBM) hay que introducir la fecha actual. A partir de este momento comienza el periodo de activación (plazo de 30 días en el que hay que registrar la licencia del sistema de comunicación).
3) **Activación de licencia**

   El cliente o el técnico de servicio activa las licencias con la Gestión basada en Web (WBM) en línea con el código de autorización de licencia (activación de licencia online) o sin conexión, directamente con el archivo de licencia (activación de licencia offline).
4) **Asignación de licencias**

   El cliente o el técnico de servicio asigna a las extensiones y líneas las licencias adquiridas mediante Gestión basada en Web (WBM). Una vez terminada la asignación, se liberan las prestaciones con licencia.

8.3.1 CLS Connect

CLS Connect le permite efectuar una cantidad ilimitada de realojamientos de los sistemas OpenScape Business. Para ello, el flag **CLS Connect** debe estar activado.

Nota: Después de la activación, este flag no se puede desactivar.

Si el sistema pierde la conexión con CLS, comienza el período a prueba de fallos. Si la conexión no se restablece pasados 30 días, el sistema pasa al modo de emergencia y se considera que está sin licencia.

Nota: Cuando es necesario reprogramar un sistema OpenScape Business con CLS Connect activo, no es posible crear un archivo de copia de seguridad. Este debe volver a cargarse con el mismo ID MAC e ID SIEL. CLS Connect no se puede activar sin una licencia básica activa. El archivo de licencia existente de CLS se puede cargar manualmente en el sistema a través del WBM.

8.3.1.1 Cómo activar CLS Connect

CLS Connect le permite efectuar una cantidad ilimitada de realojamientos de los sistemas OpenScape Business.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced**.

Para establecer conexión con CLS, necesita un acceso a Internet.

Esta es la configuración del firewall:

a) El puerto 7790 se libera para tráfico IP saliente

Los nuevos sistemas de software V3R3 utilizan el puerto 7791 para la activación de licencias en línea.

b) IP 188.64.16.4 se libera para tráfico IP saliente

Nota: Para que las reglas de firewall sean más seguras, se recomienda permitir solo comunicación saliente.

La conexión con CLS es posible; consulte Cómo comprobar la conexión de Central License Server (CLS)

Nota: Cuando se activa CLS Connect, no es posible desactivarlo.

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Activar CLS Connect**.
3) Active **CLS Connect** seleccionando la casilla de verificación.
4) Haga clic en **Activar**.

Nota: En el área de notificaciones de la página de aterrizaje, aparecerá el mensaje siguiente si el control de licencia en línea está activado:

'Modo de licencia: "CLS Connect".'

8.3.1.2 Pasar de CLS connect

Pasar de la CLS connect a una licencia permanente o PAYGO.

Si actualmente utiliza un sistema de licencias "CLS Connect" y desea pasar a una licencia permanente o PAYGO, debe seguir algunos pasos para garantizar una transición sin problemas:

Paso a paso

1) Active la función CLS Connect Stop para el archivo de licencia del sistema. Para ello, abra una ticket de soporte CLS.
2) Active un nuevo archivo de licencia para el OSBiz para restablecer el bit seguro. Una vez hecho esto, puede activar PAYGO o la licencia local permanente para el sistema en CLS. A continuación, recibirá un nuevo archivo que podrá activar en el sistema.

Nota: Si tiene un entorno OSBiz en red con licencia en CLS Connect, los nodos esclavos también tendrán el bit seguro activado. Si tiene previsto utilizar un nodo esclavo como sistema independiente con una licencia que no sea de CLS Connect en algún momento, envíe un ticket de soporte para conocer los pasos necesarios.

8.3.2 Activación de licencia (Standalone)

Después de adquirir un producto o una prestación, debe activar las licencias suministradas con dicho producto o prestación. Una vez hecha la activación, se realiza la asignación de licencias.

Tiene dos opciones para activar licencias:

- **Activación de licencia en línea** (con el código de autorización de licencia)

  El cliente o el técnico de servicio utiliza Gestión basada en Web (WBM) para transferir el código de autorización de licencia por Internet al servidor de licencias central (CLS). Para la activación de licencia, junto con el LAC se utiliza el ID de bloqueo del sistema de comunicación. A partir de los datos, el

CLS genera un archivo de licencia y lo envía de vuelta al sistema que lo usa para activar las licencias adquiridas.

Para acceder al CLS necesita una conexión a Internet. En la Gestión basada en Web (WBM), la dirección IP del CLS está almacenado en **Administración de licencias** > **Configuración** y, si es necesario, los datos pueden ser modificados por los administradores con el perfil **Experto**.

Nota: Para la activación de licencia en línea se utiliza el puerto 7790 de forma predeterminada. Este puerto debe estar liberado en el firewall de la red de clientes.

Los nuevos sistemas de software V3R3 utilizan el puerto 7791 para la activación de licencias en línea.

Nota: Para poder hacer el registro de licencia en línea, hay que registrar correctamente todos los datos de registro.

- **Activación de licencia offline** (directamente con el archivo licencia)

  El cliente o el técnico de servicio se registra en el servidor de licencias central (CLS) e indica el código de autorización de licencia junto con el ID de bloqueo del sistema de comunicación. El CLS genera un archivo de licencia a partir de esos datos. El cliente o el técnico de servicio descarga el archivo de licencia y lo ejecuta en la Gestión basada en Web (WBM). A continuación, el sistema activa las licencias adquiridas.

  En la Gestión basada en Web (WBM), la dirección IP del CLS está almacenado en **Administración de licencias** > **Configuración** y, si es necesario, los datos pueden ser modificados por los administradores con el perfil **Experto**.

Si se quiere ampliar el sistema de comunicación se pueden adquirir más licencias. Al adquirir licencias adicionales se suministra un nuevo código de autorización de licencia (LAC) con el que se pueden activar las licencias recién adquiridas.

Nota: Las licencias adicionales adquiridas también se pueden comprar de forma remota.

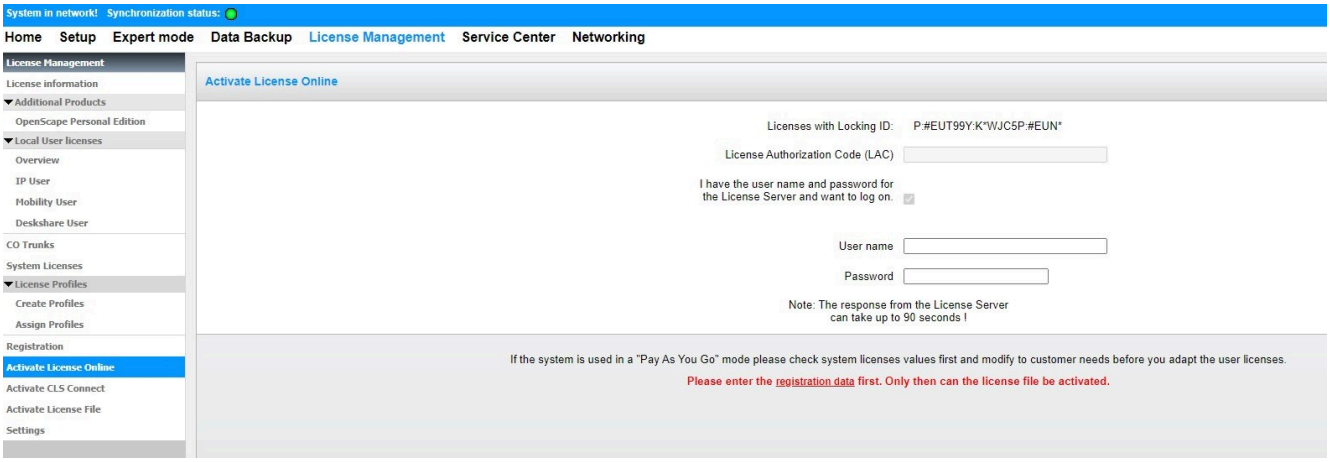
8.3.2.1 Cómo activar licencias en línea (Standalone)

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Conoce el código de activación de licencia (LAC) para la activación de licencia.

Para la conexión con el servidor de licencias, el sistema de comunicación debe tener una conexión con Internet.



Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Registro**.
3) Introduzca sus datos y haga clic en **Aceptar**.
4) En el árbol de navegación, haga clic en **Activar licencia online**.
5) En el campo **Código de autorización de licencia (LAC)** indique el LAC.
6) Active la casilla de verificación **Tengo el nombre de usuario y la contraseña para el servidor de licencias y quiero iniciar sesión**.
7) Introduzca el **Nombre de usuario** y la **Contraseña** para iniciar sesión en el servidor de licencia.
8) Haga clic en **Activar**. Se establece conexión con el servidor de licencias y las licencias se transfieren al sistema de comunicación Una vez activada la licencia, la conexión se restablece automáticamente.

8.3.2.2 Cómo activar licencias offline (Standalone)

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

El archivo de licencia se crea y almacena en el servidor central de licencias. Conoce el lugar de almacenamiento del archivo de licencia.

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Activar archivo de licencia**.
3) En **Archivo licencia**, haga clic en **Examinar** y seleccione el lugar de almacenamiento del archivo de licencia.
4) Haga clic en **Activar**.

8.3.3 Asignación de licencias (independiente)

Una vez activadas las licencias adquiridas, se deben asignar a las extensiones y las líneas. En un sistema independiente, las funciones en el ámbito del sistema están habilitadas desde el momento de la activación.

Asignaciones de licencias de usuario y orientadas a usuarios

Se pueden asignar a suscriptores licencias de usuario y licencias orientadas a usuarios.

Las licencias de usuario se pueden asignar a los siguientes tipos de suscriptor:

Icono	Licencia de usuario	Descripción
	Usuario IP	Para usar teléfonos IP del sistema (HFA o SIP) y teléfonos SIP
	Usuario TDM	Para usar teléfonos del sistema UP0, teléfonos RDSI, teléfonos analógicos y teléfonos DECT
	Usuario Mobility	Para usar myPortal to go, Mobility Entry y DISA (One Number Service)
	Usuario de Deskshare	Para usar DeskSharing en extensiones IP

Las licencias de usuario permanecen asignadas a los números de teléfono de los suscriptores. Si se elimina un suscriptor o se asigna a un número de teléfono otro tipo de suscriptor, se libera la licencia de usuario correspondiente.

Hay un asterisco rojo al lado de algunas licencias. Este asterisco indica que estas licencias también se pueden considerar asignando otra licencia.

Con registro de licencia flexible, también se pueden asignar a usuarios TDM, Mobility y DeskShare licencias de usuario IP. Si todas las licencias de usuarios TDM, DeskShare y Mobility están ya asignadas a suscriptores y se requieren más usuarios TDM, DeskShare y Mobility, se pueden utilizar licencias de usuario IP restantes para cubrir la demanda.

Después de asignar al suscriptor una licencia de usuario, también se le puede asignar una licencia orientada a usuarios.

Se pueden asignar a las extensiones estas licencias orientadas a usuarios:

Icono	Licencia orientada a usuarios	Descripción
	Buzón de voz	Para usar el buzón de voz.
	Usuario groupware	Para usar las funciones de UC Suite mediante myPortal for Outlook.
	Usuario UC	Para usar las funciones de UC Suite mediante myPortal for Desktop.

Icono	Licencia orientada a usuarios	Descripción
	Fax	Para usar un buzón de fax en la UC Suite. Se requiere una licencia UC User o Groupware User.
	Conferencia	Para usar las funciones de conferencia de UC Suite. Se requiere una licencia UC User o Groupware User.
	myAttendant	Para usar las funciones de conmutación de la UC Suite.
	myAgent	Para usar las funciones de Centro de contactos.
	Application Launcher	Para el control relativo a llamadas de aplicaciones en un PC cliente con llamadas entrantes y salientes, por ejemplo, abrir una aplicación o visualizar datos de llamante.
	Unify Phone	Para el uso del cliente Unify Phone en combinación con OpenScape Business.
	TAPI	Para usar las aplicaciones conformes con TAPI y telefonía por PC con programas propios del cliente de diferentes desarrolladores de software.

Puede mostrar un resumen de todas las licencias de usuario y de las licencias orientadas a usuarios (a través de **Licencias de usuario local** > **Resumen)**.

En este resumen también se muestran los estados de licencias para cada suscriptor.

Estados de licencia posibles:



Asignación de licencias del sistema

Las licencias de sistema incluyen licencias para líneas y para prestaciones a nivel de sistema.

Se pueden asignar licencias a estos tipos de líneas:

- Líneas S_{2M}/T1: número de canales B
- Líneas ITSP: número de llamadas simultáneas por un ITSP

De forma predeterminada, en un sistema independiente, las licencias para prestaciones a nivel de sistema se habrán habilitado durante la activación de la licencia. Por lo tanto, no es necesario realizar más asignaciones.

Procedimiento para la asignación de licencias

Requisitos previos: el archivo de licencia está activado y las extensiones están configuradas.

- Cómo registrar licencia de extensiones

  1) Asigne una licencia de usuario a un suscriptor. Con esta asignación se genera una solicitud de licencia para el suscriptor y, al mismo tiempo, se habilita la asignación de las licencias orientadas a usuarios.

  2) Asigne a un suscriptor las licencias orientadas a usuarios. Estas asignaciones generan otras solicitudes de licencia para el suscriptor. Recuerde que algunas licencias presuponen la presencia de otras licencias (véase Combinaciones de licencias posibles).

  3) Compruebe y libere solicitudes de licencia.

  4) Si no hay suficientes licencias que liberar, las asignaciones no válidas se indicarán mediante los estados de licencia (en rojo). Corrija las asignaciones de licencia, compruebe de nuevo las licencias y libérelas.

  Nota: Para obtener una mejor visión general, puede imprimir como vista previa las asignaciones de licencia de todas las extensiones (a través de **Licencias de usuario local** > **Resumen** > **Imprimir**). Al final de la impresión aparecen enumeradas en una tabla independiente todas las asignaciones no válidas.

- Asignar licencias de línea

  Las licencias de línea se deben distribuir entre las líneas S_{2M}/T1 y las líneas ITSP requeridas.

8.3.3.1 Cómo registrar licencias para suscriptores (independientes)

Distribuya las licencias de extensión y las licencias orientadas a usuarios (User) disponibles entre las extensiones. Una vez finalizada la asignación, los suscriptores quedan registrados con licencia.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.

2) En el árbol de navegación, en **Licencias de usuario local** > **...**, desplácese hasta el tipo de suscriptor deseado. Aparece una lista de todos los suscriptores del tipo seleccionado.

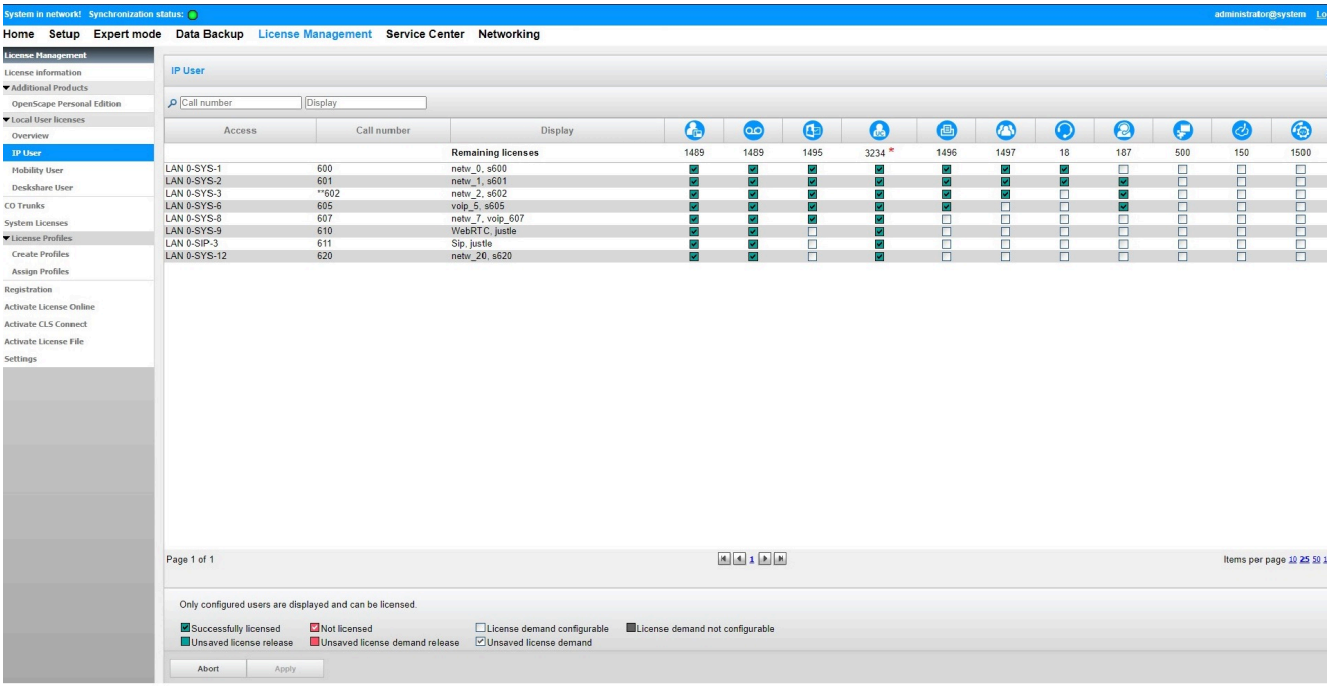
En **Licencias restantes** se indica cuántas licencias quedan por asignar a los suscriptores. En las extensiones TDM, Mobility y DeskShare, también se muestran todas las licencias de IP User restantes, dado que estas licencias también se pueden utilizar para el registro de licencia de extensiones TDM, Mobility y DeskShare (registro flexible de licencias de extensión).

Si el tipo de suscriptor seleccionado es Mobility User, también verá el número total de licencias de Unify Phone disponibles y su fecha de caducidad.

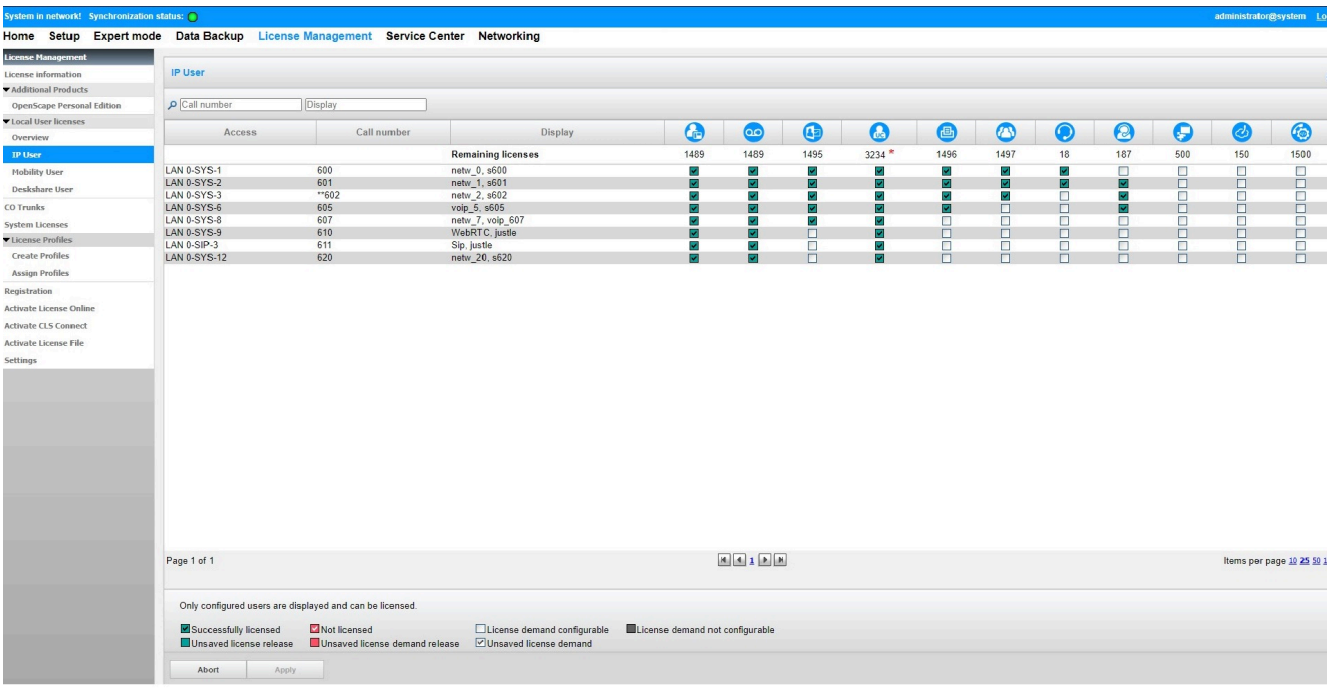
3) En la línea de la extensión deseada, active la licencia de extensión. Para ello, active la casilla de verificación de fondo claro (primera columna con

casillas de verificación). Las casillas de verificación de las demás columnas se habilitan.

Nota: Para mostrar una extensión seleccionada, introduzca el término de búsqueda en los campos de búsqueda **N° de llamada** o **Nombre** y, a continuación, pulse la tecla Intro o haga clic en el icono en forma de lupa. Si todos los campos de búsqueda están vacíos y pulsa la tecla Intro o hace clic en el icono en forma de lupa, aparece una lista de todas las extensiones.



4) En la línea del suscriptor deseado, active las licencias orientadas a usuarios. Para ello, active las casillas de verificación pertinentes.



Nota: Las licencias orientadas a usuarios (User) solo se pueden asignar a una extensión si antes se le ha asignado una licencia de extensión (paso 3).

Nota: Al asignar una licencia de Buzón de voz a una extensión, se crea un usuario de UC Suite y se restablecen todos los desvíos de llamadas activos.

Nota: En "Pago por uso", la licencia de buzón de voz se selecciona o anula automáticamente cuando se activa o desactiva una licencia de usuario de voz; pero también es posible anular una licencia de buzón de voz.

Las prestaciones de licencia de Groupware, usuario UC, myAttendant y myAgent no se pueden configurar en modo UC Smart.

Las licencias de Groupware y usuario UC son mutuamente excluyentes en el modo UC Suite.

5) Haga clic en **OK y Continuar**. Se comprueba si hay suficientes licencias para la asignación.

   Si hay suficientes licencias, con esto finaliza el registro de licencia del suscriptor.

   Nota: En "Pago por uso", aparece una ventana emergente. Haga clic en **OK** para confirmar la selección.

6) Si faltan licencias, las casillas de verificación tendrán fondo rojo. Corrija estos errores y repita el paso 5.

   Nota: Si desea retirar una licencia de extensión, deberá confirmar un mensaje de aviso. A continuación aparece una nueva casilla de verificación **Advertencias habilitadas**. Si desactiva esta casilla de verificación, puede retirar licencias de extensión adicionales sin mensajes de aviso.

8.3.3.2 Cómo registrar licencias para líneas (Standalone)

Distribuya las licencias de línea adquiridas entre las líneas SIP y S_{2M}/T1.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Líneas urbanas**. En el área **Líneas urbanas** aparece indicado el número de licencias disponibles para líneas urbanas SIP y S_{2M}/T1.
3) Para las líneas SIP: en el área **SIP trunks**, y en **Demanda de licencias para el número de llamadas de Internet simultáneas en este nodo** indique el número de llamadas Internet que se pueden realizar simultáneamente mediante un ITSP.
4) Para las líneas S_{2M}: en el área **PRI (S2M/T1)** de la línea del slot S_{2M} deseado, seleccione el número de canales B deseado en la columna **Demands** (Demandas).
5) Para las líneas T1 digitales (solo para EE.UU): en el área **PRI (S2M/T1)** de la línea del slot T1 deseado, seleccione el número de canales B deseado en la columna **Demands (Demandas)**.
6) Para líneas T1 analógicas (solo USA): active la línea T1 analógica; para ello, en el área **PRI (S2M/T1)** de la línea de la línea T1 analógica y en la lista desplegable de la columna **Demands** (Demandas), seleccione la entrada **1** (**0** significa que la línea está desactivada).
7) Haga clic en **OK & Continuar**.

   Nota: El número de líneas SIP con licencia y el número de líneas S_{2M}/T1 con licencia no puede ser superior al número de licencias de línea disponibles.

8.4 Registro de licencia de varios sistemas de comunicación (interred)

El registro de licencia de varios sistemas de comunicación se debe realizar siguiendo un determinado orden. Este orden se muestra tomando como ejemplo una interred de un OpenScape Business S (Maestro) y dos OpenScape Business X3 (esclavos).

Si hay varios OpenScape Business (nodos) conectados en una interred, el registro de licencia se realiza de forma centralizada mediante un archivo de licencia de red que se activa en el nodo maestro. Además, cada nodo esclavo de la interred requiere una licencia de sistema de red propia. El nodo con mayor ancho de banda debería ser el nodo maestro.

Con el asistente de redes de Gestión basada en Web (WBM), los nodos de la interred se configuran como nodos maestros y nodos esclavos ("Master" y "Slave"). El nodo maestro incluye el agente de licencias central (CLA central o "central Customer License Agent"). Todos los nodos esclavos de la interred utilizan el CLA para el registro de licencia. Para ello se da a conocer al nodo esclavo la dirección IP del nodo maestro mediante Gestión basada en Web (WBM).

Para toda la interred solo hay un archivo de licencia de red. Este está vinculado al nodo maestro mediante el ID de bloqueo. Si un OpenScape Business S (softswitch) es el nodo maestro, el archivo de licencia de red está vinculado mediante el ID de bloqueo del servidor Linux del softswitch o mediante el ID de bloqueo avanzad (Advanced Locking ID) del softswitch si este se utiliza en un entorno virtual. El archivo de licencia de red se almacena en el CLA central e incluye la información de licencia de la interred. Solo se puede activar en el nodo maestro mediante la Gestión basada en Web (WBM). Solo el nodo maestro tiene acceso al CLS. En todos los demás nodos este acceso está desactivado.

En la interred no se debería hacer un registro de licencia específico de nodos. Si por cada nodo ya hay un archivo de red propio, se pueden reunir en un único archivo de licencia de red en el CLS.

Comportamiento ante problemas de red (Failover)

Si se interrumpe la conexión con el nodo maestro y, con ello, con el CLA central, en la pantalla de los teléfonos de sistema se muestra el mensaje "Failover Period" (Periodo a prueba de fallos). En este periodo a prueba de fallos (con un máximo de 30 días), todos los nodos y sus prestaciones siguen manteniendo su funcionalidad. Si se resuelven los problemas de red y se restablece la conexión con el CLA central, todos los nodos recuperar en estado de licencia normal.

Si los problemas de red no se resuelven en el periodo a prueba de fallos, los nodos pasan al servicio de emergencia. A continuación, se debe volver a registrar la licencia de la interred.

Pasos para el registro de licencia en la interred con el ejemplo anterior

El OpenScape Business S (maestro) y los dos OpenScape Business X3 (esclavos) ya están instalados, configurados y conectados con una interred.

1) **Código de autorización de licencia (LAC)**

   Al comprar licencias el cliente recibe un código de autorización de licencia (LAC). Los datos acerca de las licencias adquiridas se almacenen an la base de datos del servidor de licencias central (CLS).

2) **OpenScape Business S como nodo maestro**

   El cliente o el técnico de servicio se registra en la Gestión basada en Web (WBM) de OpenScape Business S e instala OpenScape Business S como nodo maestro mediante el asistente de red.

   El sistema ya está instalado y configurado, y está en el periodo de activación (periodo de 30 días en el que se debe realizar el registro de licencia).

3) **ID de bloqueo del nodo maestro**

   El cliente o el técnico de servicio anota el ID de bloqueo o el ID de bloqueo avanzado de OpenScape Business S.

   Descripción, véase Cómo consultar el ID de bloqueo del sistema de comunicación

4) **OpenScape Business X3 como nodos esclavos**

   El cliente o el técnico de servicio se registra en primer lugar en la Gestión basada en Web (WBM) del primer OpenScape Business X3 e instala mediante el asistente de red el primer OpenScape Business X3 como nodo esclavo; después repite el mismo procedimiento en la Gestión basada en Web (WBM) del segundo OpenScape Business X3.

   Los sistemas ya están instalados y configurados, y están en el periodo de activación.

5) **ID de bloqueo de OpenScape Business X3**

   El cliente o el técnico de servicio anota el ID de bloqueo o el ID de bloqueo avanzado de los dos OpenScape Business X3.

   Descripción, véase Cómo consultar el ID de bloqueo del sistema de comunicación

6) **Activación de licencia**

   El cliente o el técnico de servicio se registra en el CLS y genera un archivo de licencia de red junto con el código de autorización de licencia y los ID de bloqueo. Carga el archivo mediante la Gestión basada en Web (WBM) en el nodo maestro.

   Descripción, véase Cómo activar licencias sin conexión (interred)

   A continuación, el sistema activa las licencias adquiridas.

7) **Asignación de licencias**

   El cliente o el técnico de servicio distribuye las licencias entre los nodos. Para ello, Gestión basada en Web (WBM) se registra en cada nodo y le asigna el número de licencias deseado. Lo importante es que se asigne a cada nodo una licencia de sistema de red ya que de lo contrario no se integrará en la interred.

   Descripción, véase Cómo asignar licencias de sistema a un nodo

8.4.1 Activación de licencia (interred)

Después de adquirir un producto o una prestación, debe activar las licencias suministradas con dicho producto o prestación. Para ello se necesita directamente el archivo de licencia. Una vez hecha la activación, se realiza la asignación de licencias.

Tiene esta opción para activar licencias:

- **Activación de licencia offline** (directamente con el archivo licencia)

  El cliente o el técnico de servicio se registra en el servidor de licencias central (CLS) e indica el código de autorización de licencia junto con los ID de bloqueo de los sistemas de comunicación. El CLS genera un archivo de licencia a partir de esos datos. El cliente o el técnico de servicio descarga el archivo de licencia y lo ejecuta en la Gestión basada en Web (WBM) del nodo maestro.

  En el nodo maestro se comprueba si los ID de bloqueo memorizados en el archivo de licencia coinciden con los de los sistemas. Si la comprobación es correcta, se activan las licencias y los sistemas pasan al estado de licencia normal. Si la comprobación no es correcta, los sistemas continúan funcionando en el periodo de activación y, una vez agotado, en modo de emergencia.

  La dirección IP del CLS se almacena en Gestión basada en Web (WBM), en **Administración de licencias** > **Configuración**.

Tiene esta opción para agrupar archivos de licencia:

- **Cómo reunir archivos de licencia en un archivo de licencia de red**

  Si ya se ha registrado la licencia de uno o varios nodos y desea unir estos nodos en una interred, el administrador debe aglutinar los distintos archivos de licencia en un archivo de licencia de red mediante el CLS y cargar este archivo en el CLA central. En todos los demás nodos hay que introducir la dirección IP del nodo maestro con el agente de licencias central a través del asistente de red de la Gestión basada en Web (WBM).

8.4.1.1 Cómo activar licencias sin conexión (interred)

Tomando como ejemplo un OpenScape Business S como nodo maestro (nodo 1) y dos OpenScape Business X3 (nodo 2 y nodo 3), se describe cómo generar y activar el archivo de licencia de red común.

Requisitos previos

Hay un acceso al CLS.

Todos los nodos están instalados e interconectados entre sí, véase Interconexión de OpenScape Business X y OpenScape Business S (multigateway).

Paso a paso

1) Inicie sesión en el CLS con su nombre de usuario y contraseña.
2) En **Licencias**, seleccione la opción **Generar y descargar clave de licencia**.

3) En **LAC** introduzca el código de autorización de licencia (LAC) y haga clic en **Buscar**.
4) Abra el producto OpenScape Business S y seleccione las prestaciones que desea asignar al nodo 1.
5) Haga clic en **Generar clave licencia**.
6) En **Dirección MAC** introduzca la dirección MAC o el ID de bloqueo avanzado de OpenScape Business S (nodo 1) y en **Dirección MAC del CLA de red** vuelva a introducir la dirección MAC o el ID de bloqueo avanzado de OpenScape Business S (nodo maestro).

Nota: La dirección MAC de OpenScape Business S es la dirección MAC de la tarjeta de red del servidor Linux de OpenScape Business S utilizado en la instalación del sistema operativo Linux. El ID de bloqueo avanzado de OpenScape Business S se utiliza en lugar de la dirección MAC si OpenScape Business S opera en un entorno virtual.

---

7) En las prestaciones, indique el número deseado y haga clic en **Continuar**.
8) Compruebe los datos del cliente y haga clic en **Continuar**.
9) Lea el aviso legal y, a continuación, haga clic en **Acepto estas condiciones**.
10) Haga clic en **Ejecutar**, para generar la clave de licencia.
11) Para el nodo 2, en **Licencias**, seleccione la entrada **Generar y descargar clave de licencia**.
12) En **LAC** vuelva a introducir el código de autorización de licencia (LAC) y haga clic en **Buscar**.
13) Abra el producto OpenScape Business X3 y seleccione las prestaciones que desea asignar al nodo 2.
14) Haga clic en **Generar clave licencia**.
15) En **Dirección MAC** introduzca la dirección MAC del nodo 2 y en **Dirección MAC del CLA de red** introduzca la dirección MAC del nodo 1 (nodo maestro).
16) En las prestaciones, indique el número deseado y haga clic en **Continuar**.
17) Haga clic en **Continuar**.
18) Confirme la advertencia. Para ello, haga clic en la casilla de verificación **Sí, acepto las condiciones**.
19) Haga clic en **Ejecutar**, para generar la clave de licencia.
20) Repita los pasos del 11 al 19 para el nodo 3.
21) Haga clic en **Clave licencia** y, a continuación, en **Descarga** para descargar el archivo de licencia de red.
22) Guarde el archivo de licencia de red.
23) Inicie sesión en la Gestión basada en Web (WBM) del nodo maestro. Para ello, en su navegador Web abra la dirección `https://<Dirección IP del nodo maestro>` y, a continuación, introduzca el nombre de usuario y la contraseña.
24) En la barra de navegación, haga clic en **Administración de licencias**.
25) En el árbol de navegación, haga clic en **Activar archivo de licencia**.
26) En **Archivo licencia**, haga clic en **Examinar** y seleccione el lugar de almacenamiento del archivo de licencia de red.

27) Haga clic en **Activar**.

8.4.1.2 Cómo reunir archivos de licencia en un archivo de licencia de red

Si se integran en una interred varios nodos que previamente no estuvieran interconectados, los archivos de licencia de los distintos nodos se deben combinar en un archivo de licencia de red común mediante CLS.

Requisitos previos

Hay un acceso al CLS y tiene derechos de acceso para el paquete de licencias de los distintos nodos.

Todos los nodos están instalados e interconectados entre sí, véase Interconexión de OpenScape Business X y OpenScape Business S (multigateway).

Paso a paso

1) Inicie sesión en el CLS con su nombre de usuario y contraseña.
2) En **Registro de licencia de red** seleccione la opción **Agregar/eliminar sistema**.
3) Seleccione la dirección MAC del nodo que desea integrar en la interred.
4) Haga clic en **Rehost**.
5) En **Dirección MAC** introduzca la dirección MAC del nodo.
6) En **Dirección MAC del CLA de red** introduzca la dirección MAC del nodo maestro. Por norma general, OpenScape Business S es el nodo maestro.

   Nota: La dirección MAC de OpenScape Business S es la dirección MAC de la tarjeta de red del servidor Linux de OpenScape Business S utilizado en la instalación del sistema operativo Linux.

7) Haga clic en **Continuar**.
8) Compruebe los datos del cliente y haga clic en **Continuar**.
9) Lea el aviso legal y, a continuación, haga clic en **Acepto estas condiciones**.
10) Haga clic en **Ejecutar**, para generar la clave de licencia.
11) Para los siguientes nodos, repita los pasos del 2 al 10.
12) Haga clic en **Clave licencia** y, a continuación, en **Descarga** para descargar el archivo de licencia de red.
13) Guarde el archivo de licencia de red.
14) Inicie sesión en la Gestión basada en Web (WBM) del nodo maestro. Para ello, en su navegador Web abra la dirección `https://<Dirección IP del nodo maestro>` y, a continuación, introduzca el nombre de usuario y la contraseña.
15) En la barra de navegación, haga clic en **Administración de licencias**.
16) En el árbol de navegación, haga clic en **Activar archivo de licencia**.
17) En **Archivo licencia**, haga clic en **Examinar** y seleccione el lugar de almacenamiento del archivo de licencia de red.
18) Haga clic en **Activar**.

8.4.2 Asignación de licencias (interred)

Una vez activadas las licencias adquiridas, se deben asignar a las extensiones y las líneas. Esta asignación se realiza en cada nodo por separado.

Asignaciones de licencias de usuario y orientadas a usuarios

Se pueden asignar a suscriptores licencias de usuario y licencias orientadas a usuarios.

Las licencias de usuario se pueden asignar a los siguientes tipos de suscriptor:

Icono	Licencia de usuario	Descripción
	Extensiones IP	Para usar teléfonos IP del sistema (HFA o SIP) y teléfonos SIP
	Extensiones TDM	Para usar teléfonos del sistema UP0, teléfonos RDSI, teléfonos analógicos y teléfonos DECT
	Extensiones móviles	Para usar myPortal to go, Mobility Entry y DISA (One Number Service)
	Extensiones DeskSharing	Para usar DeskSharing en extensiones IP
	Usuario en reserva	Para uso de telefonía básica en caso de producirse un fallo.

Las licencias de usuario permanecen asignadas a los números de teléfono de los suscriptores. Si se elimina un suscriptor o se asigna a un número de teléfono otro tipo de suscriptor, se libera la licencia de usuario correspondiente.

Con registro de licencia flexible, también se pueden asignar a usuarios TDM, Mobility y DeskShare licencias de usuario IP. Si todas las licencias de usuarios TDM, DeskShare y Mobility están ya asignadas a suscriptores y se requieren más usuarios TDM, DeskShare y Mobility, se pueden utilizar licencias de usuario IP restantes para cubrir la demanda.

Después de asignar al suscriptor una licencia de usuario, también se le puede asignar una licencia orientada a usuarios.

Se pueden asignar a las extensiones estas licencias orientadas a usuarios:

Icono	Licencia orientada a usuarios	Descripción
	Buzón de voz	Para usar el buzón de voz.
	Usuario groupware	Para usar las funciones de UC Suite mediante myPortal for Outlook.
	UC Suite	Para usar las funciones de UC Suite mediante myPortal for Desktop.
	Fax	Para usar un buzón de fax en la UC Suite. Se requiere una licencia UC User o Groupware User.

Icono	Licencia orientada a usuarios	Descripción
	Conferencia	Para usar las funciones de conferencia de UC Suite. Se requiere una licencia UC User o Groupware User.
	myAttendant	Para usar las funciones de conmutación de la UC Suite.
	myAgent	Para usar las funciones de Centro de contactos.
	Application Launcher	Para el control relativo a llamadas de aplicaciones en un PC cliente con llamadas entrantes y salientes, por ejemplo, abrir una aplicación o visualizar datos de llamante.
	Unify Phone	Para el uso del cliente Unify Phone en combinación con OpenScape Business.
	TAPI 120/170	Para usar las aplicaciones conformes con TAPI y telefonía por PC con programas propios del cliente de diferentes desarrolladores de software.

Puede mostrar un resumen de todas las licencias de usuario y de las licencias orientadas a usuarios (a través de **Licencias de usuario local** > **Resumen)**.

En este resumen también se muestran los estados de licencias para cada suscriptor.

Estados de licencia posibles:



Asignación de licencias del sistema

Las licencias de sistema incluyen licencias para líneas y para prestaciones a nivel de sistema.

Se pueden asignar licencias a estos tipos de líneas:

- Líneas S_{2M}/T1: número de canales B
- Líneas ITSP: número de llamadas simultáneas por un ITSP

Las licencias a nivel de sistema se asignan a cada sistema (nodo) de la interred. Esta configuración debe hacerse consecutivamente en cada nodo. El número total de licencias a nivel de sistema que se guardan en el archivo de licencia en el nodo maestro, se reduce al número configurado en el nodo.

Procedimiento para la asignación de licencias

Requisitos previos: el archivo de licencia está activado y las extensiones están configuradas.

- Cómo registrar licencia de extensiones

  1) Asigne una licencia de usuario a un suscriptor. Con esta asignación se genera una solicitud de licencia para el suscriptor y, al mismo tiempo, se habilita la asignación de las licencias orientadas a usuarios.

  2) Asigne a un suscriptor las licencias orientadas a usuarios. Estas asignaciones generan otras solicitudes de licencia para el suscriptor. Recuerde que algunas licencias presuponen la presencia de otras licencias (véase Combinaciones de licencias posibles).

  3) Compruebe y libere solicitudes de licencia.

  4) Si no hay suficientes licencias que liberar, las asignaciones no válidas se indicarán mediante los estados de licencia (en rojo). Corrija las asignaciones de licencia, compruebe de nuevo las licencias y libérelas.

  Nota: Para obtener una mejor visión general, puede imprimir como vista previa las asignaciones de licencia de todas las extensiones (a través de **Licencias de usuario local** > **Resumen** > **Imprimir**). Al final de la impresión aparecen enumeradas en una tabla independiente todas las asignaciones no válidas.

- Asignar licencias de línea

  Las licencias de línea se deben distribuir entre las líneas S_{2M}/T1 y las líneas ITSP requeridas.

8.4.2.1 Cómo registrar licencia para extensiones (interred)

Distribuya las licencias de extensión y las licencias orientadas a usuarios (User) disponibles entre las extensiones. Una vez finalizada la asignación, los suscriptores quedan registrados con licencia.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.

2) En el árbol de navegación, en **Licencias de usuario local** > **...**, desplácese hasta el tipo de suscriptor deseado. Aparece una lista de todos los suscriptores del tipo seleccionado.

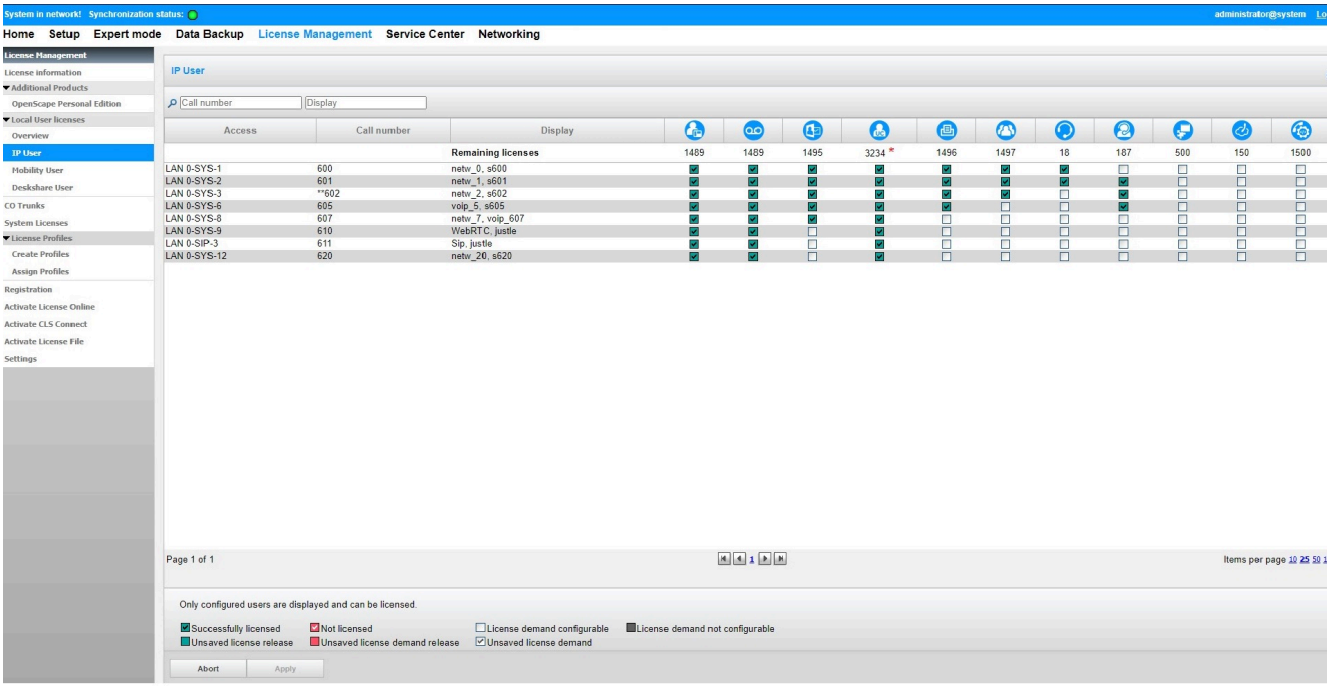
En **Licencias restantes** se indica cuántas licencias quedan por asignar a los suscriptores. En las extensiones TDM, Mobility y DeskShare, también se muestran todas las licencias de IP User restantes, dado que estas licencias también se pueden utilizar para el registro de licencia de extensiones TDM, Mobility y DeskShare (registro flexible de licencias de extensión).

Si el tipo de suscriptor seleccionado es Mobility User, también verá el número total de licencias de Unify Phone disponibles y su fecha de caducidad.

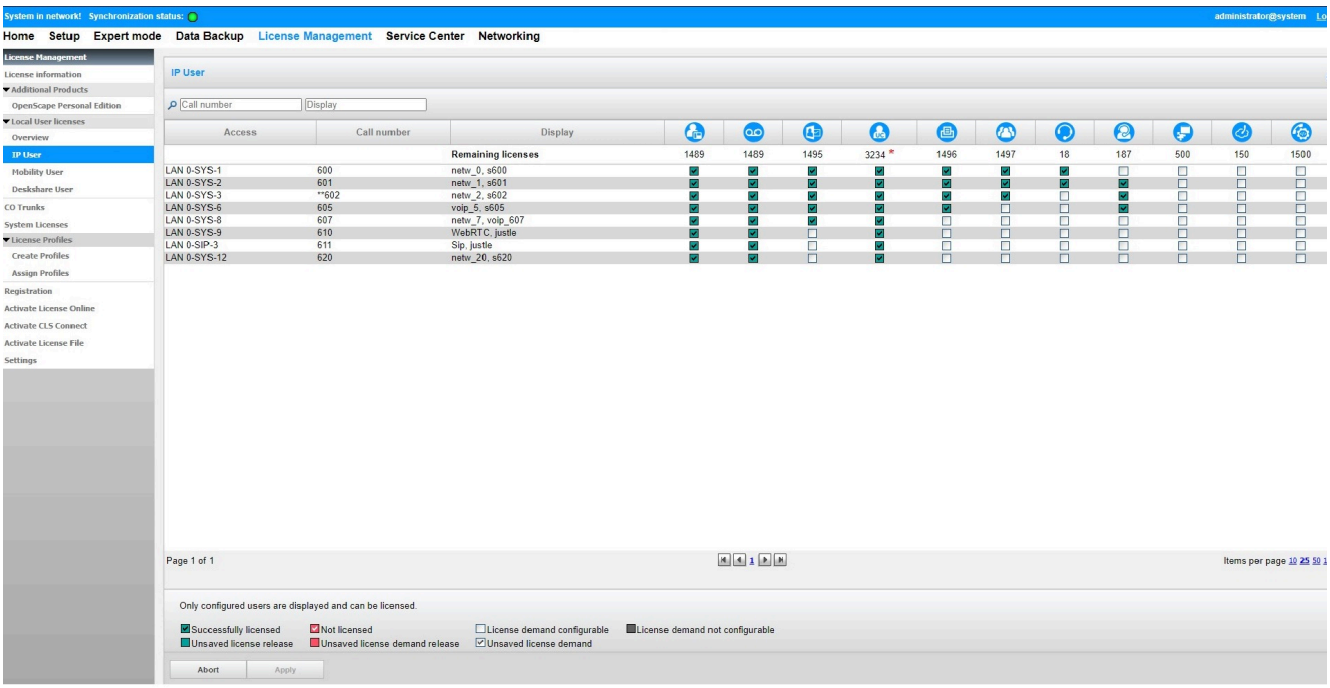
3) En la línea de la extensión deseada, active la licencia de extensión. Para ello, active la casilla de verificación de fondo claro (primera columna con

casillas de verificación). Las casillas de verificación de las demás columnas se habilitan.

Nota: Para mostrar una extensión seleccionada, introduzca el término de búsqueda en los campos de búsqueda **N° de llamada** o **Nombre** y, a continuación, pulse la tecla Intro o haga clic en el icono en forma de lupa. Si todos los campos de búsqueda están vacíos y pulsa la tecla Intro o hace clic en el icono en forma de lupa, aparece una lista de todas las extensiones.



4) En la línea del suscriptor deseado, active las licencias orientadas a usuarios. Para ello, active las casillas de verificación pertinentes.



Nota: Las licencias orientadas a usuarios (User) solo se pueden asignar a una extensión si antes se le ha asignado una licencia de extensión (paso 3).

Nota: La opción de "Pago por uso" no está disponible en caso de archivo de licencia de red.

En el caso de una red de sistemas OpenScape Business, cualquiera de los sistemas puede utilizar la opción de Pago por uso a través del Agente Central de Licencias (CLA) local.

---

5) Haga clic en **OK y Continuar**. Se comprueba si hay suficientes licencias para la asignación.

   Si hay suficientes licencias, con esto finaliza el registro de licencia del suscriptor.

6) Si faltan licencias, las casillas de verificación tendrán fondo rojo. Corrija estos errores y repita el paso 5.

Nota: Si desea retirar una licencia de extensión, deberá confirmar un mensaje de aviso. A continuación aparece una nueva casilla de verificación **Advertencias habilitadas**. Si desactiva esta casilla de verificación, puede retirar licencias de extensión adicionales sin mensajes de aviso.

8.4.2.2 Cómo registrar licencias para líneas (interred)

Distribuya las licencias de línea adquiridas entre las líneas SIP y S_{2M}/T1.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Líneas urbanas**. En el área Líneas urbanas aparece indicado el número de licencias disponibles para líneas urbanas SIP y S**2M**/T1.
3) Para las líneas SIP: en el área **SIP trunks**, y en **Demanda de licencias para el número de llamadas de Internet simultáneas en este nodo** indique el número de llamadas Internet que se pueden realizar simultáneamente mediante un ITSP.
4) Para las líneas S_{2M}: en el área **S2M** de la línea del slot deseado, seleccione el número de canales B deseado en la columna **Demands** (Demandas).
5) Para las líneas T1 (solo para EE.UU): en el área **T1** de la línea del slot deseado, seleccione el número de canales B deseado en la columna **Demands (Demandas)**.
6) Haga clic en **OK & Continuar**.

Nota: El número de líneas SIP con licencia y el número de líneas S_{2M}/T1 con licencia no puede ser superior al número de licencias de línea disponibles.

8.4.2.3 Cómo asignar licencias de sistema a un nodo

Requisitos previos

Se ha registrado en del nodo deseado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Licencias del sistema**. Aparecen todas las licencias del sistema disponibles.
3) En la columna **Licencias en uso** seleccione el número de licencias del sistema que desea asignar al nodo.

   En la columna **disponible para distribución** se indica cuántas licencias hay disponibles para toda la interred.

Nota: Compruebe que el nodo tiene asignada la licencia de sistema "Networking"; de lo contrario el nodo no está integrado en la interred.

---

4) Haga clic en **Guardar**.

8.4.2.4 Cómo asignar la licencia del sistema "Redes" a un nodo

Requisitos previos

Se ha registrado en del nodo deseado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Licencias del sistema**. Aparecen todas las licencias del sistema disponibles.
3) En la licencia del sistema **Redes** de la columna **Licencias en uso**, seleccione la entrada **1** en la lista disponible.

   En la columna **disponible para distribución** se indica cuántas licencias hay disponibles para toda la interred.
4) Haga clic en **Guardar**.

8.5 Información de licencia

Se muestra información sobre las licencias disponibles y asignadas, sobre los productos y prestaciones con Gestión basada en Web (WBM). En la interred se puede consultar la información de licencia de todos los nodos presentes en la red.

Se muestra la siguiente información:

- **Dirección MAC**: Dirección MAC de la plataforma de hardware o del servidor Linux del softswitch con el que están vinculadas las licencias.

  Nota: Si el sistema de comunicación se encuentra en el periodo de gracia, aquí puede aparecer una dirección MAC errónea. La dirección MAC correcta se puede consultar a través del **Centro de servicios**, en **Inventario** (Inventario).
- **Advanced Locking ID**: ID bloqueo avanzado del softswitch de entorno virtual con el que están vinculadas las licencias.
- **Locking ID**: el ID de bloqueo del servidor de aplicaciones con el que están vinculadas las licencias.
- **Nodo**: nombre del sistema de comunicación al que están vinculadas las licencias.
- **Nombre de producto**: nombre del producto al que está asignada la licencia.
- **Prestación**: prestación a la que está asignada la licencia.
- **Licencias en uso**: muestra de las licencias en uso y disponibles.
- **Licencias distribuibles**: indicación de las licencias todavía disponibles en la interred.
- **Estado**: estado de la licencia.

El producto OpenScape Personal Edition se registra mediante un archivo de licencia propio. Puede ver la información de licencia al respecto en **Otros productos**.

8.5.1 Información de licencia sin interred (Standalone)

Se pueden mostrar todas las licencias asignadas al sistema de comunicación y la información correspondiente.

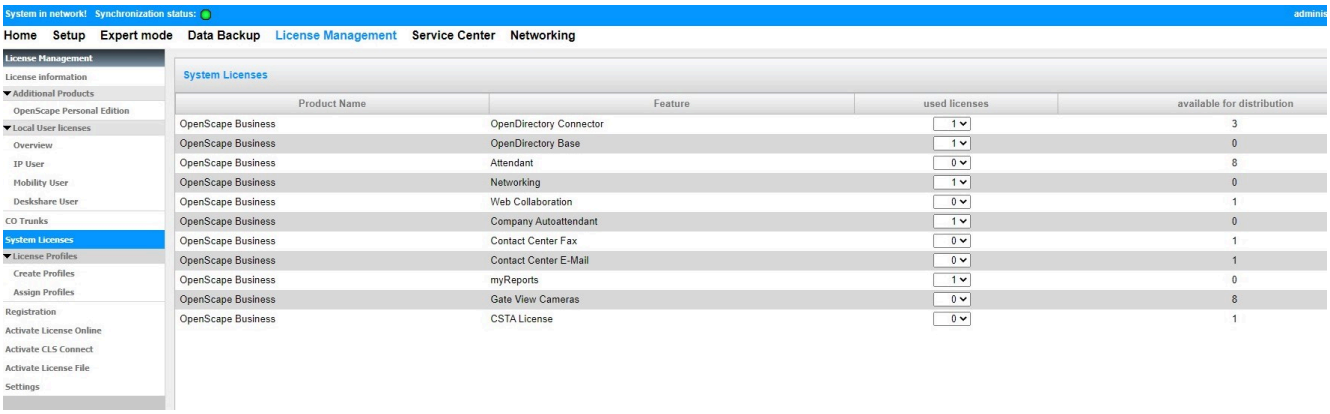
8.5.1.1 Cómo mostrar información de licencia

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

En la barra de navegación, haga clic en **Administración de licencias**. Aparece la información de licencia sobre el sistema de comunicación.



Nota: En caso de "Pago por uso" las licencias utilizadas son configurables excepto para Contact Center Fax, Contact Center E-mail y myReports en modo UC Smart.

8.5.2 Información de licencia en la interred

En una interred se pueden mostrar todas las licencias y la información correspondiente. Esta información se consulta en el archivo de licencia de red.

Todas las licencias de una interred (salvo las licencias básicas) son del tipo "floating" y se encuentran en una reserva (pool) de licencias. Si una licencia ya no se necesita en un nodo (sistema de comunicación) y se libera, se puede utilizar en otro nodo.

En una interred se pueden mostrar todas las licencias de la interred y todas las licencias utilizadas en común (floating) o vinculadas a un nodo específico.

Además, las licencias de extensión y las licencias orientadas a usuarios (User) se pueden ordenar por nodos y se pueden mostrar en una vista general.

8.5.2.1 Cómo mostrar todas las licencias de la interred

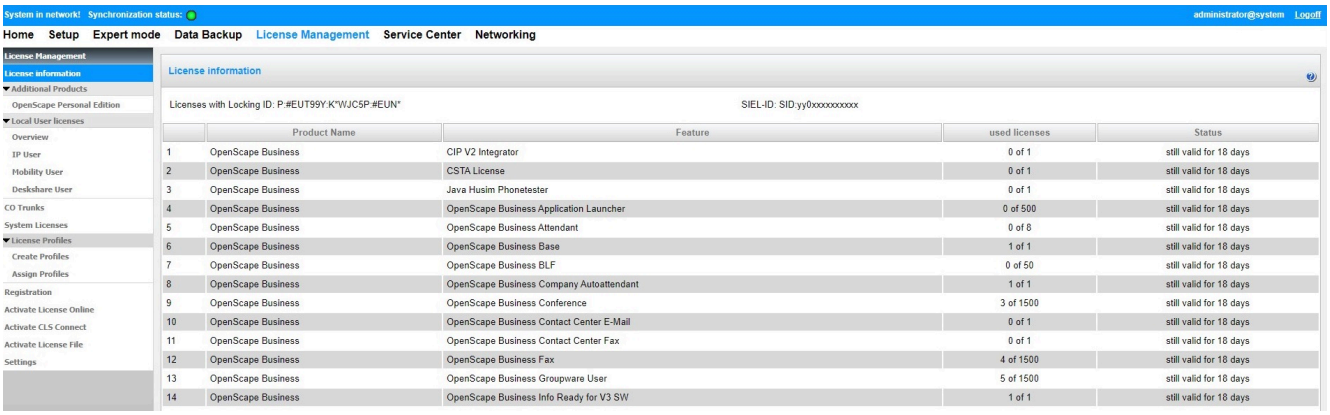
Requisitos previos

El sistema de comunicación se encuentra en una interred.

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Información de licencia**. Aparecen todas las licencias de la interred.



	Product Name	Feature	used licenses	Status
1	OpenScape Business	CIP V2 Integrator	0 of 1	still valid for 18 days
2	OpenScape Business	CSTA License	0 of 1	still valid for 18 days
3	OpenScape Business	Java Husim Phonetester	0 of 1	still valid for 18 days
4	OpenScape Business	OpenScape Business Application Launcher	0 of 500	still valid for 18 days
5	OpenScape Business	OpenScape Business Attendant	0 of 8	still valid for 18 days
6	OpenScape Business	OpenScape Business Base	1 of 1	still valid for 18 days
7	OpenScape Business	OpenScape Business BLF	0 of 50	still valid for 18 days
8	OpenScape Business	OpenScape Business Company Autoattendant	1 of 1	still valid for 18 days
9	OpenScape Business	OpenScape Business Conference	3 of 1500	still valid for 18 days
10	OpenScape Business	OpenScape Business Contact Center E-Mail	0 of 1	still valid for 18 days
11	OpenScape Business	OpenScape Business Contact Center Fax	0 of 1	still valid for 18 days
12	OpenScape Business	OpenScape Business Fax	4 of 1500	still valid for 18 days
13	OpenScape Business	OpenScape Business Groupware User	5 of 1500	still valid for 18 days
14	OpenScape Business	OpenScape Business Info Ready for V3 SW	1 of 1	still valid for 18 days

8.5.2.2 Cómo mostrar las licencias vinculadas a un nodo

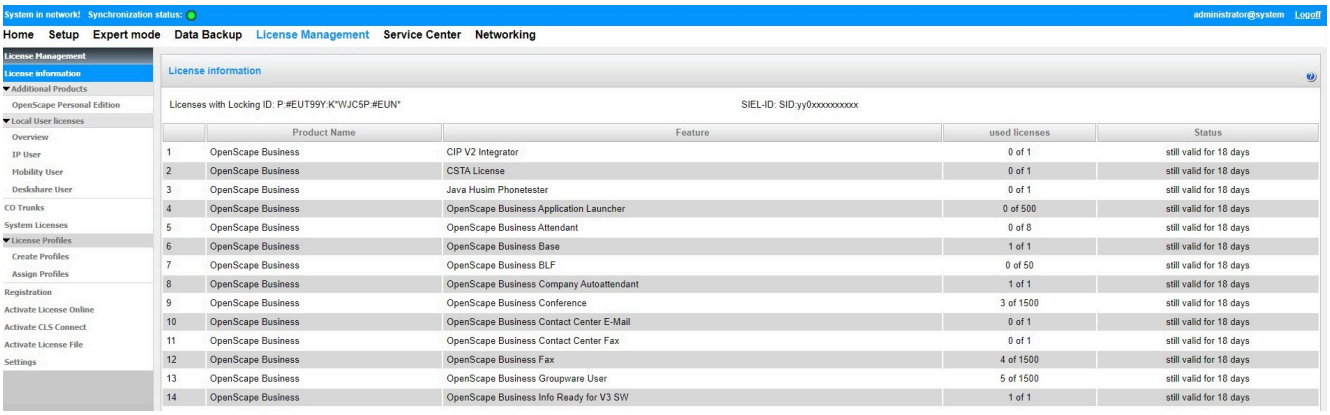
Requisitos previos

El sistema de comunicación se encuentra en una interred.

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Información de licencia**.
3) En el árbol de navegación, haga clic en el nombre del sistema o en el ID de bloqueo del nodo deseado. Se muestran las licencias vinculadas específicamente a ese nodo (p. ej., la licencia básica).



	Product Name	Feature	used licenses	Status
1	OpenScape Business	CIP V2 Integrator	0 of 1	still valid for 18 days
2	OpenScape Business	CSTA License	0 of 1	still valid for 18 days
3	OpenScape Business	Java Husim Phonetester	0 of 1	still valid for 18 days
4	OpenScape Business	OpenScape Business Application Launcher	0 of 500	still valid for 18 days
5	OpenScape Business	OpenScape Business Attendant	0 of 8	still valid for 18 days
6	OpenScape Business	OpenScape Business Base	1 of 1	still valid for 18 days
7	OpenScape Business	OpenScape Business BLF	0 of 50	still valid for 18 days
8	OpenScape Business	OpenScape Business Company Autoattendant	1 of 1	still valid for 18 days
9	OpenScape Business	OpenScape Business Conference	3 of 1500	still valid for 18 days
10	OpenScape Business	OpenScape Business Contact Center E-Mail	0 of 1	still valid for 18 days
11	OpenScape Business	OpenScape Business Contact Center Fax	0 of 1	still valid for 18 days
12	OpenScape Business	OpenScape Business Fax	4 of 1500	still valid for 18 days
13	OpenScape Business	OpenScape Business Groupware User	5 of 1500	still valid for 18 days
14	OpenScape Business	OpenScape Business Info Ready for V3 SW	1 of 1	still valid for 18 days

8.5.2.3 Cómo mostrar todas las licencias en uso común de la interred

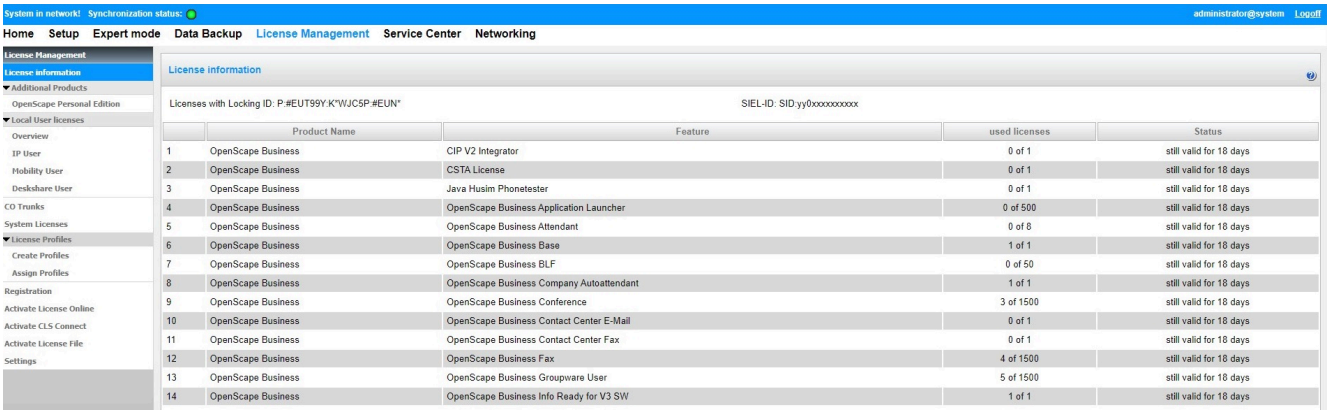
Requisitos previos

El sistema de comunicación se encuentra en una interred.

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Información de licencia**.
3) En el árbol de navegación, haga clic en **Floating**. Se muestran todas las licencias con uso común de la interred.



	Product Name	Feature	used licenses	Status
1	OpenScape Business	CIP V2 Integrator	0 of 1	still valid for 18 days
2	OpenScape Business	CSTA License	0 of 1	still valid for 18 days
3	OpenScape Business	Java Husim Phonetester	0 of 1	still valid for 18 days
4	OpenScape Business	OpenScape Business Application Launcher	0 of 500	still valid for 18 days
5	OpenScape Business	OpenScape Business Attendant	0 of 8	still valid for 18 days
6	OpenScape Business	OpenScape Business Base	1 of 1	still valid for 18 days
7	OpenScape Business	OpenScape Business BLF	0 of 50	still valid for 18 days
8	OpenScape Business	OpenScape Business Company Autoattendant	1 of 1	still valid for 18 days
9	OpenScape Business	OpenScape Business Conference	3 of 1500	still valid for 18 days
10	OpenScape Business	OpenScape Business Contact Center E-Mail	0 of 1	still valid for 18 days
11	OpenScape Business	OpenScape Business Contact Center Fax	0 of 1	still valid for 18 days
12	OpenScape Business	OpenScape Business Fax	4 of 1500	still valid for 18 days
13	OpenScape Business	OpenScape Business Groupware User	5 of 1500	still valid for 18 days
14	OpenScape Business	OpenScape Business Info Ready for V3 SW	1 of 1	still valid for 18 days

8.5.2.4 Cómo mostrar licencias orientadas a usuarios (User) o de extensión por nodos

Requisitos previos

El sistema de comunicación se encuentra en una interred.

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Resumen de licencia a nivel de red**. Se muestran todas las licencias de extensión y las licencias orientadas a usuarios (User) de la interred ordenadas por nodos.

8.6 Asignación de perfiles de licencia

Los perfiles de licencia incluyen asignaciones de licencia predefinidas y se pueden asignar a una o varias extensiones. Los perfiles de sistema son muy útiles si hay que dar a varias extensiones las mismas licencias.

Se pueden utilizar perfiles de licencia predefinidos o crear nuevos perfiles.

Un perfil de licencia siempre es válido para un tipo de extensión y solo se puede asignar a extensiones de ese tipo. Se pueden crear y nombrar varios perfiles de licencia para un tipo de extensión.

Se pueden crear perfiles de licencia para estos tipos de extensiones:

- Extensiones IP (teléfonos IP del sistema, teléfonos SIP)
- Extensiones TDM (teléfonos UP0, teléfonos RDSI, teléfonos analógicos, teléfonos DECT)
- Extensiones DeskSharing
- Extensiones móviles

En un perfil de licencia se pueden asignar licencias orientadas a usuario (User) al tipo de extensión correspondiente.

Si se modifica la asignación de licencia de una extensión del perfil de licencia por separado, la asignación de la extensión al perfil de licencia se cancela automáticamente.

8.6.1 Cómo añadir un perfil de licencia

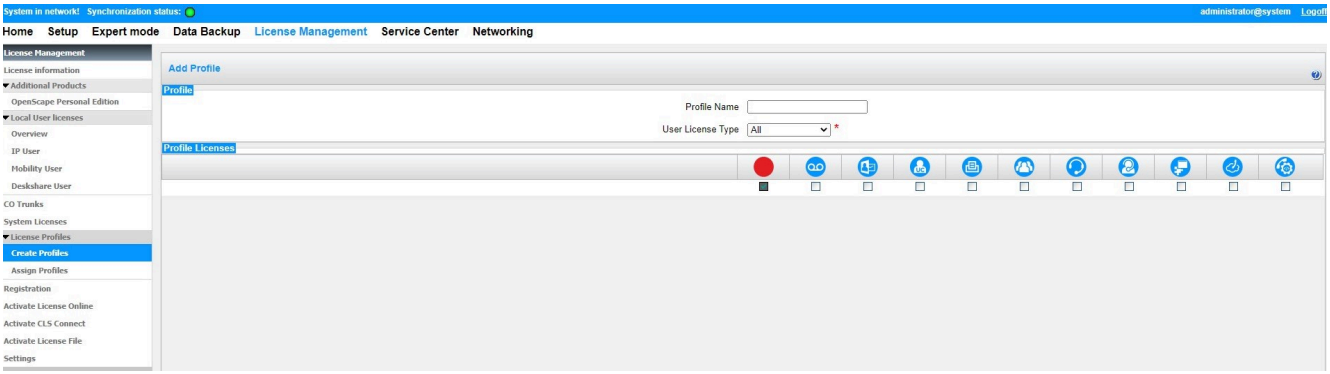
Cree un nuevo perfil de licencia.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) Haga clic en el árbol de navegación en **Perfiles de licencia** > **Crear perfiles**. Se muestran todos los perfiles de licencia existentes.
3) Haga clic en **Agregar**.



4) En el campo **Nombre perfil** introduzca un nombre de su elección para el nuevo perfil.
5) En la lista desplegable **Tipo de licencia del usuario**, seleccione el tipo de extensión al que desea aplicar el perfil.
6) Seleccione las licencias basadas en usuarios (User). Para ello, active las casillas de verificación deseadas.
7) Haga clic en **OK y Continuar**. Se comprueba que la asignación es correcta.

   Si la asignación es correcta, finaliza el registro de licencia de las extensiones.
8) Si la asignación es errónea, los errores se indican con casillas de verificación en color rojo. Corrija estos errores y repita el paso 7.

8.6.2 Cómo modificar un perfil de licencia

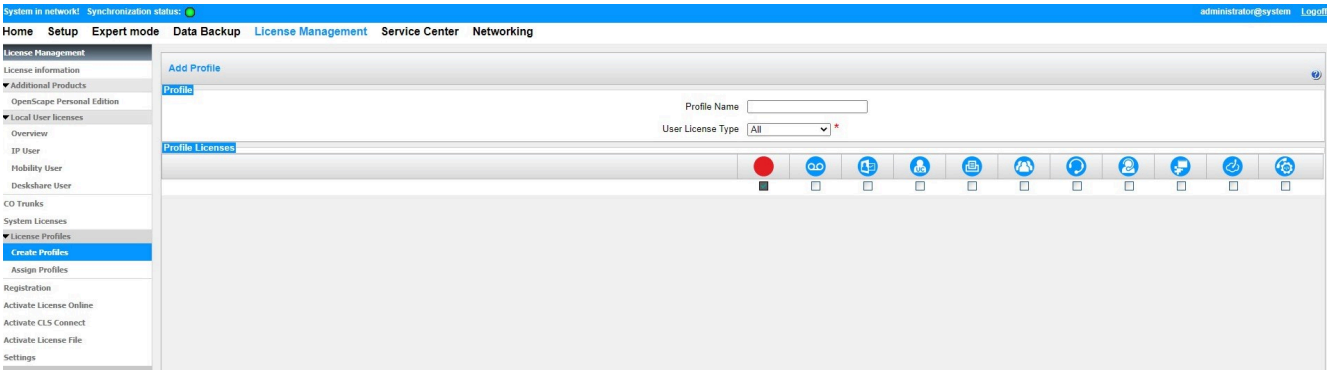
Edite un perfil de licencia existente.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) Haga clic en el árbol de navegación en **Perfiles de licencia** > **Crear perfiles**. Se muestran todos los perfiles de licencia existentes.



3) Active el campo de opción que hay delante del perfil de licencia deseado y haga clic en **Editar**.
4) Modifique el perfil de licencia como desee.
5) Haga clic en **OK y Continuar**. Se comprueba que la asignación es correcta.

   Si lo es, finaliza la edición del perfil de licencia.
6) Si la asignación es errónea, los errores se indican con casillas de verificación en color rojo. Corrija estos errores y repita el paso 5.

8.6.3 Cómo asignar un perfil de licencia a extensiones

Asigne un perfil de licencia a las extensiones disponibles.

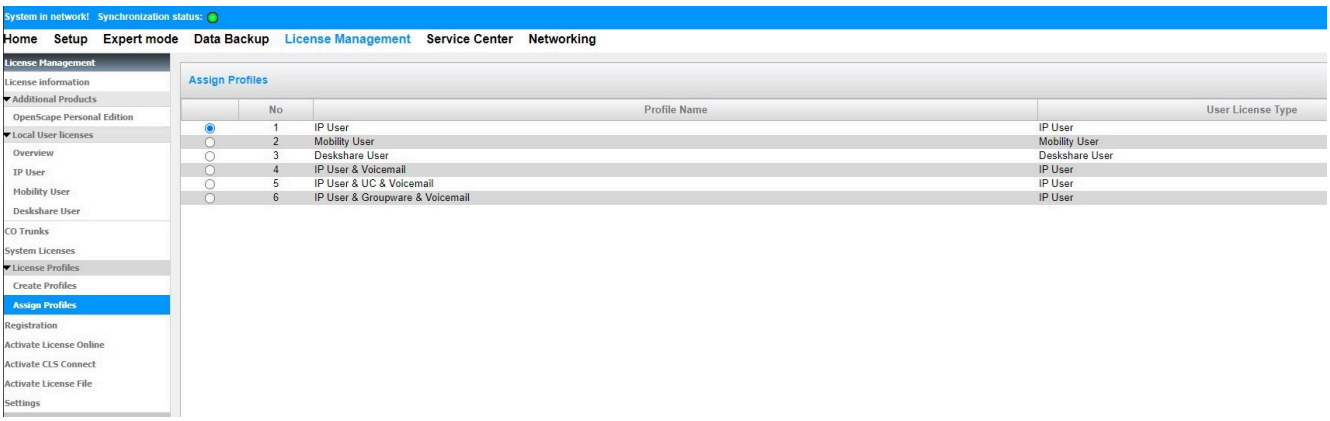
Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.

2) Haga clic en el árbol de navegación en **Perfiles de licencia** > **Asignar perfiles**. Se muestran todos los perfiles de licencia existentes.



3) Active el campo de opción que aparece delante del perfil de licencia deseado y haga clic en **OK & Continuar**.
4) En el campo **Selección** de la izquierda, marque todas las extensiones a las que desea asignar el perfil de licencia.
5) Haga clic en **Agregar**. Las extensiones seleccionadas aparecen en la ventana **Miembros** de la derecha.
6) Haga clic en **OK y Continuar**. Las licencias seleccionadas en el perfil de licencia se asignan a las extensiones.

Nota: En "Pago por uso", aparece una ventana emergente. Haga clic en **OK** para confirmar la selección.

Nota: Después también se pueden eliminar extensiones de un perfil de licencia o añadir otras nuevas.

8.6.4 Cómo borrar un perfil de licencia

Borre un perfil de licencia existente.

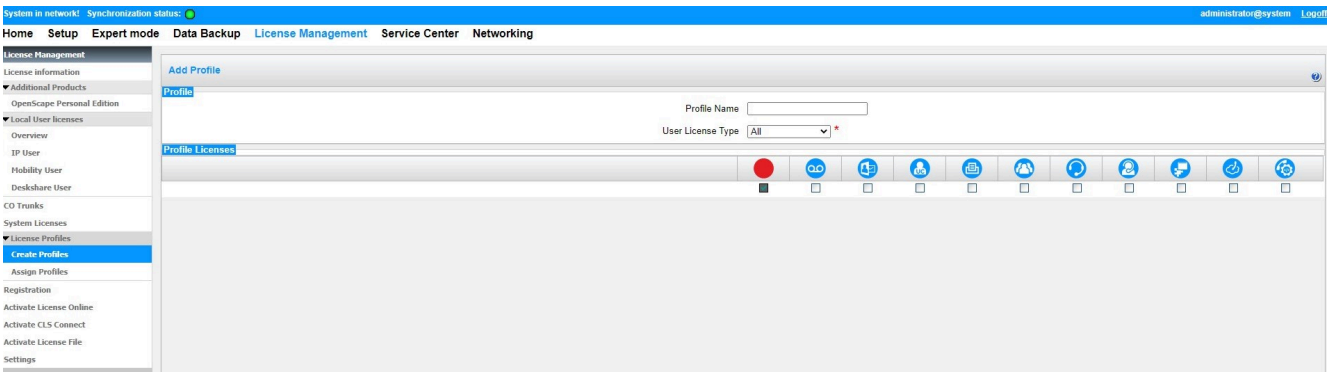
Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.

2) Haga clic en el árbol de navegación en **Perfiles de licencia** > **Crear perfiles**. Se muestran todos los perfiles de licencia existentes.



3) Active el campo de opción que aparece delante del perfil de licencia deseado y haga clic en **Borrar**.
4) Confirme la advertencia con **Aceptar**. El perfil de licencia se borra.

8.7 Rehost tras intercambio de hardware

Hay que actualizar las licencias cuando hay que reemplazar la placa base de la plataforma de hardware o la plataforma de red del servidor Linux en el sistema de comunicación. Para el rehost se necesitan la dirección MAC del hardware anterior, la dirección MAC del hardware nuevo y los datos de inicio de sesión para el servidor central de licencias (CLS).

Después de sustituir el hardware se deben restablecer los datos de configuración mediante el conjunto de copias de seguridad actual (véase Recuperación).

Las licencias están vinculadas a la dirección MAC del hardware, de esta forma, al cambiar el hardware se modifica la dirección MAC y las licencias dejan de ser válidas. Después del intercambio de hardware, el sistema de comunicación vuelve a estar en el periodo de activación. Después de registrar la dirección MAC antigua y la nueva en el CLS se puede generar un nuevo archivo de licencia. El proceso de actualización offline carga este archivo en el sistema de comunicación y, a continuación, todas las licencias disponibles se activan automáticamente.

Para el softswitch se utiliza la dirección MAC de la tarjeta de red del servidor Linux seleccionado en la instalación del sistema operativo Linux (se puede ver mediante YaST). La dirección MAC también se puede consultar mediante WBM.

Nota: Todos los rehosts se registran en el CLS. Una licencia se puede utilizar un máximo de tres veces para un rehost.

Nota: La dirección IP del CLS se puede consultar mediante la Gestión basada en Web (WBM), en **Administración de licencias** > **Configuración** y se puede modificar en caso necesario.

8.7.1 Cómo ejecutar un Rehost después de sustituir el hardware

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Se ha cambiado el hardware ha realizado un Rehost en el CLS (servidor central de licencias).

Los datos de configuración se han restablecido con ayuda del conjunto de copias de seguridad actual.

Conoce el código de activación de licencia (LAC) para la activación de licencia.

Para la conexión con el servidor de licencias, el sistema de comunicación debe tener una conexión con Internet.

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Activar licencia online**.
3) En el campo **Código de autorización de licencia (LAC)** indique el LAC.
4) Deje desactivada la casilla de verificación para el acceso al servidor de licencias con nombre de usuario y contraseña. Se accede automáticamente al servidor de licencias. (Solo necesitan introducir su nombre de usuario y contraseña los representantes comerciales).
5) Haga clic en **Activar**. Se establece conexión con el servidor de licencias y se actualizan las licencias. Una vez terminada la actualización, la conexión se restablece automáticamente.
6) Reinicie el sistema de comunicación.

Pasos siguientes

Guarde los datos de configuración en un nuevo conjunto de copias de seguridad (véase Almacenamiento inmediato).

8.8 Servidor de licencias (Central License Server, CLS)

El servidor de licencias (CLS) genera y administra los archivos de licencia.

Se genera un archivo licencia cuando el cliente envía el código de autorización de licencia al CLS mediante la Gestión basada en Web (WBM). El archivo de licencia se transmite automáticamente al sistema de comunicación por Internet. Si no se puede hacer una transmisión automática, el archivo de licencia también se puede cargar manualmente en el sistema de comunicación.

8.8.1 Cómo consultar o modificar la dirección IP del servidor de licencias

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Si se ha modificado la dirección IP del servidor central de licencias, hay que asignar la dirección IP actual.

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Configuración**. En el campo **Dirección IP del servidor central de licencias** se muestra la dirección IP del servidor de licencias central (CLS). La dirección IP válida actualmente es `188.64.16.4`.
3) Si hay que modificar la dirección IP del servidor central de licencias, en el campo **Dirección IP del servidor central de licencias** indique la nueva dirección IP del servidor central de licencias con el formato `123.124.125.126`.
4) Haga clic en **Activar**.

8.8.2 Cómo comprobar la conexión de Central License Server (CLS)

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Configuración**.
3) En el área **Central License Server**, haga clic en **Probar conexión de CLS**.

Si hay conexión a Internet, se muestra el mensaje **Conexión correcta con CLS**.

Si no hay conexión a Internet, se muestra el mensaje **No hay conexión con CLS**.

8.9 Agente de licencias (Customer License Agent, CLA)

El Agente de licencias (CLA) es parte del software de comunicación OpenScape Business y se ejecuta automáticamente en segundo plano. Administra el archivo de licencia y las licencias incluidas en él. El CLA comprueba las solicitudes de licencia y si hay suficientes licencias disponibles, las libera. Por cada sistema de comunicación solo hay un CLA (CLA local). Si hay varios sistemas de comunicación (nodos) en una interred, solo hay que utilizar un CLA (CLA central) en el nodo maestro.

Estas son las configuraciones posibles:

- **Cómo configurar la conexión con el agente de licencias local**

  Si se retira un nodo de la interred, se debe cancelar la conexión con el CLA central. Se utiliza automáticamente el CLA local instalado en el nodo. Si no funciona este mecanismo automático, la conexión con el CLA local se puede establecer también manualmente.
- **Cómo modificar la conexión con el agente de licencias central**

  Cada nodo de la interred requiere la conexión con el CLA central en el nodo maestro. Esta conexión se establece automáticamente al ejecutar el asistente **Interconexión** de la Gestión basada en Web (WBM). Si se modifica la dirección IP del nodo maestro, hay que configurar de nuevo la conexión con el CLA central en todos los nodos esclavos.

8.9.1 Cómo configurar la conexión con el agente de licencias local

Requisitos previos

Se ha registrado en del nodo deseado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Configuración**.
3) Active el campo de opción **Agente de licencia local (CLA)**.
4) Haga clic en **Activar**.

8.9.2 Cómo modificar la conexión con el agente de licencias central

Requisitos previos

El sistema de comunicación se encuentra en una interred.

Se ha registrado en del nodo deseado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Administración de licencias**.
2) En el árbol de navegación, haga clic en **Configuración**.
3) Active el campo de opción **Agente de licencia central** y en **Dirección IP del agente de licencia central** introduzca la dirección IP del nodo maestro (nodo 1) con el formato `123.124.125.126`.
4) Haga clic en **Activar**.

8.10 ID de bloqueo e ID de bloqueo avanzado

Cada sistema de comunicación tiene asignado un ID de bloqueo (Locking ID) o un ID de bloqueo avanzado (Advanced Locking ID). Para garantizar un registro de licencia inequívoco, las licencias se vinculan con estos ID de bloqueo.

ID de bloqueo

En las plataformas de hardware, el ID de bloqueo es la dirección MAC del sistema de comunicación.

En un softswitch, el ID de bloqueo es la dirección MAC de la tarjeta de red del servidor Linux. Si el servidor Linux incluye varias tarjetas de red, hay que seleccionar la tarjeta de red que se haya utilizado en la puesta de servicio inicial del servidor Linux.

Si el sistema de comunicación se encuentra en el periodo de gracia, en la información de licencia puede aparecer una dirección MAC errónea. La dirección MAC correcta se puede consultar a través del **Centro de servicios**, en **Inventario**.

ID de bloqueo avanzado

Si un softswitch opera en un entorno virtual, en lugar del ID de bloqueo se utiliza el ID de bloqueo avanzado (Advanced Locking ID o ALI). El ID de bloqueo avanzado se genera en el CLS mediante el ALI-Calculator.

Los siguientes parámetros de sistema y de red deben estar configurados, ya que se utilizan para generar el ID de bloqueo avanzado de 24 caracteres:

- Dirección IP del gateway estándar (servidor Linux)
- Nombre host del servidor Linux
- Dirección IP del servidor Linux
- Dirección IP del servidor DNS (con figurado en el servidor Linux)
- Zona horaria (servidor Linux)

Si no se han configurado uno o varios de estos parámetros de red y de sistema, no se puede generar el ID de bloqueo avanzado.

El ID de bloqueo avanzado se muestra en la Gestión basada en Web (WBM). En algunos casos es posible que el ALI generado en el CLS para el archivo de licencia no coincida con el que aparece en la Gestión basada en Web (WBM) durante el periodo de activación. Aun así, el sistema acepta el archivo de licencia con el ALI diferente.

Si cambia uno de los parámetros de red o de sistema detallados arriba, el softswitch regresa al estado sin licencia y se genera un nuevo ID de bloqueo avanzado. Para poder volver a utilizar el archivo de licencia adquirido, en el servidor de licencias central (CLS) ha de hacerse un realojamiento del antiguo al nuevo ID de bloqueo avanzado.

Si el sistema detecta un cambio en ALI, aparecerá un mensaje en el área de licencias de la página de inicio de la WBM, para informar al usuario. El usuario tiene que hacer clic en Confirmar, para confirmar que conoce el cambio. A continuación, el mensaje se borrará de la página de inicio de la WBM hasta que se detecte otro cambio de ALI. Si el usuario no hace clic en Confirmar, el mensaje seguirá apareciendo en la página de inicio.

Importante: Si se efectúa un cambio en los parámetros de ID de bloqueo (dirección IP, dirección de gateway, dirección DNS, nombre de host de sistemas S, dirección MAC de sistemas X), la licencia del sistema deja de ser válida. Debe comunicarse con un socio autorizado del servidor de licencias central para generar un nuevo archivo de licencia y el nuevo archivo de licencia debe instalarse en el sistema.

Importante: Si un usuario pulsa el botón Confirmar, no se enviará después un mensaje de correo electrónico. Solo se enviará un correo electrónico si el usuario no ha confirmado los cambios en la página de inicio. El mecanismo de envío de correos electrónicos se activa cada 24 horas, a partir del último reinicio del sistema.

8.10.1 Cómo consultar el ID de bloqueo del sistema de comunicación

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Inventario**. Aparece una vista general de los componentes del sistema de comunicación.
3) Haga clic en **OK & Continuar**. Aparece información sobre el hardware y el software. En **MACID para la licencia** encontrará el ID de bloqueo del sistema de comunicación.

8.10.2 Cómo consultar el ID de bloqueo del softswitch

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Inventario**. Se muestra información sobre el software del softswitch, sobre el espacio libre y ocupado de los discos duros y sobre el estado de la aplicación. En **MACID para la licencia** encontrará el ID de bloqueo del softswitch.

8.10.3 Cómo consultar el ID de bloqueo avanzado del softswitch

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

En la barra de navegación, haga clic en **Administración de licencias**. Se muestran todas las licencias disponibles. En **Locking ID** (ID de bloqueo) puede consultar el Advanced Locking ID (ID de bloqueo avanzado) del softswitch si este opera en un entorno virtualizado.

8.11 Cómo migrar de Placa base V2 a Placa base V3 (sistema autónomo)

Requisitos previos

- Actualice a la última versión del sistema.
- Desenchufe las tarjetas IVM, limpie los slots de tarjetas y retire la configuración IVM del sistema.

- Compruebe que los puertos del intervalo 511-532 no estén configurados. Estos puertos serán reservados por SmartVM en la placa base V3. Solo es necesario para sistemas que operan en modo UC Smart.

  Para solucionar los problemas con la funcionalidad de UC Fax durante la migración al sistema de placa base V3, se recomienda configurar el modo de funcionamiento del sistema antes de la migración. Si el sistema funciona en modo UC Smart, el administrador debe eliminar la configuración de los puertos 511-532 antes de que se realice la migración. Si el sistema funciona en modo UC Suite, los puertos SmartVM adicionales no se crearán y la configuración del fax no se verá afectada. Por ejemplo, si el juego de copia de seguridad procede de un sistema UC Suite, el modo de funcionamiento del sistema de la placa base V3 debe cambiarse al modo UC Suite antes de migrar el juego de copia de seguridad.

  Nota: Cuando actualiza un sistema OpenScape Business PAYGO (de pago por uso), en primer lugar debe actualizar el sistema OpenScape Business al software V3 y después, utilizar la función **regenerar clave de licencia** de CLS para conseguir un archivo de licencia válido para V3, que a su vez contendrá la licencia "OpenScape Business Info Ready for V3 SW F31505-K158-D129". A continuación, es preciso activar manualmente el archivo de licencia regenerado, lo cual se hace en el apartado de Gestión basada en Web (WBM) de OpenScape Business System, en la sección **Administración de licencias**.

Nota: Cuando actualiza un sistema OpenScape Business PAYGO (de pago por uso), en primer lugar debe actualizar el sistema OpenScape Business al software V3 y después, utilizar la función **regenerar clave de licencia** de CLS para conseguir un archivo de licencia válido para V3, que a su vez contendrá la licencia "OpenScape Business Info Ready for V3 SW F31505-K158-D129". A continuación, es preciso activar manualmente el archivo de licencia regenerado, lo cual se hace en el apartado de Gestión basada en Web (WBM) de OpenScape Business System, en la sección **Administración de licencias**.

Paso a paso

1) Active el modo de servicio apropiado del sistema.

No es posible utilizar una copia de seguridad del sistema realizada en un modo de funcionamiento para otro modo. Por ejemplo, si realiza una copia de seguridad del sistema en modo UC Suite, antes de restablecer la copia

de seguridad, tendrá que configurar el sistema actualizado en UC Suite. No es posible restablecer esa copia de seguridad en el modo UC Smart.

El sistema Placa base V3 funciona en modo UC Smart:

Los puertos de Smart VM adicionales se crearán como hoy, el administrador debe eliminar la configuración del rango de puertos mencionado anteriormente en el sistema OCC antes de que se lleve a cabo la migración.

El sistema Placa base V3 está funcionando en modo UC Suite:

Los puertos SmartVM adicionales no se crearán, por lo que la configuración del fax no se verá afectada.

2) Active la licencia del sistema.

CLS Connect	Acción
Activado	Regenere la licencia para la dirección MAC de V3 en CLS.
No activado	Importe la nueva licencia y actívela en el sistema OpenScape Business V2. Se activará la solicitud del código de confirmación, que mostrará el código de confirmación en la página de inicio de la Gestión basada en Web, WBM.

3) Haga una copia de seguridad del sistema V2, incluida la configuración del sistema.

Si la placa OCC está conectada con un servidor Booster Server, será preciso descargar y guardar un conjunto de copias de seguridad completo de Booster Server.

4) Cambie la placa base.

5) Importar la nueva licencia

CLS Connect	Acción
Activado	Importe el archivo de licencia V3 desde CLS a OpenScape Business y se activará **CLS Connect** en la Placa base V3.
No activado	Genere una nueva licencia V3 con la ayuda del código de confirmación en CLS, con la dirección MAC de Placa base V3. A continuación, importe el nuevo archivo de licencia V3 a OpenScape Business.

6) Restablezca la copia de seguridad de V2 en la Placa base V3.

7) Cambie la configuración de dirección IP de los clientes de UC.

Cuando se establezca la primera conexión de clientes de UC tras la migración, utilice la nueva dirección IP en la Placa base V3.

Solo el modo Fullduplex es compatible con la Placa base V3.

Los dispositivos OptiPoint 4xx/5xx ya no son compatibles con la Placa base V3.

8.12 Cómo migrar de Placa base V2 a Placa base V3 como nodo maestro de un sistema conectado en red

Requisitos previos

El sistema tiene una licencia de red.

Paso a paso

1) Se actualizan todos los nodos esclavos de OpenScape Business a V3.

Escenario	Procedimiento que se debe seguir
Actualización con CLS Connect	Actualización de V2 a V3 con CLS Connect en la página 354
Actualización sin CLS Connect	Actualización de V2 a V3 sin CLS Connect en la página 354

2) Migre el nodo maestro del sistema.

Siga las instrucciones de Cómo migrar de Placa base V2 a Placa base V3 (sistema autónomo) en la página 350

Mientras no concluya la migración del nodo maestro, los nodos esclavos se mantendrán en modo de conmutación por error. Volverán a ser plenamente funcionales cuando termine la migración del nodo maestro.

8.13 Cómo migrar de Placa base V2 a Placa base V3 el nodo esclavo de un sistema conectado en red

Requisitos previos

El sistema tiene una licencia de red.

Nota: Si CLS Connect no está activado, primero debe eliminar el sistema esclavo de la red en CLS.

Paso a paso

1) Migre el sistema esclavo.

Siga las instrucciones de Cómo migrar de Placa base V2 a Placa base V3 (sistema autónomo) en la página 350

2) Actualice o migre el nodo maestro.

Escenario	Procedimiento que se debe seguir
Migración de la placa base V2 a la V3	Cómo migrar de Placa base V2 a Placa base V3 (sistema autónomo) en la página 350
Actualización de software con CLS Connect	Actualización de V2 a V3 con CLS Connect en la página 354
Actualización de software sin CLS Connect	Actualización de V2 a V3 sin CLS Connect en la página 354

8.14 Migración de sistemas HiPath 3000 al software OSBiz V3 con placa base V3

La migración de software se realiza mediante el proceso normal de migración de HiPath 3000 a OSBiz utilizando la herramienta Manager E. Las licencias existentes de HiPath 3000 ComScendo y S2m se actualizan a la dirección MAC de la placa base OCCe. Las licencias TDM y el indicador de software V3 son generados por el CLS, basándose en la información del archivo XML que se crea desde ManagerE durante este procedimiento.

En el caso de una placa base OCC reutilizada de una migración anterior de OSBiz a OCCe, no es posible la migración de licencias. Es necesario adquirir todas las licencias.

En el caso de un OCC procedente de existencias de piezas de repuesto o recién adquiridas (la dirección MAC no está bloqueada en CLS), es posible actualizar HiPath 3000 a esa dirección MAC y se genera un nuevo archivo de licencia (al igual que con la migración a OSBiz V2).

8.15 Actualización de V2 a V3 con CLS Connect

Es necesario contar con la versión más reciente de V2R7 para actualizar el sistema y **CLS Connect** debe estar activado. Las licencias ya existentes de OpenScape Business V2 que están ligadas a la dirección MAC de la placa base OCC también son válidas para V3.

Tras la actualización del software, en el arranque, el software de OpenScape Business V3 indica en CLS que las licencias funcionan en combinación con software V3. Se añade información de V3 al archivo de licencia y se transfiere automáticamente de vuelta al sistema a través de la conexión de CLS durante el arranque. No es necesario intervenir manualmente de ninguna manera.

En caso de tratarse de una actualización de software sin migración para los sistemas esclavos con una licencia de red, no se requiere ninguna acción. En este caso, los sistemas esclavos se pueden actualizar y sus licencias se actualizarán automáticamente después de la actualización/migración del sistema maestro.

8.16 Actualización de V2 a V3 sin CLS Connect

Requisitos previos

- CLS Connect no está activado
- OpenScape Business S necesita acceso a Internet
- En caso de una actualización de un nodo esclavo en un sistema conectado a red, primero elimine el esclavo de CLS.

Paso a paso

1) Active la licencia de upgrade (actualización) del software en CLS como licencia normal para el sistema OpenScape Business. Activar la licencia de upgrade de software en CLS genera un nuevo archivo de licencia que contiene:

   - La nueva licencia de V3

- El ID del nuevo archivo de licencia (incrementado)
- Si el sistema es OSBiz S, se agrega CLS Connect Start al certificado.

2) Importe este nuevo archivo de licencia al sistema OpenScape Business V2 y actívelo.

3) Ejecute la actualización o upgrade de software de V2 a V3.

Durante el arranque, tras la actualización del software a V3, el sistema OpenScape Business comprueba el archivo de licencia y permite la funcionalidad de licencia solamente si el componente de licencia de V3 está disponible en dicho archivo de licencia.

9 Integración en la red de datos interna (LAN)

La integración del sistema de comunicación en la red de datos interna (LAN) permite usar las soluciones UC y la administración del sistema de comunicación con los PC de la red interna.

Hay que configurar los siguientes parámetros de red en la Gestión basada en Web (WBM):

- Plataforma de hardware OpenScape Business X: dirección IP y máscara de red de la placa principal y de la tarjeta UC Booster Card (si la hay). Estos ajustes se realizan durante la instalación inicial, pero se pueden modificar más adelante.

  Softswitch OpenScape Business S: dirección IP y máscara de red del servidor Linux en el que se ejecuta el software de comunicación. Estos ajustes se realizan durante la instalación Linux, pero también se pueden modificar más adelante.
- De forma opcional, el sistema de comunicación se puede configurar como servidor DHCP (con suministro de parámetros específicos de red como máscara de red, gateway estándar, servidor DNS) o como agente DHCP Relay. La configuración como servidor DHCP se realiza durante la instalación inicial, pero se puede modificar más adelante. La configuración como agente DHCP Relay se realiza a través del Modo Experto.
- Dirección IP del router estándar y del servidor DNS (externo) para acceder a otras redes IP (p. ej. Internet). Estos ajustes se realizan durante la instalación inicial, pero se pueden modificar más adelante.

9.1 Interfaz LAN

Para integrar el sistema de comunicación en la infraestructura LAN, las direcciones IP y el área de direcciones IP interna del sistema de comunicación se deben ajustar al esquema de direcciones IP de la red interna (LAN).

9.1.1 Dirección IP y máscara de red de la interfaz LAN

La Dirección IP y la máscara de red del sistema de comunicación se definen en la instalación inicial, pero también se pueden modificar a posteriori. En ocasiones hay que ajustar la dirección IP o la máscara de red al rango de direcciones IP de la LAN.

Plataforma de hardware

De forma predeterminada la plataforma de hardware tienen asignada una dirección IP y una máscara de subred. La UC Booster Card también necesita una dirección IP. Esté insertada o no la UC Booster Card, se puede configurar su dirección IP.

Para integrarse en la LAN, la plataforma de hardware utiliza la interfaz "LAN" de la placa base. Si la UC Booster Card está insertada hay que conectar además la interfaz "LAN" de la UC Booster Card con la LAN. La plataforma de hardware y la UC Booster Card deben estar en la misma subred.

Para activar los cambios de la dirección IP o de la máscara de red hay que reiniciar la plataforma de hardware.

Los cambios realizados en la dirección IP y en la máscara de red se mantienen al actualizar el software, pero se restablecen al volver a cargar la plataforma de hardware con los valores estándares. Estos cambios no se pueden guardar en un conjunto de copias de seguridad.

Softswitch

Con el softswitch, el servidor Linux en el que se ejecuta el software de comunicación se puede integrar en la LAN con su tarjeta de red.

Los cambios de la dirección IP o de la máscara de red se activan después de reiniciar la aplicación (véase Restart, Reload, Shutdown).

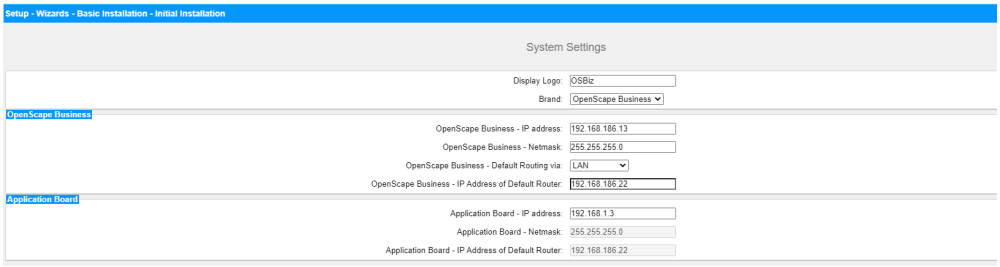
9.1.1.1 Cómo modificar la dirección IP y la dirección de red de la plataforma de hardware

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) Haga clic en **Editar** para iniciar el asistente **Instalación inicial**.



3) En **OpenScape Business - Dirección IP**, modifique la dirección IP de la plataforma de hardware. La dirección IP debe coincidir con el esquema de direcciones IP de la red interne y no puede estar asignada a ningún cliente de red existente, ya que, de lo contrario, se produciría un conflicto de direcciones IP. De forma predeterminada, hay que introducir la dirección IP `192.168.1.2`.
4) En **OpenScape Business - Máscara de red**, modifique la máscara de red de la plataforma de hardware. La máscara de red debe coincidir con el esquema de direcciones IP de la red interna. De forma predeterminada, hay que introducir la máscara de subred `255.255.255.0`.
5) Haga clic en **OK & Continuar**.
6) Haga clic varias veces en **OK & Continuar** hasta que aparezca un mensaje avisando de que la prestación ha sido configurada.
7) Haga clic en **Salir**. La plataforma de hardware se reinicia automáticamente.

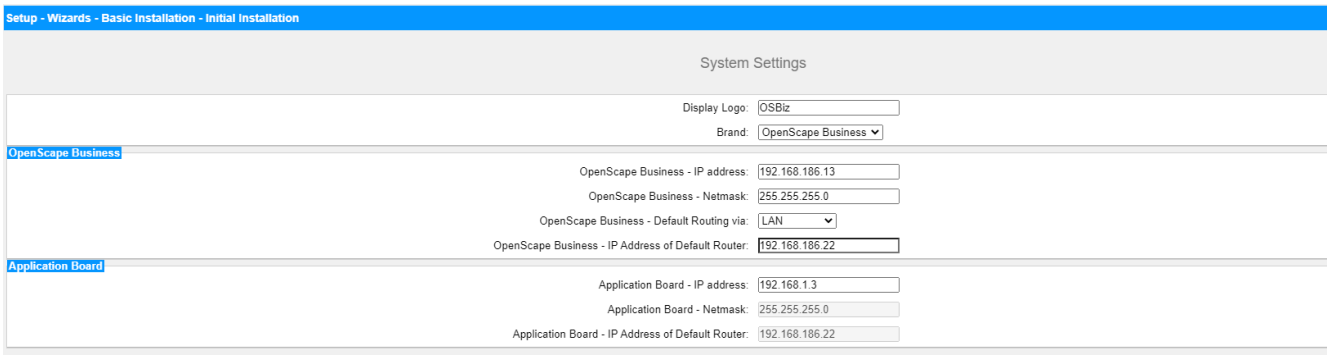
9.1.1.2 Cómo modificar la dirección IP de la UC Booster Card

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) Haga clic en **Editar** para iniciar el asistente **Instalación inicial**.



3) En **UC Booster Card - Dirección IP** modifique la dirección IP de la UC Booster Card. La dirección IP debe coincidir con el esquema de direcciones IP de la red interne y no puede estar asignada a ningún cliente de red existente, ya que, de lo contrario, se produciría un conflicto de direcciones IP. De forma predeterminada, está registrada la dirección IP `192.168.1.3`.
4) Haga clic en **OK y Continuar**.
5) Haga clic varias veces en **OK & Continuar** hasta que aparezca un mensaje avisando de que la prestación ha sido configurada.
6) Haga clic en **Finalizar**. La plataforma de hardware se reinicia automáticamente.

9.1.1.3 Cómo modificar la dirección IP y la máscara de red del softswitch

Paso a paso

1) En la barra de tareas, haga clic en **Computer** (Equipo).
2) En el grupo de menús, haga clic en **System** > **YaST** (Sistema > YaST).
3) Introduzca la contraseña del usuario "root" y haga clic en **Continue** (Continuar). Se abre el YaST Control Center.
4) En el grupo de menús, haga clic en **Network Devices** (Dispositivos de red).
5) En el área **Network Devices**, haga clic en **Network Settings** (Configuración de red).
6) En la ventana **Overview** (Vista general), seleccione la tarjeta de red deseada y haga clic en **Edit** (Editar).
7) Active el campo de opción **Statically assigned IP Address** (Dirección IP asignada estadísticamente).
8) En **IP Address** (Dirección IP) modifique la dirección IP del servidor Linux, en el que se ejecuta el software del softswitch. La dirección IP debe coincidir con el esquema de direcciones IP de la red interne y no puede

estar asignada a ningún cliente de red existente, ya que, de lo contrario, se produciría un conflicto de direcciones IP.

9) En **Subnet Mask** (Máscara de subred), modifique la máscara de subred del servidor Linux. La máscara de subred debe coincidir con el esquema de direcciones IP de la red interna.

10) Haga clic en **Continuar** y, a continuación, en **Aceptar**.

11) Cierre el **YaST Control Center**.

9.1.2 Área de direcciones IP interna de la interfaz LAN

El área de direcciones IP interna de la interfaz LAN que utiliza la plataforma de hardware para la comunicación interna de sus módulos se puede modificar en caso necesario.

La plataforma de hardware utiliza de forma predeterminada el área de direcciones IP interna 192.168.3.xxx. También se puede modificar con el área de direcciones IP deseada. La máscara de subred interna es 255.255.255.0 y no se puede modificar.

Para activar los cambios del área de direcciones IP interna hay que reiniciar la plataforma de hardware.

Los cambios realizados en el área de direcciones IP interna se conservan al hacer una actualización de software, pero al hacer una recarga (Reload) se restablecen a los valores estándar. Estos cambios no se pueden guardar en un conjunto de copias de seguridad.

9.1.2.1 Cómo modificar el área de direcciones IP interna de la plataforma de hardware

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

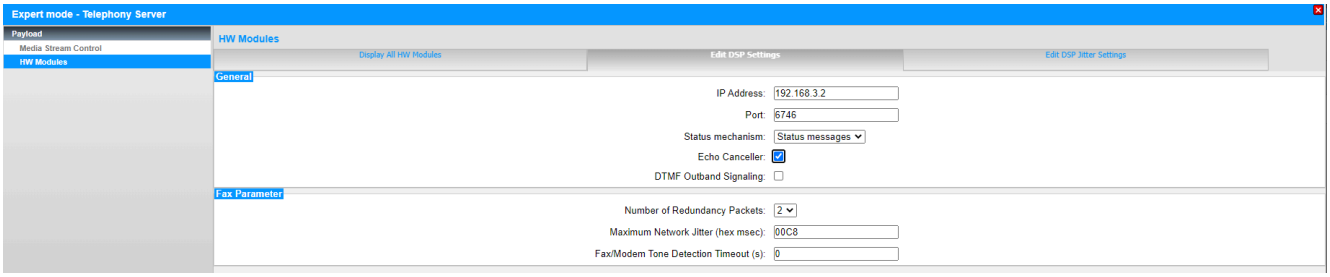
Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Payload**.

3) En el grupo de menús, haga clic en **Módulos de Hardware**.

4) Haga clic en la pestaña **Editar ajustes DSP**.



5) En el área **General**, en **Dirección IP**, introduzca una dirección IP para el sistema de comunicación que esté en el área deseada, por ejemplo, `192.168.40.2`. Toda el área de direcciones IP (en el ejemplo `192.168.40.xxx`) está bloqueada para otros clientes de la LAN.

6) Haga clic en **Aplicar** y confirme con **Aceptar**.

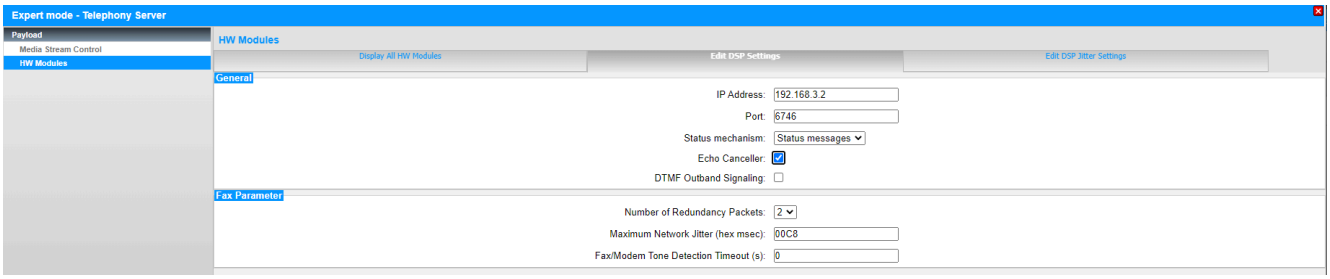
9.1.2.2 Cómo restablecer el área de direcciones IP interna de la plataforma de hardware

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Payload**.
3) En el grupo de menús, haga clic en **Módulos de Hardware**.
4) Haga clic en la pestaña **Editar ajustes DSP**.



5) En el área **General** y en **Dirección IP**, introduzca la dirección IP `192.168.3.2`. Todo el área de direcciones IP (`192.168.3.xxx`) está bloqueada para otros clientes en la LAN.
6) Haga clic en **Aplicar** y confirme con **Aceptar**.

9.2 DHCP

DHCP (Dynamic Host Configuration Protocol) permite la asignación dinámica de datos específicos de red a las extensiones IP de una red (p. ej. LAN) mediante un servidor DHCP.

Mediante DHCP se puede realizar la integración automática de una extensión IP (p. ej., teléfonos IP o PC) en una LAN existente. La extensión IP debe estar configurada para la recepción automática de los datos específicos de la red, lo que la convierte en un cliente DHCP. El servidor DHCP suministra a las extensiones IP los datos específicos de red a demanda.

9.2.1 Agente DHCP Relay

Si se utiliza el servidor DHCP interno de la plataforma de hardware, el servidor DHCP interno y los clientes DHCP tienen que estar en el mismo segmento de red. Si no es así, hay que configurar la plataforma de hardware como agente DHCP Relay. Así, las consultas DHCP de las extensiones IP se transfieren desde la plataforma de hardware al servidor DHCP en sí.

9.2.1.1 Cómo configurar la plataforma de hardware como agente de retransmisión DHCP

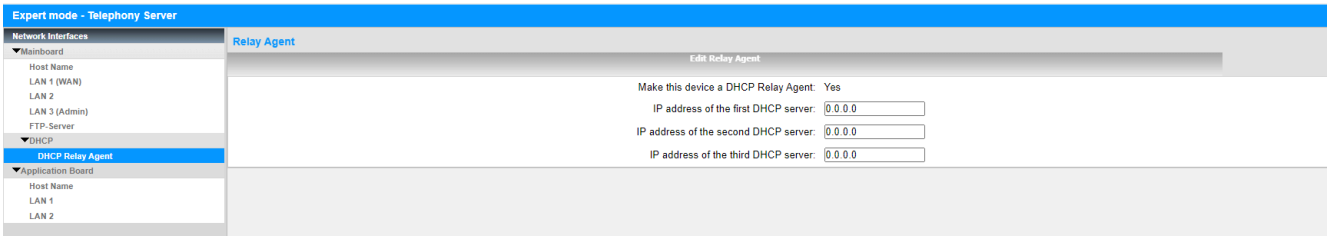
Si la plataforma de hardware está configurada como un agente de retransmisión DHCP, retransmite las solicitudes DHCP al servidor DHCP externo.

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) Haga clic en **Servidor de telefonía** > **Interfaces de red** en el árbol de navegación.
3) Haga clic en **Tablero principal** > **DHCP** en el árbol de menú.
4) Habilite el botón de opción **Agente de retransmisión DHCP.**
5) Haga clic en **Aplicar** y confirme con **OK**.
6) Haga clic en **Agente de retransmisión DHCP** en el árbol de menú.



7) Introduzca la **dirección IP del primer servidor DHCP.**
8) Introduzca la **dirección IP del segundo servidor DHCP.**
9) Introduzca la **dirección IP del tercer servidor DHCP.**

Consejo: Puede ingresar hasta tres servidores DHCP. La entrada del primer servidor DHCP es obligatoria.

10) Haga clic en **Aplicar**, seguido de **Aceptar**.

9.2.2 Servidor DHCP

El servidor DHCP asigna a las extensiones IP (teléfonos IP, teléfonos SIP, PC, puntos de acceso WLAN, etc.) los datos específicos de la red de forma dinámica, por ejemplo: la dirección IP que se debe usar, la máscara de red de la extensión IP, la dirección IP del gateway estándar, la dirección IP del servidor SNTP, etc.

Como servidor DHCP se puede utilizar el servidor DHCP del sistema de comunicación o un servidor DHCP externo (por ejemplo, el servidor DHCP del router Internet).

Con la plataforma de hardware, el servidor DHCP integrado está activado de forma predeterminada. Si se quiere utilizar un servidor DHCP externo hay que desactivar el servidor DHCP interno. De lo contrario se producirán conflictos con el servidor DHCP externo.

En un softswitch, el servidor Linux se puede configurar como servidor DHCP.

En la puesta en servicio inicial hay que decidir si se va a usar el servidor DHCP interno del sistema de comunicación o un servidor DHCP externo. El servidor DHCP interno también se puede activar o desactivar a posteriori. También los datos específicos de red se pueden configurar más tarde.

Servidor DHCP interno

Si se utiliza el servidor DHCP interno, este suministra a las extensiones IP automáticamente los siguientes datos específicos de red:

- Dirección IP y máscara de red de la extensión IP
- Dirección IP del sistema de comunicación (gateway estándar)
- Dirección IP del servidor SNTP (para suministrar fecha y hora)
- Dirección IP del servidor DNS (para la resolución de nombres)
- Dirección IP del servidor SIP (para la autenticación de extensiones SIP)
- Dirección IP del servidor DLS externo o DLI interno (para la actualización de software de los teléfonos IP del sistema)
- Reglas de encaminamiento

Servidor DHCP externo

Si se utiliza un servidor DHCP externo, debe ser compatible con un Vendor Specific Option Space, que permite suministrar parámetros específicos del fabricante. En el servidor DHCP externo hay que introducir los siguientes datos específicos de la red:

- Dirección IP y máscara de red de la extensión IP
- Dirección IP del router predeterminado = Opción 3
- Dirección IP del sistema de comunicación (gateway predeterminado) = Opción 33
- Dirección IP del servidor DNS (para la resolución de nombres = Opción 6
- Dirección IP del servidor DLS externo o DLI interno (para la actualización de software de los teléfonos IP del sistema) = Opción 43
- Solo para teléfonos SIP: dirección IP del servidor SIP (Registrador SIP para la autenticación de extensiones SIP) = Opción 120
- Solo para teléfonos SIP: dirección IP del servidor SNTP (para el suministro de fecha y hora a los teléfonos SIP) = Opción 42

Nota: Puede consultar más información sobre los servidores DHCP en entornos Windows aquí: http://wiki.unify.com/wiki/DHCP_Server_in_a_Windows_environment.

Si no se puede realizar una entrada en el servidor DHCP externo, hay que introducir estos datos directamente en los teléfonos IP del sistema. Solo entonces los teléfonos IP del sistema reciben automáticamente, por ejemplo, la fecha y la hora actuales y la última actualización de software.

Para obtener más información, consulte la siguiente página wiki para expertos en Internet: http://wiki.unify.com/wiki/DHCP

Pool de direcciones DHCP (rango de direcciones IP)

Si una extensión IP se registra en el servidor DHCP recibe asignada, entre otras cosas, una dirección IP dinámica. El administrador puede establecer un área de direcciones IP que utilizará el servidor DHCP para asignar las

direcciones IP a las extensiones IP. Así, por ejemplo, se puede determinar que no se asignen todas las direcciones de la banda 192.168.1.x, sino únicamente las direcciones comprendidas entre 192.168.1.50 y 192.168.1.254, a fin de reservar las direcciones IP por debajo de 192.168.1.49 para extensiones IP con direcciones IP estáticas.

En el Modo Experto (**Interfaces de red**) se pueden configurar incluso varios rangos de direcciones IP para el servidor DHCP interno.

9.2.2.1 Cómo habilitar y configurar el servidor DHCP de la plataforma de hardware

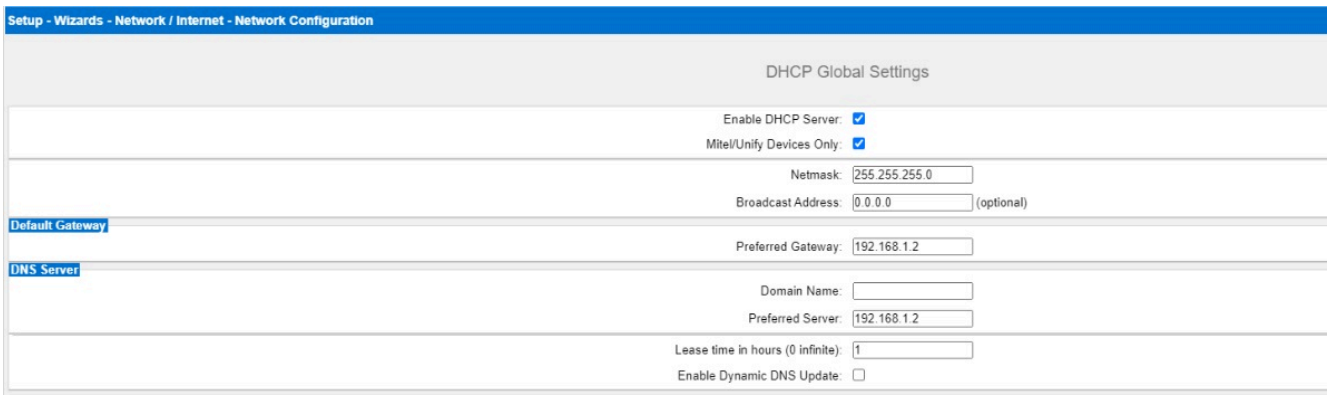
El asistente de **configuración de red** se puede utilizar para habilitar y configurar el servidor DHCP de la plataforma de hardware.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Red/Internet**.
3) Haga clic en **Editar** para iniciar el asistente de **Configuración de red**.



4) Marque la casilla **Habilitar servidor DHCP**.
5) Si es necesario, habilite la casilla de verificación **Solo dispositivos Mitel/ Unify.**

Nota: Esta opción sólo está disponible para placas base V3.

---

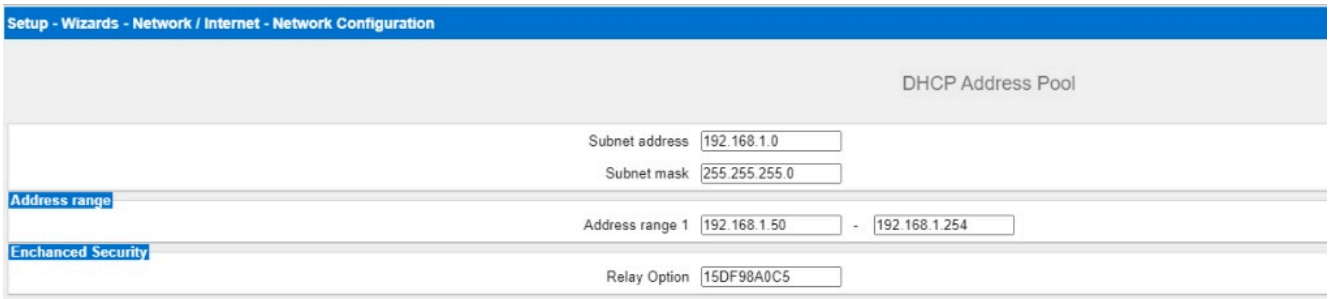
6) Introduzca la máscara de subred de su red en el campo **Máscara de subred** (por ejemplo, `255.255.255.0`).
7) En el campo **Dirección de transmisión**, ingrese la dirección de transmisión (la "última" dirección IP de la red o subred, predeterminada: `0.0.0.0`) si es necesario.
8) En el campo **Gateway preferido**, introduzca la dirección IP del gateway predeterminado. Como regla general, la dirección IP del enrutador de Internet suele ser `192.168.1.1`.
9) Si necesita un nombre de dominio completo para el servidor DHCP, ingréselo en **Nombre de dominio** (máximo 80 caracteres).

10) En el campo **Servidor preferido**, ingrese la dirección IP de un servidor DNS disponible, por ejemplo, la dirección IP del enrutador de Internet, `192.168.1.1`.
11) Si es necesario, ingrese el tiempo máximo de arrendamiento en horas (predeterminado: 1 h, 0 = tiempo de arrendamiento infinito) en el campo **Tiempo de arrendamiento en horas (0 = infinito)**.
12) Si desea permitir actualizaciones dinámicas del servidor DNS, habilite la opción **Habilitar actualización dinámica de DNS** (predeterminado: deshabilitado).

Nota: Si la opción Actualización de DNS dinámico está habilitada, es obligatorio configurar el **Nombre de dominio** en el campo Nombre de dominio correspondiente del Grupo de direcciones IP.

---

13) Haga clic en **Aceptar & Siguiente**. Se muestran las configuraciones para el grupo de direcciones DHCP.



14) En el campo **Dirección de subred**, ingrese la dirección IP más baja de la subred en la que se encuentra el rango de direcciones IP deseado (en nuestro ejemplo, `192.168.1.0`).
15) Introduzca la máscara de subred del rango de direcciones IP deseado en el campo **Máscara de subred** (por ejemplo, `255.255.255.0`).
16) Introduzca el umbral superior e inferior para el rango de direcciones IP deseado en el campo **Rango de direcciones 1** (por ejemplo, `192.168.1.50` a `192.168.1.254`).
17) Si es necesario, especifique el valor del campo **Opción de retransmisión.**

Nota: Esta opción sólo está disponible para placas base V3.

---

18) Haga clic en **Aceptar & Siguiente**. Aparece la ventana **Configuración de enrutamiento.**
19) En el campo **Dirección IP del servidor DNS**, ingrese la dirección IP de un servidor DNS disponible, por ejemplo, la dirección IP del enrutador de Internet, `192.168.1.1`.
20) Seleccione el elemento **LAN** de la lista desplegable **vía de enrutamiento predeterminado.**
21) Si el acceso a Internet se produce a través de un enrutador de Internet, ingrese la dirección IP del enrutador de Internet (por ejemplo, `192.168.1.1`) en el campo **Dirección IP del enrutador predeterminado.**
22) Haga clic en **Aceptar & Siguiente** seguido de **Finalizar**.

9.2.2.2 Cómo deshabilitar el servidor DHCP de la plataforma de hardware

El asistente de **configuración de red** se puede utilizar para desactivar el servidor DHCP de la plataforma de hardware.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Red/Internet**.
3) Haga clic en **Editar** para iniciar el asistente de **Configuración de red**.
4) Desmarque la casilla de verificación **Habilitar servidor DHCP.**
5) Siga haciendo clic en **Aceptar & Siguiente** hasta que reciba un mensaje que indique que se ha instalado la función.
6) Haga clic en **Finalizar**.

9.2.2.3 Cómo activar y configurar el servidor DHCP del softswitch

Paso a paso

1) En la barra de tareas, haga clic en **Computer** (Equipo).
2) En el grupo de menús, haga clic en **System** > **YaST** (Sistema > YaST).
3) Introduzca la contraseña del usuario "root" y haga clic en **Continue** (Continuar). Se abre el YaST Control Center.
4) En el grupo de menús, haga clic en **Network Services** (Servicios de red).
5) En el área **Network Services**, haga clic en **DHCP Server** (Servidor DHCP).
6) Marque la tarjeta de red deseada y haga clic en **Select** (Seleccionar).
7) Active la casilla de verificación **Open Firewall for Selected Interfaces** (Abrir firewall para interfaces seleccionadas).
8) Haga clic en **Continuar**.
9) Si necesita un nombre de dominio totalmente cualificado para el servidor DHCP, indíquelo en **Domain Name** (Nombre de dominio) (máx. 80 caracteres).
10) En el campo **Primary Name Server IP** (IP de servidor de nombre primario) introduzca la dirección IP de un servidor DNS disponible, por ejemplo, la dirección IP del router Internet, `192.168.1.1`.
11) En el campo **Default Gateway (Router)** (Gateway predeterminado, router), indique la dirección IP del gateway predeterminado. Por norma general, es la dirección IP del router Internet, por ejemplo, `192.168.1.1`.
12) En el campo **NTP Time Server** (Servidor de hora NTP) introduzca el servidor SNTP establecido en la puesta en servicio inicial.
13) Haga clic en **Continuar**.
14) En el campo **First IP Address** (Primera dirección IP), introduzca el valor límite inferior, y en el campo **Last IP Address** (Última dirección IP), el límite superior del rango de direcciones IP deseado (por ejemplo, de `192.168.1.50` a `192.168.1.254`).

15) Active la casilla de verificación **Allow Dynamic BOOTP** (Permitir BOOTP dinámico).
16) Haga clic en **Continuar**.
17) Active el campo de opción **When Booting** (Al arrancar).
18) Haga clic en **Salir**.
19) Cierre el **YaST Control Center**.

9.2.2.4 Cómo desactivar el servidor DHCP del softswitch

Paso a paso

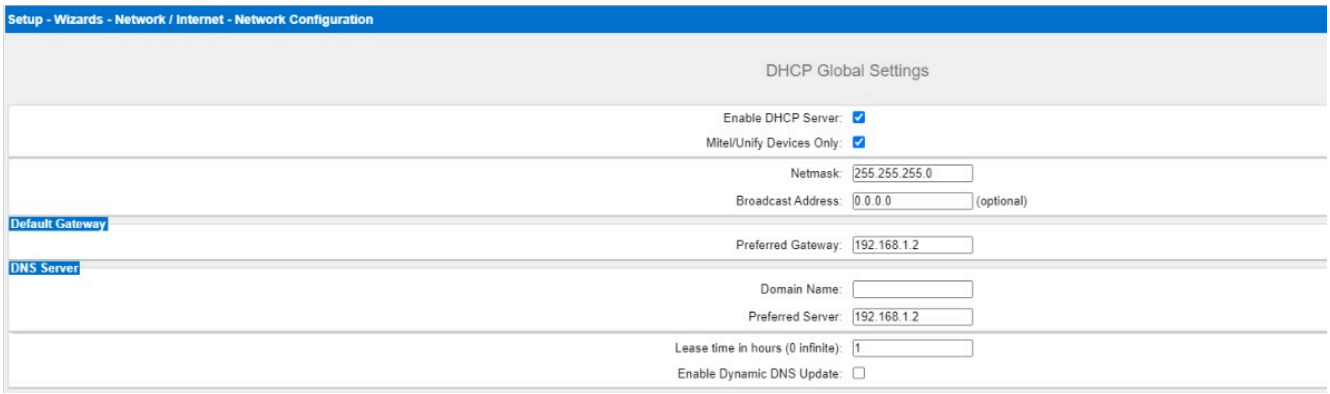
1) En la barra de tareas, haga clic en **Computer** (Equipo).
2) En el grupo de menús, haga clic en **System** > **YaST** (Sistema > YaST).
3) Introduzca la contraseña del usuario "root" y haga clic en **Continue** (Continuar). Se abre el YaST Control Center.
4) En el grupo de menús, haga clic en **Network Services** (Servicios de red).
5) En el área **Network Services**, haga clic en **DHCP Server** (Servidor DHCP).
6) Desactive la casilla de verificación **Start DHCP Server** (Iniciar servidor DHCP).
7) Haga clic en **Salir**.
8) Cierre el **YaST Control Center**.

9.2.2.5 Cómo habilitar DHCP solo para dispositivos Mitel/Unify

Esta opción permite al administrador del sistema activar el servicio DHCP de OpenScape Business exclusivamente para dispositivos Mitel y Unify.

Requisitos previos

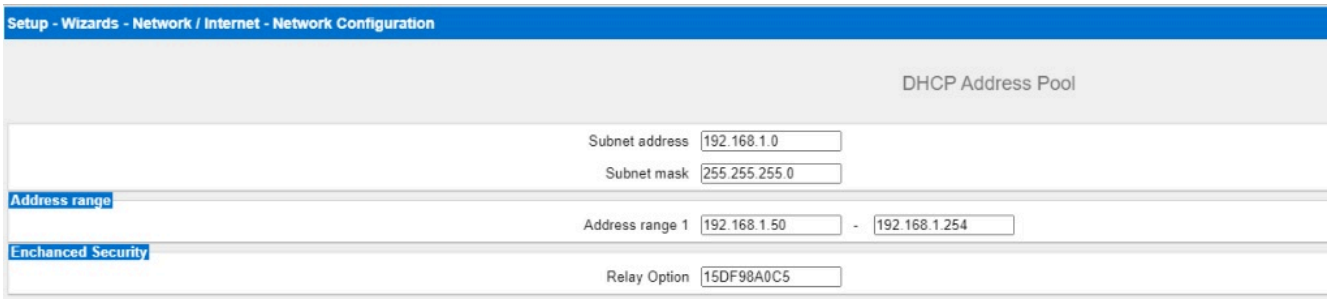
Está en la ventana **Configuración global de DHCP**.



Paso a paso

1) Deje la casilla de verificación **Habilitar servidor DHCP** habilitada.
2) Haga clic para habilitar la casilla de verificación **Solo dispositivos Mitel/ Unify.** Consulte Servidor DHCP > Parámetros globales para obtener más información sobre esta opción.

3) Vaya al campo **Máscara de red** y ajuste la máscara de subred a su rango de direcciones IP (por ejemplo, `255.255.255.0`).
4) En el campo **Gateway preferido**, ingrese la dirección IP del enrutador de Internet (por ejemplo, `192.168.1.1`).
5) En el campo **Servidor preferido**, ingrese la dirección IP del servidor DNS (por ejemplo, la dirección IP del enrutador de Internet, `192.168.1.1`.
6) Haga clic en **Aceptar & Siguiente**. Aparece la ventana del **grupo de direcciones DHCP**.



7) Especifique los valores para la dirección de subred , **Máscara de subred** y **Rango de direcciones 1** para definir el rango de direcciones IP que será administrado por el servidor DHCP interno.

   Si la red interna utiliza direcciones IP estáticas (por ejemplo, para un servidor de impresora), se debe seleccionar el rango de direcciones IP (grupo de direcciones DHCP) de modo que las direcciones IP fijas no se incluyan dentro de este rango.

   Ejemplo:

   Enrutador de Internet: `192.168.1.1`

   OpenScape Business: `192.168.1.2`

   Tarjeta de refuerzo UC: `192.168.1.3`

   Dirección de subred: `192.168.1.0`

   Máscara de subred: `255.255.255.0`

   Servidor de impresión: `192.168.1.10`

   Grupo de direcciones DHCP: `192.168.1.50` a `192.168.1.254`
8) Especifique el valor del campo **Opción de retransmisión**.
9) Haga clic en **Aceptar & Siguiente**.

Pasos siguientes

Configure los ajustes de país y hora.

9.3 DNS - Resolución de nombre

El servicio DNS (Domain Name Service) permite implementar nombres en direcciones numéricas. Eso permite traducir nombres de equipo o nombres de dominio en direcciones IP, y a la inversa.

DNS utiliza una base de datos jerárquica que administra el espacio de nombres de Internet y que está distribuida por servidores de todo el mundo. El espacio de nombres se subdivide en las denominadas zonas (dominios). Para cumplir

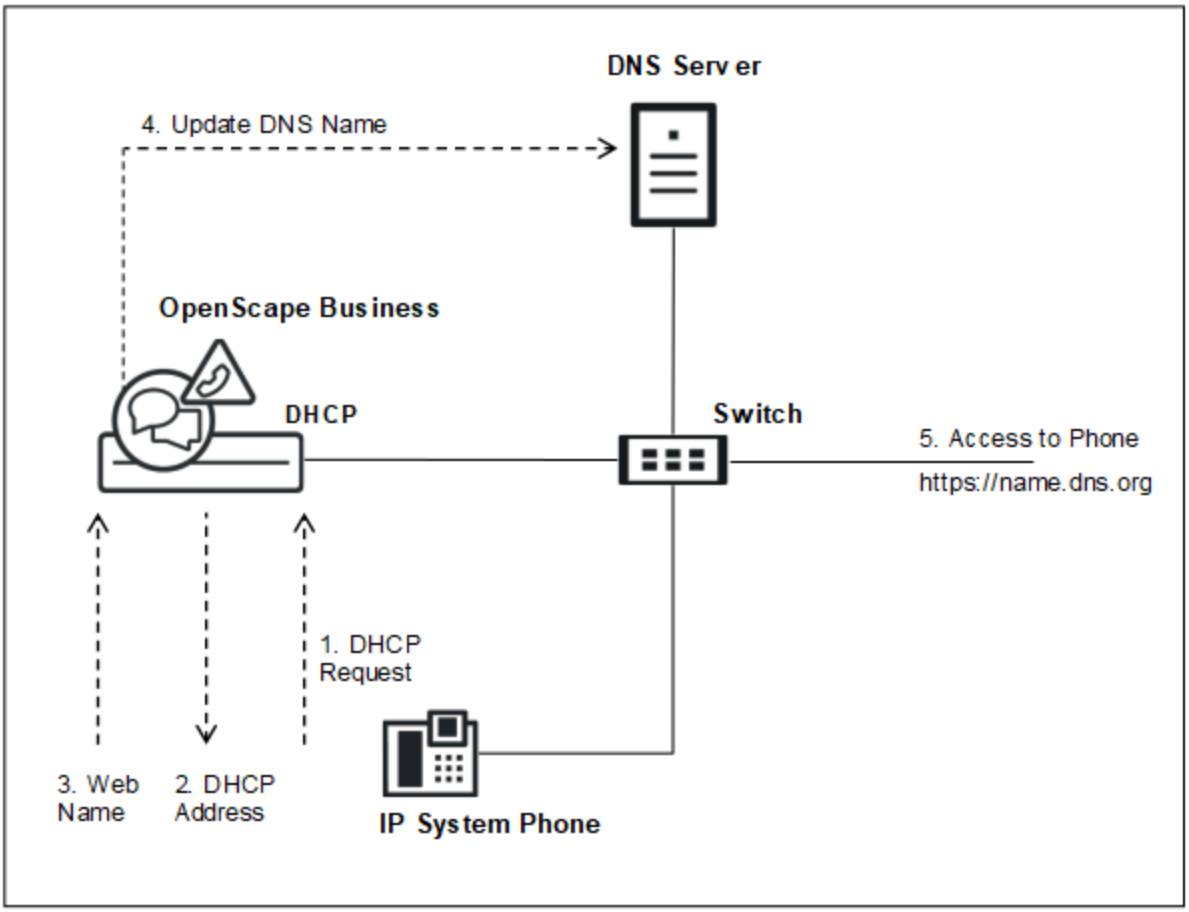
con las necesidades locales de una red de empresa, por ejemplo, se suele desplegar un servidor DNS independiente de Internet.

Resolución de nombre en teléfonos del sistema IP

Hay que cumplir estos requisitos:

- Servidor DNS Windows 2008 (con la versión de parche actual y el ajuste para permitir actualizaciones "no seguras" activado)
- Servidor DHCP interno activo
- La función "Actualiz. dinámica de DNS" está activa en el servidor DHCP interno (véase Servidor DHCP)
- El nombre web está registrado en el teléfono del sistema IP.

El teléfono del sistema IP envía una solicitud DHCP (1) y el servidor DHCP interno le envía una dirección IP válida y los demás datos específicos de la red (2). Después de recibir estos datos, el teléfono del sistema IP envía el nombre web configurado al servidor DHCP interno (3), que transfiere el nombre automáticamente al servidor DNS configurado (4). El servidor DNS identifica el nombre correspondiente a la dirección IP del teléfono del sistema IP. Solo se puede acceder al teléfono de sistema IP mediante la Gestión basada en Web (WBM) con su nombre Web (5).



Servidor DNS

El servidor DNS (denominado también servidor de nombres) es un programa que responde a consultas de nombres de dominio o de equipo. También el PC en el que se ejecuta el programa se puede denominar servidor DNS.

En las consultas de nombre de dominio o de equipo, el servidor DNS envía la dirección IP correspondiente.

Por ejemplo: para `www.wikipedia.org`, los servidores DNS de Internet devuelven la dirección IP `91.198.174.2`.

Si el servidor DNS favorito no puede responder la consulta, la deriva a otro servidor DNS.

Con el softswitch, el servidor Linux en el que se ejecuta el software de comunicación se puede configurar como servidor DNS. La plataforma de hardware no se puede utilizar como servidor DNS. Tanto en el softswitch como en la plataforma de hardware se puede indicar un servidor DNS externo.

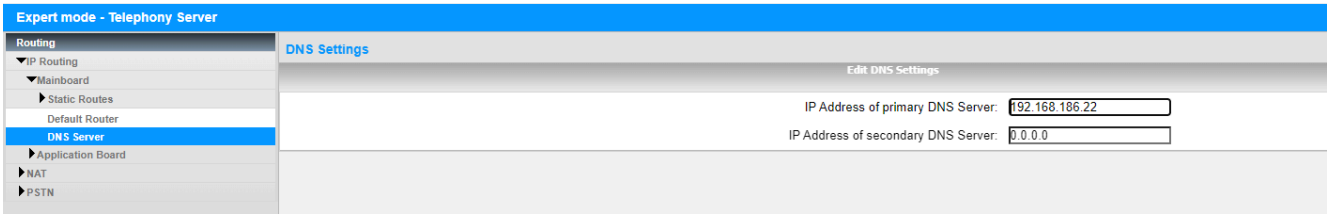
9.3.1 Cómo establecer un servidor DNS externo

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Encaminamiento**.
3) En el grupo de menús, desplácese hasta **Encamin. IP** > **Placa base** > **Servidor DNS**. Se abre la ventana **Editar ajustes DNS**.



4) En el campo **Dirección IP del servidor DNS** introduzca la dirección IP del servidor DNS externo.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Nota: Con un sistema OpenScape Business S, hay que reiniciar el sistema para aplicar los cambios.

9.4 Encamin. IP

En la técnica de datos, el encaminamiento IP es la definición de rutas para los flujos de datos dentro de redes. El encaminamiento IP es necesario si el remitente y el destinatario están en redes diferentes.

Router estándar

Para garantizar que las extensiones IP también pueden acceder a destinos que están fuera de la red propia y que no están detallados explícitamente en una tabla de encaminamiento, hay que indicar un gateway para la transferencia

de esos paquetes (router estándar). El router estándar transfiere entonces los datos a la red subordinada.

El encaminamiento IP mediante un router estándar se puede activar o desactivar para la placa base y para el tablero de aplicaciones.

Rutas estáticas

Las rutas estáticas se utilizan para establecer la ruta a una red a la que no se puede acceder por el router estándar.

Se pueden crear rutas estáticas para la placa base y para el tablero de aplicaciones.

9.4.1 Cómo activar o desactivar el router estándar

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Encaminamiento**.
3) En el grupo de menús, desplácese hasta **Encamin. IP** > **Placa base / Tablero de aplicaciones** > **Router estándar**. Aparece la ventana **Editar router estándar**.



4) Si quiere activar el encaminamiento IP mediante un router estándar, en la lista desplegable **Encam. estándar vía** seleccione la entrada **LAN** y en `Dirección IP del router estándar` indique la dirección IP del router estándar, por ejemplo, la dirección IP del router Internet **192.168.1.1**.
5) Si quiere activar el encaminamiento IP mediante un router estándar, en la lista desplegable **Encam. estándar vía** seleccione la entrada **Ninguna interfaz.**
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

9.4.2 Cómo añadir ruta estática

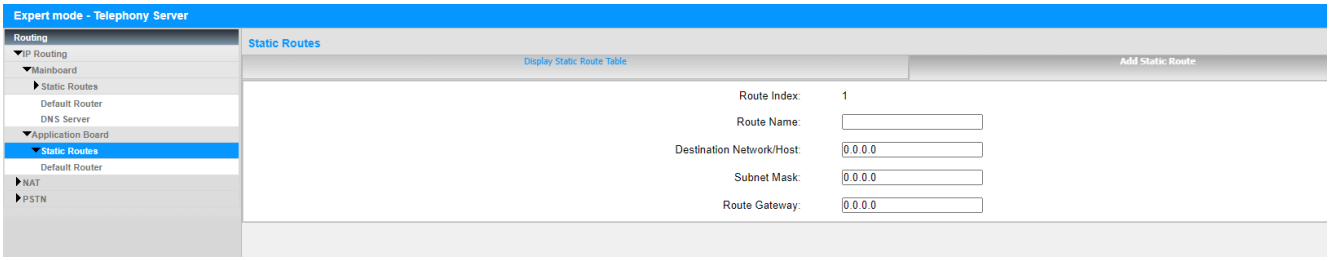
Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Encaminamiento**.
3) En el grupo de menús, desplácese hasta **Encamin. IP** > **Placa base / Tablero de aplicaciones** > **Rutas estáticas**. Aparece la ventana **Rutas estáticas**.
4) Haga clic en la pestaña **Añadir ruta estática**. El **Índice ruta** muestra qué ruta se va a añadir.



5) En el campo **Nombre de ruta** indique el nombre deseado para la ruta.
6) Indique la dirección IP del **Red destino/host**.
7) Indique la dirección IP de la **Másc. red de destino** (Máscara de subred).
8) En el campo **Gateway de ruta**, indique la dirección IP del router por el que se deberá acceder a la red de destino deseada.
9) Si ha creado una o varios rutas estáticas para la placa base, puede copiar todas las rutas estáticas de la placa base en el tablero de aplicaciones con el botón **Copiar en OCAB**.
10) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

9.4.3 Cómo borrar rutas estáticas

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Encaminamiento**.
3) En el grupo de menús, desplácese hasta **Encamin. IP** > **Placa base/ Tablero de aplicaciones** > **Rutas estáticas**.
4) Seleccione la ruta que desea borrar.
5) Pase a la pestaña **Borrar ruta estática**.
6) Haga clic en **Borrar**.
7) Confirme el mensaje de advertencia y, a continuación, haga clic en **Aceptar**.

9.5 Deployment Service (DLI y DLS)

Mediante DLI y DLS se pueden administrar componentes IP de forma centralizada y suministrarles software. El DLI está integrado en el sistema de comunicación. El DLS es una aplicación independiente que hay que instalar en un PC de servidor externo.

DLI (Deployment Server Integrated)

DLI es un componente integrado en el sistema de comunicación que ofrece la funcionalidad DLS con restricciones. Con el DLI interno se pueden configurar de forma centralizada todos los teléfonos IP del sistema conectados con el sistema de comunicación y suministrarles automáticamente el software telefónico más reciente. Para Desk Phone CP 400/600/600E/700/700X/710, cuando DLI está activado, los siguientes parámetros del servidor UC se configuran automáticamente: Protocolo UC, dirección del servidor UC, puerto del servidor UC.

El DLI interno colabora con el servidor FTP integrado en el que está almacenado el software telefónico más reciente.

Si el servidor DHCP conoce la dirección IP del DLI, el servidor DCHP envía los datos al teléfono del sistema IP (HFA, SIP) en cuanto inicia sesión en la red interna. De esta forma, el teléfono puede recoger el software actualizado en el servidor FTP del sistema de comunicación. En el servidor DHCP interno está configurado el DLI de forma predeterminada. Si en lugar de eso desea utilizar un servidor DLS externo, hay que configurar su dirección IP en el servidor DHCP interno.

DLS (Deployment Service)

El DLS es una aplicación cliente/servidor para la administración central de los componentes IP. El servidor DLS está integrado en el sistema de comunicación y se tiene que instalar por separado en un PC de servidor. El cliente DLS se ejecuta en los componentes IP. La administración se realiza mediante un navegador Web.

Los componentes IP son teléfonos IP del sistema, teléfono SIP, clientes SIP y gateways IP.

Nota: Puede consultar las características y prestaciones del DLS en la descripción del producto del DLS y no se describen en esta documentación.

DLI o DLS con servidor DHCP externo

Para poder actualizar automáticamente el software de los teléfonos IP de sistema (HFA, SIP) al utilizar un servidor DHCP externo, existen las siguientes opciones:

- Configurar la dirección IP del DLI o DLS en el servidor DHCP externo

  En el servidor DHCP externo, hay que registrar los datos específicos de red y la dirección IP del servidor de despliegue utilizado (DLI o servidor DLS externo). Además, en el servidor DLS externo debe guardarse el software actual del teléfono.
- Configurar todos los teléfono IP del sistema

  En cada teléfono IP del sistema hay que registrar como dirección DLS la dirección IP del servidor de despliegue utilizado (dirección IP del sistema de comunicación para el DLI interno o dirección IP del servidor DLS externo).

Funciones y restricciones

Función	DLI	DLS
Configuración central de los parámetros de los componentes IP Los parámetros de los componentes IP se configuran mediante plantillas XML modificables.	sí	sí
Puesta en servicio plug&play de los componentes IP Mediante un servidor DHCP, los componentes IP se pueden registrar automáticamente en el sistema, por ejemplo, con una nueva conexión o al intercambiar un componente IP.	Sí	Sí
Actualización de software central y automática de los componentes IP Los componentes IP reciben automáticamente la versión de software más reciente en el primer registro o cuando hay disponible una nueva versión de software. En el componente IP debe estar configurada la dirección IP del DLI/DLS.	Sí	Sí En el DLS debe estar memorizado el software de teléfono más reciente.
Gestión de inventario central de los componentes IP Los datos sobre las configuraciones de hardware de los componentes IP se pueden consultar de forma central.	no	Sí
Compatibilidad de IP Mobility (DeskSharing) Los datos de telefonía de un usuario se memorizan de forma central y se pueden consultar en otros teléfonos (por ejemplo, programaciones de teclas, entradas de listín, diarios).	Sí No para teléfonos SIP, No disponible en la interred.	Sí No para teléfonos SIP, En redes homogéneas (solo sistemas OpenScape Business) solo con numeración cerrada, No disponible en redes no homogéneas (con OpenScape 4000 o OpenScape Voice).
Compatibilidad de SPE en redes	Es posible utilizar SPE en redes. Hay que utilizar DLS (no DLI).	Sí Las claves y certificados a distribuir deben estar disponibles en el DLS.
Suministro central de varias plataformas diferentes	no	Sí
Liberación de la 2.ª interfaz LAN de los teléfonos del sistema IP (PC Ethernet Mode). Consulte Configuración básica> Despliegue de parámetros del teléfono	Sí	Sí

Deployment and Licensing Client (DLSC)

Para poder utilizar funciones DLS (como el gestor de elementos), el sistema de comunicación debe permitir que el DLS acceda a los datos de configuración. El sistema de comunicación funciona entonces como cliente de despliegue y licencias.

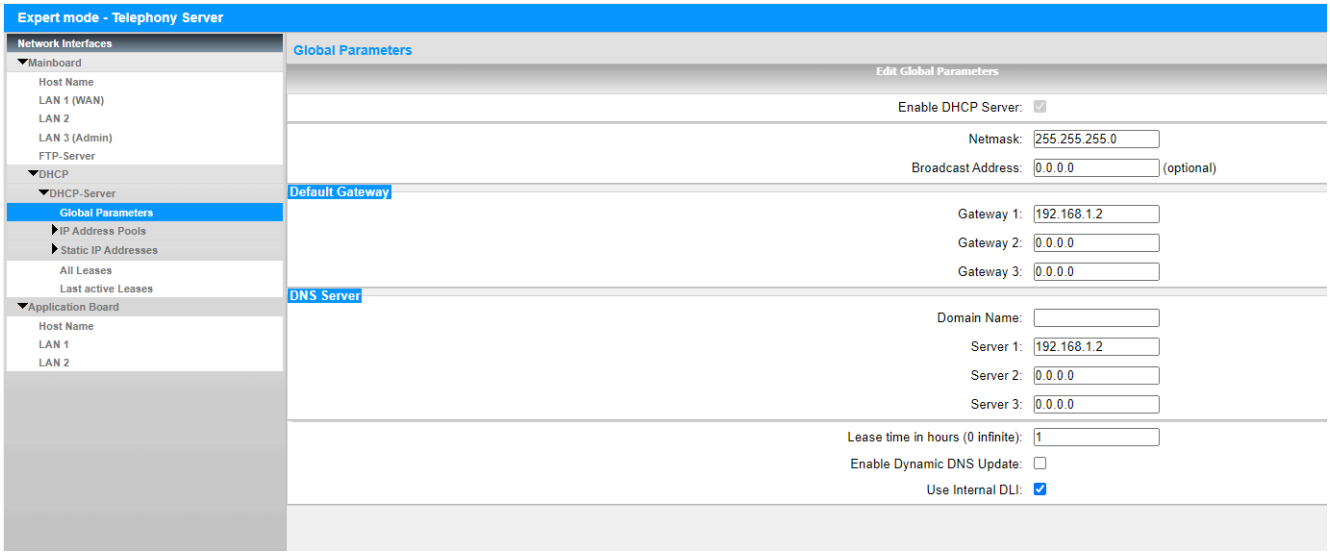
9.5.1 Cómo configurar un servidor DLS externo en el servidor DHCP interno

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) Haga clic en **Servidor de telefonía** > **Interfaces de red** en el árbol de navegación.
3) Navegue en el árbol de menús hasta **Placa base** > **DHCP** > **Servidor DHCP** > **Configuración global**. Se abre la ventana **Editar parámetros globales**.



4) Desactive la casilla de verificación **Utilizar DLI interno**.
5) En el campo **Dirección IP** introduzca la dirección IP con la que se puede acceder al servidor DLS externo.
6) En el campo **Puerto**, introduzca el puerto que utiliza el servidor DLS. Este puerto debe estar liberado en el firewall.
7) Haga clic en **Aplicar**, seguido de **Aceptar**.

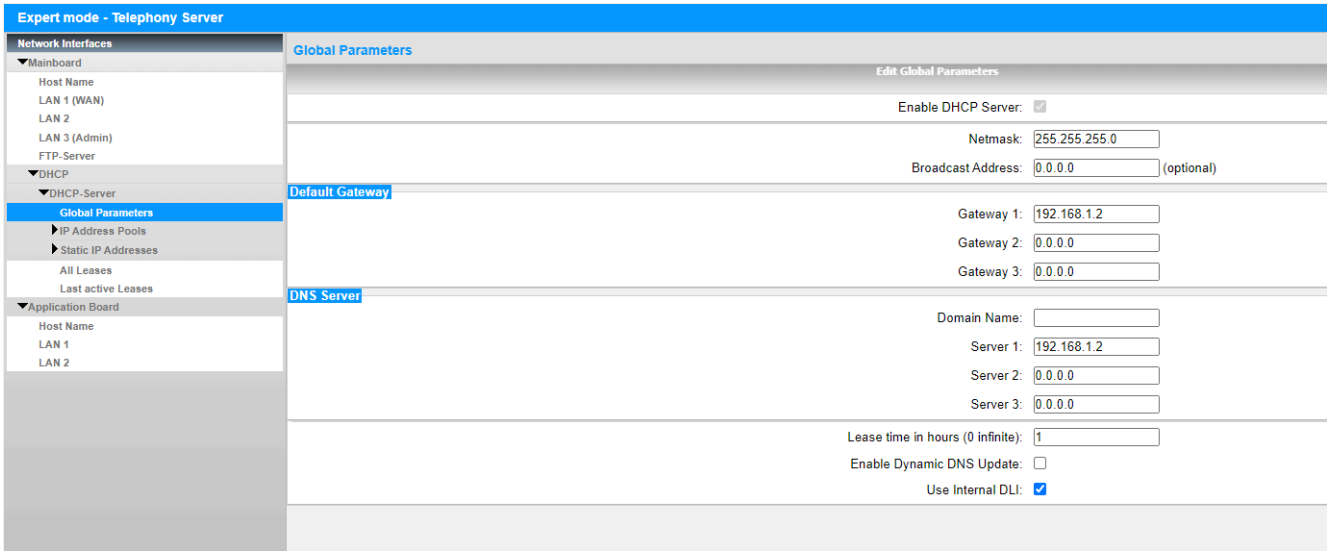
9.5.2 Cómo activar el DLI interno

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) Haga clic en **Servidor de telefonía** > **Interfaces de red** en el árbol de navegación.
3) Navegue en el árbol de menús hasta **Placa base** > **DHCP** > **Servidor DHCP** > **Configuración global**. Se abre la ventana **Editar parámetros globales**.



4) Active la casilla de verificación **Utilizar DLI interno**. La casilla de verificación está activa de forma predeterminada.
5) Haga clic en **Aplicar**, seguido de **Aceptar**.

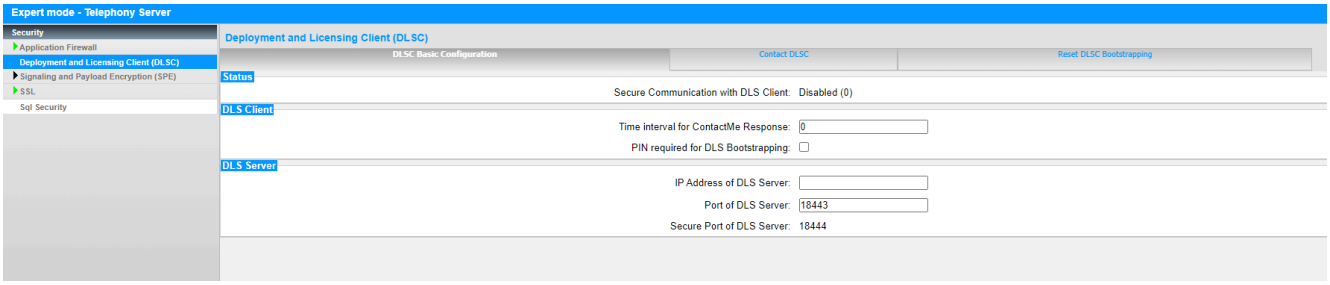
9.5.3 Cómo configurar el sistema de comunicación como cliente de implementación y licencias (Deployment & Licensing Client)

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Seguridad**.
3) En el grupo de menús, haga clic en **Deployment and Licensing Client (DLSC)**.



4) En la pestaña **Configuración básica de DLSC**, en el área **Servidor DLS** y en el campo **Dirección IP del servidor DLS**, indique la dirección IP con la que se accede al servidor DLS externo.
5) Si es necesario, en **Puerto del servidor DLS** modifique el puerto que utiliza el servidor DLS. Los dos puertos mostrados deben liberarse en el firewall.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10 Conexión al proveedor de servicios

El sistema de comunicación admite la conexión con redes de comunicación públicas. La conexión con la red IP permite acceder a Internet y a la telefonía Internet; el acceso de línea urbana permite acceder a la red RDSI y a la red analógica.

El acceso a Internet se realiza a través de un módem Internet o a través de un router Internet.

En las plataformas de hardware, el acceso a línea urbana RDSI se realiza a través de la placa base o de módulos insertables adicionales. En el softswitch no está disponible el acceso a línea urbana RDSI.

En las plataformas de hardware, la línea urbana analógica necesita además un módulo insertable. En el softswitch no está disponible el acceso a línea urbana analógico.

10.1 Acceso a Internet

Para acceder a Internet se requiere una conexión de banda ancha (conexión DSL o conexión por cable). Esto permite una transferencia de datos rápida dentro del ancho de banda disponible.

Acceso a Internet por conexión DSL

La conexión de banda ancha a Internet por DSL (Digital Subscriber Line) se realiza a través de la línea telefónica convencional. El acceso a Internet se puede utilizar de forma paralela al teléfono normal. El fax, el teléfono analógico y el RDSI siguen disponibles durante la conexión DSL. De esta forma, se puede implementar un acceso a Internet disponible permanentemente en caso de línea dedicada (tarifa plana).

Para un acceso a Internet por DSL necesita una conexión telefónica (analógica o RDSI) y un ISP (proveedor de servicios de Internet). El ISP pondrá a su disposición un splitter y un módem Internet o un router Internet con módem Internet integrado. El splitter divide la señal en las partes DSL y de telefonía y transmite las señales DSL al módem Internet.

El sistema de comunicación se puede conectar directamente al módem Internet o al router Internet con módem Internet integrado. En el primer caso es necesario indicar los datos de acceso del ISP en el sistema de comunicación; en el segundo caso, hay que comunicar al sistema de comunicación el router Internet. Los datos de acceso del ISP se almacenan en el router Internet.

Para poder utilizar telefonía Internet, necesita además un ITSP (Internet Telephony Service Provider, proveedor de servicios de telefonía por Internet).

Acceso a Internet a través de conexión por cable

La conexión de banda ancha a Internet a través de cable se realiza a través de la conexión por cable del televisor. La conexión de televisión, además de para la transmisión de señales de televisión, también se puede utilizar para el acceso a Internet y para las llamadas telefónicas. De esta forma, se puede navegar por Internet y telefonear sin línea telefónica.

Para acceder a Internet por cable necesita un proveedor de cable que ofrezca esta prestación. Será también, al mismo tiempo, su ISP (proveedor de servicios de Internet). El proveedor de cable le ofrece una conexión por cable con un canal trasero y un módem por cable. La conexión transmite los datos a través de la red de televisión por cable. La conexión de cable y el sistema de comunicación se conectan al módem por cable a través de Ethernet. El filtrado de datos de Internet se realiza en el propio módem por cable.

El sistema de comunicación se puede conectar directamente con el módem por cable o con un router Internet que, a su vez, esté conectado con el módem por cable. En ambos casos, el sistema de comunicación debe conocer el módem por cable o el router Internet.

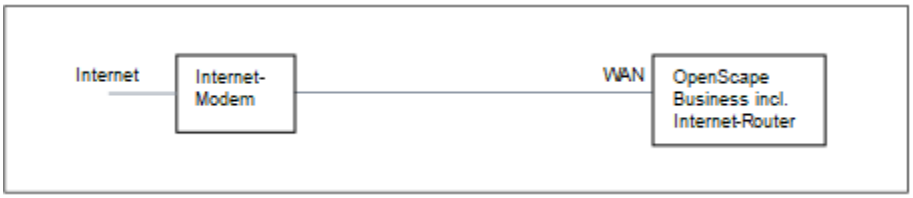
Para poder utilizar telefonía Internet, necesita además un ITSP (Internet Telephony Service Provider, proveedor de servicios de telefonía por Internet).

Configuración del acceso a Internet

La configuración del acceso a Internet en la Gestión basada en Web (WBM) depende de si el acceso a Internet ya está configurado en un router externo o si se hace mediante un módem Internet y, por tanto, debe configurarse en la Gestión basada en Web (WBM).

- **Acceso a Internet mediante un módem Internet** (**DSL directamente a interfaz WAN**)

  Desea operar el sistema de comunicación directamente en un módem de Internet (DSL, Cable, UMTS, …). OpenScape Business tiene integrado el router Internet. Introduzca los datos de acceso del proveedor de servicios de Internet (ISP) directamente en el sistema de comunicación y utilice la conexión WAN del sistema de comunicación. Esta opción no está disponible en el softswitch.

  Tiene las siguientes opciones:

  – Acceso a Internet a través de ISP preconfigurados
  – Acceso a Internet a través de PPPoE ISP estándar
  – Acceso a Internet a través de PPTP ISP estándar

  Si su ISP no está en la lista de ISP preconfigurados, utilice el PPPoE o PPTP de ISP estándar.

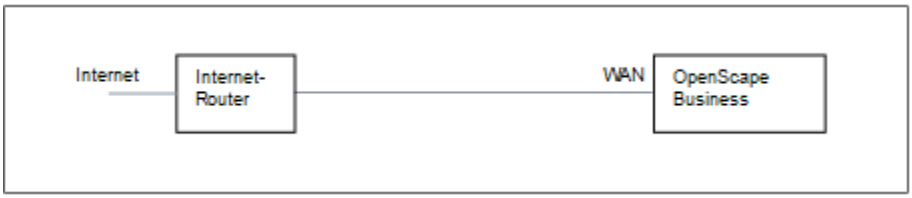
- **Acceso a Internet a través de un router de Internet externo**

  Desea operar el sistema de comunicación en un router Internet externo. El proveedor de servicios de Internet ya está configurado en el router Internet.

  Tiene las siguientes opciones:

  – **Acceso a Internet a través de un router Internet externo en la conexión WAN**

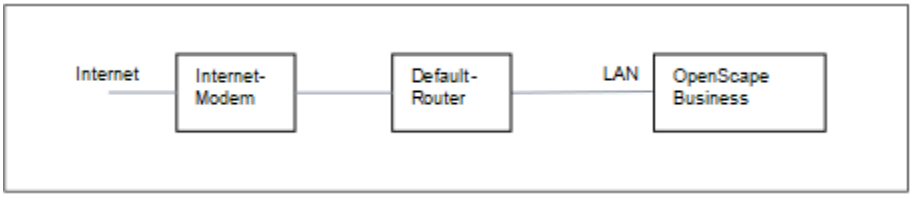
    (**TCP/IP en interfaz WAN a través de un router externo**)

    Para ello, utilice la conexión WAN del sistema de comunicación. OpenScape Business reconoce el router Internet o funciona como cliente DHCP. Esta opción se puede utilizar si el router Internet está en otro segmento de red y tiene un servidor DHCP propio.

  – **Acceso a Internet a través de un router Internet externo en la conexión LAN**

    (**TCP/IP en puerto LAN a través de un router externo**)

    Para ello, utilice la conexión LAN del sistema de comunicación. OpenScape Business solo conoce el router estándar y no la infraestructura de base. Para activar la conexión con el router Internet, hay que comunicar al sistema de comunicación la dirección IP del router estándar y del servidor DNS.

- **Desactivar el acceso a Internet** (ajuste estándar)

  No quiere utilizar Internet. En tal caso, deje desactivado el acceso a Internet.

10.1.1 Acceso a Internet a través de un router Internet externo

Con el asistente **Configuración de Internet** puede configurar su acceso a Internet a través de un router Internet adicional.

Para configurar el acceso a Internet dispone de estas opciones:

- **Acceso a Internet a través de un router Internet externo en la conexión LAN**

  Para ello, utilice la conexión LAN del sistema de comunicación. Para activar la conexión con el router Internet, hay que comunicar al sistema de comunicación la dirección IP del router estándar y del servidor DNS.

- **Acceso a Internet a través de un router Internet externo en la conexión WAN**

  Para ello, utilice la conexión WAN del sistema de comunicación. Esta opción se puede utilizar si el router Internet está en otro segmento de red y tiene un servidor DHCP propio.

10.1.1.1 Cómo configurar el acceso a Internet a través de un router de Internet externo mediante la conexión LAN

Con el asistente **Configuración de Internet** puede configurar el acceso a Internet, si el sistema de comunicación va a operar tras un router Internet adicional. El sistema de comunicación y el router Internet se encuentran en el mismo segmento LAN. Para ello, debe indicar la dirección IP del router Internet y del servidor DNS.

Requisitos previos

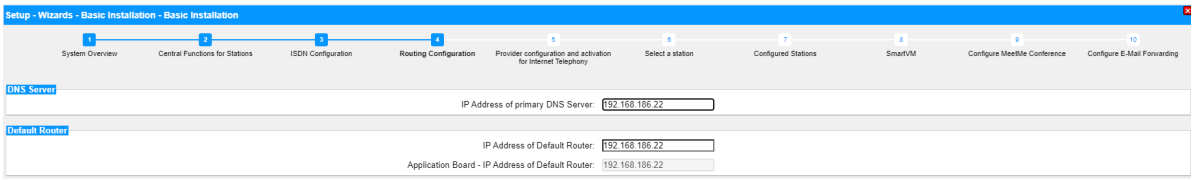
Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Para OpenScape Business X: El sistema de comunicación está conectado con la red de clientes mediante la interfaz "LAN". La conexión no se puede establecer a través de la interfaz "WAN".

Para OpenScape Business S: el servidor Linux está conectado con la red de clientes a través de la interfaz LAN de la tarjeta de red.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Red / Internet**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de Internet**.
4) Desactive la casilla de verificación **Sin acceso a Internet**.
5) Active la opción **TCP/IP en puerto LAN a través de un router externo** y haga clic en **OK & Continuar**.



6) En el campo **Dirección IP del servidor DNS**, introduzca la dirección IP del servidor DNS local (por ejemplo, router Internet) o del servidor DNS de Internet (por ejemplo, para Telefonía Internet).
7) En el campo **Dirección IP del router estándar** introduzca la dirección IP del router Internet externo.
8) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

10.1.1.2 Cómo configurar el acceso a Internet a través de un router de Internet externo mediante la conexión WAN

Con el asistente **Configuración de Internet** puede configurar el acceso a Internet, si el sistema de comunicación va a operar tras un router Internet adicional. El sistema de comunicación y el router Internet deben estar en el mismo segmento LAN.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

El sistema de comunicación tiene que estar conectado con el segmento de la LAN de la red de cliente en que se encuentra el router Internet a través de la interfaz "WAN".

Se encuentra en la ventana **Configuración de Acceso a Internet**.

Paso a paso

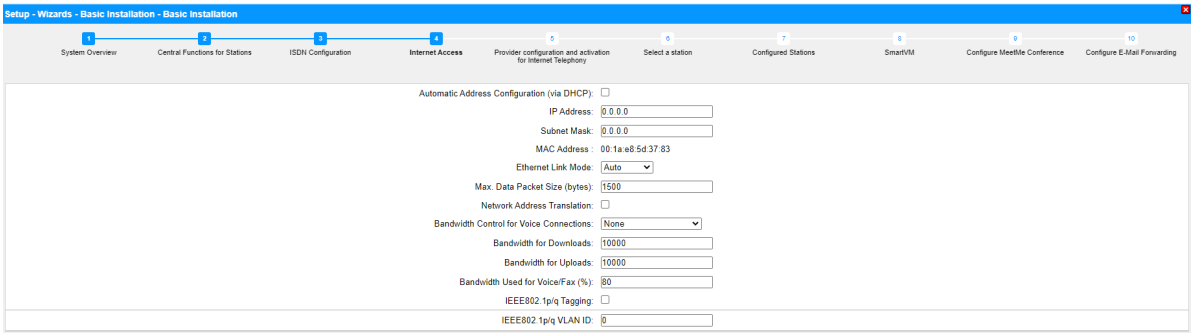
1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Red / Internet**.

3) Haga clic en **Editar** para iniciar el asistente **Configuración de Internet**.

4) Desactive la casilla de verificación **Sin acceso a Internet**.

5) Active la opción **TCP/IP en interfaz WAN a través de un router externo** y haga clic en **OK & Continuar**.



6) Si los datos específicos de red de la interfaz WAN se deben obtener de un servidor DHCP ya activo:

a) Active la casilla de verificación **Configuración de dirección automática (con DHCP)**.

b) Active la casilla de verificación **Aceptar dirección IP del router estándar**.

c) Si es necesario, active la casilla de verificación **Aceptar dirección IP del servidor DNS**.

d) Si es necesario, active la casilla de verificación **Aceptar dirección IP del servidor SNTP**.

7) Si desea asignar a la interfaz WAN una dirección IP fija:

a) Desactive la casilla de verificación **Configuración de dirección automática (con DHCP)**.

b) Introduzca la **Dirección IP** y la **Máscara de red** deseadas de la interfaz WAN.

8) Active la casilla de verificación **Traducción dirección red (NAT)**.

9) Si también quiere utilizar telefonía Internet, en la lista desplegable **Control ancho banda para conex. voz**, seleccione la entrada **Sólo carga** o **Carga y descarga**, según sus necesidades. Si el ancho de banda de la descarga es alto y el de carga es bajo, el control de ancho de banda sólo se debería activar para la dirección de carga, garantizando así que el ancho de banda de descarga reservado para la transmisión de voz no sea innecesariamente elevado.
10) En los campos **Ancho de banda para descargas** y **Ancho de banda para cargas**, seleccione el ancho de banda en Kbit/s para la descarga o para la carga. El valor le será suministrado por su ISP.
11) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

10.1.1.3 Cómo configurar el acceso a Internet a través de un enrutador de Internet externo sobre la LAN con un puerto WAN dedicado a ITSP

Requisitos previos

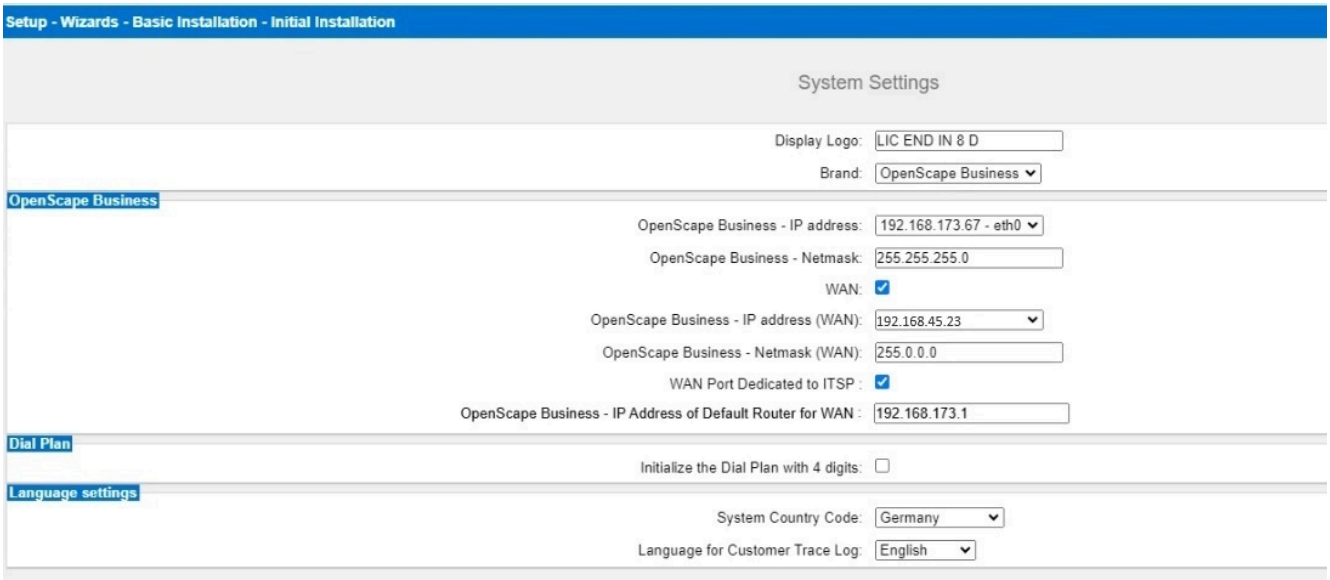
Ha creado una nueva interfaz de red en SLES.

Se encuentra en la ventana **Configuración del sistema** del asistente de **instalación inicial**.

Tenga en cuenta que esta función solo se aplica a los ITSP que no requieren el uso de STUN en la configuración del proveedor.

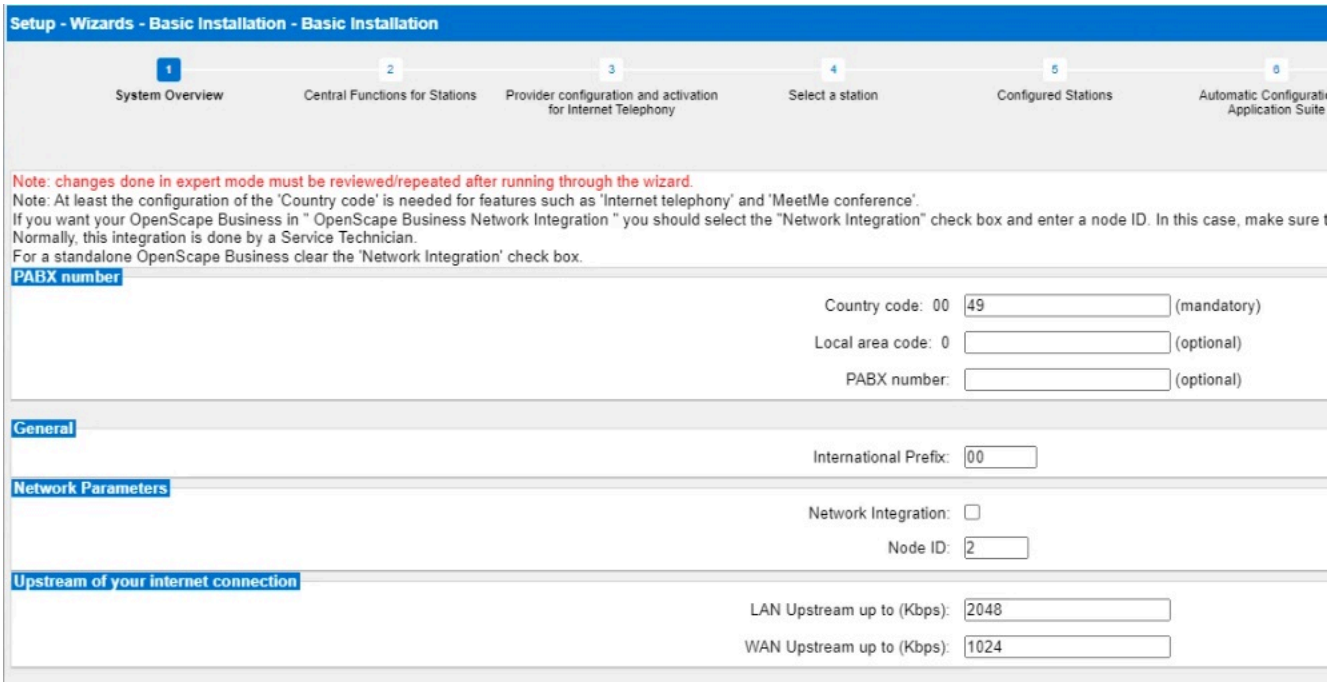
Paso a paso

1) Habilite la casilla de verificación **WAN** y seleccione la interfaz de red adecuada.
   La opción **Interfaz WAN dedicada a ITSP** se hace disponible.
2) Haga clic para habilitar la casilla de verificación **Interfaz WAN dedicada a ITSP.**



3) Haga clic en **Aceptar & Siguiente**.
4) Vaya a **Configuración > Instalación básica** y ejecute el asistente **Instalación básica**.

5) Configure los valores máximos de subida en los campos correspondientes **Subida de LAN hasta (Kbps)** y **Subida de WAN hasta (Kbps).**



6) Haga clic en **Aceptar & Siguiente**.

7) Después de aplicar la configuración, es necesario reiniciar el sistema.

10.1.2 Acceso a Internet a través de un módem Internet

Con el asistente **Configuración de Internet**, configure el acceso a Internet a través de un módem Internet. Para ello, la conexión WAN del sistema de comunicación se conecta directamente a un módem Internet. Puede utilizar un ISP preconfigurado en el sistema de comunicación o un tipo ISP estándar (pida el tipo a su ISP).

Para configurar el acceso a Internet dispone de estas opciones:

- **Configurar el acceso a Internet a través de ISP preconfigurados**

  Utiliza un sistema de comunicación con ISP preconfigurado. Puede seleccionar su ISP preconfigurado desde una lista.
- **Configurar el acceso a Internet a través de PPPoE ISP estándar**

  Utiliza el tipo ISP estándar **PPPoE de proveedor**. Solicite los ajustes necesarios a su ISP.
- **Configurar el acceso a Internet a través de PPTP ISP estándar**

  Utiliza el tipo ISP estándar **PPTP de proveedor**. Solicite los ajustes necesarios a su ISP.

Interrupción de la conexión en función del modelo de tarifas

En función del modelo de tarifas se puede definir si la conexión con el ISP debe mantenerse o no en caso de inactividad.

- El el modelo de tarifas de tarifa plana, no es necesario interrumpir la conexión a Internet en caso de inactividad. Muchos ISP imponen un corte

forzoso de la conexión cada 24 horas. Se puede especificar el momento del corte de la conexión.

- En el modelo de tarifas basada en tiempo, se debería cortar la conexión a Internet en caso de inactividad. Se puede especificar el tiempo de inactividad tras el cual interrumpir la conexión (por ejemplo, 60 segundos). La conexión se restablece automáticamente en cuanto se vuelve a hacer una solicitud a Internet. Si está configurado VPN, la conexión no se interrumpe en caso de inactividad (se debe seleccionar el modelo de tarifa plana).

Nota: Los programas o servicios basados en red pueden establecer automáticamente una conexión a Internet, de lo que pueden derivar cargos de conexión adicionales en este tipo de tarifa.

Ancho de banda

El ISP ofrece distintos anchos de banda para la descarga y para la subida de datos. El ancho de bandas se indica en Kbit/s. Si se utiliza también telefonía Internet, la transmisión de voz y la de datos comparten el ancho de banda. Por eso es útil reservar un ancho de banda suficiente para mantener la calidad de la transmisión de voz. Esto, sin embargo, puede producir cuellos de botella en la transmisión de datos (por ejemplo, descargas más lentas) cuando la transmisión de voz es intensiva.

Puede elegir si el control de ancho de banda solo debe estar activo para la carga o para carga y descarga. Si el ancho de banda de la descarga es alto y el de carga es bajo, el control de ancho de banda solo se debería activar para la dirección de carga, garantizando así que el ancho de banda de descarga reservado para la transmisión de voz no sea innecesariamente elevado.

Nota: Para una llamada por Internet se reservan un ancho de banda de unos 128 Kbit/s.

10.1.2.1 Cómo configurar el acceso a Internet a través de un ISP preconfigurado

Con el asistente **Configuración de Internet** puede configurar su acceso a Internet a través de un ISP (proveedor de servicios de Internet) preconfigurado en el sistema de comunicación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Dispone de los datos de acceso a Internet de su ISP (p. ej. identificación de usuario, contraseña).

Paso a paso

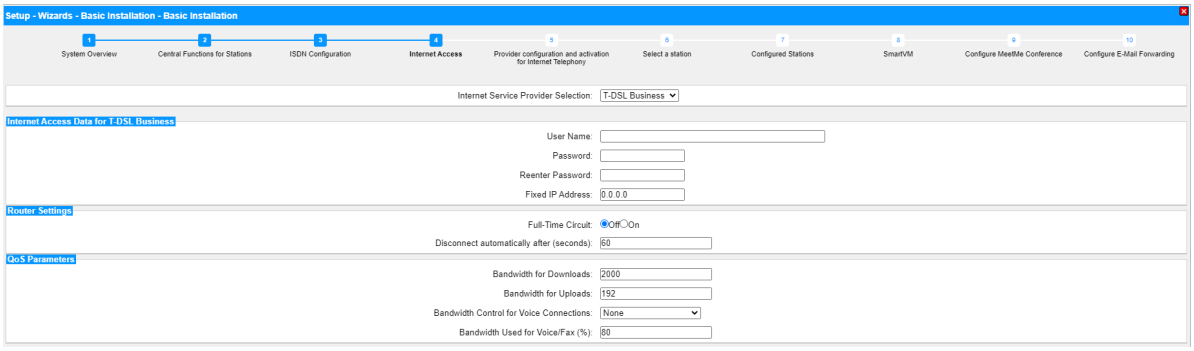
1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Red / Internet**.

3) Haga clic en **Editar** para iniciar el asistente **Configuración de Internet**.

4) Desactive la casilla de verificación **Sin acceso a Internet**.

5) Active la opción **DSL directamente a interfaz WAN** y haga clic en **OK & Continuar**.



6) En la lista desplegable **Selección de ISP**, seleccione su proveedor de servicios de Internet.

7) En la sección **Datos de acceso a Internet para**, indique los datos de acceso que le ha entregado su ISP. Los campos de este área dependen del proveedor. Al introducir los datos, compruebe el uso de mayúsculas y minúsculas.

8) En la sección **Ajustes de router**, y en **Conexión permanente**, seleccione una de ambas opciones en función de su modelo de tarifas:

   - Si tiene una tarifa plana como modelo de tarifas, active el campo de opción **Act.**. En el campo **Desconexión forzosa a las (hrs:min)**, establezca la hora en la que se desconectará la conexión a Internet (por ejemplo, 04:59).
   - Si tiene un modelo de tarifa basado en tiempo, active la casilla de verificación **Desact.**. En el campo **Cortar automáticamente tras (segundos)**, indique el tiempo de inactividad tras el cual deberá interrumpirse la conexión (por ejemplo, 60 segundos).

9) En la sección **Parámetro QoS** ajuste estos valores:

   a) En los campos **Ancho de banda para descargas** y **Ancho de banda para cargas**, seleccione el ancho de banda en Kbit/s para la descarga o para la carga. El valor le será suministrado por su ISP.

   b) Si también quiere utilizar telefonía Internet, en la lista desplegable **Control ancho banda para conex. voz**, seleccione la entrada **Solo carga** o **Carga y descarga**, según sus necesidades. En el campo **Ancho banda para conex. voz/fax (%)** indique, en valores porcentuales, cuánto ancho de banda va a reservarse para las conexiones de voz y fax (valor estándar: 80%).

10) Haga clic en **OK & Continuar**. Es conducido a la ventana **Configurar cuenta DynDNs**.

11) Si desea utilizar la red privada virtual o el acceso remoto y no tiene una dirección IP estática pública, debe haber solicitado y configurado una cuenta DynDNS (por ejemplo, en dyndns.org).

   a) Si su proveedor DynDNS aparece en la lista desplegable **Nombre dominio**, selecciónelo (p.ej. dyndns.org).

   b) Si su proveedor DynDNS no aparece en la lista desplegable **Nombre dominio**, active la casilla de verificación **Dominio definido por el usuario**. En el campo **Nombre dominio**, introduzca el proveedor DynDNS deseado y en el campo **URL de actualización**, la URL de actualización del proveedor DynDNS. La estructura de la URL

depende del proveedor DynDNS. Además, hay que indicar parámetros específicos del cliente (en el ejemplo, marcados en *cursiva*).

```
http://www.anydns.info/update.php?
user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>
```

c) Introduzca el **Nombre de usuario** y **Contraseña** de su cuenta DynDNS.
d) En el campo **Nombre host**, indique el nombre de host suministrado por el proveedor DynDNS sin el nombre de dominio, por ejemplo, myhost. Su nombre de dominio completo será, por ejemplo, mihost.dyndns.org.
e) Compruebe la cuenta DynDNS con **Prueba de conexión**.
f) Si la comprobación termina con éxito, haga clic en **Aceptar**.
g) Haga clic en **OK & Continuar**.

12) Si tiene una dirección IP estática pública o desea utilizar la red privada virtual o el acceso remoto, haga clic en **Sin DynDNS**.

13) Haga clic en **Salir**. El sistema de comunicación se reinicia.

10.1.2.2 Cómo configurar el acceso a Internet a través de un PPPoE ISP estándar

Con el asistente **Configuración de Internet** puede configurar su acceso a Internet a través del PPPoE ISP estándar.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Dispone de estos datos de acceso a Internet de su ISP:

Campo	Descripción	Valor del ISP
Parámetros IP (solo con dirección IP fija)		
Dirección IP remota de la conexión PPP	Dirección IP del servidor de su ISP.	
Dirección IP local de la conexión PPP	Dirección IP suministrada por el proveedor de servicios de Internet.	
Autenticación (por PAP o CHAP). Hoy en día PAP a penas se utiliza porque la autenticación no está codificada.		
Nombre usuario PPP	Nombre de usuario para la conexión PPP, suministrado por el ISP.	
Modo autenticación PAP	Modo de autenticación para la conexión PPP sobre PAP: **Cliente PAP**, **Anfitrión PAP** o **No utilizado**.	
Clave PAP	Contraseña para la autenticación por PAP, suministrada por el ISP.	
Modo autentificación CHAP	Modo de autenticación para conexión PPP vía CHAP: **Cliente CHAP**, **Anfitrión CHAP**, **Cliente y host CHAP** o **No utilizado**.	
Clave CHAP	Contraseña para la autenticación por CHAP, suministrada por el ISP.	
Parámetros QoS de la interfaz		

Campo	Descripción	Valor del ISP
Ancho de banda para descargas	Valora el ancho de banda en Kbit/seg para la descarga desde el ISP.	
Ancho de banda para cargas	Valora el ancho de banda en Kbit/seg para la carga al ISP.	

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Red / Internet**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de Internet**.
4) Deshabilite **Sin acceso a Internet** casilla de verificación.
5) Active el botón de opción **DSL en el puerto WAN directamente** y haga clic en **OK & Siguiente**.
6) En la lista desplegable **Selección de ISP** seleccione el tipo ISP estándar **PPPoE de proveedor**.
7) En el área **Parámetros IP** active la casilla de verificación **Parámetros IP** solamente si el ISP requiere un ajuste. En tal caso, en los campos **Dir. IP colateral de conex. PPP**, **Dirección IP local de conex. PPP** y **Long. máx. paquetes datos (bytes)** indique los valores que le hayan sido suministrados por su ISP. En la lista desplegable **Negociación dir. IP** seleccione la entrada **Utilizar dirección IP config.**.
8) En la sección **Ajustes de router**, y en **Conexión permanente**, seleccione una de ambas opciones en función de su modelo de tarifas:
   - Si tiene una tarifa plana como modelo de tarifas, active el campo de opción **Act.**. En el campo **Desconexión Forzada a las (hora:min)**, introduzca la hora a la que se desactivará la conexión a Internet (p. ej., 04:59).
   - Si tiene un modelo de tarifa basado en tiempo, active la casilla de verificación **Desact.**. En el **Desconectarse automáticamente después de (segundos)**, ingrese la duración de la inactividad después de la cual se debe interrumpir la conexión (por ejemplo, 60 segundos).
9) Los ajustes de la sección **Autenticación** dependen de si su ISP exige o no una autenticación por PPP.
   - Autenticación requerida por el ISP: Asegúrese de que la casilla de verificación **Autenticación PPP** está habilitada. Indique como nombre de usuario PPP el nombre de acceso a Internet del ISP. El estándar habitual es el modo de autenticación **Cliente CHAP**.
   - Autenticación no requerida por el ISP: Asegúrese de que la casilla de verificación Autenticación PPP esté desactivada.
10) Si desea utilizar NAT, en la sección **Traduc. dirección**, active la casilla de verificación **NAT** (activada de forma predeterminada).
11) En la sección **Parámetros QoS de la interfaz** establezca estos valores:
    a) En los campos **Ancho de banda para descargas** y **Ancho de banda para cargas**, seleccione el ancho de banda en Kbit/s para la descarga o para la carga. El valor le será suministrado por su ISP.
    b) Si también quiere utilizar telefonía Internet, en la lista desplegable **Control ancho banda para conex. voz**, seleccione la entrada **Solo carga** o **Carga y descarga**, según sus necesidades. En el campo **Ancho de banda utilizado para voz/fax (%)**, ingrese cuánto ancho

de banda se reservará para las conexiones de voz y fax como valor porcentual (valor predeterminado: 80%).

12) Haga clic en **Aceptar & Siguiente**. Es conducido a la ventana **Configurar cuenta DynDNs**.

13) Si desea utilizar la red privada virtual o el acceso remoto y no tiene una dirección IP estática pública, debe haber solicitado y configurado una cuenta DynDNS (por ejemplo, en dyndns.org).

a) Si su proveedor DynDNS aparece en la lista desplegable **Nombre dominio**, selecciónelo (p.ej. dyndns.org).

b) Si su proveedor DynDNS no aparece en la lista desplegable **Nombre dominio**, active la casilla de verificación **Dominio definido por el usuario**. En el campo **Nombre dominio**, introduzca el proveedor DynDNS deseado y en el campo **URL de actualización**, la URL de actualización del proveedor DynDNS. La estructura de la URL depende del proveedor DynDNS. Además, hay que indicar parámetros específicos del cliente (en el ejemplo, marcados en *cursiva*).

`http://www.anydns.info/update.php?user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

c) Introduzca el **Nombre de usuario** y **Contraseña** de su cuenta DynDNS.

d) En el campo **Nombre host**, indique el nombre de host suministrado por el proveedor DynDNS sin el nombre de dominio, por ejemplo, mihost. Su nombre de dominio completo será, por ejemplo, mihost.dyndns.org.

e) Compruebe la cuenta DynDNS con **Prueba de conexión**.

f) Si la comprobación termina con éxito, haga clic en **Aceptar**.

g) Haga clic en **Aceptar & Siguiente**.

14) Si tiene una dirección IP pública estática o no desea utilizar una VPN o acceso remoto, haga clic en **No DynDNS**.

15) Haga clic en **Salir**.

10.1.2.3 Cómo configurar el acceso a Internet a través de un PPTP ISP estándar

Con el asistente **Configuración de Internet** puede configurar su acceso a Internet a través del PPTP estándar del ISP.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Dispone de estos datos de acceso a Internet de su ISP:

Campo	Descripción	Valor del ISP
Parámetros IP (solo con dirección IP fija)		
Dir. IP colateral de conex. PPP	Dirección IP del servidor de su ISP.	
Dirección IP local de conex. PPP	Dirección IP suministrada por el proveedor de servicios de Internet.	
Parámetros PPTP		

Campo	Descripción	Valor del ISP
Dirección IP local de conex. control	Dirección IP suministrada por el proveedor de servicios de Internet para la conexión PPTP. El valor preestablecido es 10.0.0.140.	
Dirección IP colateral de conex. control	Dirección IP del servidor ISP para la conexión PPTP. El valor preestablecido es 10.0.0.138.	
Másc. red colateral para conex. control	Máscara de red suministrada por el proveedor de servicios de Internet para la conexión PPTP. El valor preestablecido es 255.255.255.248.	
Autenticación (por PAP o CHAP). Hoy en día PAP a penas se utiliza porque la autenticación no está codificada.		
Nombre usuario PPP	Nombre de usuario para la conexión PPP, suministrado por el ISP.	
Modo autenticación PAP	Modo de autenticación para la conexión PPP por PAP: **Cliente PAP**, **Host PAP** o **Sin utilizar**.	
Clave PAP	Contraseña para la autenticación por PAP, suministrada por el ISP.	
Modo autentificación CHAP	Modo de autenticación para la conexión PPP por CHAP: **Cliente CHAP**, **Host CHAP**, **Cliente y host CHAP** o **Sin utilizar**.	
Clave CHAP	Contraseña para la autenticación por CHAP, suministrada por el ISP.	
Parámetros QoS de la interfaz		
Ancho de banda para descargas	Valora el ancho de banda en Kbit/seg para la descarga desde el ISP.	
Ancho de banda para cargas	Valora el ancho de banda en Kbit/seg para la carga al ISP.	

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Red / Internet**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de Internet**.
4) Desactive la casilla de verificación **Sin acceso a Internet**.
5) Active la opción **DSL directamente a interfaz WAN** y haga clic en **OK & Continuar**.
6) En la lista desplegable **Selección de ISP**, seleccione el tipo ISP estándar **PPTP de proveedor**.
7) En el área **Parámetros IP** active la casilla de verificación **Parámetros IP** solamente si el ISP requiere un ajuste. En tal caso, en los campos **Dir. IP colateral de conex. PPP**, **Dirección IP local de conex. PPP** y **Long. máx. paquetes datos (bytes)** indique los valores que le hayan

sido suministrados por su ISP. En la lista desplegable **Negociación dir. IP** seleccione la entrada **Utilizar dirección IP config.**.

8) En la sección **Parámetros PPTP**, indique los valores suministrados por su ISP.

9) Si tiene un modelo de tarifa basado en tiempo, active la casilla de verificación **Modo reten. breve**. En el campo **Tiempo reten. breve (s)**, indique el tiempo de inactividad tras el cual deberá interrumpirse la conexión (por ejemplo, 60 segundos).

10) Los ajustes de la sección **Autenticación** dependen de si su ISP exige o no una autenticación por PPP.

- El ISP solicita autenticación: asegúrese de que la casilla de verificación **Autenticación PPP** está activada. Indique como nombre de usuario PPP el nombre de acceso a Internet del ISP. Establezca la configuración PAP y CHAP siguiendo los ajustes suministrados por su ISP.
- El ISP no solicita autenticación: asegúrese de que la casilla de verificación Autenticación PPP está desactivada.

11) Si desea utilizar NAT, en la sección **Traduc. dirección**, active la casilla de verificación **NAT** (activada de forma predeterminada).

12) En la sección **Parámetros QoS de la interfaz** establezca estos valores:

a) En los campos **Ancho de banda para descargas** y **Ancho de banda para cargas**, seleccione el ancho de banda en Kbit/s para la descarga o para la carga. El valor le será suministrado por su ISP.

b) Si también quiere utilizar telefonía Internet, en la lista desplegable **Control ancho banda para conex. voz**, seleccione la entrada **Solo carga** o **Carga y descarga**, según sus necesidades. En el campo **Ancho banda para conex. voz/fax (%)** indique, en valores porcentuales, cuánto ancho de banda va a reservarse para las conexiones de voz y fax (valor estándar: 80%).

13) Haga clic en **OK & Continuar**. Es conducido a la ventana **Configurar cuenta DynDNs**.

14) Si desea utilizar la red privada virtual o el acceso remoto y no tiene una dirección IP estática pública, debe haber solicitado y configurado una cuenta DynDNS (por ejemplo, en dyndns.org).

a) Si su proveedor DynDNS aparece en la lista desplegable **Nombre dominio**, selecciónelo (p.ej. dyndns.org).

b) Si su proveedor DynDNS no aparece en la lista desplegable **Nombre dominio**, active la casilla de verificación **Dominio definido por el usuario**. En el campo **Nombre dominio**, introduzca el proveedor DynDNS deseado y en el campo **URL de actualización**, la URL de actualización del proveedor DynDNS. La estructura de la URL depende del proveedor DynDNS. Además, hay que indicar parámetros específicos del cliente (en el ejemplo, marcados en *cursiva*).

```
http://www.anydns.info/update.php?
user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>
```

c) Introduzca el **Nombre de usuario** y **Contraseña** de su cuenta DynDNS.

d) En el campo **Nombre host**, indique el nombre de host suministrado por el proveedor DynDNS sin el nombre de dominio, por ejemplo, mihost. Su nombre de dominio completo será, por ejemplo, mihost.dyndns.org.

e) Compruebe la cuenta DynDNS con **Prueba de conexión**.

f) Si la comprobación termina con éxito, haga clic en **Aceptar**.
g) Haga clic en **OK & Continuar**.

15) Si tiene una dirección IP estática pública o desea utilizar la red privada virtual o el acceso remoto, haga clic en **Sin DynDNS**.

16) Haga clic en **Salir**. El sistema de comunicación se reinicia.

10.1.3 Interfaz WAN

Se admite el uso de WAN (**W**ide **A**rea **N**etwork) para poder interconectar entre sí diferentes redes LAN (**L**ocal **A**rea **N**etwork) y distintos PC. En la interfaz WAN se puede conectar un módem Internet para el acceso a Internet.

La interfaz WAN no se puede usar para interconectar nodos de red ni para conectar extensiones o clientes IP.

10.1.4 DynDNS

DynDNS (Dynamic Domain Name Service) es un servicio de Internet que asigna un nombre DNS fijo a una dirección IP que cambia dinámicamente.

OpenScape Business X ofrece el servicio DynDNS si hay conectado un módem Internet con el puerto WAN de OpenScape Business X y el sistema de comunicación se utiliza como router Internet. Si no se así, DynDNS se configura en el router externo de la infraestructura del cliente.

Nombre DNS

Con DynDNS, un cliente que se conecta a Internet con una dirección IP dinámica, puede ser accedido siempre con el mismo nombre, el nombre DNS. Para hacerlo, se necesita tener una cuenta DynDNS en un proveedor DynDNS (por ejemplo, www.dyndns.org). Si se asigna una nueva dirección IP al sistema de comunicación (por ejemplo, por parte del SIP), la nueva dirección IP se envía automáticamente al proveedor DynDNS y se guarda en la cuenta DynDNS. Se puede configurar el intervalo de tiempo de la actualización. Si se accede a un nombre DNS, se envía una solicitud al proveedor DynDNS para que lo traduzca a la dirección IP válida en ese momento. El nombre DNS completo (también denominado nombre de dominio) se compone de un hombre de host a su elección (por ejemplo, myhost) y del proveedor DynDNS elegido (por ejemplo, dyndns.org), por ejemplo mihost.dyndns.org. Puede encontrar más información, por ejemplo, en la dirección de Internet:

`http://www.dyndns.org/services/dyndns`

Con DynDNS también se puede crear una red privada virtual (VPN) a través de un ISP que suministre direcciones IP dinámicas. De esta forma, por ejemplo, los teletrabajadores pueden acceder a la red interna a través de Internet. Puede encontrar información adicional en Red privada virtual VPN .

Mail Exchanger

El registro Mail Exchange (MX-Record) del DNS (Domain Name Service), indica a qué dirección IP se enviarán los correos electrónicos de los nombres de dominio configurados (por ejemplo, mihost.dyndns.org). El servidor de correo (Mail Exchanger) debe estar situado detrás de la dirección IP indicada.

Una dirección de correo electrónico para este nombre de dominio sería, por ejemplo, así: mimail@mihost.dyndns.org.

Con la función Backup MX, los correos electrónicos que no se pudieron integrar al Mail-Exchanger indicado arriba, se guardan en la memoria intermedia y se entregan en cuanto Mail Exchanger vuelve a estar disponible.

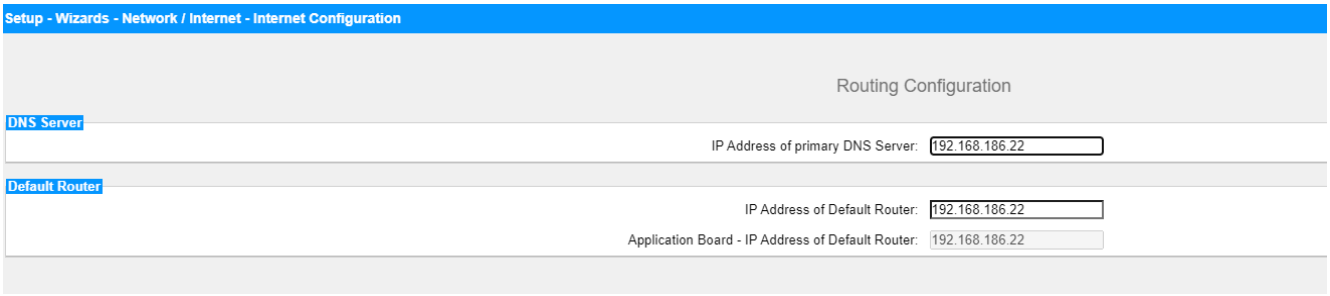
10.1.4.1 Cómo configurar el servicio DynDNS

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

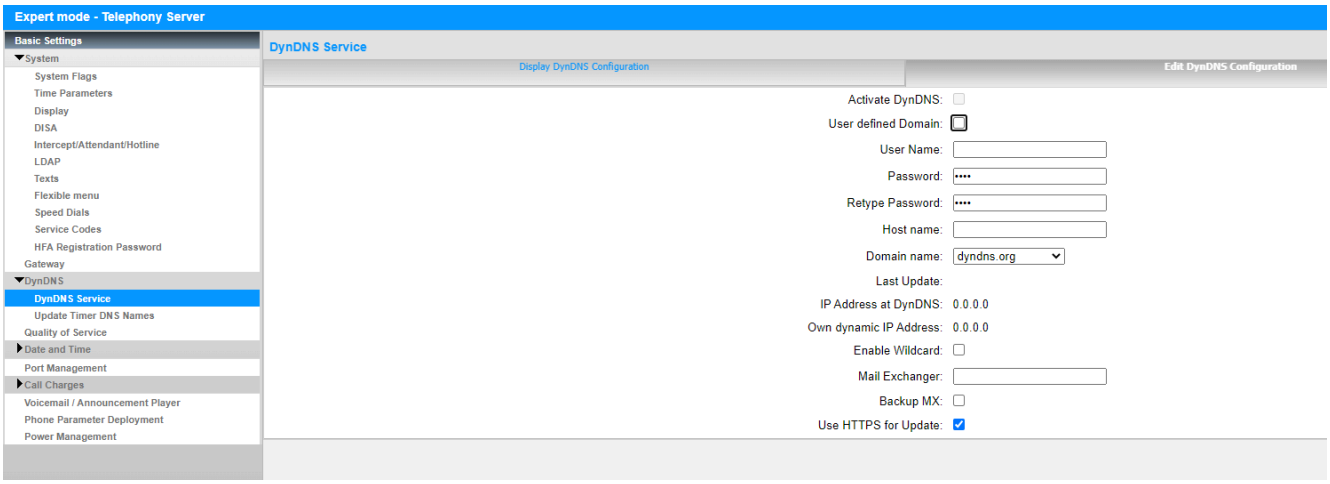
1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **DynDNS**.
4) Haga clic en **Tiempo actualiz. nombres DNS**.



5) Active la opción **Actualizar nombres DNS**.
6) Este valor de tiempo solo es válido para VPN: en el campo **Valor timer para actualiz. de nombres DNS (s)**, indique el tiempo en segundos tras el que el componente VPN comprobará si los nombres DNS en uso de la configuración VPN se resuelven con nuevas direcciones IP (VPN con direcciones IP dinámicas). En tal caso, VPN se configura de nuevo con las nuevas direcciones IP.

   El campo tiene como valor estándar `180`, lo que corresponde a un intervalo de actualización de 3 minutos.
7) En el grupo de menús, haga clic en **Servicio DynDNS**.

8) Haga clic en la pestaña **Editar configuración DynDNS**.



9) Active la casilla de verificación **Activar DynDNS**.

10) Si su proveedor DynDNS aparece en la lista desplegable **Nombre dominio**, selecciónelo (p.ej. dyndns.org).

11) Si su proveedor DynDNS no aparece en la lista desplegable **Nombre dominio**, active la casilla de verificación **Dominio definido por el usuario**. En el campo **Nombre dominio**, introduzca el proveedor DynDNS deseado y en el campo **URL de actualización**, la URL de actualización del proveedor DynDNS. La estructura de la URL depende del proveedor DynDNS. Además, hay que indicar parámetros específicos del cliente (en el ejemplo, marcados en *cursiva*).

`http://www.anydns.info/update.php?`
`user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`

Ejemplo de una URL de actualización con autenticación cifrada con Base64:

`https://<b64><username>:<pass></`
`b64>@members.dyndns.org/nic/update?`
`hostname=<domain>&myip=<ipaddr>&wildcard=NOCHG&mx=NOCHG&backmx`

<b64>...</b64> para parámetros codificados con Base64

12) En el campo **Nombre de usuario** indique el nombre de usuario de su cuenta DynDNS de su proveedor.

13) En los campos **Contraseña** y **Repetir contraseña**, indique la contraseña de la cuenta DynDNS de su proveedor.

14) En el campo **Nombre host**, indique el nombre de host suministrado por el proveedor DynDNS sin el nombre de dominio, por ejemplo, mihost. Su nombre de dominio completo será, por ejemplo, mihost.dyndns.org.

15) Solo se puede ver con proveedores DynDNS incluidos en la lista desplegable **Nombre dominio**: Active el campo de opción **Act. comodín** para aceptar también consultas a un nombre de dominio subordinado, como beliebig.myhost.dyndns.org.

16) Solo se puede ver con proveedores DynDNS incluidos en la lista desplegable **Nombre dominio**: Active el campo de opción **Utilizar HTTPS para actualiz.** para que la dirección IP se actualice mediante una conexión segura con el proveedor DynDNS.

17) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

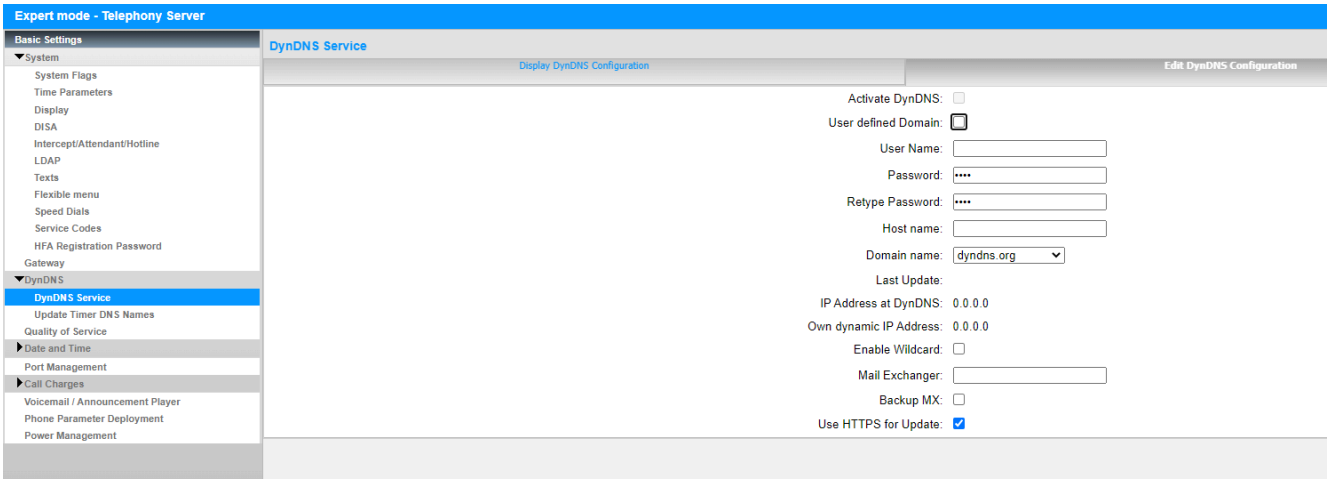
10.1.4.2 Cómo definir Mail Exchanger

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **DynDNS**.
4) Haga clic en **Servicio DynDNS**.
5) Haga clic en la pestaña **Editar configuración DynDNS**.



6) En el campo **Mail Exchanger**, indique la dirección IP del servidor de correo (registro Mail Exchange o MX-Record).
7) Si es necesario, active la opción **Backup MX**.
8) Haga clic en **Aplicar**, seguido de **Aceptar**.

10.2 Línea urbana mediante ITSP

Para poder telefonear por Internet, requiere acceso a un proveedor de servicios de telefonía por Internet (ITSP, SIP-Provider). Para ello, hay que solicitar a un ITSP una conexión de telefonía por Internet y una cuenta de usuario.

Conexión con el ITSP

El sistema de comunicación utiliza las opciones descritas en el capítulo "acceso a Internet" para contactar con el ITSP (OpenScape Business X: por LAN o WAN / OpenScape Business S: solo por LAN).

El acceso de ITSP se basa en SIP (Session Initiation Protocol) para la señalización y en RTP (Realtime Transport Protocol) para voz y datos.

No todos los proveedores de servicios de telefonía Internet ofrecen el mismo abanico de prestaciones SIP. Por ello para el sistema de comunicación solo deberían usarse ITSP certificados. En el siguiente enlace encontrará una lista con los ITSP certificados y el proceso de certificación:

http://wiki.unify.com/wiki/Collaboration_with_VoIP_Providers

Nota: Los números de teléfono especiales y los números de llamada de emergencias que el ITSP no admita se ejecutan a través de las conexiones de red fija.

Si se produce una caída del ITSP, se puede implementar una solución de respaldo con las conexiones de red fija a través de Least Cost Routing (LCR).

Cuenta de usuario ITSP

La cuenta de usuario ITSP (Cuenta de usuario SIP) se solicita al ITSP. El ITSP ofrece para ello un servidor de registrador SIP en el que previamente se debe registrar el sistema de comunicación (depende del proveedor).

Nota: No es necesario hacer un registro si el ITSP utiliza autenticación IP o túneles VPN.

Número de Mobile Extension (MEX)

Algunos operadores de telefonía móvil ofrecen esta prestación junto con el servicio MDA (Mobile Direct Access). De esta forma, se pueden integrar en un sistema de comunicación teléfonos móviles/smartphones como extensiones internas.

Esta prestación solo se puede utilizar con una conexión de marcación directa de telefonía por Internet. Para ello, al configurar el ITSP hay que registrar el número MEX que haya proporcionado el ITSP. En el ITSP, el número de teléfono móvil está vinculado con el número MEX. Además, el teléfono móvil/smartphone debe estar configurado en el sistema de comunicación como extensión Mobility (véase Configuración de myPortal to go y Mobility Entry).

Descripción breve:

- El operador de telefonía móvil ofrece una tarifa planta para el teléfono móvil.
- One Number Service: se puede acceder al teléfono móvil con un solo número de red fija que también se transmite al interlocutor.
- El estado de presencia y el estado de conexión de los teléfonos móviles se pueden ver como con las extensiones internas.
- Todas las llamadas en las que participen teléfonos móviles se realizan a través de OpenScape Business en combinación con un ITSP certificado.
- El número de teléfono móvil no es conocido en el exterior, es decir, no se puede llamar directamente al teléfono móvil. El teléfono, a su vez, tampoco puede realizar llamadas salientes directas. Todas las llamadas pasan por OpenScape Business.
- El teléfono móvil se puede integrar el equipos internos del sistema.
- Las aplicaciones de UC como myPortal for Desktop y myPortal for Outlook se pueden utilizar como en las extensiones internas.
- myPortal to go se puede utilizar de forma móvil.
- Cuando se realizan llamadas en extensiones internas, los teléfonos móviles integrados se identifican con el nombre.
- La evaluación de la marcación y el Call Routing en el sistema o en la red se realizan como en cualquier otra extensión interna (p.ej., números de teléfono autorizados, números de teléfono prohibidos, reglas LCR).

- El ITSP utiliza una señalización especial de las llamadas desde/hacia OpenScape Business, que hay que administrar pertinentemente.
- Todos los teléfonos móviles integrados requieren una licencia Mobility User.
- Para utilizar aplicaciones de UC, se requiere también una licencia UC Client.

10.2.1 Configuración de un ITSP

Se pueden configurar proveedores de servicios de telefonía (ITSP) por Internet nuevos y predefinidos. Por cada ITSP se pueden configurar una o varias cuentas. Puede haber activos hasta 8 ITSP de manera simultánea.

Encontrará más información sobre ITSP y sus prestaciones aquí:

`http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#Overview`

Nota: En Internet, en la **wiki para expertos en Internet** (*OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*, puede consultar ejemplos de configuración.

Asignación de los números de teléfono de ITSP

- En las **conexiones de extensión de telefonía por Internet**, el ITSP proporciona números de teléfono individuales (p.ej. 70005555, 70005556, etc.). Estos números se asignan de forma manual a los números de teléfono internos de las extensiones.
- En las **conexiones de centralita de telefonía por Internet**, el ITSP proporciona un área de números de teléfono (p.ej. de (+49) 89 7007-100 a (+49) 89 7007-147). Los números de teléfono del área se asignan de forma manual a los números de teléfono internos de las extensiones.

Los dos tipos de conexión se pueden combinar.

Como alternativa, para ambos tipos de conexión, en la configuración de las extensiones se pueden registrar los números de teléfono del ITSP como números de marcación directa de las extensiones.

Número de llamada Interno	Nombre	Marc. dir.
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

Los números de teléfono del ITSP resultan del número de teléfono de centralita configurado (p.ej. código de país 49) y de los números de marcación directa registrados en formato largo. Esto supone ciertas ventajas en la evaluación de la marcación y la gestión de llamadas, también en una interred. Así, por ejemplo, la conexión ITSP tiene capacidad de marcación directa a otro nodo.

En este caso, solo se puede establecer otra conexión de línea urbana mediante RDSI con restricciones.

Gestión multisitio

Los usuarios del sistema de comunicación pueden asignarse a diferentes sitios (por ejemplo, con distintos códigos de área). Cada sitio está asignado a una ruta y cada ruta, a un registro de ITSP. Se pueden administrar 8 registros de ITSP como máximo. Es posible un registro por ITSP o varios registros en un solo ITSP. Se puede asignar un prefijo local a cada registro de ITSP y, a continuación, varias extensiones. La conexión de las extensiones de las diferentes ubicaciones con el sistema de comunicación se realiza mediante VPN. Todos los sitios deben estar ubicados en un país y utilizar el mismo código urbano (consulte también *Interconexión de OpenScape Business en entornos de hosting*, escenario 1b).

Uso de plantillas de ITSP

Lo estándar es usar una plantilla de ITSP preconfigurada. En estas plantillas se registran los números de acceso y los números de teléfono propios y, a continuación, se activan.

En el modo Experto también se puede modificar una plantilla de ITSP preconfigurada y guardarla como nueva.

Actualización de plantillas de ITSP

Las plantillas de ITSP preconfiguradas se actualizan automáticamente tras una actualización de software del sistema, siempre que en esa actualización haya nuevas plantillas de ITSP preconfiguradas o valores estándares más actuales para plantillas preconfiguradas existentes.

Si ya está activado el ITSP de una plantilla, la actualización no se realiza automáticamente, ya que en la actualización de los valores estándares se podrían sobrescribir ajustes importantes. Por esto, la actualización se puede ejecutar de forma manual a través del modo Experto en caso necesario. A continuación hay que ajustar de nuevo los valores estándares según las necesidades.

Modo de dirección de línea

Los diferentes canales de una línea ITSP se pueden bloquear para el tráfico entrante o saliente. Se pueden utilizar los siguientes modos de dirección de línea:

- Solo salientes
- Solo entrantes
- Salientes y entrantes (estándar)

La dirección de la línea se evalúa cuando el sistema de comunicación debe reservar una línea ITSP para una llamada entrante o saliente.

10.2.1.1 Cómo configurar un ITSP predefinido

El asistente de **telefonía por Internet** se puede utilizar para configurar y activar un proveedor de servicios de telefonía por Internet (ITSP) predefinido. Puede configurar una o varias cuentas para cada ITSP.

Requisitos previos

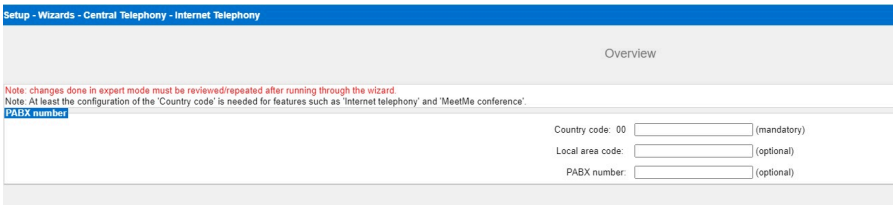
La conexión a Internet está lista para el servicio.

Los datos de acceso de telefonía por Internet de su ITSP están disponibles (por ejemplo, cuenta de usuario, contraseña y número de telefonía por Internet).

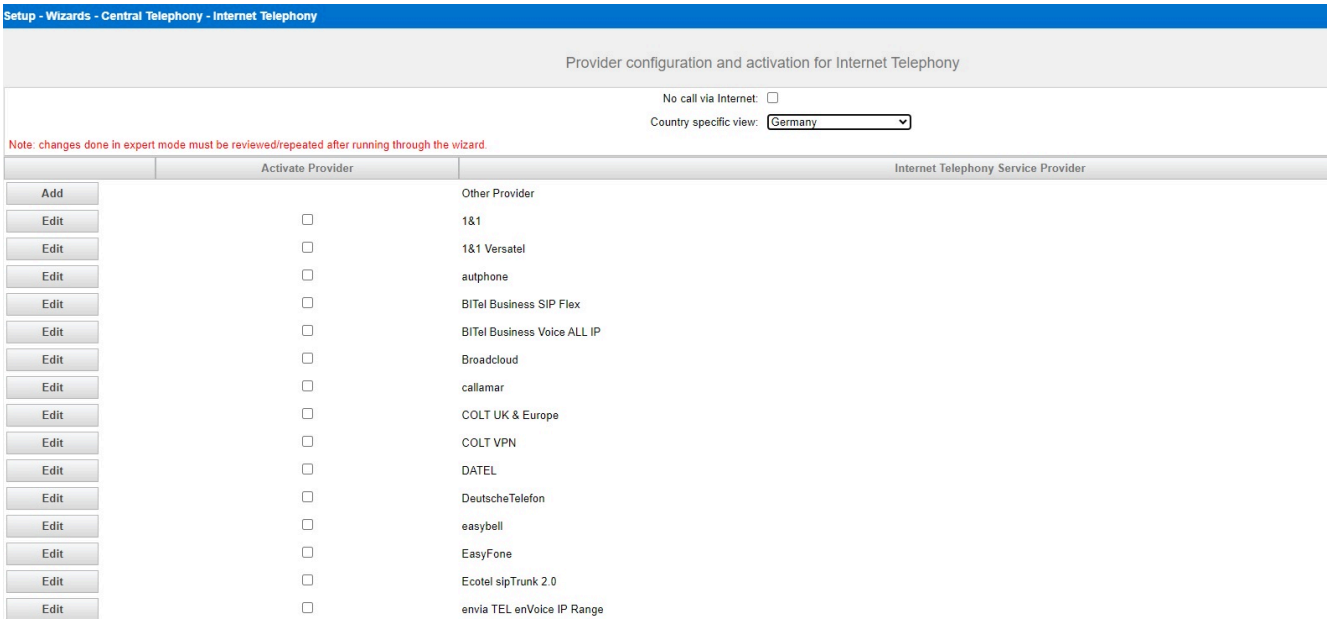
Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Telefonía por Internet**.



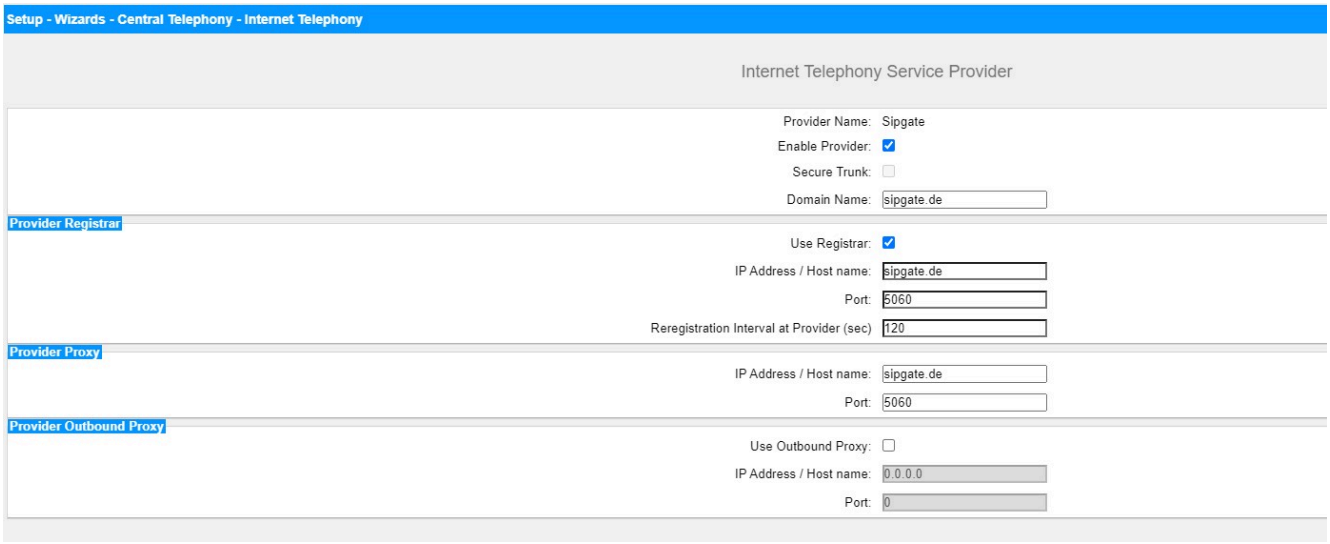
4) Borre la casilla de verificación **No hay llamada vía Internet**. Se muestra una lista de los ITSP disponibles en función del país. La lista contiene los ITSP predefinidos para el país seleccionado y los ITSP que ha creado.



5) Si desea modificar el país preestablecido, en la lista desplegable **Vista específica de país** seleccione el país deseado. Se muestran los ITSP disponibles para el país seleccionado.
6) Si es necesario, haga clic en **Mostrar estado**, para consultar qué ITSP están ya activados y qué extensiones de telefonía Internet están configuradas para cada uno de los ITSP. Se pueden activar, como máximo, 8 ITSP. Haga clic en **Aceptar** cuando esté terminado.
7) Para configurar el ITSP predefinido, haga clic en **Editar** en la línea asociada al ITSP deseado.
8) Active la casilla de verificación **Activar proveedor**.
9) Si el proveedor admite una conexión segura, se puede activar la casilla de verificación **Troncal segura**.

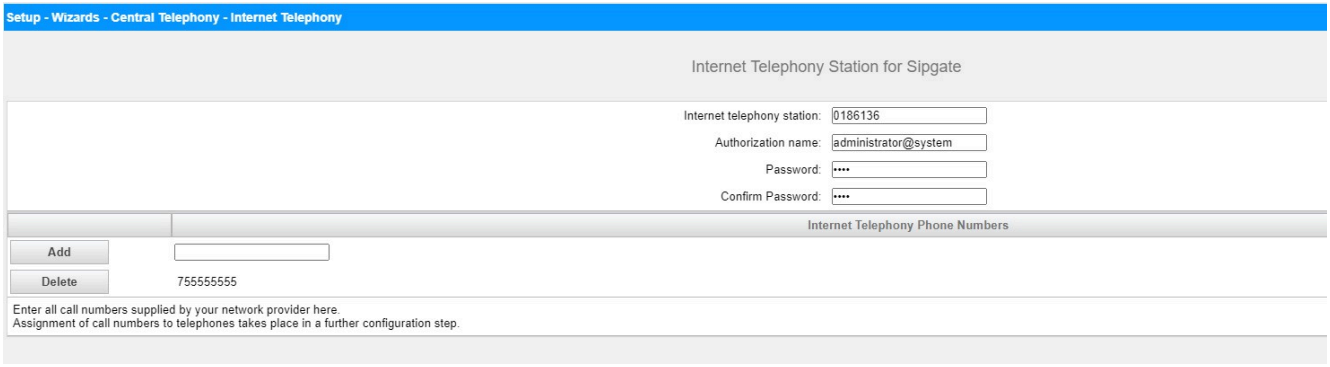
10) Los valores para "**Registrador del proveedor**", "**Proxy del proveedor**", "**Proxy de salida del proveedor**" y "**Función del proveedor**" (si está habilitado) están predefinidos según las necesidades de la mayoría de los ITSPs. Para algunos ITSP se utilizan direcciones de servidor específicas del cliente. En tal caso, los campos que no aparecen en gris se deben completar de acuerdo con la documentación recibida del ITSP.

11) Si el proveedor admite el desvío de llamadas, se muestra la sección Función del proveedor y puede activar la función de desvío de llamadas. Cuando la desviación de llamadas está activada, el reenvío de llamadas se realiza en la red del proveedor, la gestión de llamadas en el sistema no es efectiva.



12) Haga clic en **Aceptar & Siguiente**.

13) Haga clic en **Agregar** para configurar sus cuentas ITSP con los números de telefonía Internet correspondientes. Los campos que aparecen dependen del proveedor.



14) En el campo **Extensión de telefonía por Internet**, introduzca los datos de acceso de su cuenta. Los datos le son suministrados por su ITSP. En función del ITSP se utilizarán aquí distintas denominaciones (por ejemplo, Usuario SIP, ID SIP, etc.

Se pueden encontrar más detalles en http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers

15) En el campo **Nombre de autorización**, introduzca el nombre de autorización. Los datos le son suministrados por su ITSP. Si no ha recibido

ningún nombre de autorización, indique los mismos datos en **Extensión de telefonía por Internet**.

Nota: Si no se utiliza ningún registro, **Nombre de autorización** está en gris y no se puede configurar.

---

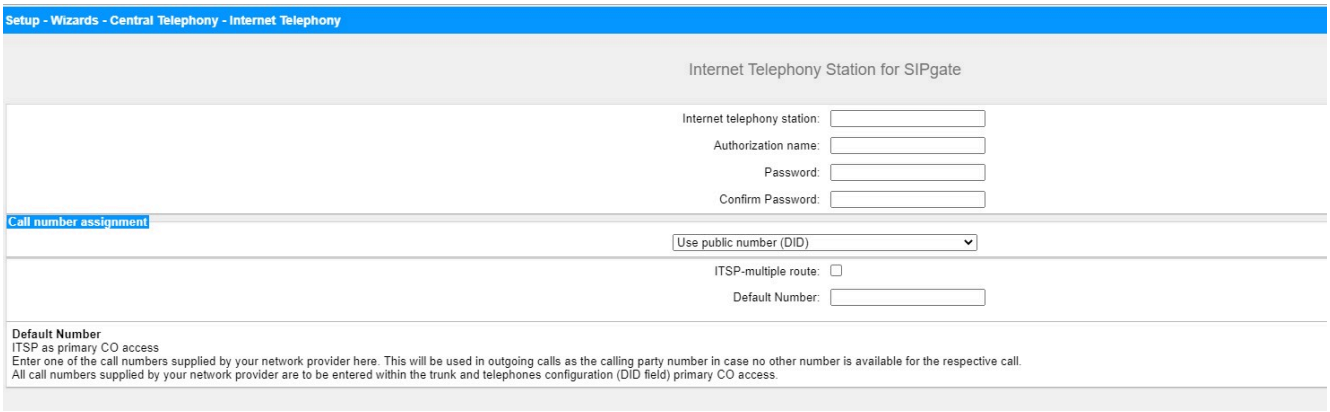
16) En los campos **Nueva contraseña** y **Repetir clave** introduzca la contraseña que le ha suministrado el ITSP. En función del ITSP se utilizarán aquí distintas denominaciones (por ejemplo, Contraseña, Contraseña SIP, etc.)

Nota: Si no se utiliza ningún registro, **Contraseña** está en gris y no se puede configurar.

---

17) Asignación de números de teléfono de telefonía por Internet - Opción 1:

Utilizar número público (DID): los números de teléfono de telefonía por Internet (DID) de su conexión de telefonía por Internet se configuran en la configuración de las estaciones (en los campos **DID**). No es necesaria ninguna configuración de mapeo durante la configuración de ITSP.

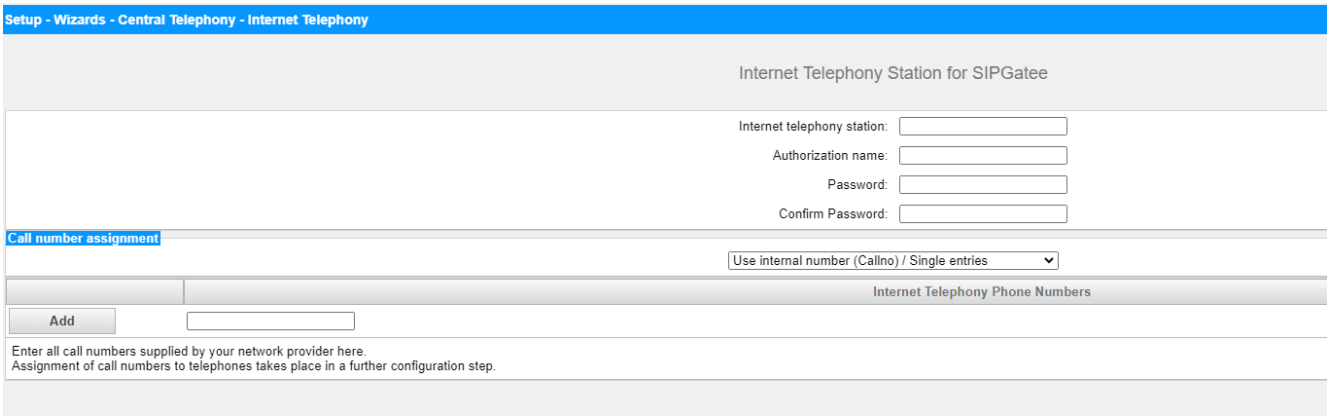


a) En el área **Asignación de números de teléfono**, seleccione el campo de opción **Número de teléfono público (DuWa)**.
b) En **Número predeterminado**, ingrese el número de teléfono que se utilizará para las llamadas salientes cuando no haya ningún número DID de la persona que llama disponible.
c) Si su ITSP admite la prestación "Mobile Extension (MEX)", en **Número MEX** introduzca el número MEX que le haya proporcionado el ITSP (8 posiciones, solo números). Si su ITSP no admite la función "Extensión móvil (MEX)", el campo **Número MEX** no se muestra.
d) Si es necesario configurar varias rutas, active la casilla de verificación **ITSP-múltiples rutas**.
e) Ingrese los **prefijos de ruta ITSP** asignados a la ruta y haga clic en **Agregar**.

18) Asignación de números de teléfono de telefonía por Internet - Opción 2:

Usar número interno (CalIno) / Entradas individuales: Tiene un ITSP que necesita el registro SIP para cada número de llamada (por ejemplo, 70005555, 70005556,...). Para cada número de llamada se debe crear una estación de telefonía por Internet y asignar un único número de llamada.

Si su ITSP permite múltiples números de llamada con un solo registro, se debe utilizar la Opción 1.



a) En el área **Asignación de números de teléfono**, seleccione el campo de opción **Utilizar número interno (n.º llamada)/Entradas individuales**.

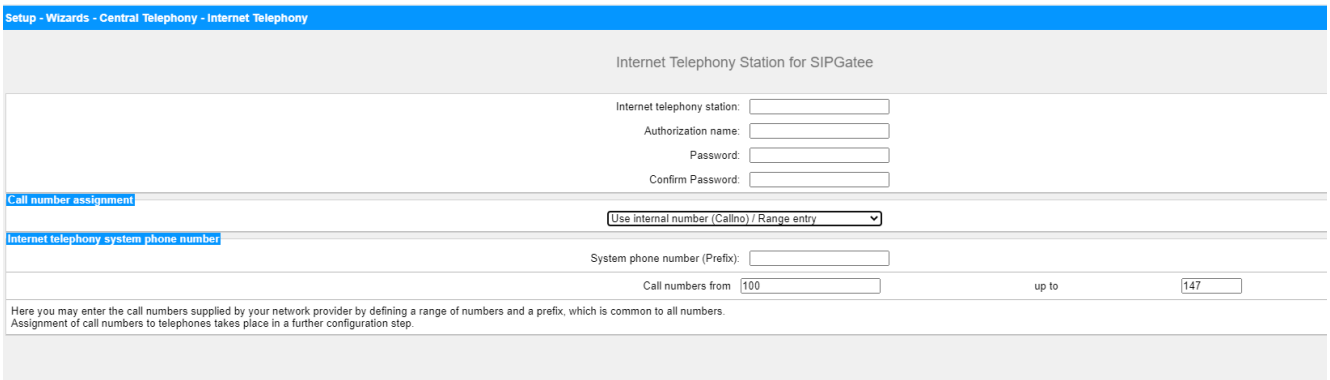
b) En el área **Números de llamada de extensión de telefonía DSL**, y en el campo junto al botón **Agregar**, introduzca un número de teléfono de telefonía Internet que le haya sido comunicado por el proveedor de servicios de telefonía por Internet y haga clic en **Agregar**.

c) Si desea asignar a la cuenta más números de telefonía Internet, repita el paso b).

19) Asignación de números de teléfono de telefonía por Internet - Opción 3:

Utilizar número interno (CalIno) / Entrada de rango:el uso de esta opción está obsoleto, para la configuración DID se debe utilizar la opción 1.

Tiene una conexión de centralita de telefonía por Internet y ha recibido un intervalo de números de teléfono como números de teléfono de telefonía Internet, por ejemplo (+49) 89 7007-100 a (+49) 89 7007-147. A continuación, asigne los números de llamada del intervalo de números de llamada a los números de llamadas internas de los suscriptores.



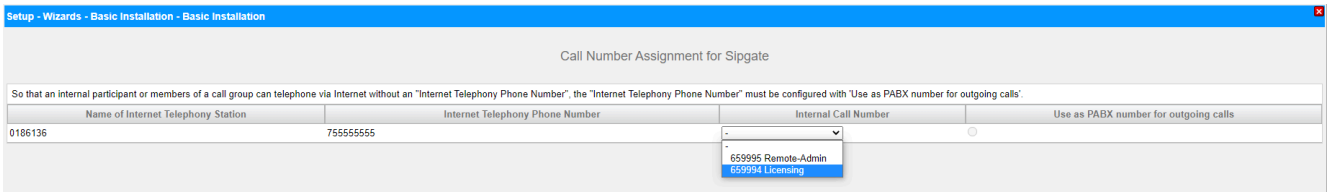
a) En el área **Asignación de números de teléfono**, seleccione el campo de opción **Utilizar número interno (n.º llamada)/Intervalo**.

b) En **Número de llamada del sistema (prefijo)** introduzca el número de teléfono del sistema.

c) En los campos **Rango de marcación directa de** y **hasta** indique el rango de marcación directa deseado para la extensión de telefonía por Internet. Por defecto están registrados los valores 100 - 147.

20) Haga clic en **Aceptar & Siguiente**.
21) Si desea configurar cuentas adicionales, repita los pasos 13 hasta 20.
22) Haga clic en **Aceptar & Siguiente**. Verá un resumen con los números de teléfono de telefonía Internet asignados y a qué cuentas lo están.
23) Asigna todos los números de telefonía por Internet a un número de teléfono interno de una extensión.

    No es necesario dar este paso si para asignar los números de telefonía por Internet ha seleccionado la opción 1. En este caso, la asignación se realiza en la configuración de las extensiones, en el campo **DuWa**. La pantalla también es visible en este caso pero no editable.



    a) En la línea correspondiente de la lista desplegable **N.° llam. interno** seleccione un número de teléfono interno.
    b) Si desea permitir que extensiones sin número de telefonía Internet o que los miembros de un grupo de llamadas realicen llamadas telefónicas externas por Internet, active el campo de opción **Utilizar como número de llamada del sistema saliente**. El campo de opción solo puede estar activado en un único número de telefonía Internet.

24) Haga clic en **Aceptar & Siguiente**. Aquí podrá ver nuevamente una descripción general de los posibles ITSP. Los ITSP activados aparecen marcados en la columna **Activar proveedor** con un signo de verificación. Con Mostrar Estado puede comprobar el estado de la conexión. Si tiene problemas de conexión con un ITSP ya activado, puede registrarlo nuevamente con **Reiniciar ITSP** en esta página.
25) Haga clic en **Aceptar & Siguiente**.
26) En el campo **Flujo saliente hasta (kbps)**, introduzca el valor de la velocidad de carga de su conexión a Internet. No debe confundirse con la velocidad de descarga.

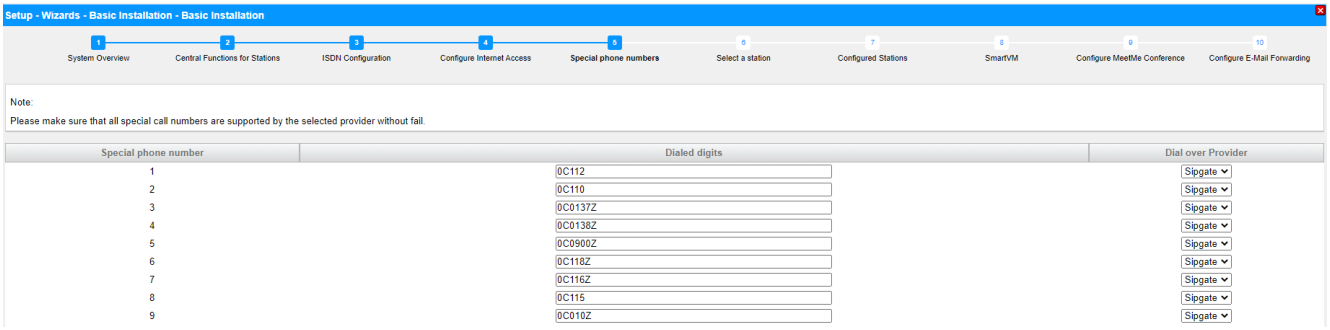
    Nota: En el campo **Cantidad de llamadas telefónicas Internet simultáneas** se indica el número de llamadas telefónicas Internet que puede realizar simultáneamente. Si la carga de red tiene efectos negativos en la calidad de las llamadas, reduzca el número.

    Para obtener más información sobre la cantidad de llamadas simultáneas por Internet, consulte Restricción del número de llamadas simultáneas por ITSP en la página 842.

    ---

27) Haga clic en **Aceptar & Siguiente**.

28) En la columna **Cifras marcadas** introduzca los números de teléfono especiales deseados.



Son válidas estas entradas de número de teléfono:

- 0 a 9: dígitos permitidos
- -: Separador de campos
- X: Cualquier dígito del 0 al 9
- N: Cualquier dígito del 2 al 9
- Z: Siguen, hasta el final de la marcación, uno o varios dígitos
- C: Tono de marcado simulado (se puede ingresar hasta tres veces)

29) En la columna **Marcar a través de proveedor** seleccione si el número de teléfono especial se marcará a través de RDSI o a través de un ITSP. Solo aparecen los ITSP activos.

Nota: Asegúrese de que siempre se pueden marcar los números de teléfono de emergencia. Si desea que los números de teléfono de emergencia se marquen a través de un ITSP, el proveedor debe admitir la función.

---

30) Haga clic en **Aceptar & Siguiente**. Se muestra el estado de los ITSP.

31) Haga clic en **Siguiente** seguido de **Finalizar**. A continuación de este paso, ejecute el asistente de **CO Trunk ISDN/Analog/ITSP** para establecer la priorización para la toma de línea de intercambio (por ejemplo: Toma de línea de intercambio (primero a través de ITSP y luego a través de ISDN).

10.2.1.2 Cómo agregar un nuevo ITSP

El asistente de **telefonía por Internet** se puede utilizar para configurar y activar un nuevo proveedor de servicios de telefonía por Internet (ITSP). Puede configurar una o varias cuentas para cada ITSP.

Requisitos previos

La conexión a Internet está lista para el servicio.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Están disponibles los siguientes datos de acceso a Internet específicos del ITSP:

Campo	Descripción	Valor del ISP
Nombre de dominio de Gateway	Nombre de dominio de Gateway del ITSP Generalmente idéntico al nombre de host (por ejemplo, sip-voice.de)	
Registrador de proveedores		
Registrador de uso	Predefinido por el ITSP y generalmente siempre configurado (no es necesario para los ITSP que usan autenticación de IP estática).	
Dirección IP/Nombre de host	Nombre de host o dirección IP del servidor del registrador (por ejemplo, sip-voice.de).	
Puerto	Número de puerto del servidor del registrador (por ejemplo, 5060).	
Intervalo de reinscripción en el proveedor (seg.)	Intervalo (en segundos) en el que se repite el registro ITSP. El valor del intervalo no debe ser 0 ni demasiado alto, ya que al repetir el registro en el ITSP también se puede detectar una conexión interrumpida y se puede seleccionar una ruta alternativa (a través de ISDN o un proveedor alternativo) si es necesario. Valor estándar: 120 segundos.	
Proxy del proveedor		
Dirección IP/Nombre de host	Nombre de host o dirección IP del servidor proxy (por ejemplo, sip-voice.de). Esto suele ser idéntico a la entrada del Registrador del proveedor.	
Puerto	Número de puerto del servidor proxy (por ejemplo, 5060). Generalmente esto es idéntico al número de puerto del registrador del proveedor.	
Característica del proveedor		
Desvío de llamadas	Visible solo si la plantilla base seleccionada admite la desviación de llamadas	
Proxy de salida del proveedor		
Utilizar proxy de salida	Sólo se establece si el ITSP utiliza un proxy saliente.	
Dirección IP/Nombre de host	Nombre de host o dirección IP del proxy saliente	
Puerto	Número de puerto del proxy de salida	
Proxy entrante del proveedor		

Campo	Descripción	Valor del ISP
Utilizar proxy entrante	Sólo se establece si el ITSP utiliza un segundo proxy.	
Dirección IP/Nombre de host	Nombre de host o dirección IP del segundo proxy	
Puerto	Número de puerto del segundo proxy	
Proveedor STUN		
Usar STUN	Se usa sólo si se requiere la funcionalidad STUN. También habilita el modo STUN global.	
Dirección IP/Nombre de host	Dirección IP STUN si el ITSP está utilizando un servidor STUN.	
Puerto	Número de puerto STUN si el ITSP está utilizando un servidor STUN.	

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Telefonía por Internet**.
4) Borre la casilla de verificación **No hay llamada vía Internet**. Se muestra una lista de los ITSP disponibles en función del país. La lista contiene el ITSP predefinido para el país seleccionado y el ITSP ya creado (si lo hay).
5) Si es necesario, haga clic en **Mostrar estado**, para consultar qué ITSP están ya activados y qué extensiones de telefonía Internet están configuradas para cada uno de los ITSP. Se pueden activar, como máximo, 8 ITSP. Haga clic en **Aceptar** cuando esté terminado.
6) Haga clic en **Agregar** para establecer un nuevo ITSP. Aparece una ventana de configuración para el nuevo ITSP.
7) Seleccione una **plantilla base** de la lista desplegable. Esta opción permite tener el mismo ITSP configurado en varias rutas.
8) Asigne un nombre de su elección para el ITSP en el campo **Nombre del proveedor**.

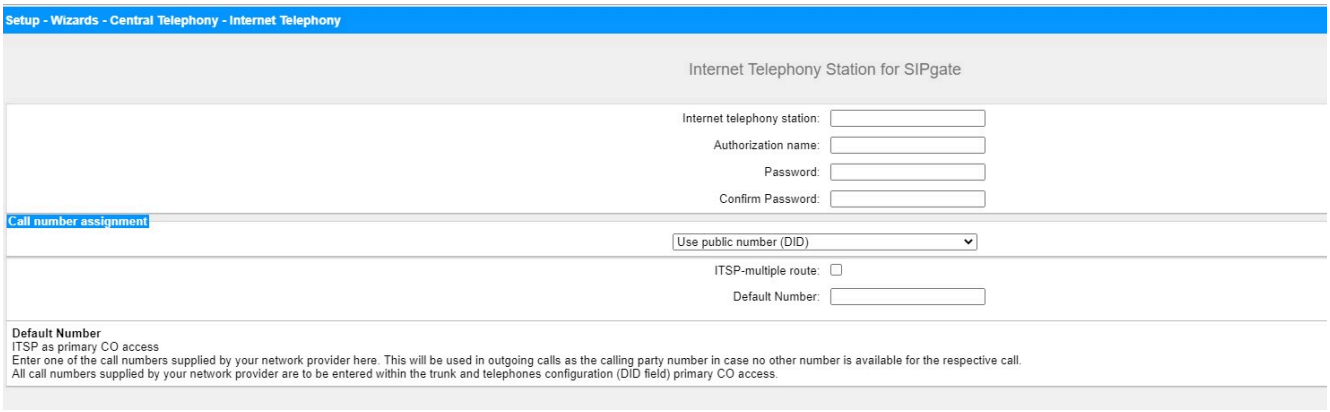
   Nota: El límite máximo de caracteres es 10.

9) Active la casilla de verificación **Activar proveedor**.
10) Ingrese los valores proporcionados por su ITSP en las áreas restantes (consulte la tabla inmediatamente después de los requisitos previos).

    Nota: Los valores bajo "Datos extendidos del proveedor SIP" sólo pueden ser modificados por personal de servicio autorizado, en colaboración con Desarrollo!

11) Haga clic en **Aceptar & Siguiente**.

12) Haga clic en **Agregar** para configurar sus cuentas ITSP con los números de telefonía Internet correspondientes. Los campos que aparecen dependen del proveedor.



13) En el campo **Extensión de telefonía por Internet**, introduzca los datos de acceso de su cuenta. Los datos le son suministrados por su ITSP. En función del ITSP se utilizarán aquí distintas denominaciones (por ejemplo, Usuario SIP, ID SIP, etc.

    Se pueden encontrar más detalles en http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers

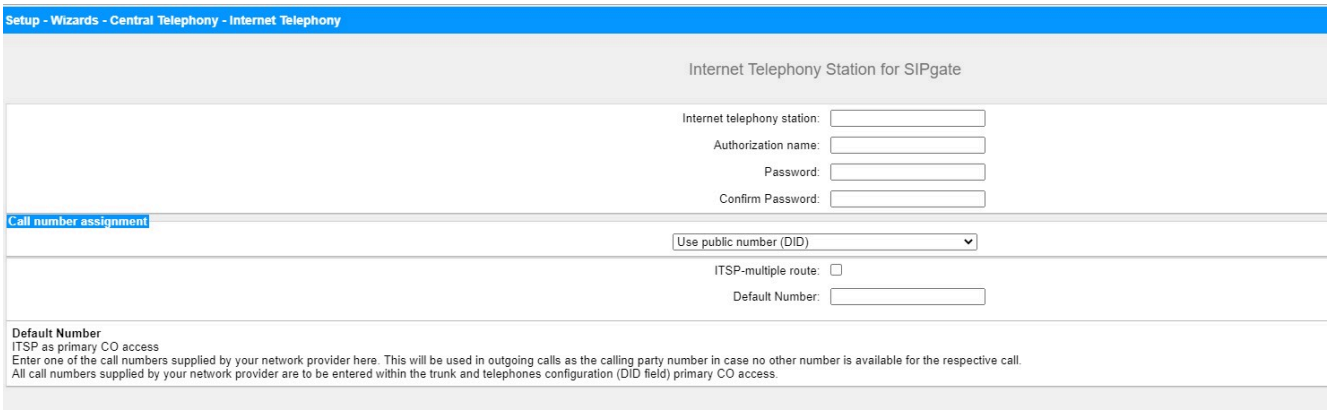
14) En el campo **Nombre de autorización**, introduzca el nombre de autorización. Los datos le son suministrados por su ITSP. Si no ha recibido ningún nombre de autorización, indique los mismos datos en **Extensión de telefonía por Internet**.

15) En los campos **Nueva contraseña** y **Repetir clave** introduzca la contraseña que le ha suministrado el ITSP. En función del ITSP se utilizarán aquí distintas denominaciones (por ejemplo, Contraseña, Contraseña SIP, etc.)

16) Asignación de números de teléfono de telefonía por Internet - Opción 1:

    Utilizar número público (DID): los números de teléfono de telefonía por Internet (DID) de su conexión de telefonía por Internet se configuran en

la configuración de las estaciones (en los campos **DID**). No es necesaria ninguna configuración de mapeo durante la configuración de ITSP.



a) En el área **Asignación de números de teléfono**, seleccione el campo de opción **Número de teléfono público (DuWa)**.
b) En **Número predeterminado**, ingrese el número de teléfono que se utilizará para las llamadas salientes cuando no haya ningún número DID de la persona que llama disponible.
c) Si su ITSP admite la prestación "Mobile Extension (MEX)", en **Número MEX** introduzca el número MEX que le haya proporcionado el ITSP (8 posiciones, solo números).
d) Activar la casilla de verificación **ITSP-ruta múltiple**.
e) Ingrese los **prefijos de ruta ITSP** asignados a la ruta y haga clic en **Agregar**.

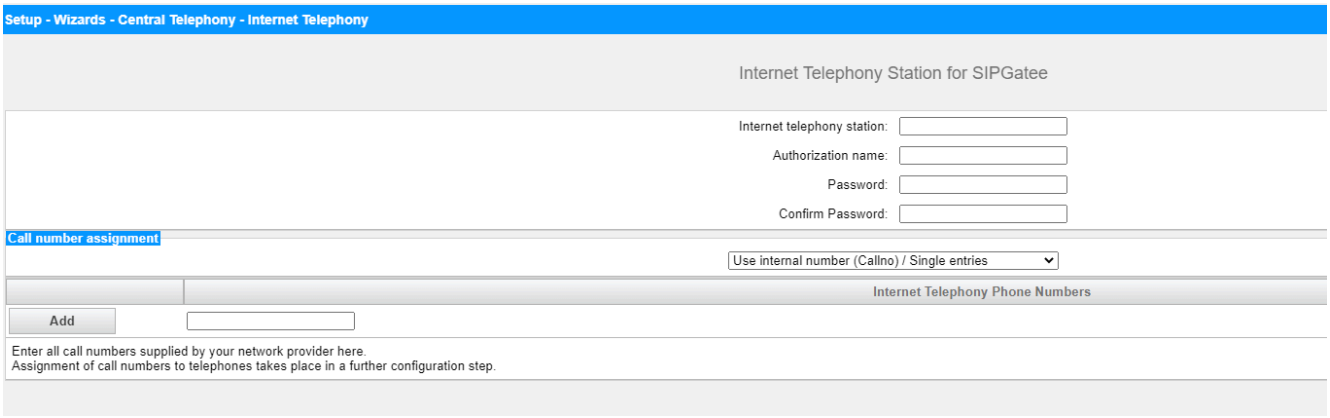
Nota: Para configurar varias rutas es necesario repetir los pasos anteriores. Puede encontrar más información en la wiki de Unify en: http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#…General_Configuration_guides

---

17) Asignación de números de teléfono de telefonía por Internet - Opción 2:

Usar número interno (CalIno) / Entradas individuales: Tiene un ITSP que necesita el registro SIP para cada número de llamada (por ejemplo, 70005555, 70005556,...). Para cada número de llamada se debe crear una estación de telefonía por Internet y asignar un único número de llamada.

Si su ITSP permite múltiples números de llamada con un solo registro, se debe utilizar la Opción 1.

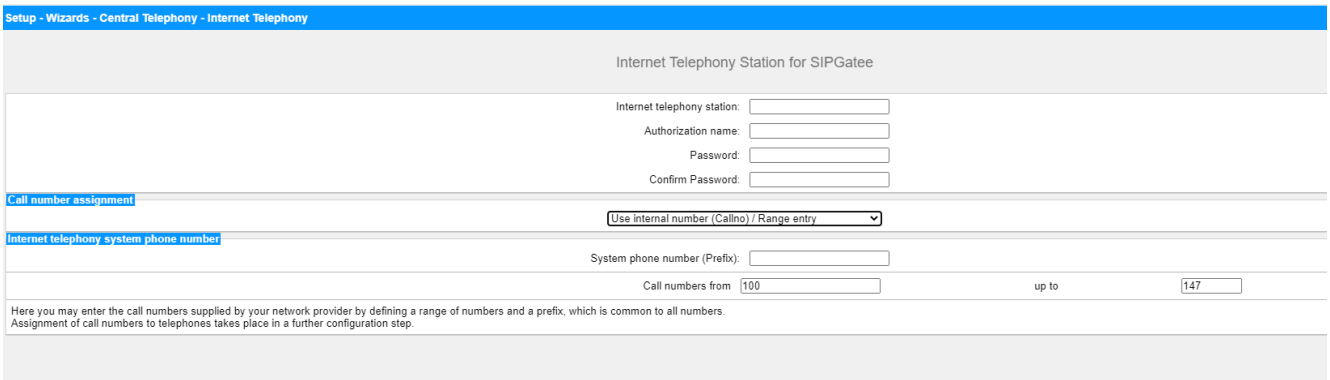


a) En el área **Asignación de números de teléfono**, seleccione el campo de opción **Utilizar número interno (n.º llamada)/Entradas individuales**.
b) En el área **Números de llamada de extensión de telefonía DSL**, y en el campo junto al botón **Agregar**, introduzca un número de teléfono de telefonía Internet que le haya sido comunicado por el proveedor de servicios de telefonía por Internet y haga clic en **Agregar**.
c) Si desea asignar a la cuenta más números de telefonía Internet, repita el paso b).

18) Asignación de números de teléfono de telefonía por Internet - Opción 3:

Utilizar número interno (Callno) / Entrada de rango:el uso de esta opción está obsoleto, para la configuración DID se debe utilizar la opción 1.

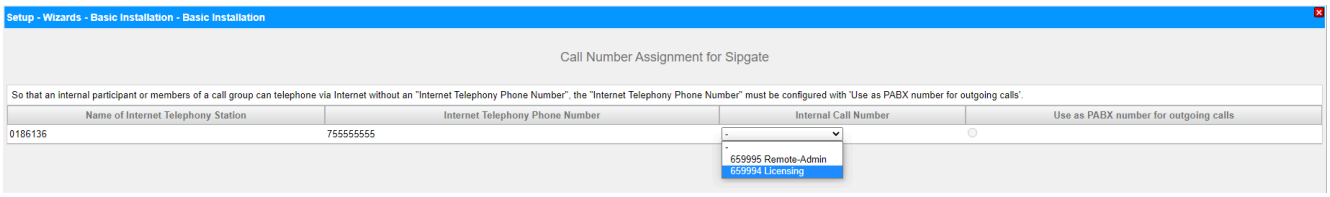
Tiene una conexión de centralita de telefonía por Internet y ha recibido un intervalo de números de teléfono como números de teléfono de telefonía Internet, por ejemplo (+49) 89 7007-100 a (+49) 89 7007-147. A continuación, asigne los números de llamada del intervalo de números de llamada a los números de llamadas internas de los suscriptores.



a) En el área **Asignación de números de teléfono**, seleccione el campo de opción **Utilizar número interno (n.º llamada)/Intervalo**.
b) En **Número de llamada del sistema (prefijo)** introduzca el número de teléfono del sistema.
c) En los campos **Rango de marcación directa de** y **hasta** indique el rango de marcación directa deseado para la extensión de telefonía por Internet. Por defecto están registrados los valores 100 - 147.

19) Haga clic en **Aceptar & Siguiente**.
20) Si desea configurar cuentas adicionales, repita los pasos 12 hasta 19.
21) Haga clic en **Aceptar & Siguiente**. Verá un resumen con los números de teléfono de telefonía Internet asignados y a qué cuentas lo están.
22) Asigna todos los números de telefonía por Internet a un número de teléfono interno de una extensión.

    No es necesario dar este paso si para asignar los números de telefonía por Internet ha seleccionado la opción 1. En este caso, la asignación se realiza en la configuración de las extensiones, en el campo **DuWa**. La pantalla también es visible en este caso pero no editable.



    a) En la línea correspondiente de la lista desplegable **N.° llam. interno** seleccione un número de teléfono interno.
    b) Si desea permitir que extensiones sin número de telefonía Internet o que los miembros de un grupo de llamadas realicen llamadas telefónicas externas por Internet, active el campo de opción **Utilizar como número de llamada del sistema saliente**. El campo de opción solo puede estar activado en un único número de telefonía Internet.

23) Haga clic en **Aceptar & Siguiente**. Aquí podrá ver nuevamente una descripción general de los posibles ITSP. Los ITSP activados aparecen marcados en la columna **Activar proveedor** con un signo de verificación. Con Mostrar Estado puede comprobar el estado de la conexión. Si tiene problemas de conexión con un ITSP ya activado, puede registrarlo nuevamente con **Reiniciar ITSP** en esta página.
24) Haga clic en **Aceptar & Siguiente**.
25) En el campo **Flujo saliente hasta (kbps)**, introduzca el valor de la velocidad de carga de su conexión a Internet. No debe confundirse con la velocidad de descarga.

    Nota: En el campo **Cantidad de llamadas telefónicas Internet simultáneas** se indica el número de llamadas telefónicas Internet que puede realizar simultáneamente. Si la carga de red tiene efectos negativos en la calidad de las llamadas, reduzca el número.

    Para obtener más información sobre la cantidad de llamadas simultáneas por Internet, consulte Restricción del número de llamadas simultáneas por ITSP en la página 842.

    ---

26) Haga clic en **Aceptar & Siguiente**.

27) En la columna **Cifras marcadas** introduzca los números de teléfono especiales deseados.

Son válidas estas entradas de número de teléfono:

- 0 a 9: dígitos permitidos
- -: Separador de campos
- X: Cualquier dígito del 0 al 9
- N: Cualquier dígito del 2 al 9
- Z: Siguen, hasta el final de la marcación, uno o varios dígitos
- C: Tono de marcado simulado (se puede ingresar hasta tres veces)

28) En la columna **Marcar a través de proveedor** seleccione si el número de teléfono especial se marcará a través de RDSI o a través de un ITSP. Solo aparecen los ITSP activos.

Nota: Asegúrese de que siempre se pueden marcar los números de teléfono de emergencia. Si desea que los números de teléfono de emergencia se marquen a través de un ITSP, el proveedor debe admitir la función.

---

29) Haga clic en **Aceptar & Siguiente**. Se muestra el estado de los ITSP.

30) Haga clic en **Siguiente** seguido de **Finalizar**. A continuación de este paso, ejecute el asistente de **CO Trunk ISDN/Analog/ITSP** para establecer la priorización para la toma de línea de intercambio (por ejemplo: Toma de línea de intercambio (primero a través de ITSP y luego a través de ISDN).

10.2.1.3 Cómo configurar Multisite mediante ITSP

El asistente **Multisite Management (Gestión multisitio)** permite definir hasta 8 ubicaciones para el sistema de comunicación. Puede asignar a cada ubicación un registro ITSP y varias extensiones.

Requisitos previos

En uno o varios ITSP se crean tantos registros cómo ubicaciones se van a configurar.

Todas las ubicaciones están en un mismo país.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.

3) Haga clic en **Editar** para iniciar el asistente **Multisite Management (Gestión multisitio)**.

4) En **Cód. local**, indique un prefijo local para cada ubicación (incluido cero inicial, por ejemplo, `069` para Fráncfort y `030` para Berlín). Se pueden registrar prefijos locales diferentes o idénticos.

5) En **Área** indique un nombre para cada ubicación (por ejemplo, las ciudades que se corresponden con los prefijos locales `Fráncfort` y `Berlín` o, si el prefijo es el mismo, las denominaciones de departamento `Servicio` y `Ventas`).

6) En la lista desplegable **Ruta dedicada**, asigne una ruta a cada ubicación. Por cada registro de ITSP se reserva automáticamente una ruta (hasta 8).
7) Si desea borrar una o varias ubicaciones, marque las ubicaciones en la columna **Eliminar** y haga clic en **Guardar**.
8) Haga clic en **OK y Continuar**.
9) Asigne las extensiones y los grupos a las ubicaciones:
   a) Marque las extensiones y los grupos deseados.

   Nota:

   También puede buscar extensiones y grupos; para ello, introduzca el término de búsqueda en los campos **N° llam.**, **Marc. dir.** O **Nombre** y, a continuación, haga clic en el icono en forma de lupa. Si todos los campos de búsqueda están vacíos y hace clic en el icono en forma de lupa, aparece una lista de todas las extensiones y de todos los grupos.

   La selección **Tipo** permite visualizar todos los tipos de extensiones (por ejemplo, **Clientes SIP** o **Clientes sist.**).

   Las extensiones y los grupos encontrados se pueden marcar por separado en la columna **Selección** o bien, se pueden marcar todos con la casilla **Selecc. todo**.

   b) En **Por área**, seleccione la ubicación deseada.
   c) Haga clic en **Guardar**.
   d) Para nuevas ubicaciones, repita los pasos anteriores.
10) En caso necesario, también puede asignar las extensiones y los grupos de una ubicación a otra ubicación:
   a) En **Desplazar selección de área**, seleccione la ubicación cuyas extensiones y grupos desea asignar a otra ubicación. Aparecen todas las extensiones y todos los grupos de la ubicación.
   b) Marque las extensiones deseadas por separado en la columna **Selección** o bien, marque todas con la casilla **Selecc. todo**.
   c) En **Por área**, seleccione la ubicación nueva.
   d) Haga clic en **Guardar**.
   e) Para nuevas ubicaciones, repita los pasos anteriores.
11) Haga clic en **OK y Continuar**.

10.2.1.4 Cómo guardar una plantilla ITSP preconfigurada como una nueva plantilla

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Gateway de voz**.
3) En el árbol de menú, haga clic en **Proveedor de servicios de telefonía por Internet**.

4) Haga clic en la pestaña **Agregar proveedor de servicios de telefonía por Internet**.
5) Seleccione la plantilla ITSP deseada de la lista **Plantilla base.**
6) Ingrese el nombre deseado para la nueva plantilla ITSP en el campo **Nombre del proveedor.**
7) Edite los valores de la plantilla para adaptarlos a sus necesidades. Puede encontrar una explicación de los valores en Gateway de voz>Proveedor de servicios de telefonía por Internet.
8) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.2.1.5 Cómo adaptar una plantilla de ITSP preconfigurada

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Gateway de voz**.
3) En el grupo de menús, haga clic en **Proveedor de servicios de telefonía por Internet**.
4) En el grupo de menús, haga clic en la plantilla de ITSP deseada.
5) Haga clic en la pestaña **Modificar proveedor de servicios de telefonía por Internet**.
6) Adapte los valores de la plantilla según sus necesidades. Puede consultar una explicación de los valores en Gateway voz>Proveedor de servicios de telefonía por Internet.

Nota: Con el botón **Reponer valores estándar** puede restablecer los valores que haya modificado a los valores estándares. Si el ITSP de la plantilla ya está activado, todas las cuentas del ITSP cierran sesión inmediatamente y se registran de nuevo con los valores estándares.

Nota: Con el botón **Actualizar** puede actualizar los valores estándares siempre que se haya ejecutado una actualización de software y que tenga valores estándares más recientes para esa plantilla.

---

7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.2.1.6 Cómo actualizar manualmente una plantilla de ITSP preconfigurada

Requisitos previos

El ITSP de la plantilla está activado.

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Gateway de voz**.
3) En el grupo de menús, haga clic en **Proveedor de servicios de telefonía por Internet**.
4) En el grupo de menús, haga clic en la plantilla de ITSP deseada.
5) Haga clic en la pestaña **Modificar proveedor de servicios de telefonía por Internet**.
6) Anote los valores de la plantilla que haya modificado respecto a los valores estándar (p.ej., haga una captura de pantalla).
7) Haga clic en **Actualizar**. Los valores predeterminados de la plantilla se actualizan si se ha realizado una actualización de software del sistema y en esta actualización hay valores predeterminados más actuales para la plantilla.
8) Adapte los valores de la plantilla de nuevo según sus necesidades. Puede consultar una explicación de los valores en Gateway voz>Proveedor de servicios de telefonía por Internet.

   Nota: Con el botón **Reponer valores estándar** puede restablecer los valores que haya modificado a los valores estándares. Al hacerlo se cierra sesión en todas las cuentas del ITSP y se repite el registro con los valores estándares.

9) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.2.2 STUN (Simple Traversal of UDP through NAT)

Si el sistema de comunicación opera tras un router NAT, STUN determina el puerto o la dirección IP pública propia que requieren algunos ITSP. Las funciones se hacen disponibles en Internet a través de servidores STUN, cuyas direcciones IP deben estar almacenadas en la configuración del sistema de comunicación.

El modo STUN necesario depende de la estructura de ITSP y del router Internet que se utilice. STUN no es necesario si el ITSP anula NAT Traversal mediante el uso de componentes de infraestructura en la red de proveedor como, por ejemplo, Session Border Controller (SBC).

En el sistema de comunicación se pueden configurar los siguientes modos STUN:

- **Automático (estándar)**

  Si no hay activo ningún ITSP, STUN está totalmente desactivado en este modo. Si hay un ITSP activo, STUN determina el tipo de firewall (tipo NAT) utilizado al arrancar el sistema y durante el servicio puede detectar cambios en las direcciones IP. Según el tipo NAT establecido, STUN modifica determinados parámetros de los mensajes SIP.

  Nota: El NAT simétrico no es compatible.

- **Siempre**

  STUN siempre está activo. En función del tipo NAT establecido se ajustan determinados parámetros de los mensajes SIP.
- **Utilizar IP estática**

  El módem DSL o el router Internet utilizan una dirección IP estática (dirección IP pública) y el ITSP requiere una autenticación IP estática. Además hay que indicar el puerto y la dirección IP estática que utiliza el módem o el router.
- **Router con mantenimiento del puerto**

  La dirección IP pública se determina mediante STUN. El puerto se registra si cambios en los mensajes SIP.

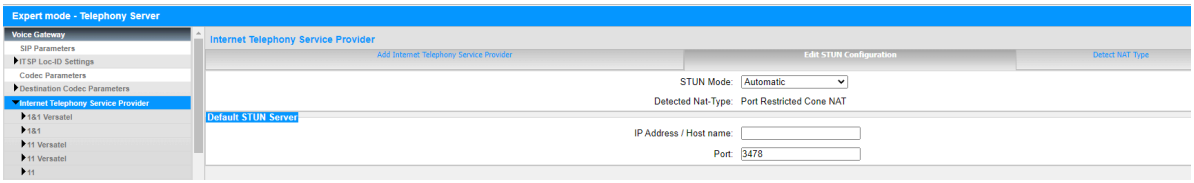
10.2.2.1 Cómo definir el modo STUN

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Gateway de voz**.
3) En el grupo de menús, haga clic en **Proveedor de servicios de telefonía por Internet**.
4) Haga clic en la pestaña **Editar configuración STUN**.



5) En la lista desplegable **Modo STUN** seleccione el modo STUN deseado.
6) Si ha seleccionado el modo STUN **Utilizar IP estática**, en **Dirección IP pública** y **Puerto SIP público** introduzca la dirección IP estática y el puerto del módem DSL o del router Internet.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3 Acceso a línea urbana mediante líneas analógicas y digitales

El acceso a línea urbana mediante líneas RDSI o analógicas, conecta las plataformas de hardware con la red pública (PSTN).

Con los asistentes resulta más sencillo configurar una línea urbana RDSI o una línea urbana analógica.

10.3.1 Líneas

Las líneas unen las plataformas de hardware con la red pública (PSTN). Cada línea debe tener asignada una ruta o dirección que permite asignarle diferentes propiedades.

De forma predeterminada, todas las líneas tienen asignado un código de línea y una ruta o dirección. El administrador puede modificar estas asignaciones.

En una conexión de línea urbana RDSI, las líneas también se denominan canales B.

Código de línea

El sistema de comunicación utiliza el código de línea para ocupar la línea asignada a dicho código. El código de línea también permite programar una tecla de línea o comprobar una línea.

Asignación MSN

El proveedor de servicios asigna a cada acceso individual RDSI (PMP, Point-to-Multipoint) uno o varios MSN (Multiple Subscriber Number). Estos se pueden asignar directamente a una línea.

Números de teléfono del sistema

Los números de teléfono del sistema incluyen el prefijo internacional, el prefijo local y nacional y el número de teléfono del sistema o uno o varios MSN.

Protocolo RDSI

El protocolo RDSI utilizado se rige por el código de país. Solo se debería modificar si la conexión PSTN necesita, expresamente, un determinado protocolo, distinto al utilizado. Hay disponible un gran número de plantillas de protocolo que se pueden adaptar a las necesidades específicas de cada caso. Su proveedor de servicios le proporcionará toda la información necesaria.

Modo de ocupación de canales B

Los diferentes canales B de una línea RDSI se pueden bloquear para el tráfico entrante o saliente.

Se pueden utilizar los siguientes modos de ocupación de los canales B:

- Solo salientes
- Solo entrantes
- Salientes y entrantes (estándar)

El modo de ocupación de canales B solo se evalúa cuando el sistema de comunicación debe proponer un canal B. Esto sucede, por ejemplo, en las siguientes situaciones:

S_2 saliente:	En este caso, el sistema de comunicación tiene que proponer un canal B.
S_2 entrante:	El colateral está obligado a proponer un canal B. Este canal B es asumido por el sistema de comunicación sin verificación del ajuste. El ajuste no tiene por tanto repercusión alguna.

S_0 saliente:	Puesto que el sistema de comunicación no propone ningún canal B (any channel), el ajuste no tiene repercusión alguna.
S_0 entrante:	Si el colateral establece comunicación sin preasignar el canal B, el sistema de comunicación propone uno. Para hacer esta propuesta se toma en consideración el modo de ocupación de canal B configurado.

Procedimiento de marcación para líneas urbanas analógicas (HKZ)

Cada vez que se produce una ocupación de línea, el sistema de comunicación identifica automáticamente el procedimiento de marcación. En determinados casos, el procedimiento de marcación también se puede configurar directamente como procedimiento de marcación multifrecuencia (MF) o decádica (DEC).

10.3.1.1 Cómo configurar el acceso a línea urbana RDSI

Con el asistente **Línea urbana RDSI / analógico / ITSP** puede configurar la línea urbana RDSI. En función de los puertos disponibles en el sistema de comunicación para las líneas urbanas (RDSI o analógico), el asistente seguirá distintos pasos.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

El sistema de comunicación está conectado a una línea urbana RDSI.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Línea urbana RDSI / analógica / ITSP**. El asistente mostrará un resumen del buzón o buzones, slots y puertos S_0.
4) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo `49` para Alemania o `1` para EE. UU.
5) En el campo **Código de red local**, indique el prefijo local, por ejemplo 89 para Múnich.
6) Si se trata de una conexión de centralita, en el campo **Nº teléfono del sistema**, indique el número de teléfono del sistema de la conexión urbana, por ejemplo 7007 (su número de conexión).
7) Solo debe cambiar el campo **Prefijo internacional** cuando se necesario. Para Alemania se usa `00` y para EE. UU. `011`).

   En las llamadas al extranjero, delante del número de teléfono se pone el prefijo internacional y el prefijo del país. Por ejemplo, de Alemania a EE.UU `00-1` y de EE. UU. a Alemania `011-49`.
8) Haga clic en **OK & Continuar**.

9) Seleccione uno de estos tipos de conexión de la conexión (Box, slot y puerto S_0):
   - Si desea configurar una conexión de centralita, active el campo de opción **Conexión de centralita**.
   - Si desea configurar un acceso individual, active el campo de opción **Acceso individual**.
10) Haga clic en **OK & Continuar**.
11) Si se trata de un acceso individual, introduzca el MSN de la conexión (Box, slot y puerto S_0) y haga clic en **OK & Continuar**.
12) No modifique el ajuste de la casilla de verificación **Sin telefonía a través de Internet** y haga clic en **Saltar**.
13) En la lista desplegable **Primero a través de** seleccione la línea urbana preferida y haga clic en **OK & Continuar**.
14) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

10.3.1.2 Cómo configurar el acceso analógico a línea urbana

Con el asistente **Línea urbana RDSI / analógico / ITSP** puede configurar la línea urbana analógica.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

El sistema de comunicación está conectado a una línea urbana analógica.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Línea urbana RDSI / analógica / ITSP**. El asistente mostrará un resumen del buzón o buzones, slots y puertos analógicos.
4) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo `49` para Alemania o `1` para EE. UU.
5) En el campo **Código de red local**, indique el prefijo local, por ejemplo 89 para Múnich.
6) Si se trata de una conexión de centralita, en el campo **Nº teléfono del sistema**, indique el número de teléfono del sistema de la conexión urbana, por ejemplo 7007 (su número de conexión).
7) Solo debe cambiar el campo **Prefijo internacional** cuando se necesario. Para Alemania se usa `00` y para EE. UU. `011`).

   En las llamadas al extranjero, delante del número de teléfono se pone el prefijo internacional y el prefijo del país. Por ejemplo, de Alemania a EE.UU `00-1` y de EE. UU. a Alemania `011-49`.
8) Haga clic en **OK & Continuar**.
9) Haga clic en **Ignorar RDSI**.
10) No modifique el ajuste de la casilla de verificación **Sin telefonía a través de Internet** y haga clic en **Saltar**.

11) En la lista desplegable **Protocolo**, seleccione el protocolo para visualizar el número de teléfono (depende del proveedor de servicios):
    - Si desea utilizar el protocolo FSK (Frequency Shift Keying), seleccione **FSK**.
    - Si desea utilizar el procedimiento de marcación por multifrecuencia, seleccione **MF**.
    - Si no desea utilizar la indicación de números de teléfono, seleccione **ninguno**.
12) Haga clic en **OK & Continuar**.
13) Haga clic en **Editar** para configurar las propiedades de la línea en cuestión. Si es necesario, modifique **Procedimiento de marcación**, **Reconocimiento llam. urbana**, **Flash**, **Longitud de línea** y **Flags** y, a continuación, haga clic en **Aceptar**.
14) Haga clic en **OK & Continuar**.
15) Haga clic en **Saltar** y en **OK & Continuar**.
16) En la lista desplegable **Primero a través de** seleccione la línea urbana preferida y haga clic en **OK & Continuar**.
17) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

10.3.1.3 Cómo mostrar todas las líneas

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Líneas**. En función de la estructura del sistema de comunicación se muestran todas las líneas posibles, incluidos el código de línea y la ruta.

10.3.1.4 Cómo mostrar líneas individuales

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús **Líneas/Interconexión** > **Líneas** > **...**, desplácese hasta la línea deseada. Podrá ver la línea conectada con el sistema de comunicación, incl. código de línea y ruta.
4) Haga clic en **Aceptar**.

10.3.1.5 Cómo modificar código de línea

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús **Líneas/Interconexión** > **Líneas** > **...**, desplácese hasta la línea deseada.
4) Haga clic en la pestaña **Editar línea**.
5) En el campo **Código**, indique el valor deseado.

   Nota: Si no se ha introducido ningún valor de código, esta línea no tiene código de línea.

6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.1.6 Cómo asignar MSN a una línea

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Asignar MSN**.
4) En la sección **Asignar MSN** del grupo de menús, haga clic en la entrada que desea editar.
5) Introduzca la **MSN**.
6) En la lista desplegable **Línea**, seleccione la línea que desea asignar.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.1.7 Cómo modificar el protocolo RDSI

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús **Líneas / Interconexión** > **Líneas** > **...**, desplácese hasta el puerto deseado.
4) Haga clic en la pestaña **Editar flags RDSI**.

5) En la sección **Protocolo: Descripción**, seleccione el protocolo deseado en la lista desplegable.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.1.8 Cómo modificar el modo de asignación del canal B

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús **Líneas / Interconexión** > **Líneas** > **...**, desplácese hasta el puerto deseado.
4) Haga clic en la pestaña **Cambiar canal B**.
5) En cada canal desactive las casillas de verificación de las columnas **saliente** y **entrante** según sus preferencias.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.1.9 Cómo modificar el procedimiento de marcación

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús **Líneas / Interconexión** > **Líneas** > **...**, desplácese hasta el puerto deseado.
4) Haga clic en la pestaña **Editar flags HKZ**.
5) Configure el procedimiento de marcación multifrecuencia (MF) o el procedimiento de marcación decádica (DEC).
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.2 Rutas

Las rutas permiten agrupar en haces las líneas (canales B). Se pueden configurar parámetros propios para cada haz de líneas (=ruta).

Cada línea se puede asignar a una ruta. De forma predeterminada, todas las líneas tienen asignada la ruta 1.

Se puede asignar un nombre y un código de ruta a cada ruta.

Consejo: Los códigos de ruta solo se aplican a las ocupaciones de línea urbana salientes si LCR no está activo.

Distribución de canales B

Se denomina distribución de canales B a la división de los canales B entre diferentes haces de líneas. Para conexiones de línea urbana RDSI con muchos canales B (p. ej., conexiones S_{2M}) puede ser conveniente distribuir los canales B entre distintos haces de líneas.

En caso de comunicaciones salientes solo se seleccionan canales B incluidos en el haz (por ejemplo, haz seleccionado mediante el código de ruta, haz de desbordamiento o haz seleccionado mediante LCR).

Las comunicaciones salientes siempre se aceptan, independientemente del haz. Por norma general, se ocupa el canal B ofrecido por el colateral. Por ello la distribución de canales B configurada en el sistema también debe ser compatible en el lado del colateral (instalación o red pública). Si no es así, no se puede garantizar que la llamada se asigne correctamente al haz de líneas adecuado.

Tecla de Ruta

Un usuario puede programar una tecla de ruta en el teléfono. Una tecla de ruta está reservada a las llamadas salientes. Las llamadas establecidas por medio de teclas de ruta están sujetas a los niveles y las reglas del control de marcación COS.

Una vez que el usuario ha pulsado una tecla de ruta (o seleccionado un código de ocupación), el sistema de comunicación ocupa una línea disponible asignada a la ruta correspondiente para establecer la conexión. El teléfono muestra en el display el número de línea. Si todas las líneas de la ruta están ocupadas, se ilumina el LED correspondiente, también en caso de desbordamiento.

Ruta de desbordamiento con LCR desactivado

El administrador puede establecer una ruta de desbordamiento por cada ruta. Si todas las líneas de una ruta están ocupadas en un intento de ocupación, la búsqueda continúa en todas las líneas de esta ruta de desbordamiento. Si también en la ruta de desbordamiento están todas las líneas ocupadas, no tiene lugar ningún desbordamiento más.

Ruta de desbordamiento con LCR activado

Al configurar LCR, el administrador puede configurar también hasta 16 entradas por cada tabla de rutas que en caso de desbordamiento se procesarán consecutivamente.

Tipo de ocupación

En el caso de una ocupación de ruta saliente, el administrador puede especificar los criterios que utilizará el sistema de comunicación al buscar una línea disponible en la dirección necesaria. Para ello, el tipo de ocupación se define de esta forma:

- cíclico:

  Tras la última línea ocupada saliente: la búsqueda comienza por el número de línea inmediatamente superior en relación con la última línea ocupada en dirección saliente de la ruta. De esta forma, todas las líneas se utilizan prácticamente con la misma frecuencia.

- lineal:

  Siempre la primera línea libre: la búsqueda comienza por el número de línea más bajo asignado a esa ruta.

Número de teléfono del sistema entrantes y salientes

El administrador puede definir por separado el número de teléfono del sistema entrante y el número de teléfono del sistema saliente. De esta forma, el número de teléfono propio se puede mostrar en las llamadas salientes de forma diferente que como es necesario para garantizar la accesibilidad con las llamadas entrantes. Las partes para prefijo del país, código de red local y número teléfono del sistema se deben registrar por separado. Diferentes entradas para los números de teléfono del sistema entrantes y salientes requieren la disponibilidad de la prestación "CLIP no screening" en la línea urbana. Si no hay configurado ningún número de teléfono del sistema saliente, el sistema de comunicación utiliza siempre los datos del número de teléfono del sistema entrante.

En caso de ocupación entrante en una línea RDSI, el sistema de comunicación oculta la parte del número recibido que se corresponda con el número del sistema entrante de acuerdo con el tipo tipo de número de llamada (Type Of Number = TON, véase la Tabla en Transmisión del número de teléfono) recibido desde la izquierda e interpreta la parte restante como número de marcación directa. En la información sobre números de teléfono que se transmite al PSTN, el sistema de comunicación inserta automáticamente la parte del número de teléfono del sistema saliente de acuerdo con el tipo de número de llamada saliente configurado delante del número de teléfono. En Alemania, la parte del número de teléfono del sistema se debe indicar en la conexión de línea urbana sin código de red local y sin código de interceptación (0).

Transmisión del número de teléfono

El número de teléfono enviado al PSTN y al destinatario puede tener los siguientes elementos:

Type Of Number (TON), saliente	**Número de llamada transmitido al PSTN**
Desconocido TON=Unknown	Solo número de marcación directa (ajuste estándar)
Número de teléfono del sistema TON=Subscriber	Nº teléfono del sistema + Número de marcación directa
Código de red local TON=National	Código de red local + Nº teléfono del sistema + Número de marcación directa
Prefijo del país TON=International	Prefijo del país + Código de red local + Nº teléfono del sistema + Número de marcación directa

Type Of Number (TON), saliente	Número de llamada transmitido al PSTN
Internas TON=Intern	Solo con sistemas interconectados: con un plan de numeración cerrado no se pueden utilizar prefijos de números. En este caso los números de teléfono no se amplían con prefijos.

Además es posible indicar qué información sobre números de teléfono de la extensión que realiza la marcación se debe enviar a la extensión de destino.

Tipo de número de teléfono	Número de llamada transmitido al PSTN
Internas	Aquí solo se envía una pieza de información sobre el número de teléfono interno. Si la extensión de destino es externa no se envía ningún número o se envía el número de teléfono del puesto de operadora. En las extensiones de destino internas se puede mostrar el número de teléfono interno.
Marcación directa	Solo se envía una pieza de información sobre el número de marcación directa. En las extensiones de destino internas en otros nodos el número de llamada interno no se muestra en el display. Para los destinos externos basta la información sobre números de teléfono.
Interna / Marc. directa	En una interconexión en red este ajuste es el que debe seleccionarse preferentemente. Tanto el número de llamada interno como el de marcación directa se envían a la extensión de destino. Cuando en una interconexión se llama a una extensión interna, se puede mostrar a ésta el número de llamada interno del llamante. Si la extensión de destino interna, por ejemplo, ha activado un desvío de llamadas con un destino externo se puede enviar en tal caso un número de marcación directa.

Además se puede definir también el tratamiento deseado para el prefijo de ruta:

- Llamada entrante

  Al hacer la transferencia al bus S0, se añade el código de ruta al número del llamante (-> formato de marcación para devolución de llamada) o se suministra de forma transparente. Estándar: activado.
- Llamada saliente

  El número de teléfono marcado se muestra en el teléfono del sistema con o sin prefijo de ruta. Estándar: activado.

Segundo prefijo de marcación

Se define un segundo prefijo de marcación cuando el sistema de comunicación está subordinado a otro sistema de comunicación o interconectado con varios sistemas de comunicación. Solo es relevante para rutas de interconexión (tipo de ruta=PABX). En este caso, el segundo prefijo de marcación sirve como código de ocupación para el sistema principal. Dentro de una interconexión, los códigos de ocupación de línea urbana, los códigos de ruta y el segundo

prefijo de marcación se deben configurar uniformemente. El valor estándar en Alemania es 0.

10.3.2.1 Cómo modificar la asignación de ruta

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús **Líneas/Interconexión** > **Líneas** > **...**, desplácese hasta la línea deseada.
4) Haga clic en la pestaña **Editar línea**.
5) En la lista desplegable **Ruta** seleccione la ruta que desea asignar a la línea.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.2.2 Cómo modificar el nombre de ruta

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Ruta**.
4) En el grupo de menús, bajo **Ruta**, seleccione la entrada que desee editar.
5) En el campo **Nombre de ruta** introduzca el valor deseado.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.2.3 Cómo modificar el código de ruta

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Nota: Los códigos de ruta solo son efectivos si LCR no está activo.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Ruta**.
4) En el grupo de menús, bajo **Ruta**, seleccione la entrada que desee editar.

5) En el campo **Códigos de ruta**, indique el valor deseado.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.2.4 Cómo configurar una ruta de desbordamiento si LCR está desactivado

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Ruta**.
4) En el grupo de menús, bajo **Ruta**, seleccione la entrada que desee editar.
5) En la lista desplegable **Ruta de desbordamiento**, seleccione la entrada deseada.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.2.5 Cómo configurar una ruta de desbordamiento con LCR activado

Si LCR está activado, el desbordamiento se realiza mediante el procesamiento sucesivo de los distintos registros de una tabla de rutas LCR dentro de una configuración de LCR (véase LCR (Least Cost Routing, Ruta más económica)).

10.3.2.6 Cómo configurar el tipo de ocupación

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Ruta**.
4) En el grupo de menús, bajo **Ruta**, seleccione la ruta que desee editar.
5) Haga clic en la pestaña **Modificar parámetros de ruta**.
6) En la lista desplegable **Tipo de ocupación**, seleccione **Cíclico** o **Lineal**.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.2.7 Cómo introducir números de teléfono del sistema entrantes y salientes

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Ruta**.
4) En el grupo de menús, bajo **Ruta**, seleccione la entrada que desee editar.
5) En la sección **Número de teléfono del sistema entrante**, en los campos **Prefijo de país**, **Código de red local** y **Número de llamada del sistema**, introduzca los valores correspondientes in ceros delante.
6) En la sección **Número de teléfono del sistema saliente**, en los campos **Prefijo de país**, **Código de red local** y **Número de llamada del sistema**, introduzca los valores correspondientes sin ceros delante.
7) Elija una de estas opciones:
   - Si desea suprimir el número de extensión, active la casilla de verificación **Suprimir núm. llam. de extensión**.
   - Si no desea suprimir el número de extensión, desactive la casilla de verificación **Suprimir núm. llam. de extensión**.
8) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.2.8 Cómo configurar el formato del número de teléfono transmitido

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Ruta**.
4) En el grupo de menús, bajo **Ruta**, seleccione la ruta que desee editar.
5) Haga clic en la pestaña **Modificar parámetros de ruta**.
6) En la lista desplegable **Tipo de número de llamada, saliente** seleccione el formato deseado del ´numero de teléfono transmitido.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.2.9 Cómo configurar el tipo de número de teléfono transferido

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Ruta**.
4) En el grupo de menús, bajo **Ruta**, seleccione la ruta que desee editar.
5) Haga clic en la pestaña **Modificar parámetros de ruta**.

6) En la lista desplegable **Tipo de número de llamada**, seleccione la entrada **interno**, **Marcación directa** o **Interna / Marc. directa**.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.2.10 Cómo configurar el prefijo de ruta

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Ruta**.
4) En el grupo de menús, bajo **Ruta**, seleccione la ruta que desee editar.
5) Haga clic en la pestaña **Modificar parámetros de ruta**.
6) Elija una de estas opciones:
   - Si desea incluir el código de ruta en la indicación de números de teléfono para las llamadas entrantes, en el área **Flags de ruta** active la casilla de verificación **Act. prefijo ruta entrantes**.
   - Si no desea incluir el código de ruta en la indicación de números de teléfono para las llamadas entrantes, en el área **Flags de ruta** desactive la casilla de verificación **Act. prefijo ruta entrantes**.
   - Si desea incluir el código de ruta en la indicación de números de teléfono para las llamadas salientes, en el área **Flags de ruta** active la casilla de verificación **Act. prefijo ruta salientes**.
   - Si no desea incluir el código de ruta en la indicación de números de teléfono para las llamadas salientes, en el área **Flags de ruta** desactive la casilla de verificación **Act. prefijo ruta salientes**.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.2.11 Cómo definir una ruta para la interconexión y cómo registrar un segundo código urbano

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Ruta**.
4) En el grupo de menús, bajo **Ruta**, seleccione la entrada que desee editar.
5) En el campo **Código urbano (2º AKZ)**, introduzca el valor deseado.
6) Haga clic en la pestaña **Modificar parámetros de ruta**.
7) En la lista desplegable **Tipo de ruta**, seleccione la entrada **PABX**.
8) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.3 Supervisión de tono de marcación

Al establecer conexión a través de una línea urbana analógica, los dígitos marcados solo se pueden enviar la línea urbana cuando se detecta un tono de marcación (tono audible). Como el tiempo que transcurre hasta la entrada del tono de marcación varía en función del operador y del estado de la red, hay que supervisar esa entrada.

El tiempo de supervisión del tono de marcación y el tiempo de marcado de dígitos se configuran con Manager E.

Tiempo de retardo de la supervisión del tono de marcación

La supervisión del tono de marcación se puede realizar inmediatamente o después de una pausa. En algunos casos hay que reproducir al usuario tonos adicionales una vez realizada la asignación de línea, por ejemplo, para comunicarle que hay activo un desvío en la línea urbana. Para estos casos se puede programar un tiempo de retardo para la supervisión del tono de llamada (Pausa antes de marcar, 1-9 segundos). Los dígitos marcados se envían a la línea urbana una vez finalizada la pausa.

Nota: Indicación para Brasil:

Si se utiliza el procedimiento de marcación MF desde terminales analógicos en conexión con líneas urbanas analógicas (TLAx y TML8W) y procedimiento de marcación decádica tras la supervisión del tono de marcación, puede haber problemas con el control de la marcación si el prefijo del país está configurado en Brasil. En este caso, las señales MF de los terminales analógicos se transmiten directamente a las líneas urbanas analógicas. Se pierden todas las señales MF marcadas antes de recibir el tono de marcación. En este caso se debe activar la búsqueda de rutas automática (LCR) para garantizar el funcionamiento correcto del procedimiento de marcación y del control de marcación del terminal.

Tiempo supervisión tono marcación

Se puede configurar el tiempo durante el que se esperará el tono de marcación. Si después del tiempo configurado no se identifica ningún tono de marcación, la línea se pone fuera de servicio. El sistema comprueba a intervalos regulares si vuelve a haber tono de marcación. Si es así, la línea correspondiente se vuelve a poner el servicio.

Tiempo de marcación de dígitos

Se puede configurar cuántos segundos deben pasar después de detectar el tono de marcación para enviar el primer dígito marcado a la línea urbana (valor estándar: 0 s).

Evaluación del segundo tono de marcación

El sistema de comunicación puede identificar un tono de marcación adicional (2° tono audible). Es relevante para operadores de red públicos que envían un segundo tono de marcación para las llamadas a otro país (por ejemplo, para Bélgica después de 00 y para Francia después de 16 o 19). Esta función no es relevante para países como Alemania.

10.3.3.1 Cómo configurar el tiempo de retardo de la supervisión del tono de marcación

Requisitos previos

Hay un puerto analógico con el acceso a línea urbana analógico.

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Ruta**.
4) En el grupo de menús, en **Ruta**, seleccione la ruta que desee editar.
5) Haga clic en la pestaña **Modificar parámetros de ruta**.
6) Si desea que el tono de marcación se supervise inmediatamente, en el área **Pausa antes de marcar** seleccione la opción **sin pausa**.
7) Si desea que el tono de marcación comience a supervisarse después de un tiempo de retardo, en el área **Pausa antes de marcar** seleccione el tiempo de retardo, en segundos.
8) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.3.3.2 Cómo configurar Tiempo supervisión tono marcación

Requisitos previos

Hay conectado un módulo de tronqueo analógico.

Paso a paso

1) En el PC de administración, inicie sesión en Manager E.
2) En la barra de menús, haga clic en **Archivo | Transferir**.
3) Seleccione la pestaña **Comunicación**.
4) En la sección **Acceso**, active la opción correspondiente al tipo de conexión del PC de administración con el sistema de comunicación.
5) Active la opción **Leer/escribir KDS** y haga clic en **Sistema -> PC**.
6) Haga clic en **Aceptar**. La memoria de datos de cliente (KDS) se transfiere automáticamente desde el sistema de comunicación al Manager E.
7) Una vez concluida correctamente la transferencia, haga clic en **Aceptar** y, a continuación, en **Cerrar**.
8) En el Manager E, en el grupo de menús de la vista del sistema, haga clic en **Configuración** > **Parámetros del sistema** > **Parámetros de tiempo**.
9) En la lista de **Tiempo supervisión tono marcación**, utilice los valores de **Base** y **Factor** para ajustar el tiempo máximo durante el que se esperará al tono de marcación (estándar: Base = `1S`, Factor = `10`).
10) Haga clic en **Aplicar**.
11) En la barra de menús, haga clic en **Archivo | Transferir**.
12) Seleccione la pestaña **Comunicación**.
13) Haga clic en **PC -> Sistema** y, a continuación, en **Aceptar**. Los ajustes de comunicación se transfieren al sistema de comunicación.
14) Por último, haga clic en **Aceptar** y **Cerrar**.

10.3.3.3 Cómo configurar el tiempo de marcación de dígitos

Requisitos previos

Hay conectado un módulo de tronqueo analógico.

Paso a paso

1) En el PC de administración, inicie sesión en Manager E.
2) En la barra de menús, haga clic en **Archivo | Transferir**.
3) Seleccione la pestaña **Comunicación**.
4) En la sección **Acceso**, active la opción correspondiente al tipo de conexión del PC de administración con el sistema de comunicación.
5) Active la opción **Leer/escribir KDS** y haga clic en **Sistema -> PC**.
6) Haga clic en **Aceptar**. La memoria de datos de cliente (KDS) se transfiere automáticamente desde el sistema de comunicación al Manager E.
7) Una vez concluida correctamente la transferencia, haga clic en **Aceptar** y, a continuación, en **Cerrar**.
8) En el Manager E, en el grupo de menús de la vista del sistema, haga clic en **Configuración** > **Parámetros del sistema** > **Parámetros de tiempo**.
9) En la opción **Tiempo entre evaluación tono audible y marcación troncal HKZ** de la lista, use las opciones **Base** y **Factor** para configurar el tiempo (en segundos) que debe transcurrir desde la detección de tono de marcación para enviar el primer dígito marcado a la línea urbana (valor estándar: Base = `10ms`, Factor = `0`).
10) Haga clic en **Aplicar**.
11) En la barra de menús, haga clic en **Archivo | Transferir**.
12) Seleccione la pestaña **Comunicación**.
13) Haga clic en **PC -> Sistema** y, a continuación, en **Aceptar**. Los ajustes de comunicación se transfieren al sistema de comunicación.
14) Por último, haga clic en **Aceptar** y **Cerrar**.

10.3.3.4 Cómo activar o desactivar la evaluación del segundo tono de marcación

Requisitos previos

Hay un puerto analógico con el acceso a línea urbana analógico.

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Ruta**.
4) En el grupo de menús, en **Ruta**, seleccione la ruta que desee editar.
5) Haga clic en la pestaña **Modificar parámetros de ruta**.
6) Si desea activar la evaluación del segundo tono de marcación, en el área **Flags de ruta** active la casilla de verificación **Evaluación 2° tono audible**.
7) Si desea desactivar la evaluación del segundo tono de marcación, en el área **Flags de ruta**, desactive la casilla de verificación **Evaluación 2° tono audible/Supervisión de línea**.

8) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10.4 Prioridad de la ocupación de línea urbana con LCR activado

En la definición de prioridades para la ocupación de línea urbana se establece el orden en que se seleccionarán los distintos proveedores (RDSI/Analógico o ITSP).

Habitualmente, la ocupación de línea urbana se produce a través de la marcación previa del código "0". Dentro de este código se establecen prioridades para distintos proveedores (según la configuración previa). De esta forma se puede establecer en primer lugar a través de un ITSP y, si la ocupación no puede establecerse correctamente, a través de RDSI.

10.4.1 Cómo asignar prioridades a la ocupación de línea urbana

El asistente **Línea urbana RDSI / analógico / ITSP** permite configurar el orden de la ocupación de línea urbana a través de RDSI/analógica y ITSP.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)). Hay configurados distintos ITSP.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.

3) Haga clic en **Editar** para iniciar el asistente **Línea urbana RDSI / analógica / ITSP**. El asistente mostrará un resumen del buzón o buzones, slots y puertos analógicos.

4) Haga clic en **OK & Continuar**.

5) Haga clic varias veces en **OK & Continuar**, hasta llegar a la ventana **Prioriz. para ocupación de línea urbana**.

6) En la sección **Intentar ocupación de línea urbana**, y en la lista desplegable **Primero a través de**, seleccione el proveedor preferido con el que el sistema de comunicación intentará acceder a una línea urbana libre en primer lugar.

7) En la lista desplegable **Después a través de**, seleccione un segundo proveedor, con el que se realizará el segundo intento de ocupación de línea urbana.

8) En la siguiente lista desplegable, **Después a través de**, seleccione el tercer proveedor para el intento de ocupación de línea urbana.

9) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

11 Estaciones

Un abonado o estación es un socio de comunicación conectado al sistema de comunicación. En general, a cada estación (excepto las virtuales) se le asigna un terminal. Un terminal es, por ejemplo, un teléfono, un PC o un dispositivo de fax. Las estaciones también podrán ser usuarias de los Clientes UC.

Existen los siguientes tipos de estaciones:

- Estaciones IP (también conocidas como clientes IP)
- Estaciones SIP (un subconjunto de estaciones IP)
- Estaciones UP0
- Estaciones DECT
- Estaciones SIP-DECT de Mitel
- Estaciones ISDN
- Estaciones analógicas
- Estaciones de movilidad (estaciones móviles, véase Movilidad)
- Extensiones virtuales

Los datos de los suscriptores (nombre, número de estación, número DID, dirección de correo electrónico, etc.) se pueden importar como un archivo XML durante la instalación inicial (consulte Plan de marcado individual). Además, los datos del suscriptor también se pueden exportar a un archivo XML (consulte Exportación de datos del suscriptor).

Procedimiento de Licencia para Estaciones

Todas las estaciones están sujetas a licencia. Para empezar, las estaciones se pueden configurar durante la instalación inicial o más tarde utilizando los asistentes de estaciones. Después de una configuración exitosa, los suscriptores pueden realizar llamadas internas. En el siguiente paso se deben activar las licencias de las estaciones y asignarlas a las mismas. Una vez asignadas exitosamente las licencias, los suscriptores también podrán realizar llamadas externas.

Conceptos relacionados

Registro de licencia en la página 301
Mobility en la página 969

11.1 Plan de numeración

Un plan de numeración es una lista de todos los números de teléfono y códigos disponibles en el sistema de comunicación. Incluye, entre otras cosas, números de teléfono internos, números de marcación directa y números de llamada de grupo. en el sistema de comunicación, los números de teléfono y los códigos tienen preasignados valores estándar. No obstante, estos valores se pueden personalizar en caso necesario.

En ocasiones, al configurar los número de teléfono o código pueden generarse mensajes de error. Esto sucede cuando el número deseado ya ha sido ocupado. Con ayuda del plan de numeración se puede comprobar qué números de teléfono restan de ser asignados.

11.1.1 Plan de numeración estándar

El plan de numeración estándar incluye todos los números de teléfono y los códigos preasignados con valores estándar en el sistema de comunicación.

Si es necesario se pueden modificar los valores estándar. Además, algunos números se pueden borrar por completo para que no sigan apareciendo una vista general del plan de numeración.

Plan de numeración estándar para las plataformas de hardware y el softswitch:

Tipo de los números de teléfono	X1	X3/X5/X8/S	Acción
Números de teléfono de extensión internos	11-30	100-742	se pueden borrar
Números de marcación directa de extensión	11 -30	100-742	se pueden borrar
Números de llamada de grupo 1-90 Números de llamada de grupo 91-800	31-40 -	350-439 sin preasignar	se pueden borrar
Números de teléfono de línea	700-703	desde 7801	se pueden borrar
Códigos de ruta (códigos externos): Ruta 1 (línea urbana RDSI, analógica) Ruta 8 (UC Suite) Ruta 12-15 (línea urbana, ITSP) Ruta 16 (interconexión)	0 = Mundial / 9 = EE. UU. - sin preasignar sin preasignar	0 = Mundial / 9 = EE. UU. 851 855-858 859	sólo se pueden modificar
Código del puesto de operadora (puesto de interceptación) interno	9 = Todo el mundo 0 = EE. UU.	9 = Todo el mundo 0 = EE. UU.	solo se pueden modificar
Código del puesto de operadora (Puesto de interceptación), marcación directa	0 = Todo el mundo – = EE.UU	0 = Todo el mundo – = EE.UU	solo se pueden modificar
Número de teléfono para el Usuario online	sin preasignar	749	solo se pueden modificar
Número de teléfono para el acceso remoto	sin preasignar	sin preasignar	solo se pueden modificar

Tipo de los números de teléfono	X1	X3/X5/X8/S	Acción
Número de teléfono para mensajes de voz UC Smart UC Suite	351 -	351 sin preasignar	solo se pueden modificar solo se pueden modificar
Números de teléfono de conferencia	-	sin preasignar	solo se pueden modificar
Número de teléfono de aparcamiento	-	sin preasignar	solo se pueden modificar
Números de teléfono de AutoAttendant	-	sin preasignar	solo se pueden modificar
Número de teléfono para puesto de operadora	9 = Todo el mundo 0 = EE. UU.	9 = Todo el mundo 0 = EE. UU.	solo se pueden modificar
Substitución por "*" (en códigos)	75	75	se pueden borrar
Substitución por "#" (en códigos)	76	76	se pueden borrar
Códigos de servicio			sólo se pueden modificar

11.1.2 Plan de numeración individual

El sistema de comunicación permite configurar un plan de numeración individual. El proceso permite modificar los valores estándar de números de teléfono y códigos. Al hacer una recarga del sistema de comunicación, se restablecen todos los valores estándar.

En la configuración de un plan de numeración individual resultan muy útiles las siguientes funciones:

- Borrar números de teléfono estándar: salvo contadas excepciones (números de teléfono estándar especiales), los números de teléfono estándar se pueden eliminar. Estos números de teléfono aparecen indicados en la columna "Acción" de la tabla del plan de numeración individual con el texto "se pueden borrar".
- Modificar números de teléfono estándar especiales: estos números de teléfono no se pueden eliminar. Sin embargo, sí se pueden modificar sus valores. Estos números de teléfono aparecen indicados en la columna "Acción" de la tabla de la plan de numeración individual con el texto "solo se pueden modificar".

- Importar números de teléfono y datos de extensión: a través de un archivo XML se pueden importar datos de extensión durante la instalación inicial. En el proceso también se importa el número de teléfono y el número de marcación directa de las extensiones. Por norma general, se hace durante la instalación inicial.

Importación de datos de extensión a través de un archivo XML

Mediante un archivo XML en formato UTF-8 se pueden importar planes de numeración individualizados en el sistema de comunicación durante la instalación inicial.

El programa de administración OpenScape Business Assistant ofrece en **Centro de servicios** > **Documentos** > **Plantillas CSV**, el archivo `csv-templates.zip`. Este archivo ZIP incluye, entre otros, estos archivos (incl. la descripción).

- `portdata_xml_import_empty.xml`

  Esta plantilla incluye registradores sin registros de datos de ejemplo. Se pueden registrar nuevos registros de datos, por ejemplo con Microsoft Excel.
- `portdata_xml_import_example.xml`

  Esta plantilla incluye registradores con registros de datos de ejemplo. Se pueden sobreescribir, por ejemplo con Microsoft Excel. Es recomendable borrar los registros de datos que no sean necesarios.
- `portdata_xml_import_syntax.txt`

  Descripción en alemán e inglés del proceso correcto para crear registros de datos.

11.1.2.1 Cómo borrar o modificar números de teléfono estándar

Puede borrar algunos de los números de teléfono estándar y definir nuevos números a través de los asistentes. En el caso de los números de teléfono estándar que no pueden ser eliminados, puede modificar los valores predefinidos.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) Haga clic en **Editar** para iniciar el asistente **Configuración básica**.

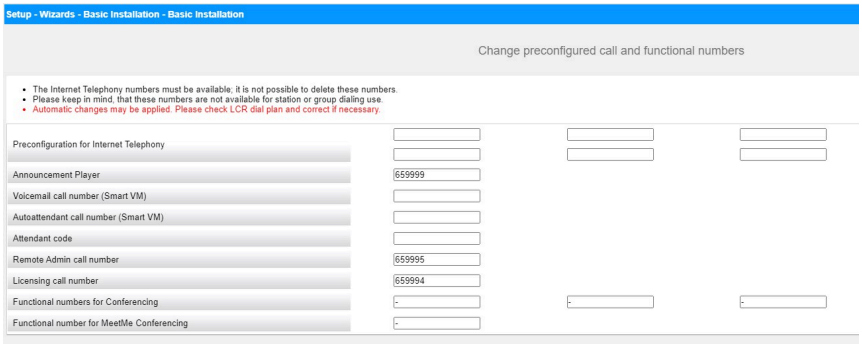
3) Haga clic en **Continuar**.

> **Nota:** Puede ver un resumen de los números de teléfono actualmente configurados activando la opción **Mostrar configuración de extensiones** y haciendo clic en **Ejecutar función**.

4) Active la opción **Borrar todos nos. llamada**.

5) En la consulta de seguridad, active la casilla de verificación **Borrar todos nos. llamada**.

6) Haga clic en **Ejecutar función**.



7) Si es necesario, en los campos modifique los valores predefinidos de los números de teléfono estándar.
8) Haga clic en **Aceptar**. Se borran los números de teléfono y, en su caso, se ejecutan las modificaciones en los números de teléfono estándar especiales.
9) Haga clic en **Cancelar** para salir del asistente **Configuración básica**.

11.1.2.2 Cómo modificar números de teléfono estándar

Puede modificar los números de teléfono predefinidos para funciones especiales.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

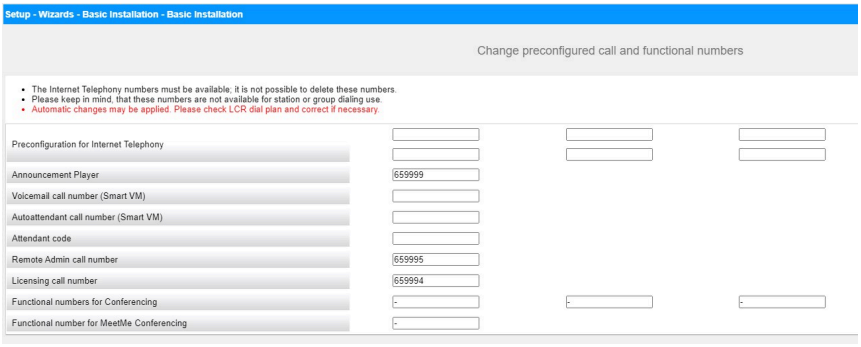
1) En la barra de navegación, haga clic en **Configuración**.
2) Haga clic en **Editar** para iniciar el asistente **Configuración básica**.
3) Haga clic en **Continuar**.

Nota: Puede ver un resumen de los números de teléfono actualmente configurados activando la opción **Mostrar configuración de extensiones** y haciendo clic en **Ejecutar función**.

---

4) Active la opción **Cambiar números de función y de llamada preconfigurados**.

5) Haga clic en **Ejecutar función**.



6) En los campos, introduzca los números de teléfono y códigos deseados y haga clic en **Aceptar**. Se guardan los nuevos números de teléfono y códigos.

Nota: Los números de teléfono aquí configurados no se pueden asignar como números de teléfono de extensión, números de marcación directa ni números de llamada de grupos.

---

7) Haga clic en **Cancelar** para salir del asistente **Configuración básica**.

11.1.2.3 Cómo importar números de teléfono y datos de extensión

Mediante un archivo XML se pueden importar datos de extensión definidos previamente.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Hay disponible un archivo XML en formato UTF-8 con los datos registrados. Puede consultar una plantilla XML en **Centro de servicios** > **Documentos** > **Plantillas CSV**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) Haga clic en **Editar** para iniciar el asistente **Configuración básica**.
3) Haga clic en **Continuar**.

Nota: Puede ver un resumen de los números de teléfono actualmente configurados activando la opción **Mostrar configuración de extensiones** y haciendo clic en **Ejecutar función**.

---

4) Active la opción **Importar archivo CSV para extensiones**.
5) Haga clic en **Ejecutar función**.
6) Mediante **Examinar** seleccione el archivo XML que ha creado y haga clic en **Abrir**.
7) A continuación, haga clic en **Aceptar**. Se importan los datos de extensión.

8) Haga clic en **Cancelar** para salir del asistente **Configuración básica**.

11.2 Requisitos a la telefonía LAN

Por Telefonía LAN se entiende la comunicación de extensiones IP dentro de la red interna (LAN). Para garantizar la calidad de la transmisión de voz en la telefonía LAN, las redes IP utilizadas y el sistema de comunicación deben cumplir determinados requisitos. La calidad de voz y la fiabilidad de la comunicación de voz dependen de la técnica de redes utilizada.

Para garantizar una transmisión sin pérdidas y una buena calidad de voz, las señales de voz se digitalizan con códecs de sonido. A su vez, las señales se identifican a través de un procedimiento especial (Quality of Service) y esa identificación permite dar un trato preferente a la transmisión de voz frente a la de datos.

Requisitos

- LAN con mín. 100 100 Mbit/s y Full Duplex
- Todos los componentes de la red IP deben estar conectados a un puerto propio, a un conmutador o a un router. No utilizar HUB.
- Retardo máximo de 50 ms en una dirección (One Way Retardo); Retardo máximo total 150 ms
- Pérdida de paquetes inferior al 3%; si se utiliza FAX/módem por G.711, la pérdida de paquetes no puede ser superior al 0,05%.
- Jitter (variación en el retardo) máximo 20 ms
- Compatibilidad para Calidad del servicio (QoS): IEEE 802.p, DiffServ (RFC 2474) o ToS (RFC 791)
- Carga de red inferior al 40%

11.2.1 Códecs de sonido

Se denomina códec de sonido un programa que codifica o y descodificar la voz en paquetes de datos digitales (paquetes IP). En función del códec de sonido que se utilice, se pueden aplicar a los datos distintos niveles de compresión. Con compresión, la transmisión del paquete IP necesita menos ancho de banda que sin compresión. Ahora bien, al descodificar los paquetes de datos se puede perder calidad de voz y continuidad de la reproducción.

Para poder descomprimir correctamente los datos de voz después del transporte, el destinatario debe tener el mismo códec que el remitente.

Códecs de sonido compatibles

Son compatibles estos códecs de sonido:

- G.729A, G.729AB: codificación de voz con 8 kbps: buena calidad de voz.
- G.711 (A-law y µ-law): codificación de voz con 56 o 64 Kbit/s: muy buena calidad de voz. G.711 se utiliza en el área de red fija (RDSI).

Los códecs de sonido reciben asignadas prioridades del 1 (alta) a 4 (baja). El sistema de comunicación intenta automáticamente utilizar un códec de

sonido con una prioridad alta en cada conexión. Si se utiliza un códec de sonido de baja compresión (buena calidad de voz), se carga más la red. Si el uso de la telefonía IP es intensivo, la calidad de voz se puede ver afectada negativamente si la red ya se sobrecarga en la transferencia de datos.

Con algunos códecs, el sistema de comunicación puede activar una detección automática de pausas de voz (VAD, Voice Activity Detection). Esto puede reducir la carga de la red durante pausas de voz prolongadas.

Se puede indicar el tamaño marco (tamaño del paquete IP) de cada códec. El valor estará entre 10 y 90 milisegundos. De esta forma, establece la frecuencia de muestreo con la que la señal de voz se dividirá en paquetes IP. Si bien un valor más alto (90 ms, por ejemplo) da como resultado una mejor relación entre la carga útil y la sobrecarga del paquete IP, también aumenta el retraso de transferencia.

Existe la opción de desactivar los códecs G.729, que consumen muchos recursos y utilizar solo los códecs G.711. De esta forma, se optimiza el número de llamadas que se pueden realizar en paralelo. Si se activa esta función, hay que reiniciar el sistema.

En los sistemas OSBiz X, la carga útil termina en el sistema, por lo que los usuarios hablan con un códec compatible con el sistema. Por ejemplo, el teléfono HFA primero configuró el códec G.722. El sistema no admite el códec G.722 y el códec G.711 se ha configurado como su primera opción. En este caso, los dos usuarios hablarán con el códec G.711. En cuanto a los sistemas OSBiz, los usuarios hablarán con el códec G.722, aunque haya carga útil de extremo a extremo.

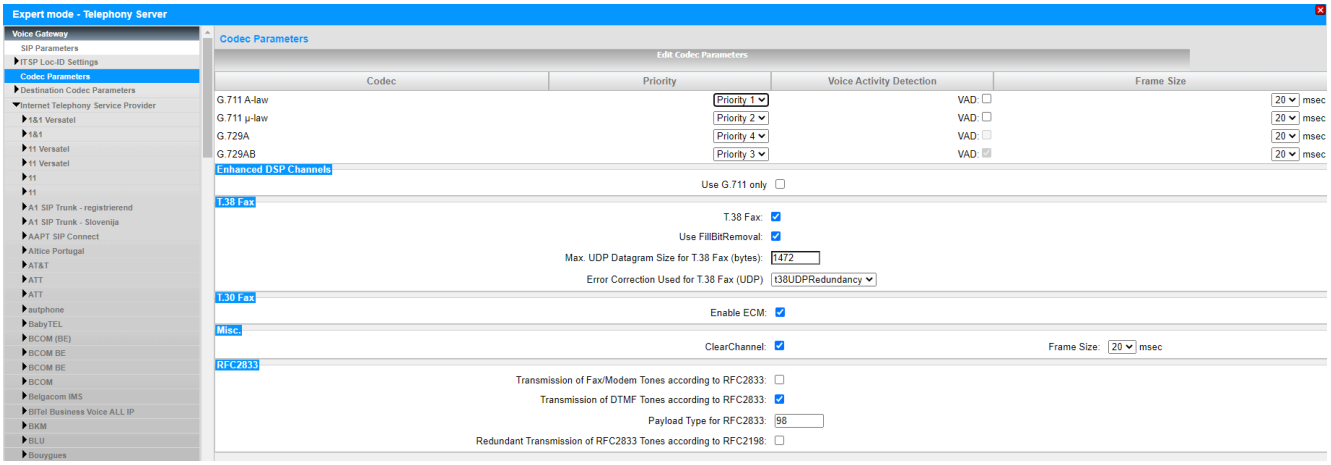
11.2.1.1 Cómo configurar parámetros de códec de sonido

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Gateway de voz**.
3) En el grupo de menús, haga clic en **Parámetros codec**.



4) A través de la lista desplegable **Prioridad** asigne a los códecs de sonido deseados una prioridad del 1 (alta) al 4 (baja).
5) Active o desactive la opción **Detección pausas voz (VAD)** en los códecs de sonido deseados.
6) En el campo **Tamaño marco** del códec de sonido deseado, establezca el tamaño en el que el códec de sonido descompondrá los paquetes de voz IP.

Nota: Debe introducir el mismo valor para todos los códecs, por ejemplo 20 mseg. No es posible configurar valores diferentes para cada códec.

---

7) Si solo desea utilizar los dos códecs de sonido G.711, en el área **Canales de DSP mejorados** active la casilla de verificación **Utilice sólo G.711**.
8) Haga clic en **Aplicar**, seguido de **Aceptar**.

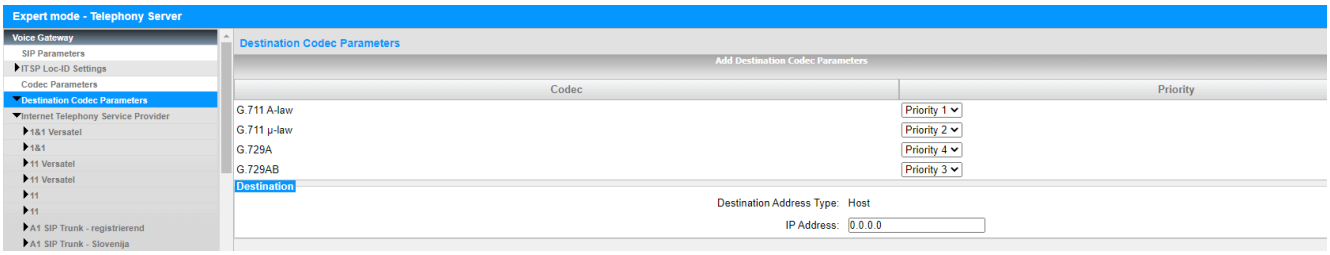
11.2.1.2 Cómo asignar parámetros de códec de sonido a un destino

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Gateway de voz**.
3) En el grupo de menús, haga clic en **Parám. codec destino**.



4) A través de la lista desplegable **Prioridad** asigne a los códecs de sonido deseados una prioridad del 1 (alta) al 4 (baja).
5) En **Dirección IP**, indique la dirección IP del destino al que quiere asignar las prioridades de los códecs de sonido definidas previamente (p. ej., `192.168.1.10`).
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

11.2.2 Transmisión de tonos MF a RFC2833

La transmisión de tonos DTMF y de fax/módem según RFC2833 se puede activar o desactivar.

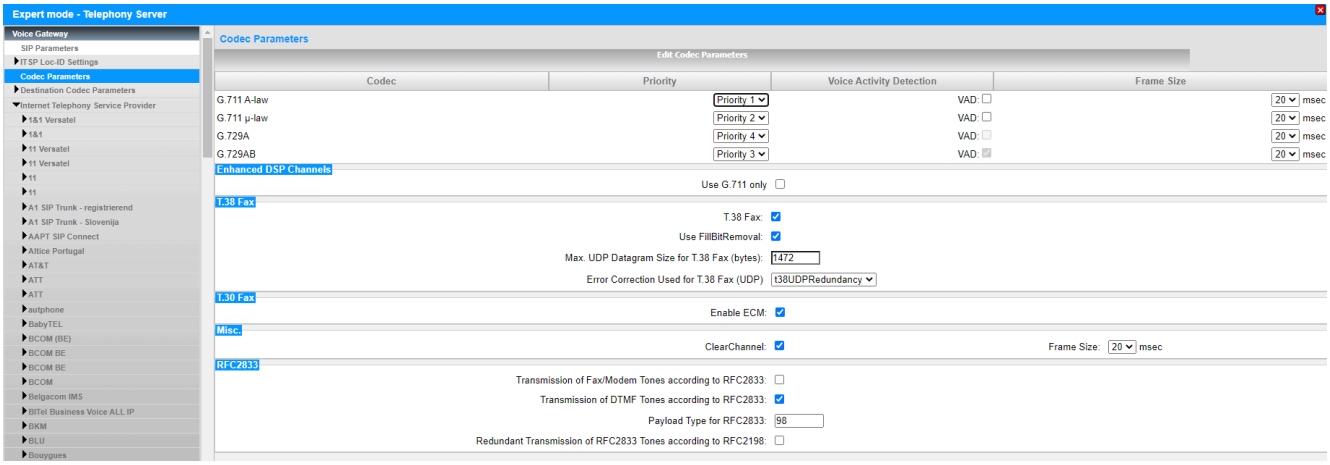
11.2.2.1 Cómo activar o desactivar la transferencia de tonos de fax y módem según RFC2833

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Gateway de voz**.
3) En el grupo de menús, haga clic en **Parámetros codec**.



4) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Transmisión de tonos fax/módem a RFC2833**.
   - Si desea desactivar la función, desactive la casilla de verificación **Transmisión de tonos fax/módem a RFC2833**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

11.2.2.2 Cómo activar o desactivar la transferencia de MF según RFC2833

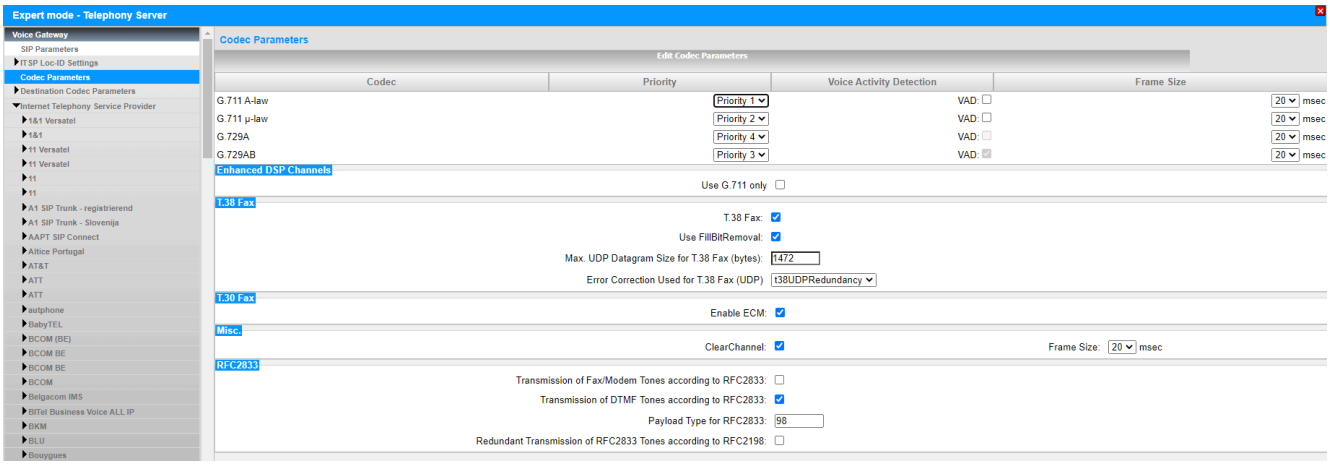
Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Gateway de voz**.

3) En el grupo de menús, haga clic en **Parámetros codec**.



4) Elija una de estas opciones:

- Si desea activar la función, active la casilla de verificación **Transmisión de tonos DTMF a RFC2833**.
- Si desea desactivar la función, desactive la casilla de verificación **Transmisión de tonos DTMF a RFC2833**.

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

11.2.3 Calidad del servicio

Calidad del servicio (QoS) es un concepto que engloba distintos procedimientos para garantizar la transmisión de paquetes de datos (paquetes IP) con la máxima calidad posible y sin pérdidas. Para conseguir una buena calidad de voz en la transmisión, QoS da mayor prioridad en la red IP a los paquetes de voz IP que a los paquetes de datos IP de otras aplicaciones.

Para la priorización, se asigna un marcado especial (punto de código) a los paquetes IP. La información de priorización crea una clasificación en distintos niveles. Si los componentes disponibles en la red IP (p. ej., sistema de comunicación, extensiones SIP y router Internet) son compatibles con QoS, pueden asignar a esas clases distintos anchos de banda y transportar así con preferencia los paquetes de voz IP.

Clases de prioridad según DiffServ

Para la priorización con el procedimiento DiffServ, se definen diferentes puntos de código para el campo Tipo de Servicio (ToS), a fin de asignar diferentes clases a la transferencia de paquetes IP.

- Punto de código Expedited Forwarding (EF / Reenvío expeditivo): garantiza un ancho de banda constante. Los paquetes IP marcados con este punto de código disponen siempre del mismo ancho de banda. Si se alcanza el valor establecido, todos los paquetes que superen ese ancho de banda son rechazados.
- Punto de código Assured Forwarding (AF / Reenvío garantizado): garantiza un ancho de banda mínimo. Los paquetes IP marcados con este punto de código tienen una prioridad más baja que los EF y deben distribuirse el

ancho de banda no utilizado por EF. Si se alcanza el valor establecido, todos los paquetes IP que superen ese ancho de banda son rechazados.

Hay cuatro clases reservadas para AF: AF1x (prioridad baja), AF2x, AF3x y AF4x (prioridad alta), donde x se corresponde con uno de tres niveles de dropping:bajo (1), medio (2) y alto (3). En el nivel bajo, los paquetes se almacenan en la memoria intermedia durante mucho tiempo mientras que con el nivel alto, se descartan rápidamente si no se pueden retransportar.

- Best Effort (BE): los paquetes IP sin marcar (campo Tipo de Servicio (ToS)=00) se tratan con la prioridad más baja.

Clases de prioridad según IP Precedence

Además del procedimiento DiffServ, existen definiciones más antiguas que priorizan sobre la base del campo ToS. Para una adaptación óptima del sistema de comunicación a los ajustes de configuración necesarios en caso necesario en la red de clientes se pueden seleccionar, por ejemplo, las clases 3 a 7 (CS3-CS7) para IP Precedence.

Clases de prioridad individuales

Si en la red de clientes no se utilizan las opciones preconfiguradas, el valor ToS también se puede configurar de forma manual. El valor configurado se configura con valor decimal 0-63 y se aplica en los 6 bits superiores del byte ToS (p.ej. 41 = 101-001-00 = 0xA4).

Tabla de clases de prioridad posibles

Clase de prioridad	Valor ToS binario	Valor ToS hexadecimal
AF (Assured Forwarding)		
AF11	001-010-00	28
AF12	001-100-00	30
AF13	001-110-00	38
AF21	010-010-00	48
AF22	010-100-00	50
AF23	010-110-00	58
AF31	011-010-00	68
AF32	011-100-00	70
AF33	011-110-00	78
AF41	100-010-00	88
AF42	100-100-00	90
AF43	100-110-00	98
EF (Expedited Forwarding)		
EF	101-110-00	B8
Best Effort (BE)		
BE	000-000-00	00
CS (Class Selector)		

Clase de prioridad	Valor ToS binario	Valor ToS hexadecimal
CS3	011-000-00	60
CS4	100-000-00	80
CS5	101-000-00	A0
CS6	110-000-00	C0
CS7	111-000-00	E0
Entrada manual	xxx-xxx-00	0-63 (decimal)

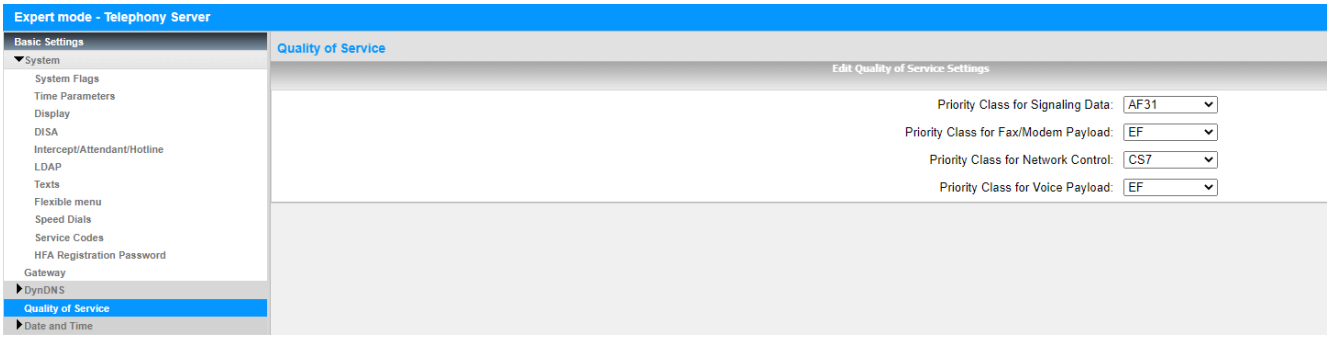
11.2.3.1 Cómo configurar Quality of Service

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Quality of Service**.



4) En la lista desplegable **Clase de prioridad para datos señalización**, seleccione la clase de prioridad deseada.
5) En la lista desplegable **Clase prioridad para payload fax/módem**, seleccione la clase de prioridad deseada.
6) En la lista desplegable **Clase de prioridad para control de red**, seleccione la clase de prioridad deseada.
7) En la lista desplegable **Clase de prioridad para payload voz** seleccione la clase de prioridad deseada.
8) Haga clic en **Aplicar**, seguido de **Aceptar**.

11.3 Extensiones IP

Las extensiones IP se conectan con el sistema de comunicación a través de la LANM. Por norma general, una extensión IP es un teléfono LAN o WLAN.

Se admiten los siguientes protocolos IP:

- Protocolo dependiente del fabricante del sistema de comunicación

  El sistema de comunicación utiliza el CorNet-IP (protocolo de Internet CorNet) desarrollado a partir de H.323 para la telefonía LAN dentro de la red interna. Con CorNet-IP se pueden utilizar todas la prestaciones telefónicas del sistema de comunicación.
- SIP (Session Initiation Protocol)

  El protocolo SIP suele utilizarse en la telefonía Internet, pero no está restringido a ella. Se puede utilizar también, por ejemplo, en la telefonía en redes internas. Con SIP, sin embargo, no se pueden utilizar todas las prestaciones telefónicas del sistema de comunicación.

Estos son los tipos de extensiones IP:

- **Cliente sist.**: un cliente del sistema es una extensión IP que puede utilizar todas las prestaciones del sistema de comunicación mediante CorNet-IP. Puede ser, por ejemplo, un teléfono de sistema IP como OpenStage 60 HFA o un PC con software CTI como OpenScape Personal Edition.
- **Cliente SIP**: un cliente SIP es una extensión IP que utiliza el protocolo SIP. A través de SIP solo puede utilizar un conjunto de prestaciones restringido del sistema de comunicación. Un clientes SIP es, por ejemplo, un teléfono SIP como OpenStage 15 S.
- **Usuario Deskshare**: un usuario Deskshare es una extensión IP que puede iniciar sesión en otro teléfono del sistema IP (Mobile Login) y utilizarlo como si fuera el suyo propio (incl. número de teléfono).
- **RAS-User**: un RAS User (Remote Access Service User) tiene garantizado el acceso a la red IP a través de la conexión RDSI. De esta forma, el sistema de comunicación se puede gestionar de forma remota.

Por cada extensión IP conectada se requiere una licencia de extensión "IP User".

Hay dos extensiones IP reservadas para el usuario online y para el acceso remoto a través de RDSI. Estas extensiones IP no necesitan licencia de extensión. Si no se requieren una o varias de las tres extensiones reservadas, se pueden convertir en extensiones IP normales a través del Modo Experto. En ese caso, para las extensiones IP se utilizan licencias de extensión.

Configuración de las extensiones IP

En una extensión IP pueden establecerse estas configuraciones:

- Configuración de los parámetros estándar con el asistente **Terminales IP** (véase Cómo configurar extensiones IP).
- Configuración de todos los parámetros (parámetros estándar y parámetros avanzados) a través del modo Experto (véase >Extensión>Extensión>Clientes IP).

Los teléfonos del sistema IP OpenScape Desk Phone se suministran de forma estándar con el software SIP. Si se configura un teléfono del sistema IP OpenScape Desk Phone en la Gestión basada en Web (WBM) como **Cliente del sistema**, el software HFA memorizado en el sistema de comunicación se carga automáticamente en el teléfono del sistema IP.

11.4 Estaciones SIP

Las estaciones SIP son estaciones IP que utilizan el Protocolo de inicio de sesión (SIP) para la comunicación. Las estaciones SIP pueden utilizar este protocolo para acceder a un número limitado de funciones del sistema de comunicación. Las estaciones SIP, al igual que las estaciones IP, están conectadas al sistema de comunicación a través de la LAN.

Una estación SIP es un teléfono WLAN o un teléfono LAN como, por ejemplo, el OpenStage 15 S.

Para cada estación SIP conectada, se requiere una licencia de estación "Usuario IP".

Autenticación SIP

Para garantizar la seguridad de la red interna, es importante que los suscriptores SIP estén autenticados en el sistema de comunicación con los valores que se describen a continuación. Estos valores deben configurarse en el WBM del sistema de comunicación para cada suscriptor SIP y también en cada teléfono SIP. Para protegerse contra ataques SIP, ¡se recomienda encarecidamente la autenticación!

- Contraseña

  Contraseña para autenticación: asignada libremente; mínimo 8 caracteres hasta un máximo de 20 caracteres. La contraseña debe contener al menos una letra mayúscula, una letra minúscula, un dígito y un carácter especial. Se debe asignar una contraseña separada para cada suscriptor SIP.
- SIP usuario / Nombre usuario

  Nombre de usuario para autenticación: preasignado, se puede cambiar si es necesario, máximo 20 caracteres. Cada suscriptor SIP tiene un ID de usuario SIP preasignado diferente.
- Ámbito

  Zona o dominio para autenticación: asignado libremente, modificable si es necesario, máx. 20 caracteres. El reino para todos los suscriptores SIP está preasignado con el mismo valor. Se puede cambiar según sea necesario, por ejemplo, en el nombre de host o en el nombre de dominio del sistema de comunicación.

Configuración de estaciones SIP en el sistema de comunicación

Las siguientes configuraciones se pueden realizar en el WBM del sistema de comunicación para una estación IP:

- Configuración de parámetros estándar con el asistente de **Teléfonos IP** (ver Cómo configurar estaciones SIP).
- Configuración de todos los parámetros (parámetros estándar y avanzados en modo Experto (ver Estación>Estación>Clientes IP).

Configuración del teléfono SIP

Los datos utilizados para autenticar un suscriptor SIP en el sistema de comunicación también deben ingresarse directamente en el teléfono SIP.

Configuración de los datos de autenticación en el teléfono SIP (ver Configuración de los datos de autenticación en el teléfono SIP).

Funciones que se pueden utilizar con teléfonos SIP

Las siguientes funciones se pueden utilizar con teléfonos SIP:

- Llamadas entrantes y salientes con visualización del número de llamada y nombre
- Mantener, alternar/conectar, consulta
- Transferencia de llamadas (filtradas/no filtradas)
- Tomar llamada
- Desvío de llamadas inmediato, en caso de ocupación y después del tiempo de espera
- Conferencia tripartita
- Listas de llamadas, indicador de mensajes en espera
- Corte de timbre en el teléfono, rechazo de llamada, desvío de llamadas
- Aviso llam. en espera
- Pertenencia a grupos (sin visualización del número de grupo)
- Diferentes convocatorias internas, externas y de retirada
- LED del buzón: indicación de mensaje en espera
- Marcación DTMF, por ejemplo, para el funcionamiento de buzones de correo de voz
- Uso de los clientes UC
- Actualizaciones automáticas de software (al utilizar DLI)

Nota: No se ha liberado la implementación con un centro de contacto multicanal (por ejemplo, transferencia a grupos UCD).

Dependiendo del teléfono, puede haber algunas restricciones en las funciones disponibles; consulte la wiki en:

`http://wiki.unify.com/wiki/SIP_devices_configuration_examples`

Las siguientes funciones, que se activan mediante códigos de servicio con * o #, se pueden utilizar con teléfonos SIP:

- Restablecer todos los servicios: #0
- Reenvío de llamadas: *1xf (x = 1 - todos, 2 - internos, 3 - externos) (f = número de reenvío)
- Desvío de llamadas desactivado: #1
- Abandonar/Volver a unirse al grupo de búsqueda: #85g/*85g (g = número de grupo, opcional - necesario cuando se está en varios grupos)
- Suprimir/Habilitar identificación de llamada (CLIR): *86/#86
- Marcación rápida: * 7nnnn (nnnn = número de marcación rápida)
- Abridor de puerta: *61

Consejo: Se recomienda utilizar códigos de sustitución * o # para una mejor compatibilidad con dispositivos SIP de terceros. El usuario SIP debe enviar la secuencia completa del código de servicio como una marcación en bloque.

Consejo: A diferencia de los dispositivos HFA, en los dispositivos SIP no hay interacción del usuario ni orientación

para las secuencias de códigos de servicio. La secuencia completa del código de servicio se debe marcar de inmediato.

Funciones que se pueden utilizar con teléfonos SIP y myPortal/ myAttendant

Los teléfonos SIP que se utilicen con myPortal y myAttendant deben cumplir los siguientes requisitos:

- Se admite 3PCC según RFC 3725.
- Se admite la función de "llamada en espera".
- El modo No molestar local está deshabilitado.

La funcionalidad completa de las funciones depende del teléfono SIP utilizado y no se puede garantizar. Se realizó una prueba exitosa de las funciones enumeradas a continuación con los teléfonos SIP OpenStage.

Funciones orientadas a la conexión/llamada:

- Llamar
- Redirigir llamada
- Tomar llamada
- Reanudar llamada
- Conferencia controlada por aplicaciones
- Poner llamada en espera
- Alternar (Alternar/Conectar)
- Consulta
- Desconectar
- Transferir

Funciones orientadas al teléfono:

- No molestar
- Desvío de llamadas

11.5 Extensiones UP0

Las extensiones UP0 utilizan una línea $U_{P0/E}$ para transmitir las señales digitales. Las extensiones UP0 se conectan con el sistema de comunicación mediante interfaces UP0 y son teléfonos del sistema como, p. ej., un OpenStage 60T. Las extensiones UP0 pueden utilizar todo el abanico de funciones del sistema de comunicación.

Estas son las opciones de conexión para las extensiones UP0:

- OpenScape Business X1

  Con las interfaces $U_{P0/E}$ de la placa base.
- OpenScape Business X3/X5

  con las interfaces $U_{P0/E}$ de la placaba base o, en muchas extensiones UP0, con módulos $U_{P0/E}$ adicionales.
- OpenScape Business X8

  con módulos $U_{P0/E}$ adicionales.
- OpenScape Business S

  sin conexión.

Por cada extensión UP0 que haya conectada se requiere una licencia de extensión "TDM User". También los teléfonos del sistema conectados en modo esclavo necesitan una licencia de extensión.

Configuración de las extensiones UP0

En una extensión UP se pueden llevar a cabo estas configuraciones:

- Configuración de los parámetros estándar con el asistente **Terminales UP0** (véase Cómo configurar extensiones UP0).
- Configuración de todos los parámetros (parámetros estándar y parámetros avanzados) a través del modo Experto (véase Extensiones>Extension>Extensiones UP0).

11.6 Extensiones DECT

Para la transmisión de las señales digitales las extensiones DECT utilizan una extensión base Cordless. Las extensiones DECT son teléfonos DECT.

Estas son las opciones de conexión de las extensiones DECT:

- OpenScape Business X1W/X1R/X3W/X3R/X5R

  Extensión base Cordless con una interfaz $U_{P0/E}$ de la placa base.
- OpenScape Business X8

  Extensión base Cordless con un módulo SLMUC o varios.
- OpenScape Business S

  Extensión base IP DECT de la LAN

La conexión de una extensión base Cordless se denomina solución Cordless integrada. Con este tipo de solución, están disponibles casi todas las funciones del sistema de comunicación.

La integración de una extensión base IP DECT en la red interna se denomina IP Cordless. En este caso solo se puede utilizar el protocolo SIP, por lo que no están disponibles todas las funciones del sistema de comunicación.

Por cada extensión DECT conectada se requiere una licencia de extensión "TDM User".

Para consultar la descripción y configuración de la solución Cordless integrada, consulte Solución Cordless integrada.

Configuración de las extensiones DECT

En una extensión DECT se pueden llevar a cabo estas configuraciones:

- Configuración de los parámetros estándar con el asistente **Terminales DECT** (véase Cómo configurar extensiones DECT).
- Configuración de todos los parámetros (parámetros estándar y avanzados en modo Experto (véase Extensión>Extensión>Extensiones DECT>Extensiones DECT).

Las extensiones IP DECT se configuran como extensiones SIP normales.

11.7 Estaciones SIP DECT de Mitel

Las siguientes opciones de conexión están disponibles para las estaciones Mitel SIP DECT:

- Sistemas OpenScape Business S
- Hardware de OpenScape Business V3 (OCCe)

Aprovisionamiento de estaciones RFP SIP DECT de Mitel

El proceso incluye los siguientes pasos generales:

1) Configure el DHCP con una dirección IP estática para la estación base OMM.
2) La estación base obtendrá una dirección IP e iniciará la aplicación OMM.
3) Configure la estación base a través de su interfaz web.
4) La estación base obtendrá automáticamente los archivos de configuración de OpenScape Business.
5) Cuando un teléfono inicia sesión, la estación base también obtendrá el archivo de configuración del usuario y configurará el teléfono.

Configuración de estaciones SIP DECT de Mitel a través de WBM

Se deben realizar los siguientes pasos de configuración:

1) Habilite el servidor DHCP y proporcione una dirección IP estática para la estación base OMM (consulte Interfaces de red > Placa base > Modo DHCP > Servidor DHCP > Direcciones IP estáticas)).
2) Configuración de parámetros estándar con el asistente de dispositivos Mitel SIP DECT (consulte Cómo configurar estaciones Mitel SIP DECT).
3) Configuración de estaciones SIP y sus parámetros a través del modo Experto (ver Cómo configurar estaciones SIP a través del modo Experto).

11.8 Extensiones RDSI

Para la transmisión de las señales digitales, las extensiones RDSI utilizan el bus S_0. Por eso, suelen denominarse también extensiones S_0. La extensión RDSI se conecta con el sistema de comunicación a través de las interfaces S_0.

Estas son las opciones de conexión para las extensiones S_0:

- OpenScape Business X1

  con una interfaz S_0 de la placa base.
- OpenScape Business X3/X5

  con una interfaz S_0 de la placa base o un módulo S_0.
- OpenScape Business X8

  con uno o varios módulos S_0.
- OpenScape Business S

  con gateways o adaptadores adicionales

Se pueden conectar las siguientes extensiones RDSI:

- Teléfono RDSI
- Fax Grupo 4

- Módem RDSI
- PC con tarjeta RDSI

Se pueden definir los siguientes tipos de extensiones RDSI:

- Estándar: para teléfono RDSI, Fax Grupo 4, Módem RDSI o PC con tarjeta RDSI
- Fax: requisito para la configuración de la tecla "Info de fax/cont. aut.". Si, por ejemplo, se conecta un PC con tarjeta RDSI y software de fax al bus S_0 y se le asigna el tipo "Fax", se puede configurar en cada terminal una tecla "Info de fax/cont. aut.". Al iluminarse, la tecla señaliza la recepción de un fax.
- Contestador automático: requisito para la telecaptura de una llamada, si el contestador automático ya ha aceptado la llamada. Si, por ejemplo, se conecta un Gigaset RDSI con contestador automático y se le asigna el tipo "Contestador automático", en cada terminal se podrá capturar una llamada que ya haya aceptado el contestador automático. Para ello, hay que programar en el terminal una tecla con el número de teléfono interno del Gigaset.

Por cada extensión RDSI conectada se requiere una licencia de extensión "TDM User".

Conexión de extensiones RDSI a la interfaz S_0

Para poder conectar extensiones RDSI al sistema de comunicación, al menos una de las interfaces S_0 utilizadas para la conexión de extensión RDSI o para la conexión de centralita RDSI debe estar configurada como bus S_0 interno (Euro-Bus S_0).

Nota: Si en un acceso individual RDSI, se conectan varias extensiones RDSI a una interfaz S_0 (hasta un máximo de 8 extensiones RDSI), cada una de las extensiones RDSI debe tener asignado un MSN único e inequívoco. Esta asignación se realiza en el menú de configuración de la extensión RDSI.

Configuración de las extensiones RDSI

En una extensión RDSI se pueden llevar a cabo estas configuraciones:

- Configuración de los parámetros estándar con el asistente **Terminales RDSI** (véase Cómo configurar extensiones RDSI).
- Configuración de todos los parámetros (parámetros estándar y parámetros avanzados) a través del modo Experto (véase Extensiónes>Extension>Extensiones RDSI).

Permitir solo números configurados para MSN

El administrador puede establecer que solo se puedan configurar otros MSN en un Bus-S0 para los números de teléfono internos ya disponibles. Es este caso, los usuarios no pueden agregar un MSN de forma no autorizada al ocupar el bus S0 con otro MSN de forma saliente y asignando al bus S0 un número de teléfono interno libre para ese MSN.

Portabilidad de terminales

El sistema de comunicación permite el cambio en el bus (TP o Portabilidad de terminales), esto es, aparcar una comunicación en el bus S_0, desconectando y

conectando a continuación el terminal en otra ubicación. Por último la llamada vuelve a ser aceptada. El usuario aparcado recibe un mensaje en display indicando que se está realizando este proceso. Para todo el proceso se dispone de tres minutos.

Esta prestación no tiene soporte en servicios como telefax, teletex o transmisión de datos.

11.8.1 Cómo configurar interfaces S_0 para extensiones RDSI

El asistente **Línea urbana RDSI / analógico / ITSP** permite configurar una o varias interfaces S_0 de forma que se puedan conectar a ellas teléfonos RDSI.

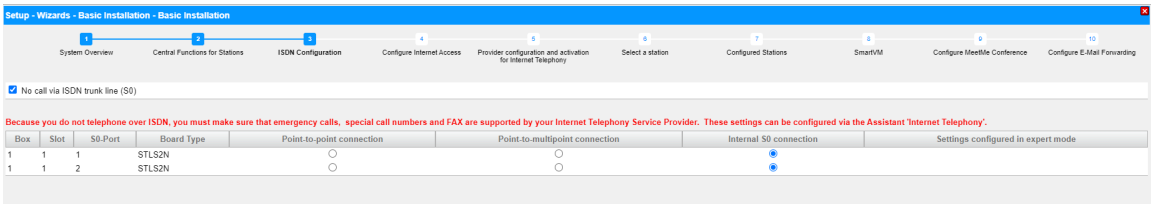
Requisitos previos

Hay disponibles una o varias interfaces S_0 libres.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) En el asistente **Línea urbana RDSI / analógico / ITSP**, haga clic en **Editar**.
4) Haga clic en **OK & Continuar**. Aparecen las interfaces S_0 (puertos S_0) disponibles.



5) No cambie el valor de la casilla de verificación **Sin comunicación a través de la lín. urbana RDSI (S0)**.
6) En las interfaces S_0 deseadas active el campo de opción **Conexión S0 interna**.

> **Nota:** Estas interfaces S_0 ya no se pueden seguir utilizando para el acceso a línea urbana RDSI.

7) Haga clic varias veces en **OK y Continuar**, hasta que aparezca un mensaje indicando que ha finalizado la modificación de la prestación.
8) Haga clic en **Salir**.

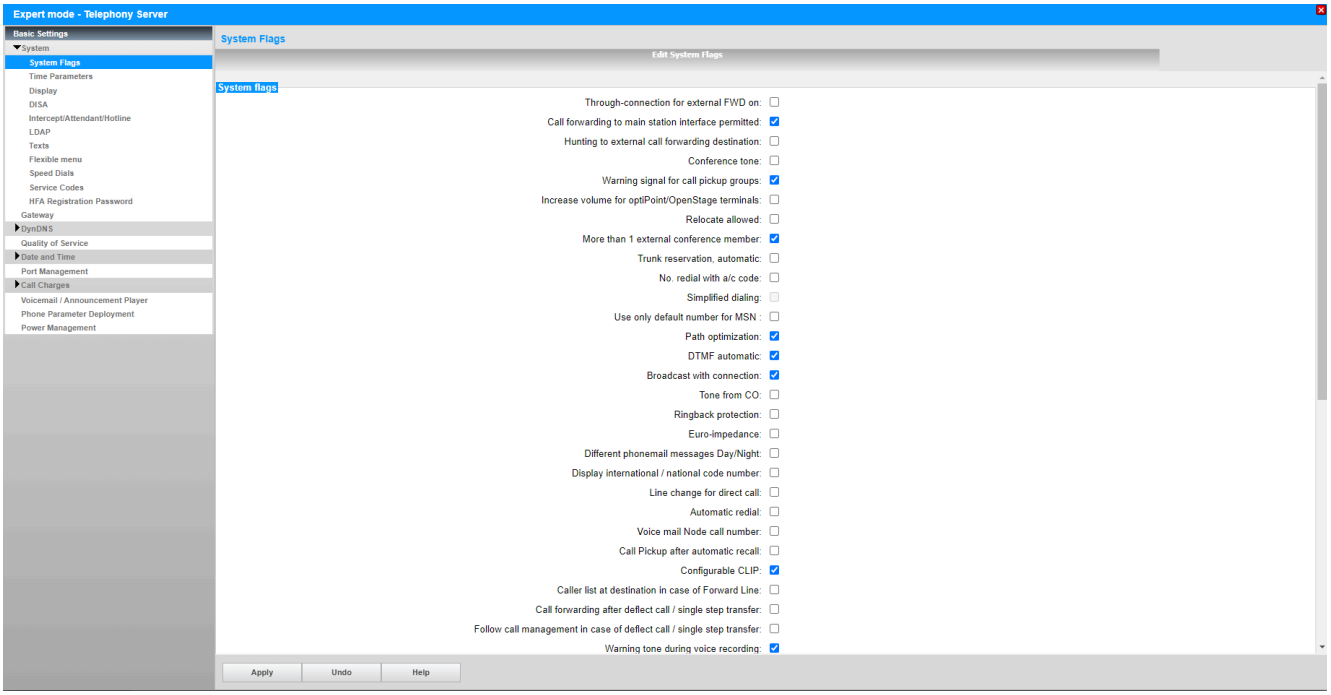
11.8.2 Cómo permitir solo números configurados para MSN

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **Flags del sistema**.



4) Si solo desea permitir números configurados para MSN, active la casilla de verificación **Utilizar solo números configurados para MSN**.
5) Si no desea permitir de forma exclusiva números configurados para MSN, desactive la casilla de verificación **Utilizar solo números configurados para MSN**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

11.9 Ext. analógicas

Una extensión analógica (extensión a/b) utiliza para la transmisión de las señales analógicas una línea a/b de dos hilos. La extensión analógica se conecta con el sistema de comunicación a través de las conexiones a/b.

Estas son las opciones de conexión para las extensiones analógicas:

- OpenScape Business X1

  Con una interfaz analógica de la placa base.
- OpenScape Business X3/X5

  con una interfaz analógica de la placa base o con un módulo analógico.
- OpenScape Business X8

  con uno o varios módulos analógicos.

- OpenScape Business S

  con gateways o adaptadores adicionales

Se pueden conectar las siguientes extensiones analógicas:

- Teléfono analógico
- Fax analógico (Grupo 3)
- Contestador automático
- Módem a partir de 9600 bit/s
- Portero eléctrico
- Altavoz

Se pueden definir los siguientes tipos de extensiones analógicas:

- Estándar: para Teléfono analógico, Grupo de fax 3, Contestador automático o Altavoz
- Fax: requisito para la configuración de la tecla "Info de fax/cont. aut.". Si por ejemplo se conecta un Grupo de fax 3 y se le asigna el tipo "Fax", en cada terminal se puede configurar una tecla "Info de fax/cont. aut.". Al iluminarse, la tecla señaliza la recepción de un fax.
- Contestador automático: requisito para la telecaptura de una llamada, si el contestador automático ya ha aceptado la llamada. Si, por ejemplo, se conecta un Gigaset con contestador automático y se le asigna el tipo "Contestador automático", en cada terminal se podrá capturar una llamada que ya haya aceptado el contestador automático. Para ello, hay que programar en el terminal una tecla con el número de teléfono interno del Gigaset.
- Módem: no se admite el uso de módems analógicos con una velocidad fija de 56 kbit/s o más ya que no se pueden procesar velocidades de 56 kbit/s o superiores.

Por cada extensión analógica conectada se necesita una licencia de extensión "TDM User".

Accesibilidad de un equipo de fax analógico en el sistema con el número de fax anterior

Como los dispositivos de fax analógico no se pueden desviar a un número de fax del sistema, existe la siguiente solución: el número de fax previo se configura en el sistema y pasa a recibir los mensajes de fax entrantes. En el equipo de fax analógico se configura un puerto con el número anterior como CLIP. La opción CLIP ajustable debe estar activada. Los mensajes de fax enviados al exterior muestran el número anterior como remitente; los destinatarios internos ven el número interno del equipo de fax.

Configuración de las extensiones analógicas

En una extensión analógica se pueden establecer estas configuraciones:

- Configuración de los parámetros estándar con el asistente **Terminales analógicos** (véase Cómo configurar extensiones analógicas).
- Configuración de todos los parámetros (parámetros estándar y parámetros avanzados) a través del modo Experto (véase Extensiónes>Extension>Ext. analógicas).

11.10 Ext. virtuales

Las extensiones virtuales se comportan como extensiones reales, pero no tienen asignado ningún terminal físico.

Se requieren extensiones virtuales, por ejemplo, para la integración de teléfono móvil y para la transferencia automática diferida. Deben configurarse como extensiones reales, por ejemplo, para ser utilizadas para la señalización de llamadas.

Configuración de las extensiones virtuales

Los parámetros de una extensión virtual se configuran en Modo Experto (véase Extensiónes>Extension>Extensiones virtuales).

11.11 Programación de teclas

Todos los teléfonos del sistema incluyen un determinado número de teclas de función. Algunas de estas teclas de función están preconfiguradas con funciones predeterminadas. Esta ocupación se puede modificar y el resto de teclas de función no ocupadas se pueden programar con funciones.

Estas son las opciones para la programación de teclas:

- Programación de teclas mediante la Gestión basada en Web (WBM)

  El asistente **Programación de teclas** de Gestión basada en Web (WBM) permite programar las teclas de los teléfonos del sistema conectados.

  Con este asistente también se puede programar una asignación de teclas para una extensión, aunque esta todavía no esté conectada con ningún teléfono del sistema.
- Programación de teclas mediante clientes de UC

  Los usuarios de los clientes de Unified Communications **myPortal for Desktop**, myPortal for Outlook y **myAttendant** pueden programar las teclas mediante los clientes de UC (consulte las Instrucciones de uso de los clientes de UC).
- Programación de teclas directamente en el teléfono del sistema

  En los teléfonos de sistema con display también se pueden programar determinadas teclas de función directamente en el teléfono del sistema.

Programación de teclas de función en distintos niveles

Las teclas de función de los teléfonos de sistema se pueden ocupar en dos niveles, concretamente, en el nivel 1 y en el nivel 2. El nivel 1 se puede ocupar con todas las funciones disponibles. El nivel 2 se puede ocupar con números de teléfono externos. Para poder utilizar el nivel 2, el teléfono de sistema debe tener configurada la tecla de cambio de nivel (tecla Mayús). Los LED de las teclas de función pertenecen siempre al primer nivel.

Nota: En caso de un **usuario, no es posible copiar la programación de teclas ya que la función de asignación de teclas automática es específica de MULAP y no debe copiarse en ninguna extensión. El prefijo** no debe eliminarse

manualmente de estos usuarios para se active la copia de teclas.

11.11.1 Cómo programar las teclas de función de los teléfonos de sistema

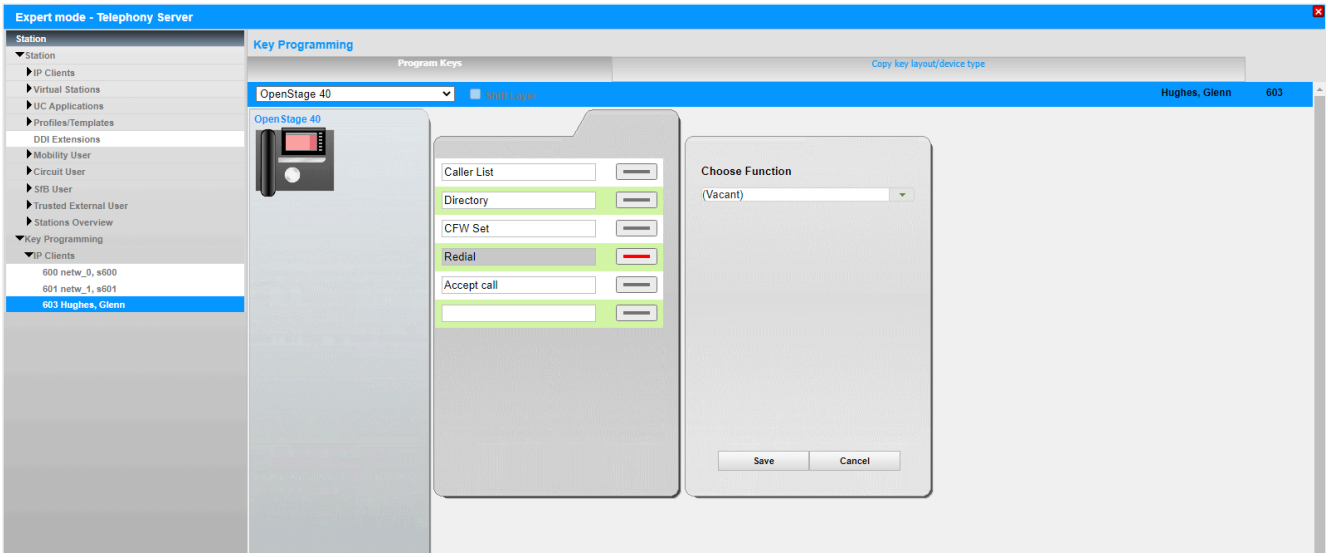
El asistente **Programación de teclas** permite configurar las teclas de función de los teléfonos de sistema.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Terminales / Extensiones**.
3) Haga clic en **Editar** para iniciar el asistente **Programación de teclas**. Aparece la lista de todas las extensiones.
4) En la línea de la extensión deseada, haga clic en **Editar**.
5) Asigne a la extensión el teléfono de sistema:
   - Si en la extensión ya hay conectado un teléfono del sistema, aparece una vista simplificada del teléfono del sistema.
   - Si en la extensión todavía no hay conectado un teléfono del sistema, en la lista desplegable seleccione el teléfono del sistema que desea conectar. A continuación, aparece una vista simplificada del teléfono del sistema seleccionado.
6) En la vista simplificada del teléfono del sistema, haga clic en el campo de teclas deseado. Aparecen las teclas de función del campo de teclas seleccionado con las funciones que tengan asignadas en ese momento.



7) Asigne las teclas de función:

a) En la tecla de función que desea asignar, haga clic en el símbolo de tecla. Aparece una lista desplegable con las funciones posibles.

b) En la lista desplegable **Seleccionar función**, seleccione una de las opciones.

c) Algunas funciones necesitan información adicional. Si es necesario, seleccione estos parámetros adicionales e introduzca los datos necesarios.

d) Haga clic en **Guardar**.

e) En el campo **Introducir nueva rotulación**, introduzca, si es necesario, la rotulación de la tecla de función.

Nota: Si tiene un teléfono del sistema con rotulación automática de teclas (p. ej., OpenStage 60 HFA), se aplica el texto del teléfono del sistema.

---

f) Haga clic en **Guardar**.

g) Si desea asignar más teclas de función, repita el paso 7.

8) Si en una tecla de función ha configurado **Conmutar nivel**, active la casilla de verificación **Conmutar nivel**. Asigne el segundo nivel de las teclas de función con los números de teléfono externos, tal y como se describe en el paso 7.

9) Haga clic en **Asumir asignación de teclas**.

10) Si desea aplicar la programación de teclas definida anteriormente en varios o en todos los teléfonos del sistema, en esos teléfonos active la casilla de verificación y, a continuación, haga clic en **Aplicar**, **Aceptar** y **OK & Continuar**.

11) Si únicamente desea aplicar la programación de teclas definida anteriormente en el teléfono del sistema seleccionado, haga clic en **Deselecc. todas las ext.** (para mayor seguridad) y, a continuación, en **OK & Continuar**.

12) Haga clic en **Cont.** y luego en **Salir**.

11.12 Perfiles de extensión

En los perfiles se guardan los valores y propiedades de las extensiones. Se pueden asignar varios miembros a un perfil. Se aplican los mismos valores y propiedades a todos los miembros de este perfil.

A los perfiles de extensión se pueden asignar extensiones con teléfonos del sistema. Se pueden crear hasta 20 perfiles de extensión. Los perfiles de extensión se pueden importar y exportar de forma individual o en conjunto. Los archivos son del tipo `xml`.

Cada extensión puede ser miembro de un perfil. Si los valores y propiedades de una extensión que es miembro de un perfil se modifican directamente (no a través del perfil), la extensión se elimina del perfil.

11.13 Configuración de las extensiones

Se pueden definir determinados valores (p. ej., número de teléfono, nombre y número de marcación directa) y propiedades (p. ej. el tipo de la señalización de llamadas) para las extensiones.

La configuración de las extensiones se divide en una configuración estándar y en una configuración avanzada. La configuración estándar se puede configurar mediante asistentes con el perfil **Avanzado**. Los ajustes avanzados solo se pueden definir con el Modo Experto y el perfil **Experto**.

Se puede modificar, cómodamente, la configuración estándar de todas las extensiones de una clase de extensión (p. ej., extensiones IP o extensiones analógicas) con una lista. Para cada usuario, se pueden cambiar ajustes adicionales de forma individual (por ejemplo, señalización de llamadas o flags de extensión).

Las extensiones virtuales se configuran íntegramente a través del Modo Experto (tanto la configuración estándar como la avanzada).

Con el perfil **Básico** no se pueden configurar las extensiones, pero sí se pueden modificar sus nombres.

Debería haber un plan de numeración para las extensiones conectadas al sistema de documentación. Los números de teléfono, los nombres y los números de marcación directa de todas las extensiones configuradas se pueden mostrar mediante el Modo Experto, en **Extensiones** > **Extensiones de marcación directa (DID)**.

Es recomendable borrar los números de marcación directa que no haya ofrecido el proveedor de servicios y que no se utilicen en el sistema, ya que de lo contrario pueden producirse conflictos con MSN o con números de extensión de telefonía Internet. Los números de marcación directa ofrecidos por un ITSP, deben asignarse al hacer la configuración del ITSP (véase Configuración de un ITSP).

Importante: Al modificar un número de teléfono de extensión, se restablece el Smart VM (Voicemail) que tuviera configurado previamente. Todos los mensajes de voz, saludos y anuncios grabados personales se pierden y se restablece la contraseña.

Configuración estándar

La configuración estándar de todas las extensiones solo se debe modificar de forma controlada y en caso de ser absolutamente necesario.

- **Número de teléfono, Nombre, Número de marcación directa**

  De forma predeterminada, todas las extensiones tienen asignado un número de teléfono (p. ej. 101). Se puede acceder a la extensión de forma interna a través de ese número de teléfono. En los teléfonos del sistema, este número de teléfono aparece indicado en el display propio y en el display del interlocutor. Si desea que en la extensión llamada externa no aparezca el número de teléfono real sino otro, puede definir ese número de teléfono alternativo.

  Además, se puede asignar a cada extensión un número de marcación directa. El número de marcación directa permite acceder directamente al usuario de forma externa. Se puede acceder al usuario, por ejemplo,

de forma interna a través del número de teléfono 101 o de forma externa a través del número de marcación directa `3654321` (MSN en el acceso individual) o del `<número de teléfono del sistema>-101` (en la conexión de centralita). En caso de conexión de centralita se puede establecer en la primera instalación si se introducirá automáticamente como número de marcación directa el número de teléfono interno. Sin embargo, el número de marcación directa también puede ser distinto al número de teléfono. Si se utiliza telefonía Internet, se puede establecer además un número de marcación directa para acceder a la extensión a través de la telefonía Internet. Ese número de teléfono es suministrado por el ITSP.

Todas las extensiones pueden tener asignado un nombre. Este nombre aparece en el display del interlocutor (solo en teléfonos de sistema).

Si hay un plan de numeración, los números de teléfono, números de marcación directa y los nombres de las extensiones deberán ajustarse en función del mismo.

- **Tipo**

  Se puede seleccionar el tipo de extensión de cada extensión. Una extensión IP, por ejemplo, puede ser del tipo de extensión **Cliente sist.** o **Cliente SIP**, una extensión analógica puede ser un teléfono analógico o un equipo de fax analógico y una extensión RDSI puede ser un teléfono RDSI o un equipo de fax RDSI.

- **Número de llamada de fax; Número DID de fax**

  Si hay que configurar un buzón de fax para un usuario (que se pueda usar con los clientes de Comunicaciones unificadas myPortal for Desktop o myPortal for Outlook, por ejemplo), asigne un número de llamada de fax (para recibir faxes internos) y un número DID de fax (para recibir faxes externos).

- **Clases de servicio**

  A una extensión se le puede asignar una de entre 15 clases de servicio diferentes. De esta forma se establece, por ejemplo, si la extensión puede aceptar y realizar llamadas externas, o qué números de teléfono puede marcar y cuáles no (véase Clases de servicio (Control de marcación)).

- **Grupos de telecaptura**

  Todos los usuarios pueden ser asignados a un grupo de telecaptura de llamadas.

- **Idioma, Señalización de llamada**

  Se puede configurar el idioma para el control de menús de los teléfonos del sistema conectados.

  Se puede seleccionar el sonido del tono de llamada para llamadas externas e internas.

- **Buzón de voz (solo con UC Smart)**

  Con la solución de Unified Communications UC Smart, se puede configurar un buzón de voz por cada extensión y elegir entre diferentes anuncios grabados de saludo. Para obtener información más detallada sobre el buzón de voz, véase Buzón de voz (SmartVM)

  Con la solución de Unified Communications UC Suite, se asigna un buzón de voz a cada extensión automáticamente. Así no hace falta realizar los ajustes del buzón de voz.

- **Flags de extensión**

  Se pueden modificar los flags de extensión de cada usuario.
  Para consultar una descripción de los flags de extensión, véase >Extensión>Extensión>Parámetros de extensión.

Configuración avanzada

A través del Modo Experto se pueden ajustar las configuraciones de todo tipo de extensiones. Para el servicio estándar no es necesario modificar los ajustes de configuración avanzada. Sólo haga cambios en esta configuración en caso de necesidad. Para información sobre la configuración avanzada, véase Extensiones.

Conceptos relacionados

Clases de servicio (Control de marcación) en la página 773
Salida de texto multilingüe en la página 1256

11.13.1 Cómo configurar extensiones IP

Con el asistente **Terminales IP** puede configurar las extensiones IP (teléfonos LAN y WLAN).

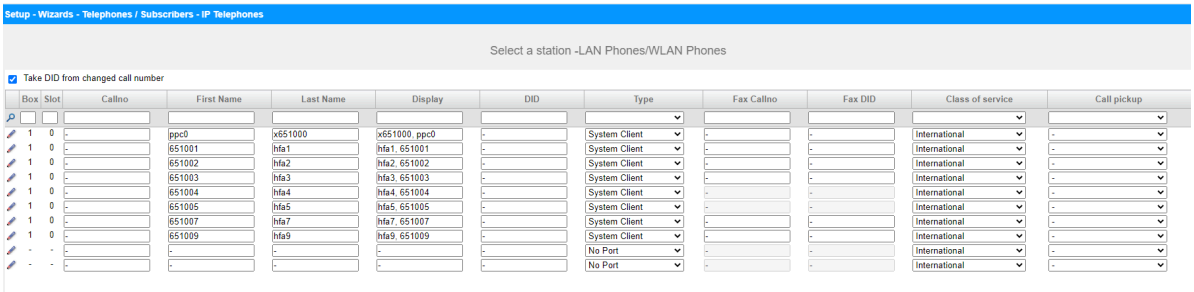
Requisitos previos

Para poder poner en servicio los teléfonos WLAN necesita una red LAN inalámbrica operativa.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Terminales / Extensiones**.
3) Haga clic en **Editar** para iniciar el asistente **Terminales IP**. Aparece una lista de todas las extensiones IP.



4) Si desea que la extensión reciba automáticamente el número de teléfono interno como número de marcación directa, active la opción **Tomar n.° llam. marc. directa del número de llamada modificado**.
5) Si desea que el número de marcación directa de la extensión sea diferente al número de teléfono, en la línea de la extensión deseada, introduzca

el número de marcación directa de la extensión en el campo **Marcación directa**:

- Solo con conexión de centralita:

  Haga clic en el campo deseado e indique el número de marcación directa a través del teclado. El número de marcación directa puede ser idéntico al número de teléfono interno.
- Solo con acceso individual:

  Seleccione un MSN a través de la lista de selección. La extensión puede configurarse, por ejemplo, de forma interna a través de un número de teléfono interno 101 o de forma externa a través del MSN 654321.
- en una conexión de centralita y acceso individual:

  En el campo deseado, y a través de la lista desplegable, seleccione la entrada **xxx - editable** (xxx es el número de teléfono interno) e indique el número de marcación directa a través del teclado o seleccione un MSN a través de la lista desplegable.

6) Si desea que la extensión reciba un número de llamada de extensión de telefonía DSL como número de marcación directa, deje desactivada la opción **Tomar n.º llam. marc. directa del número de llamada modificado**; en la lista que aparece junto al campo de opción, seleccione el proveedor de telefonía de Internet y, en la línea de la extensión deseada, seleccione el número de llamada de extensión de telefonía DSL en la lista desplegable **N.° llam. marc. directa**.

7) En la línea de la extensión deseada, en **N.º llam**, indique el número de teléfono interno de la extensión. Puede utilizar el número de teléfono preestablecido o asignar otro todavía no ocupado.

8) En la línea de la extensión deseada, y en **Nombre**, introduzca un nombre con el formato `Apellidos, Nombre` o `Nombre Apellidos`.

9) En la línea de la extensión deseada, y en la lista desplegable **Tipo**, seleccione el tipo de la extensión IP (p. ej., **Cliente de sistema** o **Usuario Deskshare**).

10) Si desea configurar un buzón de fax para la extensión (que se pueda utilizar, por ejemplo, con los clientes de UC **myPortal for Desktop** o **myPortal for Outlook**), siga este procedimiento:

a) En la línea de la extensión deseada, en el campo **Fax N.° llam**, introduzca el número de fax interno deseado con el que el usuario podrá recibir mensajes de fax internos.

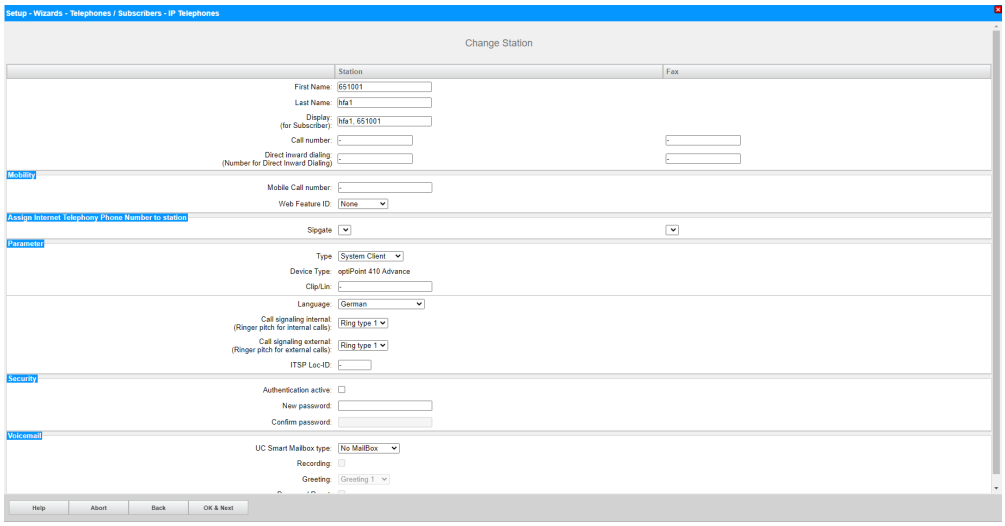
b) Si desea configurar un número de marcación directa para el buzón de fax, en la línea de la extensión deseada (en el campo **Marcación directa de fax**) introduzca el número de teléfono de fax externo deseado con el que la extensión podrá recibir mensajes de fax del exterior.

11) En la línea de la extensión deseada y utilizando la lista desplegable **Clase de servicio**, seleccione el grupo de clase de servicio deseado.

12) Para incluir las extensiones de un grupo de telecaptura, en la línea de la extensión deseada de la lista desplegable **Telecaptura de llamadas**, seleccione un grupo de telecaptura.

13) Si es necesario, realice otros ajustes:

a) En la línea de la extensión deseada, haga clic en el símbolo en forma de lápiz **Editar**.



b) Asigne un **Número de teléfono móvil** y seleccione el **Web Feature ID** (ID de prestación web) en la lista desplegable del área **Mobility**.

c) En **Clip/Lin** indique número teléfono (número de marcación directa o MSN) que aparecerá en el display del usuario llamado en lugar del número de teléfono en caso de llamada externa.

Nota: Esta prestación debe estar activada por el proveedor de red.

Nota: Se debe configurar al menos un número de marcación directa. De lo contrario, el sistema no tiene en cuenta el número CLIP del llamante, y el número de la llamada interna se formatea y se envía como número de llamante para la llamada externa.

---

d) En la lista desplegable **Idioma** seleccione el idioma para el control de menús del teléfono.

e) En la lista desplegable **Señalización de llamadas internas**, asigne a la extensión una de las ocho señalizaciones de llamada acústicas para llamadas internas posibles. De esta forma, la extensión enviará a otras

extensiones internas un tono de llamada modificado que le permite ser reconocida por dichas extensiones (Estándar: Tipo de llamada 1).

f) En la lista desplegable **Señalización de llamadas externas**, asigne a la extensión una de las tres señalizaciones de llamada para llamadas externas posibles (Estándar: Tipo de llamada 1).

g) En el campo del **ID de ubicación ITSP**, introduzca el número de índice del ID de ubicación ITSP.

h) Solo con UC Smart: En la lista desplegable **Tipo de buzón UC Smart**, seleccione si la extensión tendrá un buzón estándar o un buzón de puesto de operadora (AutoAttendant).

i) Solo con UC Smart y buzón estándar: Si desea que los llamantes puedan dejar mensajes en el buzón de voz, active la casilla de verificación **Grabación**.

j) Solo con UC Smart: En la lista desplegable **Saludo** introduzca un saludo.

k) Solo con UC Smart: Si desea restablecer la contraseña del buzón de voz, active la casilla de verificación **Reponer contraseña**.

Nota:

La casilla de verificación **Reponer contraseña** no debe estar marcada al cambiar la configuración de un buzón de voz. Hace que se restablezca la contraseña del buzón de voz. Al cambiar la configuración, el usuario ya debe modificar la contraseña inicial al acceder por primera vez al buzón de voz.

---

l) Si la extensión está conectada con Internet, la autenticación DEBE activarse y usted DEBE introducir contraseñas seguras para todas las extensiones IP. Consulte la lista de marcadores **Autenticación activa** y rellene los campos **Nueva contraseña** y **Confirmar contraseña**.

m) Haga clic en **OK & Continuar**.

n) Si es necesario, modifique los flags de extensión. Para consultar una descripción de los flags de extensión, véase Capítulo 24.3.7.10 Extensión > Extensión > Parámetros de extensión.

o) Haga clic en **OK & Continuar**.

14) Si desea configurar una extensión más, repita los pasos del 5 al 13.

15) Haga clic en **OK & Continuar**. Verá una lista de todas las extensiones IP configuradas. Si es necesario, puede imprimir la lista de extensiones IP a través de **Imprimir**.

16) Haga clic en**OK & Continuar** y, a continuación, en **Salir**.

11.13.2 Cómo configurar extensiones SIP

Con el asistente **Terminales IP** puede configurar las extensiones SIP (teléfonos LAN y WLAN).

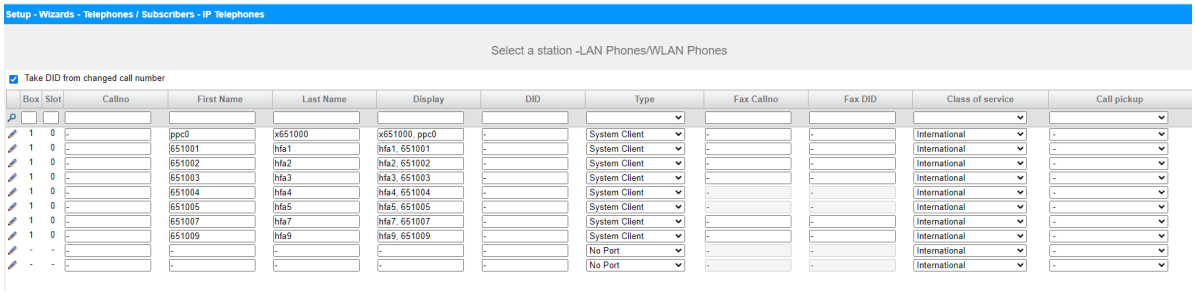
Requisitos previos

Para poder poner en servicio los teléfonos WLAN necesita una red LAN inalámbrica operativa.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Terminales / Extensiones**.
3) Haga clic en **Editar** para iniciar el asistente **Terminales IP**. Aparece una lista de todas las extensiones IP. Esta lista incluye también todas las extensiones SIP.



4) Si desea que la extensión reciba automáticamente el número de teléfono interno como número de marcación directa, active la opción **Tomar n.° llam. marc. directa del número de llamada modificado**.
5) Si desea que el número de marcación directa de la extensión sea diferente al número de teléfono, en la línea de la extensión deseada, introduzca el número de marcación directa de la extensión en el campo **Marcación directa**:
   - Solo con conexión de centralita:

     Haga clic en el campo deseado e indique el número de marcación directa a través del teclado. El número de marcación directa puede ser idéntico al número de teléfono interno.
   - Solo con acceso individual:

     Seleccione un MSN a través de la lista de selección. La extensión puede configurarse, por ejemplo, de forma interna a través de un número de teléfono interno 101 o de forma externa a través del MSN 654321.
   - en una conexión de centralita y acceso individual:

     En el campo deseado, y a través de la lista desplegable, seleccione la entrada **xxx - editable** (xxx es el número de teléfono interno) e indique el número de marcación directa a través del teclado o seleccione un MSN a través de la lista desplegable.
6) Si desea que la extensión reciba un número de llamada de extensión de telefonía DSL como número de marcación directa, deje desactivada la opción **Tomar n.º llam. marc. directa del número de llamada modificado**; en la lista que aparece junto al campo de opción, seleccione el proveedor de telefonía de Internet y, en la línea de la extensión deseada, seleccione el número de llamada de extensión de telefonía DSL en la lista desplegable **N.° llam. marc. directa**.
7) En la línea de la extensión deseada, en **N.º llam**, indique el número de teléfono interno de la extensión. Puede utilizar el número de teléfono preestablecido o asignar otro todavía no ocupado.
8) En la línea de la extensión deseada, y en **Nombre**, introduzca un nombre con el formato `Apellidos, Nombre` o `Nombre Apellidos`.

9) En la línea de la extensión deseada y en la lista desplegable **Tipo** seleccione el tipo **Cliente SIP**.

10) Si desea configurar un buzón de fax para la extensión (que se pueda utilizar, por ejemplo, con los clientes de UC **myPortal for Desktop** o **myPortal for Outlook**), siga este procedimiento:

a) En la línea de la extensión deseada, en el campo **Fax N.° llam**, introduzca el número de fax interno deseado con el que el usuario podrá recibir mensajes de fax internos.

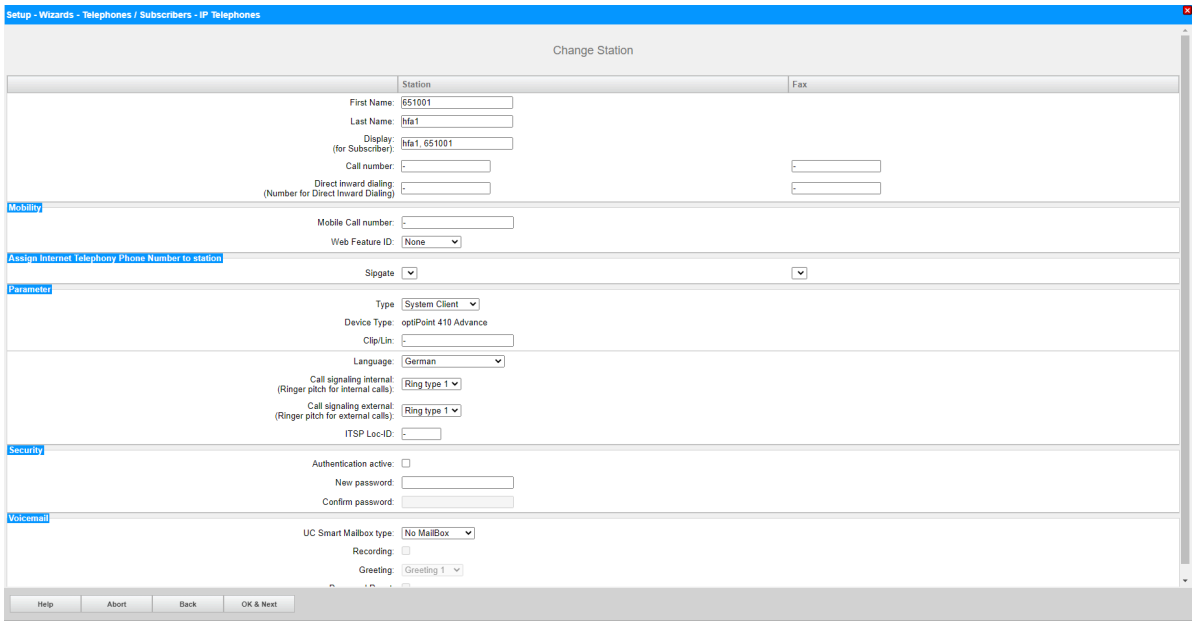
b) Si desea configurar un número de marcación directa para el buzón de fax, en la línea de la extensión deseada (en el campo **Marcación directa de fax**) introduzca el número de teléfono de fax externo deseado con el que la extensión podrá recibir mensajes de fax del exterior.

11) En la línea de la extensión deseada y utilizando la lista desplegable **Clase de servicio**, seleccione el grupo de clase de servicio deseado.

12) Para incluir las extensiones de un grupo de telecaptura, en la línea de la extensión deseada de la lista desplegable **Telecaptura de llamadas**, seleccione un grupo de telecaptura.

13) Configure los datos para el registro SIP:

a) En la línea de la extensión deseada, haga clic en el símbolo en forma de lápiz **Editar**.



b) En la sección **Seguridad**, introduzca la contraseña para la autenticación de la extensión SIP en los campos **Contraseña** y **Confirmar contraseña**.

c) En el campo **SIP usuario / Nombre usuario** asigne un nombre de usuario para la autenticación de la extensión SIP, por ejemplo, SIP-120.

d) En **Ámbito**, asigne un nombre de su elección para la zona correspondiente, p. ej., OSBIZ-SIP. Este valor debería ser el mismo para todas las extensiones SIP.

Nota: Los valores definidos aquí para contraseña, ID de usuario SIP y ámbito también se tienen que introducir en el teléfono SIP.

---

14) Si es necesario, realice otros ajustes:

a) Si este teléfono SIP se tiene que operar junto con un teléfono móvil Dual-Mode, en el área **Mobility**, en **Número de teléfono móvil**, indique el código urbano seguido por el número del teléfono móvil (p. ej., `0016012345678`). Además, en la lista desplegable **Web Feature ID**, seleccione este cliente SIP. (véase Telefonía Dual-Mode).

b) En el área **Marc. dir. para telefonía Internet** asigne un número de marcación directa para la telefonía por Internet a la extensión y, si lo desea, a su buzón de fax. Para ello, en las listas desplegables del ITSP deseado seleccione los números de marcación directa. Por cada ITSP activo se muestra una lista desplegable para la extensión y una lista desplegable para el buzón de fax.

Nota: No se puede ver el campo **Marc. dir. para telefonía Internet** si la telefonía Internet no está configurada o no hay activado ningún ITSP.

---

c) En **Clip/Lin** indique número teléfono (número de marcación directa o MSN) que aparecerá en el display del usuario llamado en lugar del número de teléfono en caso de llamada externa.

Nota: Esta prestación debe estar activada por el proveedor de red.

Nota: Se debe configurar al menos un número de marcación directa. De lo contrario, el sistema no tiene en cuenta el número CLIP del llamante, y el número de la llamada interna se formatea y se envía como número de llamante para la llamada externa.

---

d) En la lista desplegable **Idioma** seleccione el idioma para el control de menús del teléfono.

e) En la lista desplegable **Señalización de llamadas internas**, asigne a la extensión una de las ocho señalizaciones de llamada acústicas para llamadas internas posibles. De esta forma, la extensión enviará a otras extensiones internas un tono de llamada modificado que le permite ser reconocida por dichas extensiones (Estándar: Tipo de llamada 1).

f) En la lista desplegable **Señalización de llamadas externas**, asigne a la extensión una de las tres señalizaciones de llamada para llamadas externas posibles (Estándar: Tipo de llamada 1).

g) Solo con UC Smart: En la lista desplegable **Tipo de buzón UC Smart**, seleccione si la extensión tendrá un buzón estándar o un buzón de puesto de operadora (AutoAttendant).

h) Solo con UC Smart y buzón estándar: Si desea que los llamantes puedan dejar mensajes en el buzón de voz, active la casilla de verificación **Grabación**.

i) Solo con UC Smart: En la lista desplegable **Saludo** introduzca un saludo.

j) Solo con UC Smart: Si desea restablecer la contraseña del buzón de voz, active la casilla de verificación **Reponer contraseña**.

Nota: La casilla de verificación **Reponer contraseña** no debe estar marcada al cambiar la configuración

de un buzón de voz. Hace que se restablezca la contraseña del buzón de voz. Al cambiar la configuración, el usuario ya debe modificar la contraseña inicial al acceder por primera vez al buzón de voz.

k) Haga clic en **OK & Continuar**.

l) Si es necesario, modifique los flags de extensión. Para consultar una descripción de los flags de extensión, véase Extensión > Extensión > Parámetros de extensión.

m) Haga clic en **OK & Continuar**.

15) Si desea configurar una extensión más, repita los pasos del 5 al 14.

16) Haga clic en **OK & Continuar**. Verá una lista de todas las extensiones IP configuradas. Si es necesario, puede imprimir la lista de extensiones IP a través de **Imprimir**.

17) Haga clic en**OK & Continuar** y, a continuación, en **Salir**.

11.13.3 Cómo configurar estaciones UP0

Puede utilizar el asistente de **Dispositivos UP0** para configurar las estaciones UP0.

Requisitos previos

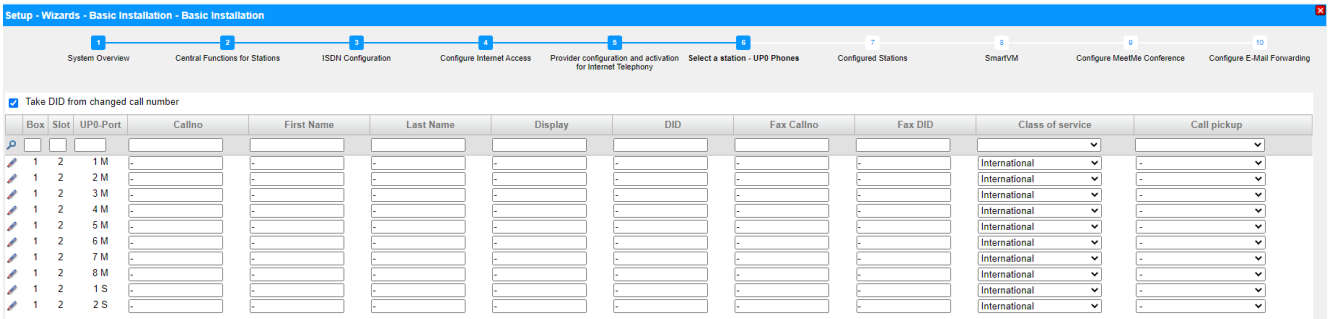
Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Teléfonos / Suscriptores**.

3) Haga clic en **Editar** para iniciar el asistente de **Dispositivos UP0**. Aparece una lista de todas las estaciones UP0.



4) Si desea que el número de llamada interna se asigne automáticamente a la estación como número de marcación entrante directa, active el botón de opción **Tomar DID del número de llamada modificado**.

5) Si desea que el número de marcación directa de la extensión sea diferente al número de teléfono, en la línea de la extensión deseada, introduzca

el número de marcación directa de la extensión en el campo **Marcación directa**:

- Solo con conexión de centralita:

  Haga clic en el campo deseado e indique el número de marcación directa a través del teclado. El número de marcación directa puede ser idéntico al número de teléfono interno.
- Solo con acceso individual:

  Seleccione un MSN a través de la lista de selección. La extensión puede configurarse, por ejemplo, de forma interna a través de un número de teléfono interno 101 o de forma externa a través del MSN 654321.
- en una conexión de centralita y acceso individual:

  En el campo deseado, y a través de la lista desplegable, seleccione la entrada **xxx - editable** (xxx es el número de teléfono interno) e indique el número de marcación directa a través del teclado o seleccione un MSN a través de la lista desplegable.

6) Si desea que se asigne un número de teléfono de telefonía por Internet a la estación como número de marcación entrante directa, deje el botón de opción **Tomar DID del número de llamada modificado** sin seleccionar y, en su lugar, seleccione el Proveedor de servicio de telefonía por Internet de la lista junto al botón de opción. Luego seleccione el número de teléfono de Telefonía por Internet de la lista desplegable **DID** en la fila de la estación deseada.

7) En la línea de la extensión deseada, en **N.º llam**, indique el número de teléfono interno de la extensión. Puede utilizar el número de teléfono preestablecido o asignar otro todavía no ocupado.

8) En la línea de la extensión deseada, y en **Nombre**, introduzca un nombre con el formato `Apellidos, Nombre` o `Nombre Apellidos`.

9) Si desea configurar un buzón de fax para la extensión (que se pueda utilizar, por ejemplo, con los clientes de UC **myPortal for Desktop** o **myPortal for Outlook**), siga este procedimiento:

a) En la línea de la extensión deseada, en el campo **Fax N.° llam**, introduzca el número de fax interno deseado con el que el usuario podrá recibir mensajes de fax internos.

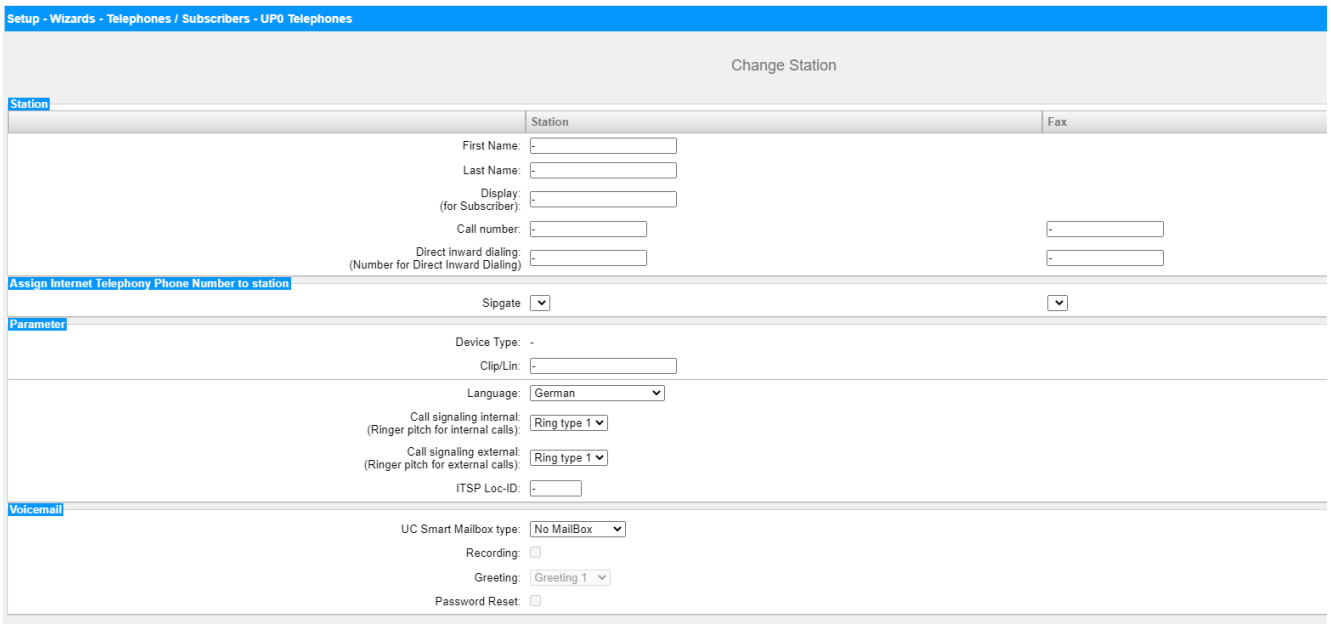
b) Si desea configurar un número DID para el buzón de fax, introduzca el número de fax externo deseado bajo el cual el suscriptor puede recibir mensajes de fax externos en el campo **DID de fax** en la fila del suscriptor deseado.

10) En la línea de la extensión deseada y utilizando la lista desplegable **Clase de servicio**, seleccione el grupo de clase de servicio deseado.

11) Para incluir las extensiones de un grupo de telecaptura, en la línea de la extensión deseada de la lista desplegable **Telecaptura de llamadas**, seleccione un grupo de telecaptura.

12) Si es necesario, realice más ajustes:

a) Haga clic en la fila de la estación deseada en el ícono de lápiz **Editar**.



b) En la sección **Mar. dir. para telefonía Internet**, utilice la lista desplegable para seleccionar un número de marcación directa. Por cada ITSP activo aparece una lista desplegable.

Nota: El campo **DID para telefonía por Internet** no es visible si la telefonía por Internet no está configurada o si no se ha activado ningún proveedor de servicios de telefonía por Internet.

---

c) En el campo **Clip/Lin**, ingrese un número de teléfono (número DID o MSN) que se mostrará en la extensión de la persona llamada en lugar del propio número de teléfono en el caso de una llamada externa.

Nota: Esta característica debe ser lanzada por el proveedor de red.

Nota: Se debe configurar al menos un número DID. De lo contrario, el sistema no tiene en cuenta el número CLIP del llamante, y el número de la llamada interna se formatea y se envía como número de llamante para la llamada externa.

---

d) En la lista desplegable **Idioma** seleccione el idioma para el control de menús del teléfono.

e) En la lista desplegable **Señalización de llamadas internas**, asigne a la extensión una de las ocho señalizaciones de llamada acústicas para llamadas internas posibles. De esta forma, la extensión enviará a otras

extensiones internas un tono de llamada modificado que le permite ser reconocida por dichas extensiones (Estándar: Tipo de llamada 1).

f) En la lista desplegable **Señalización de llamadas externas**, asigne a la extensión una de las tres señalizaciones de llamada para llamadas externas posibles (Estándar: Tipo de llamada 1).

g) Sólo con UC Smart: Seleccione si el suscriptor debe recibir un buzón predeterminado o un buzón de asistente (AutoAttendant) en la lista desplegable **Tipo de buzón UC Smart**.

h) Sólo con UC Smart y buzón predeterminado: Si una persona que llama puede dejar un mensaje en el buzón de voz, seleccione la casilla de verificación **Grabación**.

i) Sólo con UC Smart: Seleccione un saludo de la lista desplegable **Saludo**.

j) Sólo con UC Smart: Si desea restablecer la contraseña del buzón de correo de voz, seleccione la casilla de verificación **Restablecer contraseña**.

Nota: La casilla de verificación **Restablecer contraseña** debe estar desmarcada al configurar un nuevo buzón de correo de voz. Se utiliza para restablecer la contraseña del buzón de correo de voz. Cuando se crea un nuevo buzón de correo de voz, el suscriptor debe cambiar de todos modos la contraseña inicial cuando accede a su buzón de correo de voz por primera vez.

---

k) Haga clic en **OK & Siguiente**.

l) Cambie las banderas de la estación según sea necesario. Para obtener una descripción de los marcadores de la estación, consulte Estación > Estación > Parámetros de la estación.

m) Haga clic en **OK & Siguiente**.

13) Si desea configurar otra estación, repita los pasos 5 al 12.

14) Haga clic en **OK & Siguiente**. Aparece una lista de todas las estaciones UP0 configuradas. Si es necesario, puede imprimir la lista de estaciones UP0 con **Imprimir**.

15) Haga clic en **Aceptar & Siguiente** seguido de **Finalizar**.

11.13.4 Cómo configurar extensiones DECT

Puede utilizar el asistente de **Dispositivos DECT** para configurar las estaciones DECT (teléfonos DECT).

Requisitos previos

Una estación base está conectada a una interfaz UP0 o a una placa SLC instalada.

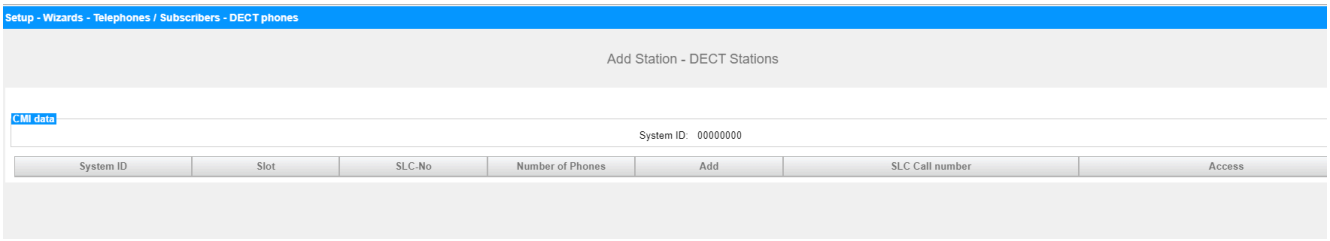
Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Teléfonos / Suscriptores**.

3) Haga clic en **Editar** para iniciar el asistente **de teléfonos DECT**. Aparece una lista de todas las estaciones DECT.



4) Si desea que el número de llamada interna se asigne automáticamente a la estación como número de marcación entrante directa, active el botón de opción **Tomar DID del número de llamada modificado**.

5) Si desea que el número de marcación directa de la extensión sea diferente al número de teléfono, en la línea de la extensión deseada, introduzca el número de marcación directa de la extensión en el campo **Marcación directa**:

   - Solo con conexión de centralita:

     Haga clic en el campo deseado e indique el número de marcación directa a través del teclado. El número de marcación directa puede ser idéntico al número de teléfono interno.
   - Solo con acceso individual:

     Seleccione un MSN a través de la lista de selección. La extensión puede configurarse, por ejemplo, de forma interna a través de un número de teléfono interno 101 o de forma externa a través del MSN 654321.
   - en una conexión de centralita y acceso individual:

     En el campo deseado, y a través de la lista desplegable, seleccione la entrada **xxx - editable** (xxx es el número de teléfono interno) e indique el número de marcación directa a través del teclado o seleccione un MSN a través de la lista desplegable.

6) Si desea que se asigne un número de teléfono de telefonía por Internet a la estación como número de marcación entrante directa, deje el botón de opción **Tomar DID del número de llamada modificado** sin seleccionar y, en su lugar, seleccione el Proveedor de servicio de telefonía por Internet de la lista junto al botón de opción. Luego seleccione el número de teléfono de Telefonía por Internet de la lista desplegable **DID** en la fila de la estación deseada.

7) En la línea de la extensión deseada, en **N.º llam**, indique el número de teléfono interno de la extensión. Puede utilizar el número de teléfono preestablecido o asignar otro todavía no ocupado.

8) En la línea de la extensión deseada, y en **Nombre**, introduzca un nombre con el formato `Apellidos, Nombre` o `Nombre Apellidos`.

9) Si desea configurar un buzón de fax para la extensión (que se pueda utilizar, por ejemplo, con los clientes de UC **myPortal for Desktop** o **myPortal for Outlook**), siga este procedimiento:

   a) En la línea de la extensión deseada, en el campo **Fax N.° llam**, introduzca el número de fax interno deseado con el que el usuario podrá recibir mensajes de fax internos.

   b) Si desea configurar un número DID para el buzón de fax, introduzca el número de fax externo deseado bajo el cual el suscriptor puede

recibir mensajes de fax externos en el campo **DID de fax** en la fila del suscriptor deseado.

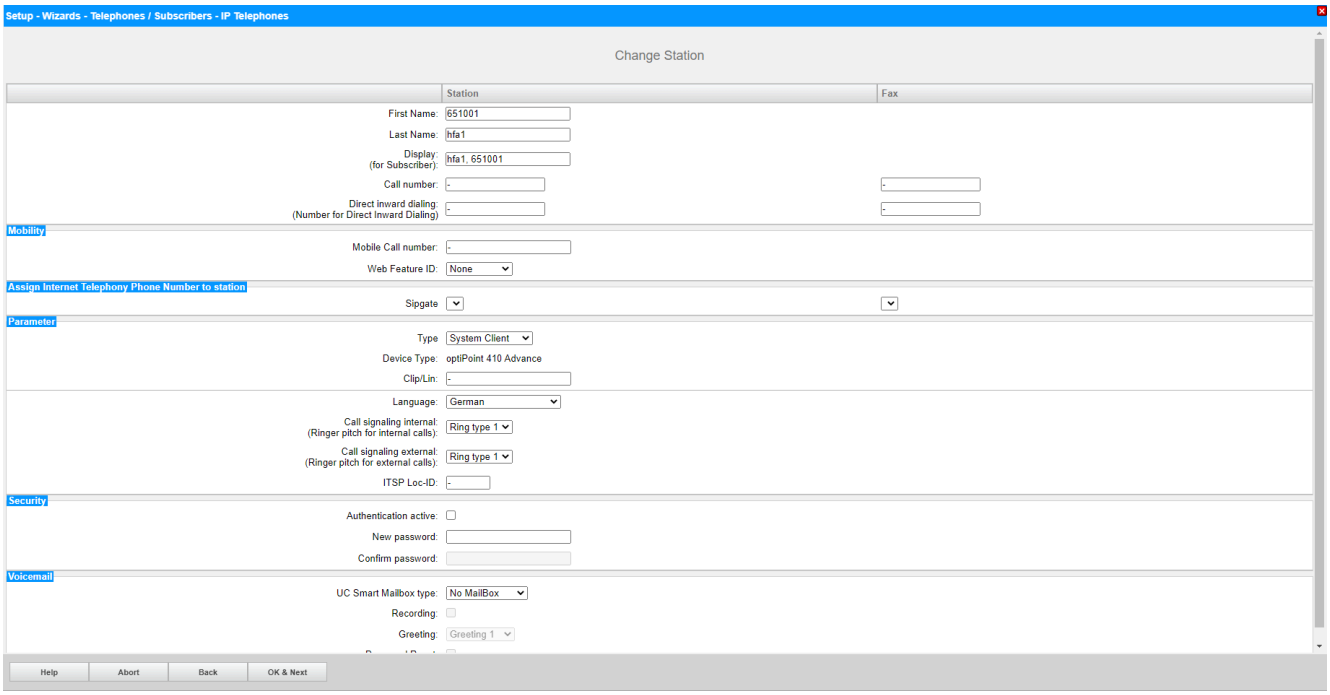
10) En la línea de la extensión deseada y utilizando la lista desplegable **Clase de servicio**, seleccione el grupo de clase de servicio deseado.

11) Para incluir las extensiones de un grupo de telecaptura, en la línea de la extensión deseada de la lista desplegable **Telecaptura de llamadas**, seleccione un grupo de telecaptura.

12) Si desea modificar el código telefónico DECT (PIN), en el campo **Código móvil** de la línea de la extensión deseada introduzca el código nuevo. La extensión DECT debe registrarse de nuevo en la extensión base con este código.

13) Si es necesario, realice más ajustes:

a) Haga clic en la fila de la estación deseada en el ícono de lápiz **Editar**.



b) En la sección **Mar. dir. para telefonía Internet**, utilice la lista desplegable para seleccionar un número de marcación directa. Por cada ITSP activo aparece una lista desplegable.

Nota: El campo **DID para telefonía por Internet** no es visible si la telefonía por Internet no está configurada o

si no se ha activado ningún proveedor de servicios de telefonía por Internet.

c) En el campo **Clip/Lin**, ingrese un número de teléfono (número DID o MSN) que se mostrará en la extensión de la persona llamada en lugar del propio número de teléfono en el caso de una llamada externa.

Nota: Esta característica debe ser lanzada por el proveedor de red.

Nota: Se debe configurar al menos un número DID. De lo contrario, el sistema no tiene en cuenta el número CLIP del llamante, y el número de la llamada interna se formatea y se envía como número de llamante para la llamada externa.

d) En la lista desplegable **Idioma** seleccione el idioma para el control de menús del teléfono.

e) En la lista desplegable **Señalización de llamadas internas**, asigne a la extensión una de las ocho señalizaciones de llamada acústicas para llamadas internas posibles. De esta forma, la extensión enviará a otras extensiones internas un tono de llamada modificado que le permite ser reconocida por dichas extensiones (Estándar: Tipo de llamada 1).

f) En la lista desplegable **Señalización de llamadas externas**, asigne a la extensión una de las tres señalizaciones de llamada para llamadas externas posibles (Estándar: Tipo de llamada 1).

g) Sólo con UC Smart: Seleccione si el suscriptor debe recibir un buzón predeterminado o un buzón de asistente (AutoAttendant) en la lista desplegable **Tipo de buzón UC Smart**.

h) Sólo con UC Smart y buzón predeterminado: Si una persona que llama puede dejar un mensaje en el buzón de voz, seleccione la casilla de verificación **Grabación**.

i) Sólo con UC Smart: Seleccione un saludo de la lista desplegable **Saludo**.

j) Sólo con UC Smart: Si desea restablecer la contraseña del buzón de correo de voz, seleccione la casilla de verificación **Restablecer contraseña**.

Nota: La casilla de verificación **Restablecer contraseña** debe estar desmarcada al configurar un nuevo buzón de correo de voz. Se utiliza para restablecer la contraseña del buzón de correo de voz. Cuando se crea un nuevo buzón de correo de voz, el suscriptor debe cambiar de todos modos la contraseña inicial cuando accede a su buzón de correo de voz por primera vez.

k) Haga clic en **OK & Siguiente**.

l) Cambie las banderas de la estación según sea necesario. Para obtener una descripción de los marcadores de la estación, consulte Estación > Estación > Parámetros de la estación.

m) Haga clic en **OK & Siguiente**.

14) Si desea configurar otra estación, repita los pasos 5 al 13.

15) Haga clic en **OK & Siguiente**. Aparece una lista de todas las estaciones DECT configuradas. Si es necesario, puede imprimir la lista de estaciones DECT con **Imprimir**.
16) Haga clic en **Aceptar & Siguiente** seguido de **Finalizar**.

Tareas relacionadas

Cómo configurar por primera vez teléfonos DECT en la página 994

11.13.5 Cómo configurar estaciones SIP DECT de Mitel mediante aprovisionamiento

Puede utilizar el asistente **Mitel SIP DECT** para configurar los dispositivos Mitel SIP-DECT y conectarlos a Open Mobility Manager (OMM).

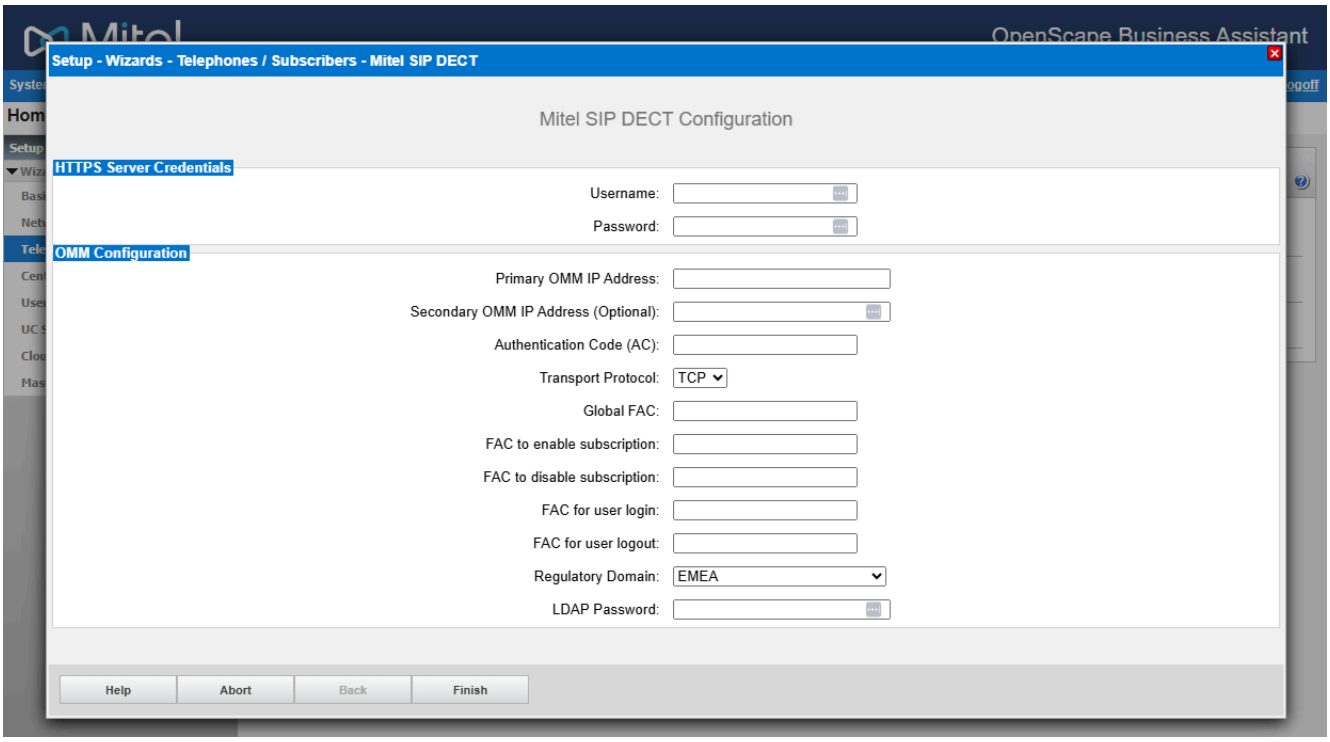
Requisitos previos

Se conoce la dirección MAC del dispositivo SIP DECT RFP.

Paso a paso

1) En la barra de navegación, haga clic en **Modo experto > Interfaces de red > DHCP**.
2) Haga clic para habilitar el **servidor DHCP**.
3) En la barra de navegación, haga clic en **Servidor DHCP > Direcciones IP estáticas**.
4) En la ventana **Direcciones IP estáticas**, haga clic en la pestaña **Agregar dirección IP estática**.
5) Ingrese la información requerida como se describe en Interfaces de red > Placa base > Modo DHCP > Servidor DHCP > Direcciones IP estáticas.
6) Haga clic en **Aplicar**.
7) En la barra de navegación, haga clic en **Configuración**.
8) En el árbol de navegación, haga clic en **Asistentes** > **Teléfonos / Suscriptores**.

9) Haga clic en **Editar** para iniciar el asistente **Mitel SIP DECT**.



10) En **Credenciales del servidor HTTPS**, proporcione las credenciales para acceder al servidor.
    a) Establezca el **nombre de usuario** y la **contraseña**.
11) En **Configuración OMM**:
12) Proporcione la **dirección IP principal del OMM** y la **dirección IP secundaria del OMM (opcional)** Dirección IP del OMM.
13) Establezca el **código de autenticación (AC)**.
14) En **Protocolo de transporte**, elija uno de los siguientes valores del menú desplegable:
    - TCP
    - UDP
    - TLS
15) Establezca los distintos códigos de acceso a funciones (FAC) en los siguientes campos:
    a) **FAC global**
    b) **FAC habilitará la suscripción**
    c) **FAC para inicio de sesión de usuario**
    d) **FAC para el cierre de sesión del usuario**
16) En **Dominio regulatorio**, elija uno de los siguientes valores del menú desplegable:
    - EMEA
    - US
    - Brasil
    - Taiwán
    - Radio 1910 - 1927 MHz 250 Mw

17) Proporcione la **contraseña LDAP** para acceder al directorio de usuarios internos de OpenScape Business.
18) Haga clic en **Salir**.
Se generan los archivos de configuración necesarios de la aplicación OMM.
19) Configure una estación SIP como se describe en Cómo configurar estaciones SIP a través del modo experto.
20) Conecte el dispositivo Mitel SIP DECT RFP a la red. Espere unos instantes hasta que el dispositivo reciba una dirección IP del servidor DHCP.
21) Conéctese a la aplicación OMM y configure la estación base, como se describe en la " *Guía de configuración del teléfono SIP DECT de Mitel* ".

11.13.5.1 Cómo configurar estaciones SIP a través del modo experto

Puede utilizar el **Modo Experto** para configurar las estaciones SIP.

Requisitos previos

Ha iniciado sesión en el WBM con el perfil **Experto**.

Paso a paso

1) En el árbol de navegación, haga clic en **Modo experto** > **Servidor de telefonía** > **Estación**.
2) En la nueva ventana, haga clic para expandir la **Estación** y luego seleccione **Cliente IP**. Aparece una lista de todas las estaciones IP/SIP.
3) En la columna **Tipo**, seleccione **Cliente SIP**.
4) Haga clic en **Aplicar**.
5) Haga clic en la flecha azul, junto al número de llamada de la estación IP, debajo de la columna **Número de llamada**.
6) En la ventana **Editar parámetros de la estación**, seleccione **Dispositivo Mitel SIP DECT** en el menú desplegable en **Aprovisionamiento de dispositivos.**
Aparece la opción de **Configuración SIP DECT de Mitel**.
7) En la opción **Configuración SIP DECT de Mitel**, configure lo siguiente:
   a) Ingrese el **PIN** del dispositivo.
   b) En **Bloqueo de teclas habilitado**, habilite (Sí) o deshabilite (No) el bloqueo de teclas del dispositivo.
   c) En **PIN de bloqueo de teclas** introduzca el PIN para el bloqueo de teclas.
   d) En **Tiempo de bloqueo de teclas** introduzca el tiempo para que el PIN de bloqueo de teclas tenga efecto.
   e) En **Mostrar directorio personal** elija si el directorio personal es visible (Sí) o no (No).
8) Haga clic en **Aplicar**.
9) Vaya a la pestaña **Editar datos del cliente del punto de trabajo**.
10) En **Parámetros**, configure los valores como se describe en Parámetros de la estación.
11) Haga clic en **Aplicar**.

11.13.6 Cómo configurar extensiones RDSI

El asistente **Terminales RDSI** permite configurar las extensiones RDSI (teléfono o fax RDSI).

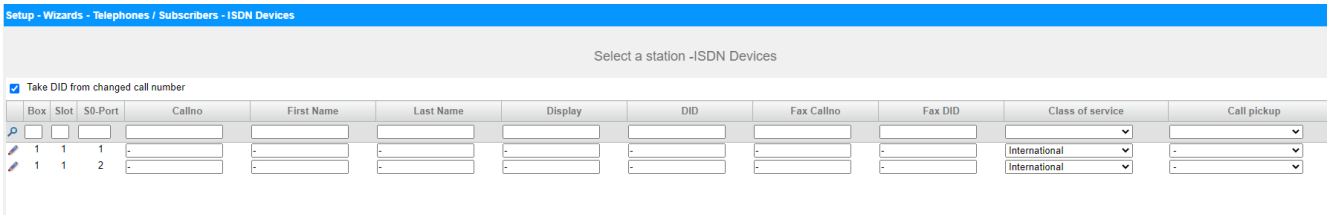
Requisitos previos

Hay al menos una interfaz S_0 libre. Si se utiliza uno de los puertos S_0 de una plataforma de hardware, debe configurarse como conexión S_0 interna.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Terminales / Extensiones**.
3) Haga clic en **Editar** para iniciar el asistente **Terminales RDSI**. Aparece una lista de todas las extensiones RDSI.



4) Si desea que el número de marcación directa de la extensión se ajuste automáticamente a su número de teléfono, active la opción **Tomar n.° llam. marc. directa del número de llamada modificado**.
5) Si desea que el número de marcación directa de la extensión sea diferente al número de teléfono, en la línea de la extensión deseada, introduzca el número de marcación directa de la extensión en el campo **Marcación directa**:
   - Solo con conexión de centralita:

     Haga clic en el campo deseado e indique el número de marcación directa a través del teclado. El número de marcación directa puede ser idéntico al número de teléfono interno.
   - Solo con acceso individual:

     Seleccione un MSN a través de la lista de selección. La extensión puede configurarse, por ejemplo, de forma interna a través de un número de teléfono interno 101 o de forma externa a través del MSN 654321.
   - en una conexión de centralita y acceso individual:

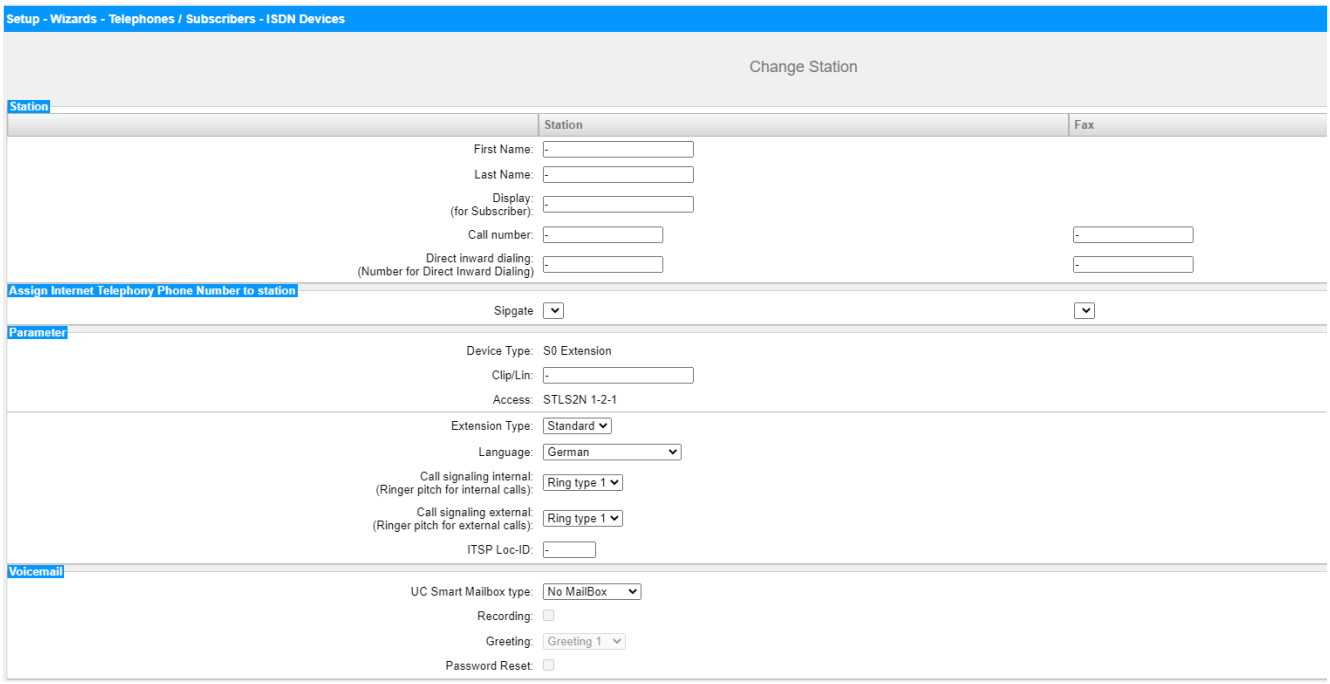
     En el campo deseado, y a través de la lista desplegable, seleccione la entrada **xxx - editable** (xxx es el número de teléfono interno) e indique el número de marcación directa a través del teclado o seleccione un MSN a través de la lista desplegable.
6) En la línea de la extensión deseada, en **N.º llam**, indique el número de teléfono interno de la extensión. Puede utilizar el número de teléfono preestablecido o asignar otro todavía no ocupado.
7) En la línea de la extensión deseada, y en **Nombre**, introduzca un nombre con el formato `Apellidos, Nombre` o `Nombre Apellidos`.

8) En la línea de la extensión deseada y utilizando la lista desplegable **Clase de servicio**, seleccione el grupo de clase de servicio deseado.

9) Para incluir las extensiones de un grupo de telecaptura, en la línea de la extensión deseada de la lista desplegable **Telecaptura de llamadas**, seleccione un grupo de telecaptura.

10) Si es necesario, realice otros ajustes:

a) En la línea de la extensión deseada, haga clic en el símbolo en forma de lápiz **Editar**.



b) En la sección **Mar. dir. para telefonía Internet**, utilice la lista desplegable para seleccionar un número de marcación directa. Por cada ITSP activo aparece una lista desplegable.

Nota: No se puede ver el campo **Marc. dir. para telefonía Internet** si la telefonía Internet no está configurada o no hay activado ningún ITSP.

---

c) En **Clip/Lin** indique número teléfono (número de marcación directa o MSN) que aparecerá en el display del usuario llamado en lugar del número de teléfono en caso de llamada externa.

Nota: Esta prestación debe estar activada por el proveedor de red.

Nota: Se debe configurar al menos un número de marcación directa. De lo contrario, el sistema no tiene en cuenta el número CLIP del llamante, y el número de

la llamada interna se formatea y se envía como número de llamante para la llamada externa.

d) En la lista desplegable **Tipo de ext**, seleccione el tipo del terminal RDSI (`Estándar` o `Fax`).
e) En la lista desplegable **Idioma** deje la selección predeterminada. Esta configuración no es importante para los terminales RDSI
f) En la lista desplegable **Señalización de llamadas internas**, asigne a la extensión una de las ocho señalizaciones de llamada acústicas para llamadas internas posibles. De esta forma, la extensión enviará a otras extensiones internas un tono de llamada modificado que le permite ser reconocida por dichas extensiones (Estándar: Tipo de llamada 1).
g) En la lista desplegable **Señalización de llamadas externas**, asigne a la extensión una de las tres señalizaciones de llamada para llamadas externas posibles (Estándar: Tipo de llamada 1).
h) Solo con UC Smart: En la lista desplegable **Tipo de buzón UC Smart**, seleccione si la extensión tendrá un buzón estándar o un buzón de puesto de operadora (AutoAttendant).
i) Solo con UC Smart y buzón estándar: Si desea que los llamantes puedan dejar mensajes en el buzón de voz, active la casilla de verificación **Grabación**.
j) Solo con UC Smart: En la lista desplegable **Saludo** introduzca un saludo.
k) Solo con UC Smart: Si desea restablecer la contraseña del buzón de voz, active la casilla de verificación **Reponer contraseña**.

Nota: La casilla de verificación **Reponer contraseña** no debe estar marcada al cambiar la configuración de un buzón de voz. Hace que se restablezca la contraseña del buzón de voz. Al cambiar la configuración, el usuario ya debe modificar la contraseña inicial al acceder por primera vez al buzón de voz.

l) Haga clic en **OK & Continuar**.
m) Si es necesario, modifique los flags de extensión. Para consultar una descripción de los flags de extensión, véase Extensión > Extensión > Parámetros de extensión.
n) Haga clic en **OK & Continuar**.

11) Si desea configurar una extensión más, repita los pasos del 5 al 10.
12) Haga clic en **OK & Continuar**. Verá una lista de todas las extensiones RDSI configuradas. Si es necesario, puede imprimir la lista de extensiones RDSI a través de **Imprimir**.
13) Haga clic en**OK & Continuar** y, a continuación, en **Salir**.

11.13.7 Cómo configurar extensiones analógicas

El asistente **Terminales analógicas** permite configurar las extensiones analógicas (p. ej. un teléfono o fax analógico).

Requisitos previos

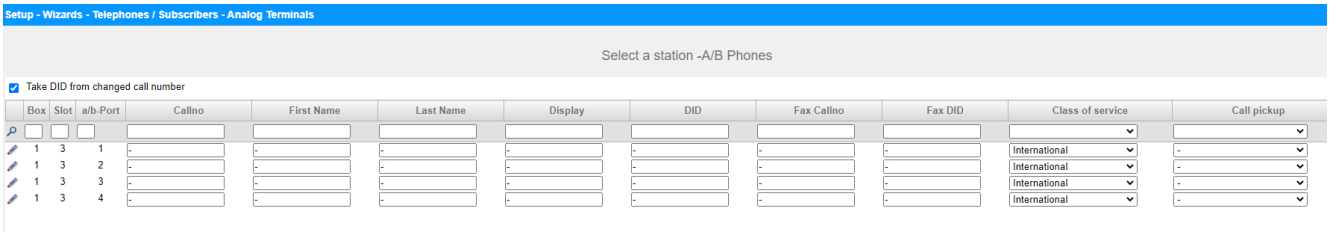
Hay disponible al menos una interfaz analógica libre.

En los dispositivos analógicos está activada la MF.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Terminales / Extensiones**.
3) Haga clic en **Editar**, para iniciar el asistente **Terminales analógicas** . Aparece una lista de todas las extensiones analógicas.



4) Si desea que el número de marcación directa de la extensión se ajuste automáticamente a su número de teléfono, active la opción **Tomar n.° llam. marc. directa del número de llamada modificado**.
5) Si desea que el número de marcación directa de la extensión sea diferente al número de teléfono, en la línea de la extensión deseada, introduzca el número de marcación directa de la extensión en el campo **Marcación directa**:
   - Solo con conexión de centralita:

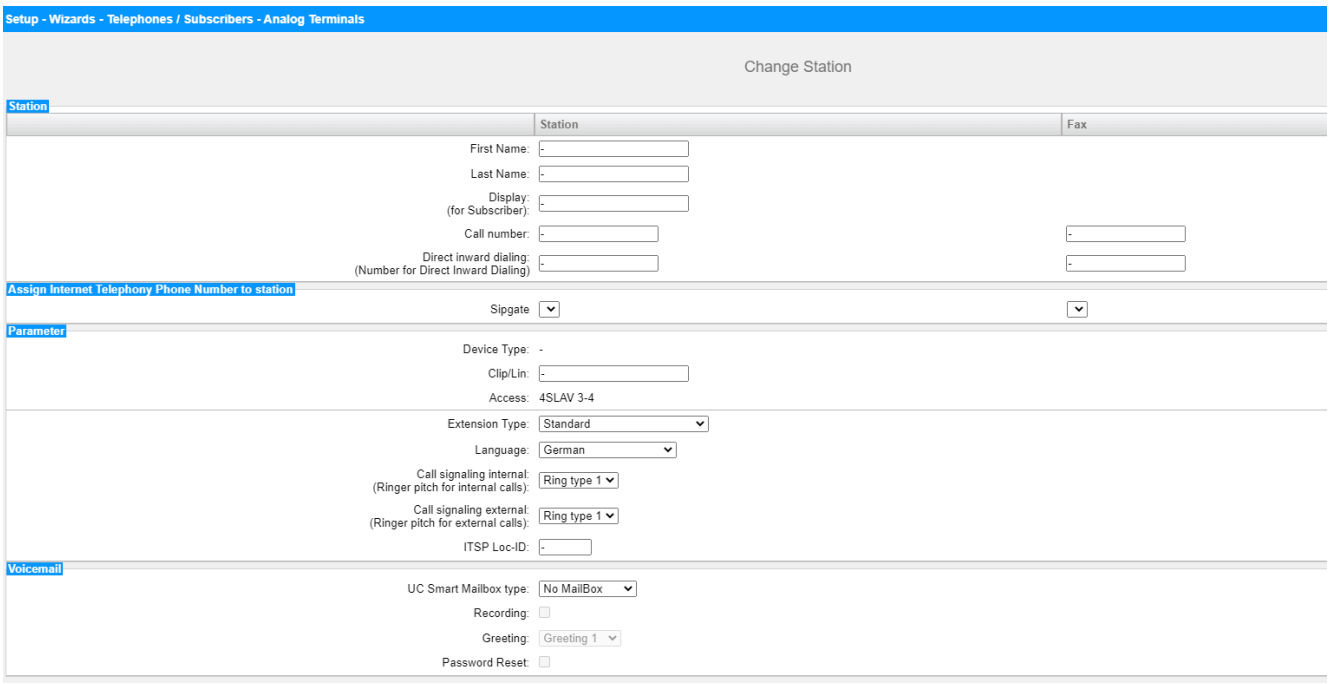
     Haga clic en el campo deseado e indique el número de marcación directa a través del teclado. El número de marcación directa puede ser idéntico al número de teléfono interno.
   - Solo con acceso individual:

     Seleccione un MSN a través de la lista de selección. La extensión puede configurarse, por ejemplo, de forma interna a través de un número de teléfono interno 101 o de forma externa a través del MSN 654321.
   - en una conexión de centralita y acceso individual:

     En el campo deseado, y a través de la lista desplegable, seleccione la entrada **xxx - editable** (xxx es el número de teléfono interno) e indique el número de marcación directa a través del teclado o seleccione un MSN a través de la lista desplegable.
6) En la línea de la extensión deseada, en **N.º llam**, indique el número de teléfono interno de la extensión. Puede utilizar el número de teléfono preestablecido o asignar otro todavía no ocupado.
7) En la línea de la extensión deseada, y en **Nombre**, introduzca un nombre con el formato `Apellidos, Nombre` o `Nombre Apellidos`.
8) En la línea de la extensión deseada y utilizando la lista desplegable **Clase de servicio**, seleccione el grupo de clase de servicio deseado.
9) Para incluir las extensiones de un grupo de telecaptura, en la línea de la extensión deseada de la lista desplegable **Telecaptura de llamadas**, seleccione un grupo de telecaptura.

10) Si es necesario, realice otros ajustes: - Para un módem analógico, seleccione aquí el tipo de extensión **Módem**.

a) En la línea de la extensión deseada, haga clic en el símbolo en forma de lápiz **Editar**.



b) En la sección **Mar. dir. para telefonía Internet**, utilice la lista desplegable para seleccionar un número de marcación directa. Por cada ITSP activo aparece una lista desplegable.

Nota: No se puede ver el campo **Marc. dir. para telefonía Internet** si la telefonía Internet no está configurada o no hay activado ningún ITSP.

---

c) En **Clip/Lin** indique número teléfono (número de marcación directa o MSN) que aparecerá en el display del usuario llamado en lugar del número de teléfono en caso de llamada externa.

Nota: Esta prestación debe estar activada por el proveedor de red.

Nota: Se debe configurar al menos un número de marcación directa. De lo contrario, el sistema no tiene en cuenta el número CLIP del llamante, y el número de

la llamada interna se formatea y se envía como número de llamante para la llamada externa.

d) En la lista desplegable **Tipo de ext.**, seleccione el tipo del terminal analógico (p. ej. Fax).

Si desea configurar un módem analógico, seleccione aquí el tipo de extensión **Módem**.

e) En la lista desplegable **Idioma** deje la selección predeterminada. Esta configuración no tiene ninguna importancia para los terminales analógicos.

f) En la lista desplegable **Señalización de llamadas internas**, asigne a la extensión una de las ocho señalizaciones de llamada acústicas para llamadas internas posibles. De esta forma, la extensión enviará a otras extensiones internas un tono de llamada modificado que le permite ser reconocida por dichas extensiones (Estándar: Tipo de llamada 1).

g) En la lista desplegable **Señalización de llamadas externas**, asigne a la extensión una de las tres señalizaciones de llamada para llamadas externas posibles (Estándar: Tipo de llamada 1).

h) Solo con UC Smart: En la lista desplegable **Tipo de buzón UC Smart**, seleccione si la extensión tendrá un buzón estándar o un buzón de puesto de operadora (AutoAttendant).

i) Solo con UC Smart y buzón estándar: Si desea que los llamantes puedan dejar mensajes en el buzón de voz, active la casilla de verificación **Grabación**.

j) Solo con UC Smart: En la lista desplegable **Saludo** introduzca un saludo.

k) Solo con UC Smart: Si desea restablecer la contraseña del buzón de voz, active la casilla de verificación **Reponer contraseña**.

Nota: La casilla de verificación **Reponer contraseña** no debe estar marcada al cambiar la configuración de un buzón de voz. Hace que se restablezca la contraseña del buzón de voz. Al cambiar la configuración, el usuario ya debe modificar la contraseña inicial al acceder por primera vez al buzón de voz.

l) Haga clic en **OK & Continuar**.

m) Si es necesario, modifique los flags de extensión. Para consultar una descripción de los flags de extensión, véase Extensión > Extensión > Parámetros de extensión.

n) Haga clic en **OK & Continuar**.

11) Si desea configurar una extensión más, repita los pasos del 5 al 10.

12) Haga clic en **OK & Continuar**. Verá una lista de todas las extensiones analógicas configuradas. Si es necesario, puede imprimir la lista de extensiones analógicas a través de **Imprimir**.

13) Haga clic en**OK & Continuar** y, a continuación, en **Salir**.

11.13.8 Cómo definir el nombre de las extensiones

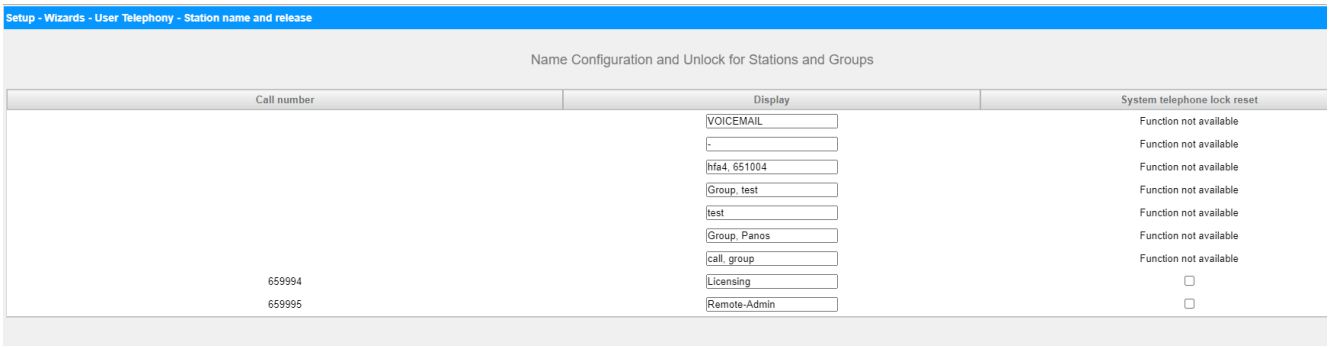
El asistente **Versión y nombre de extensión** permite modificar los nombres de las extensiones.

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Versión y nombre de extensión**.



4) En la columna **Display**, haga clic en el campo de la extensión deseada y modifica el nombre con este formato `Apellidos, Nombre` o `Nombre Apellidos`.
5) Si desea modificar los nombres de nuevas extensiones, repita el paso 4.
6) Haga clic en **OK y Continuar** y, a continuación, en **Salir**.

11.14 Configuración de los perfiles de extensiones

En los perfiles de extensiones se almacenan los valores y propiedades de las extensiones IP.

El asistente **Perfil** permite a los administradores con el perfil **Avanzado** realizar los siguientes ajustes de configuración:

- Crear nuevo perfil
- Mostrar perfiles y sus miembros
- Agregar miembros a un perfil
- Eliminar miembros de un perfil
- Exportar o importar un perfil individual

El modo Experto permite a los administradores con el perfil **Experto** realizar los siguientes ajustes de configuración adicionales:

- Modificar los valores y ajustes de configuración de un perfil existente
- Exportar o importar todos los perfiles

Los perfiles de usuario ya creados no se pueden borrar, pero se pueden sobrescribir.

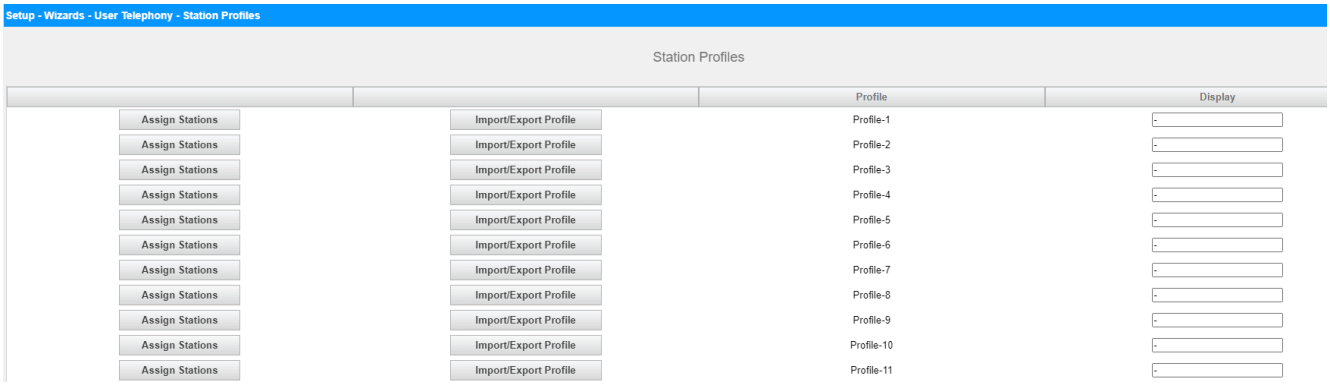
11.14.1 Cómo crear un nuevo perfil de extensiones

Requisitos previos

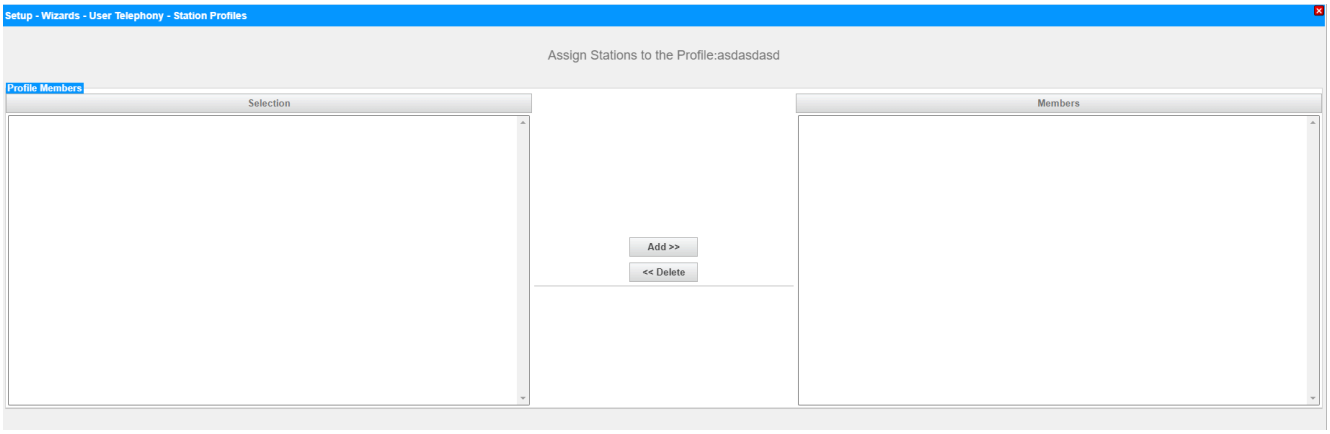
Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Perfiles de extensiones**. Se muestran todos los perfiles de extensión existentes.



4) En la línea del perfil de extensiones deseado y en la columna **Display**, introduzca un nombre para el perfil (16 caracteres como máximo).
5) En la línea del perfil de extensiones deseado, haga clic en **Asignar extensión**.



6) En la tabla **Miembros de perfil**, seleccione los miembros deseados (se pueden seleccionar varias opciones) y haga clic en **Agregar**. Estas extensiones están asignadas al perfil de extensiones y no se pueden asignar a otro perfil.
7) Haga clic en **Aceptar**.
8) Haga clic en **OK y Continuar**. Se muestran todos los perfiles de extensiones existentes y sus miembros.
9) Haga clic en**OK & Continuar** y, a continuación, en **Salir**.

11.14.2 Cómo mostrar perfiles de extensiones y sus miembros

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Perfiles de extensiones**. Se muestran todos los perfiles de extensión existentes.
4) Haga clic en **OK & Continuar**. Se muestran todos los perfiles de extensiones existentes y sus miembros.

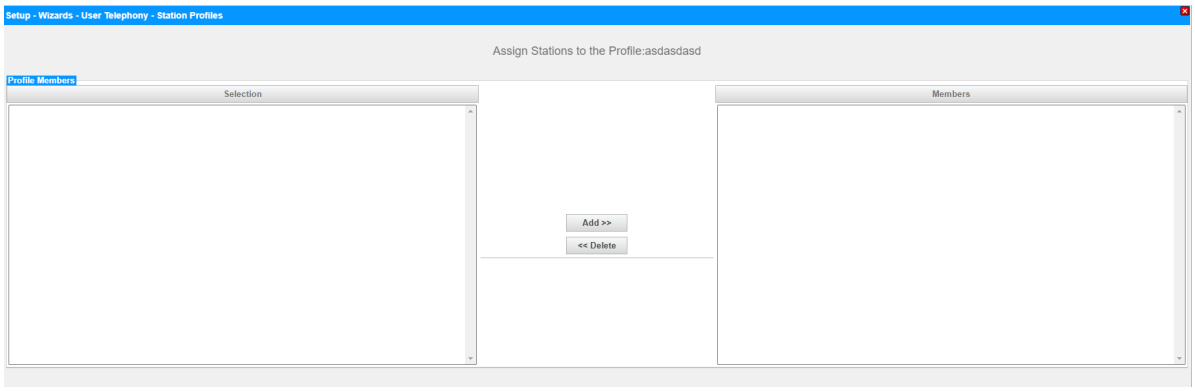
11.14.3 Cómo agregar miembros a un perfil de extensiones

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Perfiles de extensiones**. Se muestran todos los perfiles de extensiones existentes y sus miembros.
4) En la línea del perfil de extensiones deseado, haga clic en **Asignar extensión**.



5) En la lista **Miembros de perfil**, haga clic en el miembro deseado (se pueden seleccionar varias opciones) y haga clic en **Agregar**. Estas extensiones están asignadas al perfil de extensiones y no se pueden asignar a otro perfil.
6) Haga clic en **Aceptar**.
7) Haga clic en **OK & Continuar**. Se muestran todos los perfiles de extensiones existentes y sus miembros.
8) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

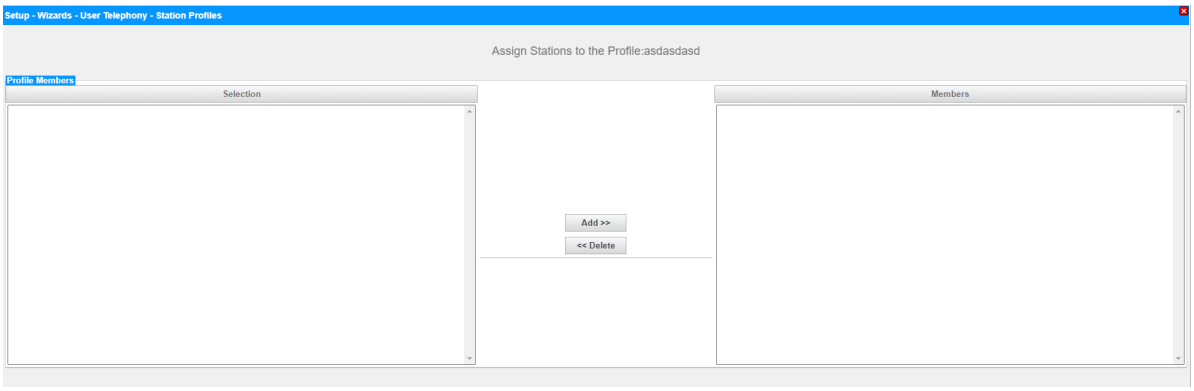
11.14.4 Cómo borrar miembros de un perfil de extensiones

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Perfiles de extensiones**. Se muestran todos los perfiles de extensiones existentes y sus miembros.
4) En la línea del perfil de extensiones deseado, haga clic en **Asignar extensión**.



5) En la lista **Miembros**, seleccione los miembros deseados (se pueden seleccionar varias opciones) y haga clic en **Borrar**. Estas extensiones se pueden asignar a otro perfil de extensiones.
6) Haga clic en **Aceptar**.
7) Haga clic en **OK & Continuar**. Se muestran todos los perfiles de extensiones existentes y sus miembros.
8) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

11.14.5 Cómo importar o exportar un perfil de extensiones individual

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Perfiles de extensiones**. Se muestran todos los perfiles de extensiones existentes y sus miembros.
4) En la línea del perfil de extensiones deseado, haga clic en **Importar/ exportar perfil**.

5) Si desea exportar el perfil de extensiones a un archivo, haga clic en **Descarga** y guarde el archivo en el directorio que desee.
6) Si desea importar un perfil de extensiones desde un archivo, haga clic en **Examinar**, desplácese hasta el lugar de almacenamiento del archivo y cargue el archivo en el sistema de comunicación.
7) Haga clic en **Aceptar**.
8) Haga clic en **OK & Continuar**. Se muestran todos los perfiles de extensiones existentes y sus miembros.
9) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

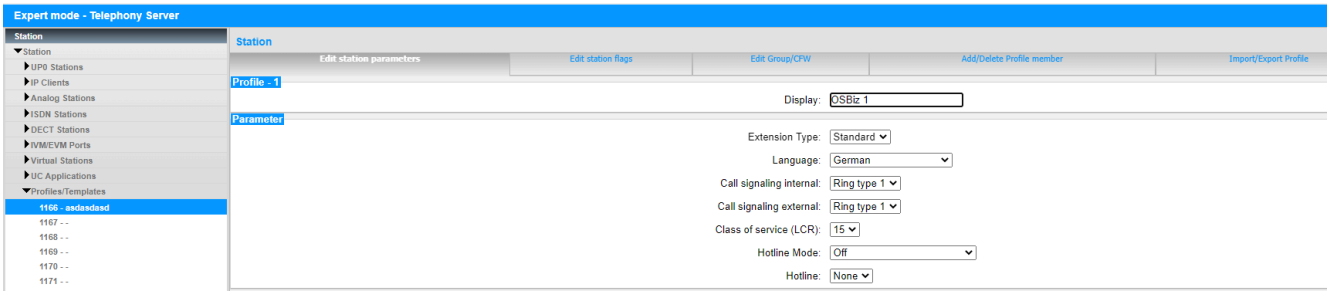
11.14.6 Cómo modificar valores y ajustes de configuración de un perfil de extensiones

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

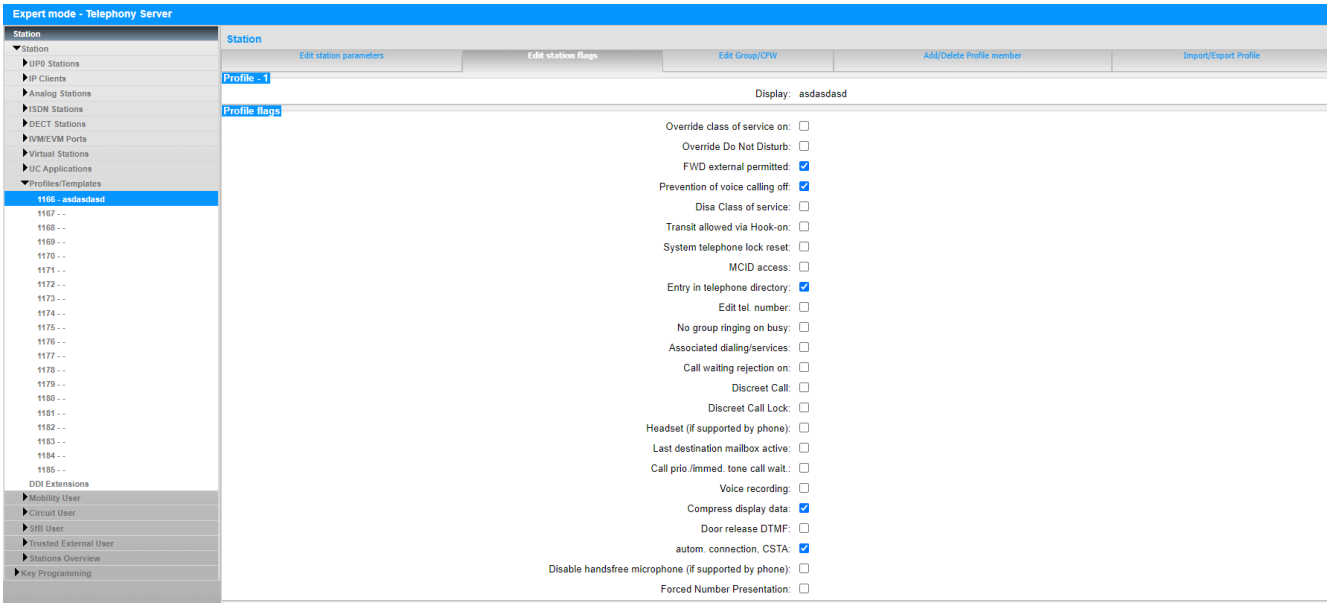
Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Extensiones**.
3) En el árbol de menús, haga clic en **Extensión** > **Perfiles/Plantillas**.
4) En el árbol de menús, haga clic en un número de perfil de extensión.

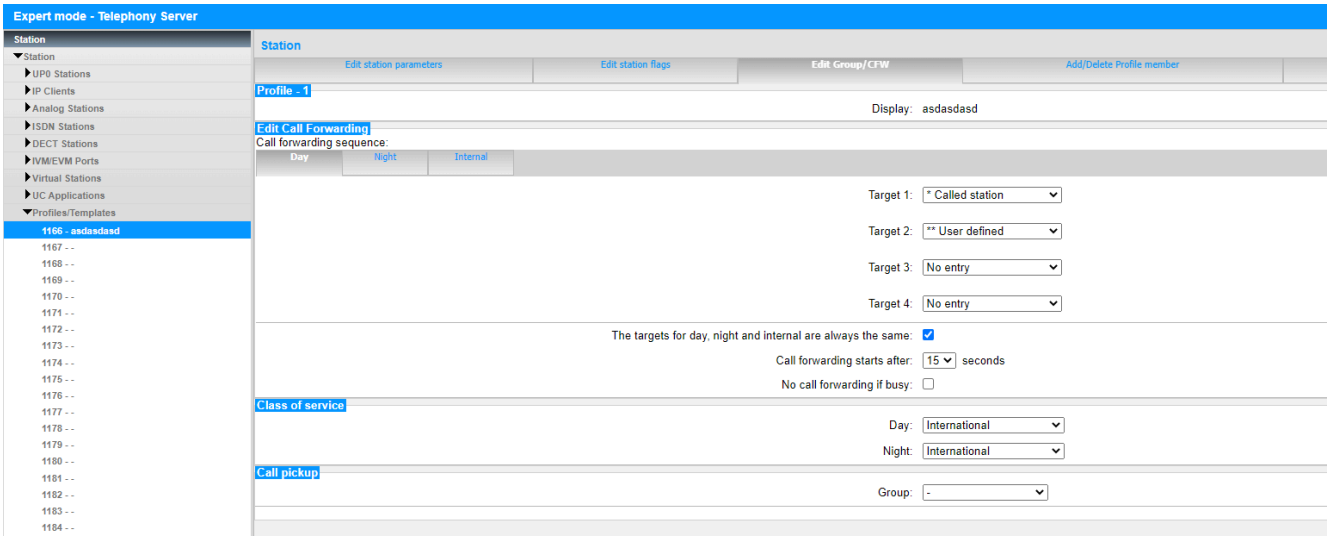


5) Si es necesario, en la pestaña **Parámetros de extensión** y en el campo **Nombre**, modifique el nombre del perfil de extensiones (16 caracteres como máximo) y haga clic en **Aplicar**.

6) Si es necesario, en la pestaña **Parámetros de extensión** modifique el parámetro de extensión deseado para el perfil de extensiones y haga clic en **Aplicar**.



7) Si es necesario, en la pestaña **Flags de extensión** modifique los flags de extensión deseados para el perfil de extensiones y haga clic en **Aplicar**.



8) Si es necesario, en la pestaña **Editar Grupos/RWS** modifique las transferencias automáticas diferidas deseadas para el perfil de extensiones y haga clic en **Aplicar**.

9) Haga clic en **Aplicar**.

11.14.7 Cómo importar o exportar todos los perfiles de extensiones

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el grupo de menús, haga clic en **Extensiones** > **Perfiles/Plantillas**.
4) Haga clic en la pestaña **Importar/Exportar todos los perfiles**.
5) Si desea exportar todos los perfiles de extensiones a un archivo, haga clic en **Descarga** y guarde el archivo en el directorio que desee.
6) Si desea importar todos los perfiles de extensiones desde un archivo, haga clic en **Examinar**, desplácese hasta el lugar de almacenamiento del archivo y cargue el archivo en el sistema de comunicación.

11.15 Configuración de los datos de autenticación en el teléfono SIP

Los datos para la autenticación de una extensión SIP en el sistema de comunicación también se tienen que registrar directamente en el teléfono SIP. Para ello hay que utilizar los datos registrados en la Gestión basada en Web (WBM) en cada extensión SIP.

Los datos siguientes se deben aplicar desde la Gestión basada en Web (WBM) y registrar en el teléfono SIP (extra en cada teléfono SIP):

- Contraseña

  Contraseña para la autenticación.
- SIP usuario / Nombre usuario

  Nombre de usuario para la autenticación.
- Ámbito

  Zona o dominio para la autenticación.

La configuración se puede realizar mediante la Gestión basada en Web (WBM) del teléfono SIP o directamente en el display del teléfono SIP.

11.15.1 Cómo configurar los datos de autenticación mediante la Gestión basada en Web (WBM) del teléfono SIP

Requisitos previos

El teléfono LAN está integrado en la LAN.

El PC de administración tiene acceso a la Gestión basada en Web (WBM) del teléfono SIP.

Conoce la dirección IP del teléfono SIP.

La configuración se describe tomando un OpenStage 60 SIP como ejemplo.

Paso a paso

1) En el PC de administración, inicie el navegador Web y abra la página de registro de la Gestión basada en Web (WBM) del teléfono SIP con esta dirección:

```
https://<Dirección IP del teléfono SIP>
```

> **Nota:** Si no consigue iniciar Gestión basada en Web (WBM), compruebe la conexión LAN y vuelva a intentarlo. Si no diera resultados, compruebe si la dirección IP está bloqueada por la configuración de su firewall. Encontrará información más detallada en la documentación de su firewall.

2) Si el navegador Web notifica un problema con un certificado de seguridad, instale el certificado (en el ejemplo se utiliza Internet Explorer V10).

a) Cierre el navegador Web.

b) Abra el navegador Web con derechos de administrador. Para ello, haga clic con el botón secundario del ratón en el símbolo del navegador Web y en el menú contextual seleccione la entrada **Ejecutar como administrador**.

c) Autorice el control de cuentas de usuario.

d) Abra la página de registro de la Gestión basada en Web (WBM) del teléfono SIP en esta dirección:

```
https://<Dirección IP del teléfono SIP>
```

e) Haga clic en **Continuar cargando este sitio Web**.

f) Haga clic en el mensaje **Error de certificado** en la barra de navegación del navegador Web.

g) Haga clic en **Mostrar certificados**.

h) Haga clic en **Instalar certificado** (solo visible con derechos de administrador).

i) Seleccione la opción **Ordenador local** y confirme la acción con **Continuar**.

j) Seleccione la opción **Colocar todos los certificados en el siguiente almacén**, haga clic en **Examinar** e introduzca **Entidades emisoras raíz de confianza**.

k) Confirme con **Aceptar** y, a continuación, con **Continuar** y **Finalizar**.

l) Confirme el certificado de importación con **Aceptar** y cierre la ventana del certificado con **Aceptar**.

m) Cierre el navegador Web.

n) Inicie de nuevo el navegador Web (sin derechos de administrador) y abra la página de registro de la Gestión basada en Web (WBM) del teléfono SIP, en esta dirección:

```
https://<Dirección IP del teléfono SIP>
```

3) Al iniciar sesión por primera vez se le pide que asigne una contraseña.

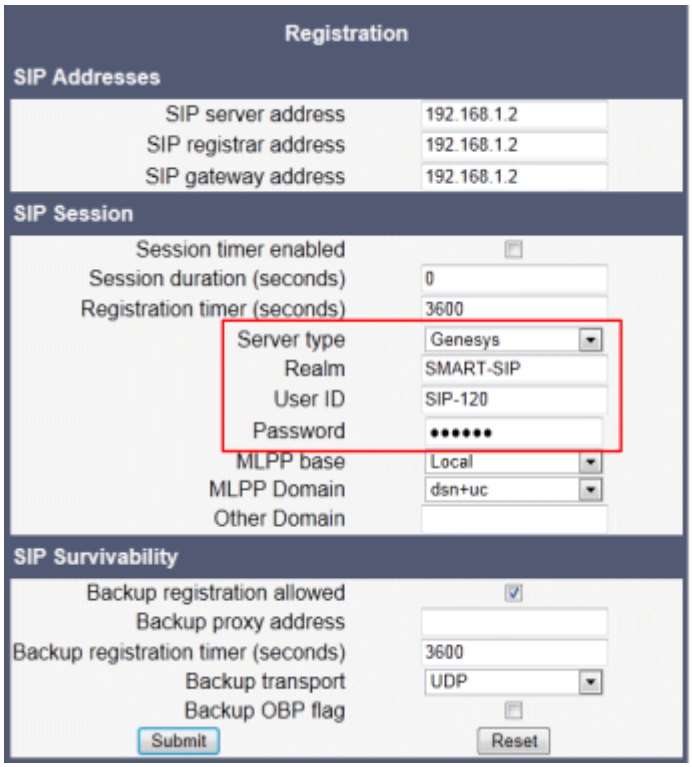
a) En los campos **Nueva contraseña** y **Confirmar nueva contraseña**, introduzca una nueva contraseña para proteger el sistema contra el uso

indebido. Compruebe el uso de mayúsculas y minúsculas y el estado de la tecla **Num**. La contraseña aparece oculta con asteriscos (*).

Nota: La contraseña debe tener una extensión mínima de 6 caracteres e incluir una cifra. Recuerde exactamente cuál es esa contraseña.

---

4) Haga clic en **Aceptar**.
5) Haga clic en la pestaña **páginas de administración (Admin)**.
6) Introduzca la contraseña de administrador (estándar: 123456) y haga clic en **Inicio de sesión**.
7) Desplácese hasta **System** > **Registration** (Sistema > Registro).



8) En el área **SIP Session** (Sesión SIP) y en la lista desplegable **Server type** (Tipo de servidor), seleccione la entrada **Genesys**.
9) En el campo **Ámbito** indique la entrada de ámbito que ha asignado en la configuración de extensiones SIP de la Gestión basada en Web (WBM) del sistema de comunicación (por ejemplo, `SMART-SIP`).
10) En el campo **ID usuario** indique el ID de usuario que ha asignado en la configuración de extensiones SIP de la Gestión basada en Web (WBM) del sistema de comunicación (por ejemplo, `SIP-120`).
11) En el campo **Contraseña**, introduzca la contraseña que ha asignado en la configuración de extensiones SIP de la Gestión basada en Web (WBM) del sistema de comunicación.
12) Haga clic en **Submit**. Se guardan los cambios.
13) Cierre sesión en la Gestión basada en Web (WBM) con el botón **Cerrar sesión**.

11.15.2 Cómo configurar los datos de autenticación en el display del teléfono SIP

Requisitos previos

Conoce los datos de autenticación (ID usuario, Contraseña y Ámbito).

La configuración se describe tomando un OpenStage 80 SIP como ejemplo.

Paso a paso

1) Para acceder al modo de administración del teléfono de sistema, en el teléfono pulse la tecla del menú de configuración/aplicaciones.

2) En la pestaña de `Configuración`, desplácese hasta `Admin` y confirme la acción con la tecla de verificación.

3) Introduzca la contraseña de administrador(valor estándar: `123456`) y confirme la entrada con la tecla de verificación.

4) Desplácese hasta `System` (Sistema) y confirme la acción con la tecla de verificación.

5) Desplácese hasta `Registration` (Registro) y confirme la acción con la tecla de verificación.

6) Desplácese hasta `SIP session` (Sesión SIP) y confirme la acción con la tecla de verificación.

7) Desplácese hasta `Server type` (Tipo de servidor) y confirme la acción con la tecla de verificación.

8) Desplácese hasta la entrada `Genesys` y confirme la acción con la tecla de verificación.

9) Desplácese hasta `Realm` (Ámbito) y confirme la acción con la tecla de verificación.

10) Indique la entrada de ámbito que haya asignado en la configuración de extensiones SIP de la Gestión basada en Web (WBM) del sistema de comunicación (por ejemplo, `SMART-SIP`). Confirme con el símbolo OK.

11) Desplácese hasta `User ID` (ID de usuario) y confirme la acción con la tecla de verificación.

12) Indique el ID de usuario que haya asignado en la configuración de extensiones SIP de la Gestión basada en Web (WBM) del sistema de comunicación (por ejemplo, `SIP-120`). Confirme con el símbolo OK.

13) Desplácese hasta `Password` (Contraseña) y confirme la acción con la tecla de verificación.

14) Indique la contraseña que haya asignado en la configuración de extensiones SIP de la Gestión basada en Web (WBM) del sistema de comunicación. Confirme con el símbolo OK.

15) Confirme la consulta de si quiere guardar los cambios; para ello, seleccione `Save` (Guardar) y confirme la acción con la tecla de verificación.

16) Con la tecla Volver, desplácese hasta el menú `Administrador`.

17) Si es necesario reiniciar el teléfono de sistema para aplicar los cambios, en el menú `Admin` aparecerá la opción de menú `Restart` (Reiniciar). Confirme el `reinicio` con la tecla de verificación y, a continuación, pulse `Yes` (Sí) y la tecla de verificación. El teléfono de sistema se reinicia e inicia sesión en el sistema de comunicación.

11.16 Exportación de datos de extensión

Los datos importantes de extensión se pueden exportar a un archivo XML.

Además de los datos de extensión (como nombre y número de teléfono, direcciones de correo electrónico y tipo de teléfono), el archivo XML también puede incluir otros datos como, por ejemplo, números de teléfono de grupo y asignaciones de licencia.

El archivo XML se puede editar con un programa de cálculo como, por ejemplo, Microsoft Office Excel.

Encontrará una plantilla con datos de ejemplo y una descripción en el archivo `csv-templates.zip`, en **Centro de servicios** > **Documentos** > **Plantillas CSV**.

11.16.1 Cómo exportar los datos de extensión

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Configuración**.
3) En el grupo de menús, haga clic en **Configuración** > **Configuración de puerto**.
4) Haga clic en la pestaña **Exportar la configuración**.
5) Haga clic en el botón **Descarga**.
6) Confirme la consulta de seguridad con **Aceptar**.
7) Haga clic en **Guardar** y seleccione el lugar de almacenamiento del archivo XML.
8) A continuación, haga clic en **Guardar**.

12 UC Smart

UC Smart está integrado en todos los modelos OpenScape Business (con y sin UC Booster) y ofrece prestaciones de Comunicaciones Unificadas como, por ejemplo, estado de presencia, mensajes de voz y conferencias.

Clientes para UC Smart

Las funciones de UC Smart se pueden utilizar con los clientes siguientes:

- myPortal @work
- myPortal to go (como app móvil de UC o como Web Edition)
- Application Launcher
- OpenScape Business Attendant / BLF
- Clientes WSI de terceros

Los límites de ampliación dependen del modelo OpenScape Business que se utilice y de las versiones de OpenScape Business UC Booster instaladas, en su caso.

Peculiaridades de UC Smart con OpenScape Business S

En base a la arquitectura del sistema, con OpenScape Business S se dan las siguientes restricciones:

- El número de mensajes de voz no aparece en la pantalla del teléfono (MWI).
- En el buzón de voz (SmartVM) no se admite el reconocimiento de fax, ocupado o No molestar. Después de aceptar una llamada, las conexiones de fax entrantes no se pueden transferir a un dispositivo de fax estándar mediante el SmartVM. Las grabaciones del SmartVM duran 2 minutos.
- Cuando una extensión está ocupada y el Company AutoAttendant conmuta la conexión, el llamante escucha un tono de ocupado. No es posible dejar mensajes de voz.
- Si al consultar un mensaje de voz se quiere hacer una transferencia al número de teléfono memorizado en el SmartVM (Calling Party Number), este número debe ser idéntico al número de teléfono del usuario configurado en el SmartVM.
- Con UC Booster Server y OpenScape Business S, en las conexiones con el buzón de voz (SmartVM) se ocupan tronqueos SIPQ. En este sentido, no se necesitan licencias de línea.
- Para anuncios grabados simultáneos se ocupan canales MEB.
- Para conexiones de voz con el buzón de voz (SmartVM) o con el AutoAttendant hay disponibles 60 canales MEB.

Nota: Después de modificar la configuración de extensiones, grupos, Mobility u otros parámetros del sistema, como códigos de acceso a línea urbana, hay que sincronizar los datos UC para UC Smart o UC Suite. La sincronización se produce cinco minutos después del último cambio de configuración. Si se modifica la configuración antes de que termine el temporizador de 5 minutos, se reinicia el reloj. Los datos UC pueden estar desactualizados hasta que comience la sincronización.

Conceptos relacionados

Funciones de UC (vista general) en la página 94

12.1 Ajustes básicos para UC Smart

Los ajustes básicos de UC Smart se pueden ajustar.

UC Smart se puede activar o desactivar. Si se utiliza UC Smart hay que desactivar la UC Suite.

Configuración de contraseña

El administrador debe asignar una contraseña inicial para todos los usuarios de UC Smart y comunicársela. La contraseña inicial puede ser la misma para todos los usuarios, o diferentes para cada uno de ellos. Los usuarios deben modificar la contraseña inicial cuando se registren por primera vez en un cliente UC Smart. Sin la asignación de una contraseña inicial, los usuarios no pueden registrarse en un cliente UC Smart.

La contraseña nueva de los usuarios debe seguir unas estrictas normas de seguridad.

Configuración avanzada para conferencias controladas por aplicación (opcional)

Durante la configuración básica, el administrador debe configurar el **Número de función para las conferencias MeetMe** (número de acceso telefónico MeetMe) y al menos un **Número de función para conferencias** (sala de conferencias) en la Gestión basada en Web (WBM).

En los sistemas OpenScape Business X, hay que asignar al número de acceso telefónico MeetMe una lista de destinos de llamada que tenga la primera entrada vacía y en la segunda, el número de teléfono del buzón de voz (SmartVM).

En los sistemas OpenScape Business S, hay que asignar al número de acceso telefónico MeetMe una lista de destinos de llamada en la que la primera entrada se corresponda con el número de teléfono del buzón de voz (ruta: Application Suite).

Por último, hay que asignar un buzón estándar al número de acceso telefónico MeetMe.

Aquí puede consultar la descripción de la configuración: Cómo configurar conferencias controladas por aplicación

Asignaciones de licencia

El administrador debe asignar una licencia UC User a cada usuario UC Smart.

De forma opcional, se pueden asignar licencias adicionales para:

- Buzón de voz (se puede utilizar sin UC Smart)
- Conferencia
- Application Launcher

12.1.1 Cómo activar UC Smart

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **Selección de aplicación**.
3) Si desea utilizar UC Smart sin UC Booster Server, haga clic en **Paquete con UC Smart**.
4) Si quiere utilizar UC Smart con UC Booster Servidor, haga clic en **Paquete con UC Smart en OSBiz UC Booster Server** y en el campo **Dirección IP del OSBiz UC Booster Server**, introduzca la dirección IP del servidor Linux externo.
5) Haga clic en **Aplicar**.

Pasos siguientes

Cómo configurar UC Smart

12.1.2 Cómo configurar UC Smart

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

En **Selección de aplicación** del modo experto, la opción **Paquete con UC Smart** está activada.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Smart**.
3) Haga clic en **Editar** para abrir el asistente **UC Smart**.
4) En el grupo de menús, haga clic en **Administración** > **Ajustes básicos**.
5) En **Habilitar/Deshabilitar UC Smart**, active la casilla de verificación **Activo**.
6) Asignar la contraseña inicial en **Política de contraseñas**:
   a) En **Contraseña inicial de UC Smart a nivel de sistema**, haga clic en **Configurar**.
   b) En el campo **En Contraseña inicial de UC Smart a nivel de sistema** introduzca la contraseña inicial para todos los usuarios UC Smart.
   c) Haga clic en **Aplicar**.
7) Definir las directrices de contraseña en **Política de contraseñas**:

   Nota: Para obtener información detallada sobre las directrices de contraseña, haga clic en el símbolo **i**.

   - Si quiere forzar el uso de normas estrictas para las contraseñas de usuario (opción recomendada), active la casilla de verificación **El usuario debe introducir una contraseña segura**.
   - Si no quiere forzar el uso de normas estrictas para las contraseñas de usuario (desaconsejado), desactive la casilla de verificación **El usuario debe introducir una contraseña segura**.

8) Definir el acceso al sistema en **Configuración de acceso**:
   - Si desea activar el acceso cifrado de los clientes UC Smart al sistema (recomendado si se usa myPortal to go por Internet), active la casilla de verificación **HTTPS**.
   - Si desea activar el acceso sin cifrar de los clientes UC Smart al sistema (no recomendado si se usa myPortal to go por Internet), active la casilla de verificación **HTTP**.
9) Si desea guardar los datos de registro también en el teléfono, active la casilla de verificación **Guardar datos de inicio de sesión en el terminal**.
10) Haga clic en **Aplicar**.

12.1.3 Cómo configurar conferencias controladas por aplicación

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

En **Selección de aplicación** del modo experto, la opción **Paquete con UC Smart** está activada.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) Haga clic en **Editar** para iniciar el asistente **Configuración básica**.
3) Omita la ventana **Resumen** con **OK y Continuar**. Aparece la ventana **Funciones centrales para extensiones**.
4) Active la opción **Cambiar números de función y de llamada preconfigurados**.
5) Haga clic en **Ejecutar función**. Se abre la ventana **Cambiar números de función y de llamada preconfigurados**.
6) En caso necesario, ajuste el **Número de función para las conferencias Meet-Me** de acuerdo a sus necesidades.
7) Asigne al menos un **Números de función para conferencias** para la sala de conferencias.
8) A continuación, haga clic en **Aceptar**. Regresa a la ventana **Funciones centrales para extensiones**.
9) Haga clic en **OK & Continuar**.
10) Para finalizar el asistente, omita todas las demás ventanas con **OK y Continuar**.
11) En la barra de navegación, haga clic en **Modo Experto**.
12) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Llamadas entrantes**.
13) En el grupo de menús, haga clic en **Llamadas entrantes** > **Transferencias automáticas diferidas**.
14) Haga clic en la pestaña **Listas de destinos de llamada - Definición**.

15) En OpenScape Business X, la lista de destinos para el número de acceso telefónico MeetMe se define de la forma siguiente:
    a) En **Lista destinos llam.**, seleccione una lista de destinos de llamada libre, por ejemplo, `500`.
    b) Seleccione **Ninguna entrada** como primer destino y como segundo, el número de teléfono del buzón de voz (por ejemplo, `Grupo VOICEMAIL 351`).
16) En OpenScape Business S, la lista de destinos para el número de acceso telefónico MeetMe se define de la forma siguiente:
    a) En **Lista destinos llam.**, seleccione una lista de destinos de llamada libre, por ejemplo, `500`.
    b) Seleccione Destino externo como primer destino (ruta: Suite de aplicaciones) e introduzca el número de teléfono del buzón de voz en el campo "Destino externo".
17) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
18) Cierre la ventana.
19) En la barra de navegación, haga clic en **Modo Experto**.
20) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Conexión**.
21) En el grupo de menús, haga clic en **Conexiones** > **SmartVM**.
22) Haga clic en la pestaña **Editar buzones SmartVM**.
23) En uno de los campos libres de la columna **Nº llam. buz. voz**, introduzca el número de acceso telefónico MeetMe para el que desea añadir el buzón.
24) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

12.1.4 Cómo determinar las direcciones IP de los componentes del sistema

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) Haga clic en el árbol de navegación en **Aplicaciones** > **Selección de aplicaciones**.

   En **Selección de aplicaciones**, se muestran las direcciones IP de varios componentes, incluidos, por ejemplo, **UC Smart**, **Application Launcher**, **CSTA Connector**, **Open Directory Service**, **UC Suite** y **Web Collaboration**.

Conceptos relacionados

Configuración básica para la UC Suite en la página 546

12.1.5 Cómo determinar el estado de UC Smart

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

En **Selección de aplicación** del modo experto, la opción **Paquete con UC Smart** está activada.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Smart**.
3) Haga clic en **Editar** para abrir el asistente **UC Smart**.
4) En el grupo de menús, haga clic en **Administración** > **Estado**.

   En **Servidor de aplicaciones** se muestra información de estado sobre UC Smart como, p. ej., **Estado**, **Versión**, **Sistema telefónico**, **Base de datos**, **EVM**, **Puntos de supervisión faltantes**, **Usuarios activos**, **Conexiones activas**, **Conexiones HTTPS activas**, **Usuarios Mobility Entry**, **Usuarios sin terminal** y **Usuarios bloqueados**.

12.2 Clientes de UC Smart

Los clientes de UC Smart ofrecen a los usuarios interfaces para las funciones de Comunicaciones Unificadas.

El sistema ofrece los siguientes clientes de UC Smart para los siguientes dispositivos:

Tipo de cliente	Cliente	Dispositivo
Cliente de comunicaciones	myPortal @work	PC
Cliente Mobile	myPortal to go (UC Smart) (véase Mobility en la página 969)	Smartphone, tableta
Cliente de comunicaciones	OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA (software Cliente a teléfono integrado)	OpenScape Desk Phone CP 400/600/600E/ 700/700X/710 HFA

12.2.1 myPortal @work

myPortal @work es una aplicación de comunicaciones unificadas (Microsoft Windows and Mac OS X) que combina todas las funciones y servicios necesarios, como la práctica marcación mediante directorios telefónicos, favoritos, conversaciones e información sobre el estado de presencia de compañeros de trabajo. Todo, en una solución única diseñada para agilizar la comunicación diaria, mejorar el trabajo en equipo y establecer contacto rápidamente con compañeros, clientes y socios.

myPortal @work se puede utilizar en los modos UC Smart o UC Suite. Las prestaciones ofrecidas en la interfaz de usuario varían según el modo. No puede cambiar el modo de funcionamiento, ya que está ajustado por el administrador del sistema. En caso de duda acerca del modo de funcionamiento actual de su cliente de myPortal @work, consulte los detalles con su administrador del sistema.

myPortal @work ofrece un cliente de telefonía de Voz por IP (VoIP). Si la opción VoIP está activada, las funciones relacionadas con la llamada de voz del cliente de myPortal @work emplea la funcionalidad VoIP.

Nota: Para usar la funcionalidad de voz sobre IP (VoIP), el usuario debe estar configurado como cliente del sistema.

Para uso remoto de voz sobre IP (VoIP) con Device@Home, consulte 1 Configuración de sistema Device@Home

---

Esta funcionalidad admite un conjunto de prestaciones además las funciones UC:

- Hacer una llamada
- Contestar una llamada
- Finalizar una llamada
- Consulta
- Transferencia después de contestar
- Transferencia ciega
- Desviar
- Desviar a mensaje de voz
- Llamada recordatoria (aún no se admite la visualización de notificaciones para una llamada recordatoria)
- Alternar
- Silenciar/Desactivar silencio (solo para la funcionalidad VoIP)
- Conferencia de sistema
- Bloqueo de avisos de llamada en espera
- En espera
- No molestar (DND)
- DTMF
- Telecaptura

Nota: Dado que el cliente myPortal @Work no permite enviar tonos DTMF a otra extensión, el envío de un tono DTMF a través del comando "generateDigits" de CSTA tampoco es posible y dicha solicitud será denegada y rechazada por el sistema.

Trabajar en equipo:

También se puede usar un cliente de VoIP de myPortal @work en:

- Grupo (p.ej. Lineal, Llamada en espera)
- MULAP como miembro MULAP

El cifrado de datos de señalización y utilización (SPE) también es compatible con el sistema de comunicación. El cliente VoIP utiliza una pila de seguridad

WebRTC moderna, por lo que también dispone de una transferencia de datos segura que usa DTLS.

Nota: También es compatible con la configuración ITSP SDES.

Se pueden iniciar códigos de servicio desde la barra de búsqueda, pero no son compatibles si existen problemas. No se proporcionan comentarios acerca de la ejecución correcta o incorrecta de códigos de servicio y, por lo tanto, se recomienda encarecidamente utilizar las opciones de entrada que ofrece la interfaz de usuario de myPortal @work para controlar las respectivas funciones.

myPortal @work en modo UC Suite se puede usar no solo de forma independiente sino también junto con el cliente existente de myPortal for Desktop/Outlook, myAgent o myAttendant (CTI, Favoritos y Conversaciones). Las licencias de usuario existentes de UC también se pueden usar con myPortal @work.

La siguiente descripción se refiere principalmente a myPortal @work en modo UC Smart. Las desviaciones para el modo UC Suite se indican en la Guía del usuario de myPortal @work.

Por norma general, myPortal @work es compatible con estas prestaciones:

- Estado de presencia
- Desvío de llamadas basado en el estado
- Directorios incluida la búsqueda por nombre
- Favoritos
- Conversaciones: se muestran hasta 25 conversaciones en el cliente y cada conversación tiene hasta 50 entradas
- Conferencia
- Marcación con tecla de acceso rápido / Búsqueda con tecla de acceso rápido / Hipervínculos de telefonía
- Funciones de llamada a través de:
  1) Dispositivo de teléfono asociado
  2) Cliente de telefonía de Voz sobre IP integrado
- Control del buzón de voz
- Ampliar / Alejar
- Pantalla compartida a través de OpenScape Web Collaboration (opcional)

Uso de myPortal @work en entorno Microsoft Terminal Server

myPortal @work ofrece funcionalidad UC y CTI en entornos de Microsoft Terminal Server, con las siguientes limitaciones:

- No dispone de compatibilidad con hipervínculos de telefonía y con funciones "clic para marcar"
- No admite la funcionalidad de abrir aplicación al inicio
- No permite cargar una imagen de usuario
- Existen limitaciones para la funcionalidad de acoplar/desacoplar, anclar/desanclar y minimizar en la bandeja
- No hay compatibilidad con la función de Voz por IP, VoIP

12.2.1.1 Requisitos para myPortal @work

Para poder utilizar el cliente UC, el PC cliente debe tener un equipamiento de software y hardware adecuado. Según la configuración, la instalación y actualización automática podrían requerir derechos de administración. El abanico de funciones disponible depende de las licencias en uso.

Hay que cumplir los siguientes requisitos para la instalación de myPortal @work:

- Derechos de administrador
- Programa de configuración de software de myPortal @work
- Direcciones IP y puertos del sistema de comunicación
- FQDN o dirección IP, puerto para conectividad WAN (device@home)
- Datos de inicio de sesión (usuario y contraseña) para su cuenta de usuario UC en el sistema de comunicación
- Información de la cuenta del buzón de voz (opcional)
- Número de llamada MULAP en caso de asignación de varios números (opcional)
- SO Windows y Apple Mac OS X

Nota: Asegúrese de que se activa TLS 1.2 en Opciones de Internet (Panel de Control) y se instalan o activan de forma manual los últimos parches de Microsoft.

Si no se realizan las acciones anteriores, se rechazará el acceso HTTPS.

Teléfonos

myPortal @work se puede utilizar junto con los siguientes teléfonos:

Nota: myPortal @work también se puede usar de forma independiente, mediante la funcionalidad VoIP, sin necesidad de un dispositivo físico.

- OpenStage HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/410/710 HFA
- Terminales analógicos
- Teléfonos RDSI
- OpenScape Personal Edition HFA
- OpenStage M3 (OpenScape Business inalámbrico)
- Teléfono OpenScape DECT S6/SL6/R6 (OpenScape Business inalámbrico)

Se admiten dispositivos más antiguos (como optiPoint 410/420/500 y Gigaset M2/SL3/S4/SL4/S5). No se pueden operar dispositivos Optiset E. En las notas de la versión puede consultar cuáles son los dispositivos comprobados y autorizados.

Nota: El cliente integrado OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA no tiene ningún requisito previo especial, aparte de la configuración y licencia estándar del cliente.

"Favoritos" en el menú del teléfono contiene teclas programables libres y no está relacionado con los favoritos de UC. Los detalles de esas teclas y cómo programarlas están disponibles en la documentación del dispositivo.

Nota: Los teléfonos analógicos y DECT no admiten el indicador de buzón. Asimismo, la indicación de informaciones en la pantalla solo tiene compatibilidad restringida.

Navegador Web

Para programar las teclas de los teléfonos mediante el cliente UC, se pueden utilizar los siguientes navegadores Web:

- Microsoft Internet Explorer Versión 10 (o superior)
- Mozilla Firefox 19 (o superior)
- Google Chrome

Archivos de instalación

El administrador puede descargar los archivos de instalación desde el **Centro de servicios** > **Software** y ponerlos a disposición de los usuarios (por ejemplo, a través de una unidad de red).

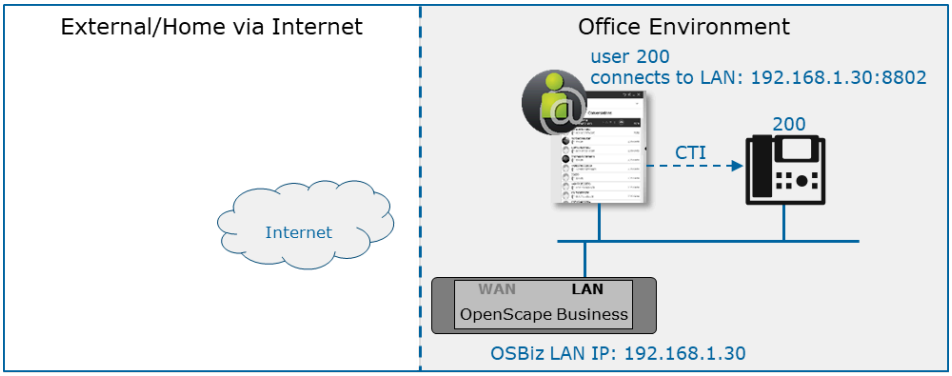
12.2.1.2 Configuración de usuario de myPortal @work

myPortal @work es una combinación de un cliente de UC y un cliente de VoIP y esas dos funcionalidades requieren las siguientes configuraciones/ licencias en función de los distintos modos UC (Smart/UC Suite) y ejemplos de aplicación.

Nota: Cuando una cuenta de usuario de myPortal @work se bloquea después de varios intentos de inicio de sesión incorrectos, en el modo UC Suite, deja de ser visible en el directorio de usuarios de UC Suite. Puede ver los usuarios de myPortal @work bloqueados en**Modo experto > Servicios web > Asistente de servicios web > Gestión de usuarios** pero puede desbloquear estas cuentas en **Modo experto > OpenScape Business UC Suite > Directorio de usuario**.

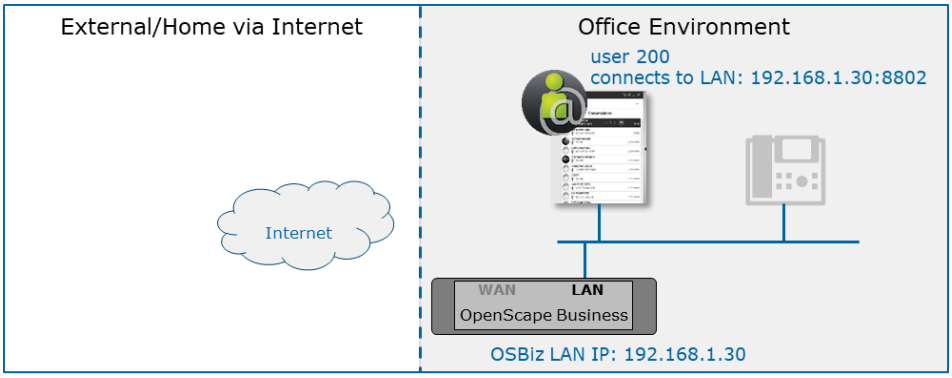
Configuración de LAN local: solo clientes UC y CTI

myPortal @work se utiliza como cliente de UC y CTI para un teléfono de sobremesa asociado sin VoIP.



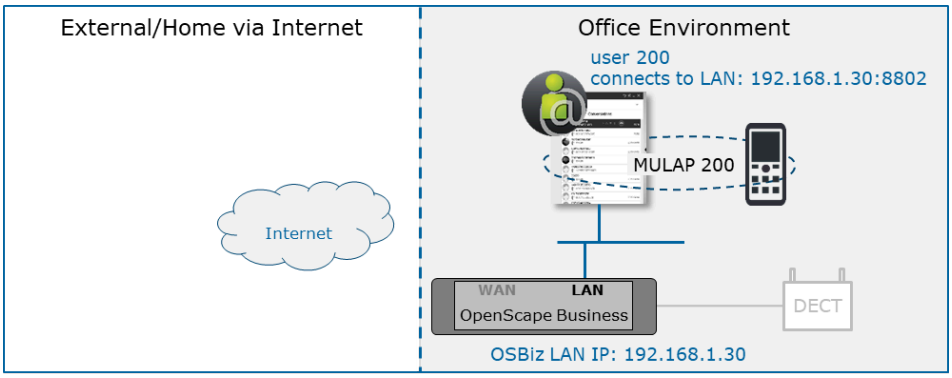
- Licencias: Usuario UC o usuario groupware
- Inicio de sesión en myPortal @work: en la pantalla de inicio de sesión, configure su nombre de usuario/contraseña de inicio de sesión/dirección IP LAN: 8802

Configuración de LAN local: clientes UC y VoIP



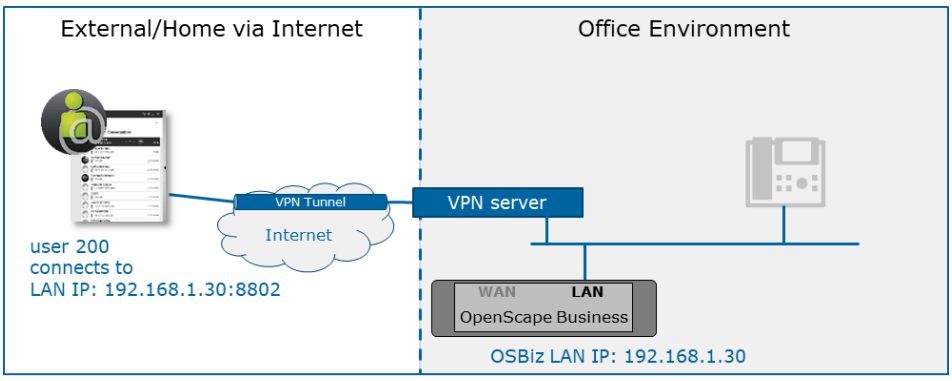
- Licencias: Usuario IP y usuario UC o licencia de Groupware
- Inicio de sesión en myPortal @work: en la pantalla de inicio de sesión, configure su nombre de usuario/contraseña de inicio de sesión/dirección IP LAN: 8802
- Registro VoIP de myPortal @work: Una vez que haya iniciado sesión correctamente, debe ir a Configuración> VoIP> Habilitar VoIP
- La conectividad STUN en el cliente no es necesaria para conexiones internas puras. Sin embargo, es necesario en algunos escenarios híbridos con otros usuarios que utilizan VoIP de myPortal @work a través de Internet público. Para verificar la conectividad STUN, vaya a Configuración> VoIP> Configuración avanzada de ICE> Comprobar el estado de ICE.

Configuración de usuario de MULAP (LAN local)



- Licencias:
  - myPortal @work: Usuario IP y usuario UC o licencia de Groupware
  - otro dispositivo Mulap - en este ejemplo DECT: Licencia TDM User o usuario IP (se recomienda la configuración Mulap para combinar con dispositivos TDM o DECT, aunque también se puede utilizar con terminales IP. En el caso de terminales IP, consulte también la sección Usuario de Deskshare a través de LAN local en la página 508 y Usuario de Remote Deskshare a través de VPN en la página 508).
- Inicio de sesión en myPortal @work: en la pantalla de inicio de sesión, configure su nombre de usuario/contraseña de inicio de sesión del número MULAP/dirección IP LAN: 8802
- Registro VoIP de myPortal @work: Una vez que haya iniciado sesión correctamente, debe ir a Configuración> VoIP> elegir el dispositivo controlado y, posteriormente, habilitar VoIP
- La conectividad STUN en el cliente no es necesaria para conexiones internas puras. Sin embargo es necesario en algunos escenarios híbridos con otros usuarios que utilizan VoIP de myPortal @work a través de Internet público. Para verificar la conectividad STUN, vaya a **Configuración> VoIP> Configuración avanzada de ICE> Comprobar el estado de ICE**.

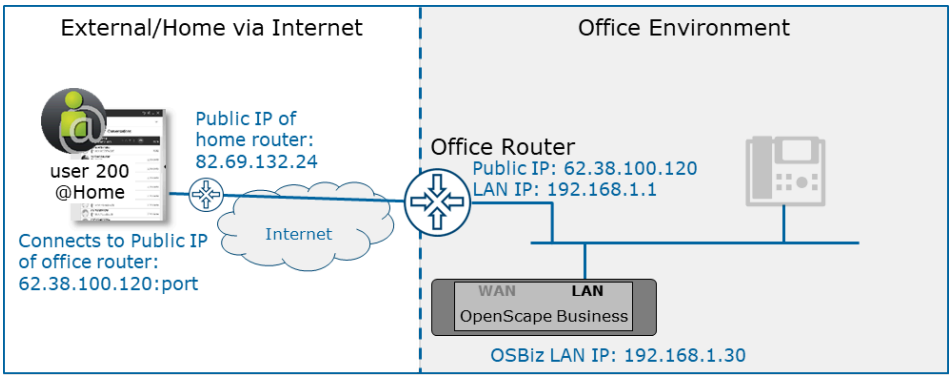
Usuario doméstico con configuración de conexión VPN



- Licencias: Usuario IP y usuario UC o licencia de Groupware
- Inicio de sesión en myPortal @work: en la pantalla de inicio de sesión, configure su nombre de usuario/contraseña de inicio de sesión/dirección IP LAN: 8802
- Registro VoIP de myPortal @work: Una vez que haya iniciado sesión correctamente, debe ir a Configuración> VoIP> Habilitar VoIP

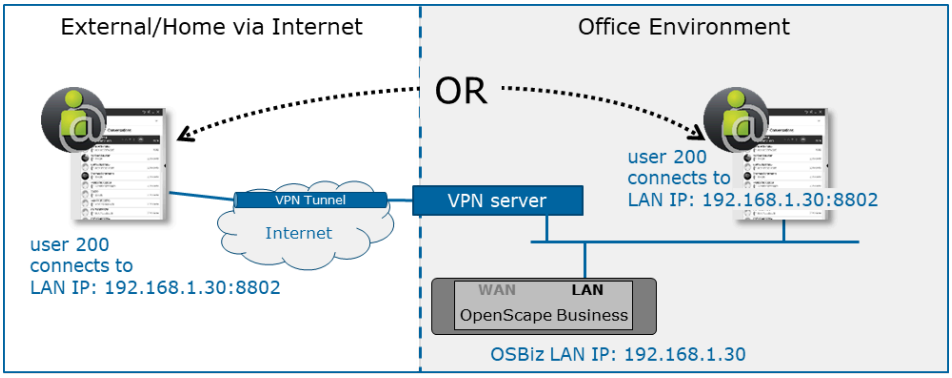
- La conectividad STUN es obligatoria. Para verificar la conectividad STUN, vaya a Configuración> VoIP> Configuración avanzada de ICE> Comprobar el estado de ICE.

myPortal @work a través de Internet público



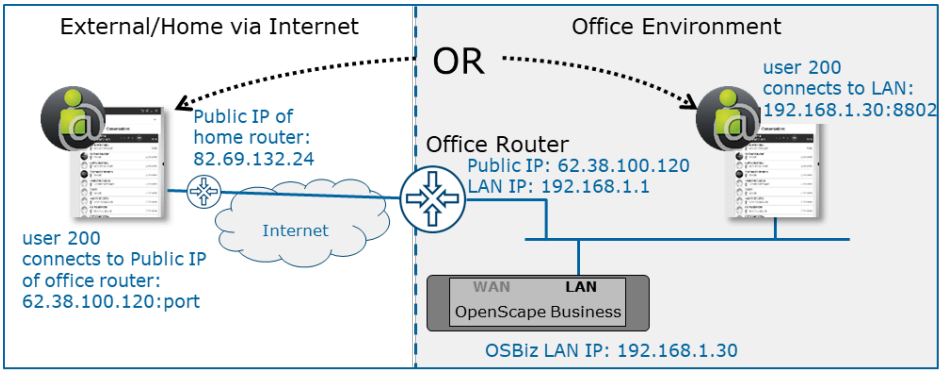
- Licencias: Usuario IP y usuario UC o licencia de Groupware
- Inicio de sesión en myPortal @work: en la pantalla de inicio de sesión, configure su nombre de usuario/contraseña de inicio de sesión/dirección IP pública: puerto configurado desde el administrador.
- Registro VoIP de myPortal @work: Una vez que haya iniciado sesión correctamente, debe ir a Configuración> VoIP> Habilitar VoIP
- Prepare el entorno de red como se describe en el capítulo Pasos de configuración para utilizar myPortal @work a través de Internet en la página 511
- El flag SBC no es necesario para myPortal @work. Solo es necesario si utiliza un dispositivo de hardware.
- No utilice la interfaz WAN de OSBiz para conectarse a Internet cuando utilice myPortal @work a través de una IP pública. Si lo hace, el SBC interno detectará la dirección IP pública de la interfaz WAN y la utilizará en la comunicación entre el cliente y OSBiz, lo que ocasionará problemas de carga útil. Configuración propuesta: Conecte el ITSP a través de la interfaz LAN, lo cual es posible a través del enrutador ISP normal o mediante un segundo enrutador y rutas estáticas.
- Se necesita conectividad STUN. Para verificar la conectividad STUN, vaya a Configuración> VoIP> Configuración avanzada de ICE> Comprobar el estado de ICE.

Usuario doméstico con configuración de VPN y LAN local (p. ej., se muda de la oficina a casa y viceversa)



- Licencias: Usuario IP y usuario UC o licencia de Groupware
- Inicio de sesión en myPortal @work: en la pantalla de inicio de sesión, configure su nombre de usuario/contraseña de inicio de sesión/dirección IP LAN: 8802
- Registro VoIP de myPortal @work: Una vez que haya iniciado sesión correctamente, debe ir a Configuración> VoIP> Habilitar VoIP
- myPortal @work se puede utilizar en ambos entornos sin cambiar la configuración.
- La conectividad STUN es estrictamente necesaria. Para verificar la conectividad STUN, vaya a Configuración> VoIP> Configuración avanzada de ICE> Comprobar el estado de ICE.

myPortal @work a través de Internet público y configuración LAN local (p. ej., se muda de la oficina a casa y viceversa)



- Licencias: Usuario IP y usuario UC o licencia de Groupware
- Inicio de sesión en myPortal @work: en la pantalla de inicio de sesión, configure su nombre de usuario/contraseña de inicio de sesión / dirección IP LAN: 8802 y dirección IP pública: puerto configurado desde el administrador. Al configurar ambas direcciones, no es necesario utilizar un segundo perfil al mudarse de la oficina a casa y viceversa.
- Registro VoIP de myPortal @work: Una vez que haya iniciado sesión correctamente, debe ir a Configuración> VoIP> Habilitar VoIP
- Prepare el entorno de red como se describe en el capítulo Pasos de configuración para utilizar myPortal @work a través de Internet en la página 511
- El flag SBC no es necesario para myPortal @work. Solo es necesario si utiliza un dispositivo de hardware.

Para el registro de VoIP

En caso de que se utilicen usuarios locales y domésticos, el usuario debe tener solo una conexión VoIP en casa o en la oficina.

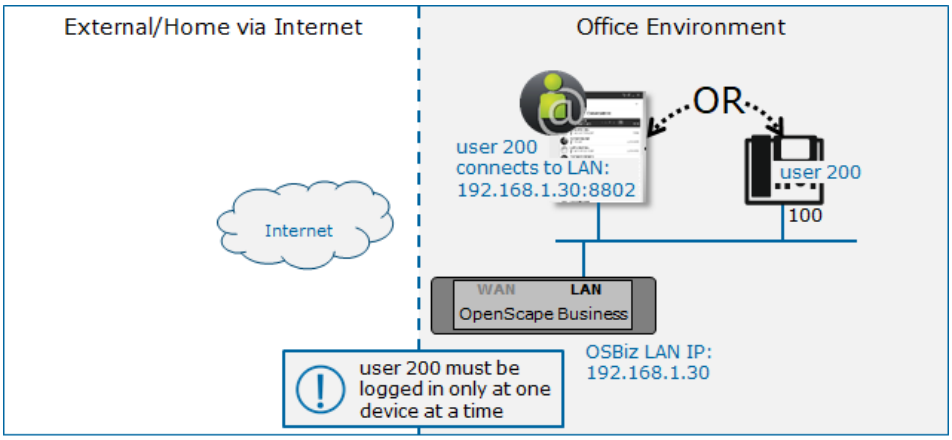
Para UC

Cuando el usuario quiere estar conectado en UC al mismo tiempo en más de un lugar:

- Modo UC Smart: El cliente de UC se puede conectar al mismo tiempo desde casa y desde la oficina, pero solo se admite un cliente de VoIP en este escenario y la funcionalidad de VoIP del otro cliente debe quedarse sin registrar.

- Modo UC Suite: Consulte el párrafo “Combinación de myPortal @work con otros clientes de UC Suite y configuración de licencias”. Solo se permite un cliente de myPortal @work.

Usuario de Deskshare a través de LAN local



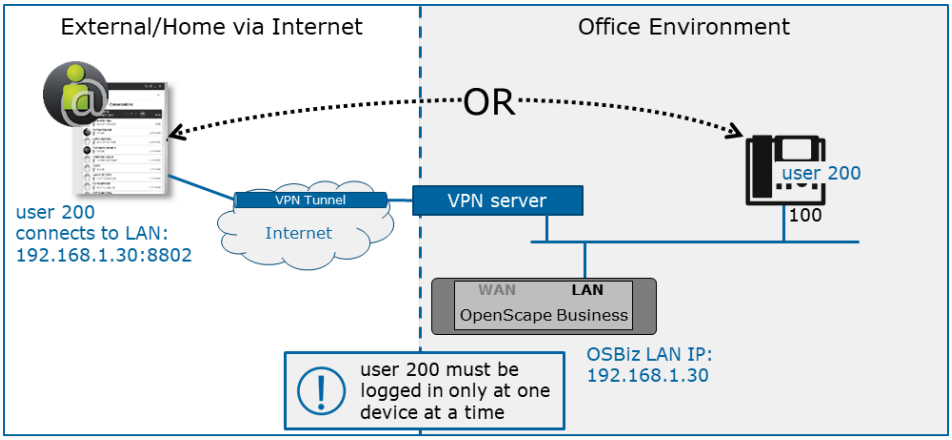
- Licencias: Licencia de Deskshare y usuario UC o licencia de Groupware
- Inicio de sesión en myPortal @work: en la pantalla de inicio de sesión, configure el inicio de sesión de la extensión de escritorio compartido con su nombre de usuario/contraseña/dirección IP LAN: 8802
- Registro VoIP de myPortal @work: Una vez que haya iniciado sesión correctamente, debe ir a Configuración> VoIP> Habilitar VoIP

Ejemplo: El dispositivo utiliza un número ficticio = "100" Conéctese a "100" con su DeskPhone como escritorio compartido, por ejemplo, 200 utilizando el código de servicio *9419.

Para utilizar myPortal @work con el usuario 200, el teléfono de escritorio se desconecta automáticamente y vuelve al número ficticio “100”. Cuando vuelva a cambiar al teléfono de escritorio, asegúrese de que myPortal @work no esté registrado (# el usuario debe salir de la aplicación o cerrar la sesión).

Usuario de Remote Deskshare a través de VPN

La misma configuración que se describe en el capítulo Usuario de Deskshare a través de LAN local en la página 508 se aplica también a los usuarios domésticos a través de VPN.



- Licencias: Licencia de Deskshare y usuario UC o licencia de Groupware

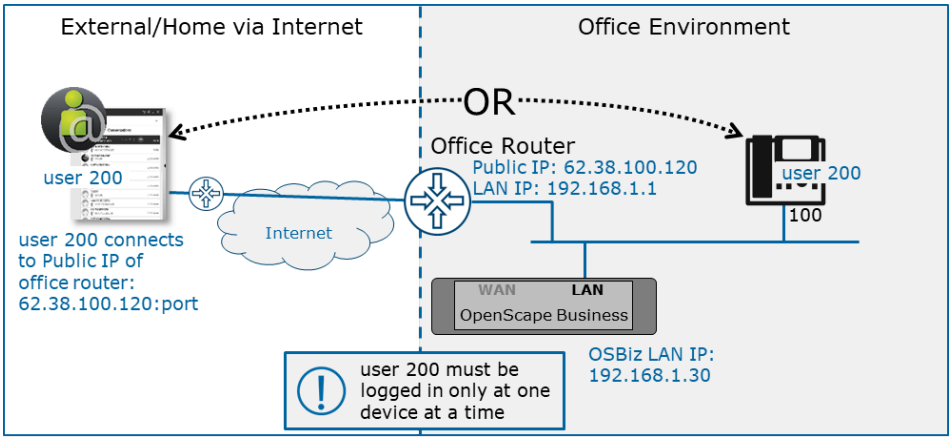
- Inicio de sesión en myPortal @work: en la pantalla de inicio de sesión, configure el inicio de sesión de la extensión de escritorio compartido con su nombre de usuario/contraseña/dirección IP LAN: 8802
- Registro VoIP de myPortal @work: Una vez que haya iniciado sesión correctamente, debe ir a Configuración> VoIP> Habilitar VoIP

Ejemplo: El dispositivo utiliza un número ficticio = "100" Conéctese a "100" con su DeskPhone como escritorio compartido, por ejemplo, 200 utilizando el código de servicio *9419.

Para utilizar myPortal @work con el usuario 200, el teléfono de escritorio se desconecta automáticamente y vuelve al número ficticio “100”. Cuando vuelva a cambiar al teléfono de escritorio, asegúrese de que myPortal @work no esté registrado (# el usuario debe salir de la aplicación o cerrar la sesión).

Usuario de Remote Deskshare a través de Internet público

La misma configuración que se describe en el capítulo Usuario de Deskshare a través de LAN local en la página 508 es técnicamente posible también con los usuarios domésticos a través de Internet público. Sin embargo, aún no se ha probado por completo y, por lo tanto, se describe de manera preliminar en esta versión del documento.



- Licencias: Licencia de Deskshare y usuario UC o licencia de Groupware
- Inicio de sesión en myPortal @work: en la pantalla de inicio de sesión, configure el inicio de sesión de la extensión de escritorio compartido con su nombre de usuario/contraseña/dirección IP LAN: 8802
- Registro VoIP de myPortal @work: Una vez que haya iniciado sesión correctamente, debe ir a Configuración> VoIP> Habilitar VoIP

Ejemplo: El dispositivo utiliza un número ficticio = "100" Conéctese a "100" con su DeskPhone como escritorio compartido, por ejemplo, 200 utilizando el código de servicio *9419.

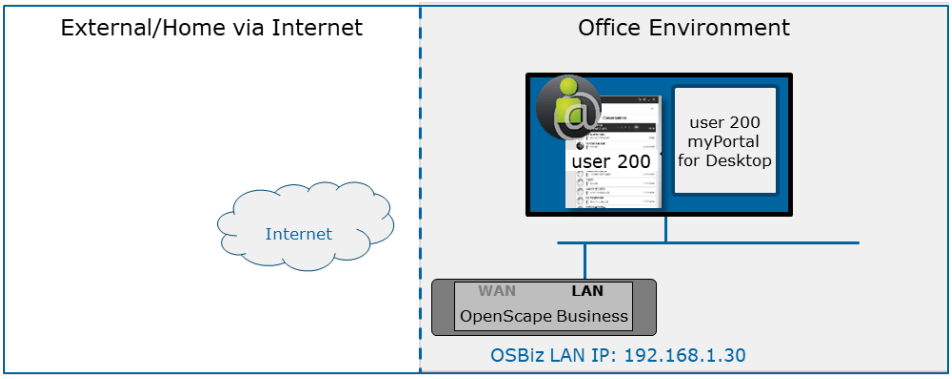
Para utilizar myPortal @work con el usuario 200, el teléfono de escritorio se desconecta automáticamente y vuelve al número ficticio “100”. Cuando vuelva a cambiar al teléfono de escritorio, asegúrese de que myPortal @work no esté registrado (# el usuario debe salir de la aplicación o cerrar la sesión).

Combinación de myPortal @work con otros clientes de UC Suite y configuración de licencias

Nota: Las configuraciones descritas en este capítulo también son compatibles con el usuario doméstico a través de VPN.

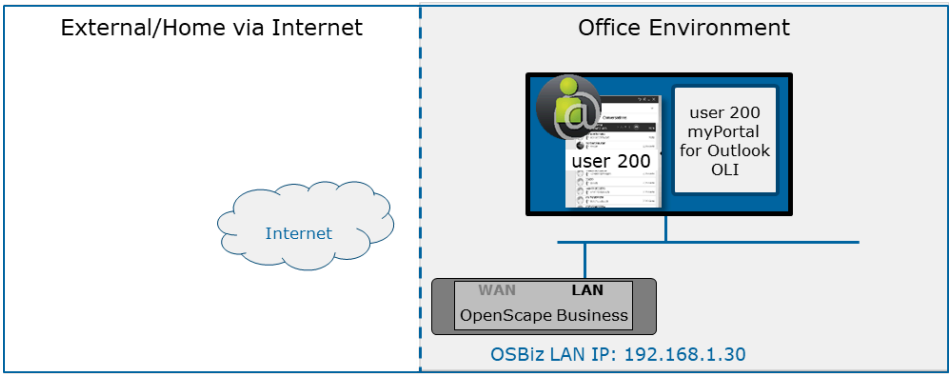
Licencia de usuario UC

El mismo usuario puede conectarse en paralelo con myPortal @work y myPortal for Desktop.



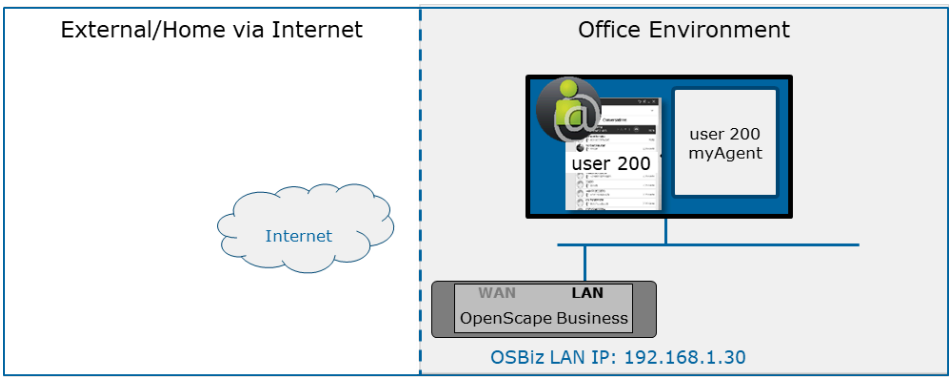
Licencia de Groupware

El mismo usuario puede conectarse en paralelo con myPortal @work y OLI.



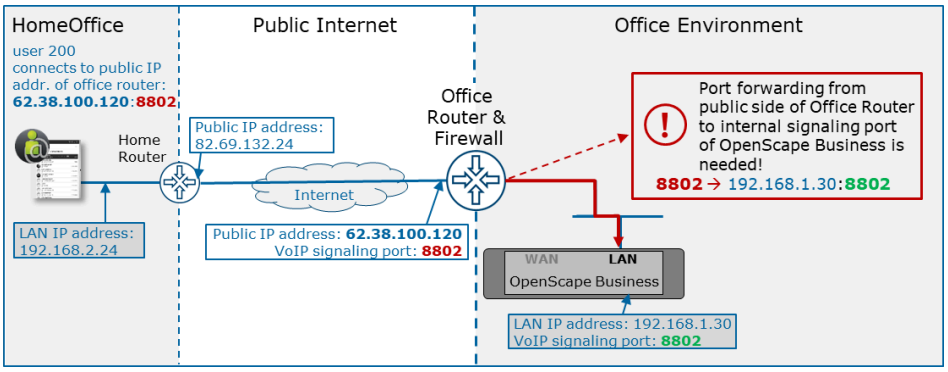
Combinación de IP, usuario UC y licencia de myAgent

La VoIP de myAgent y myPortal @work se pueden utilizar como softphone en paralelo.



12.2.1.3 Pasos de configuración para utilizar myPortal @work a través de Internet

Para utilizar myPortal @work desde Internet, OpenScape Business también debe ser accesible desde Internet. Para todos los ejemplos de este capítulo, se asume el siguiente escenario de interconexión básico.



Descripción del escenario de interconexión

OpenScape Business se encuentra dentro del entorno de la oficina, que está conectado a Internet a través del enrutador de la oficina. Se puede acceder a este enrutador desde Internet a través de la dirección IP pública de “62.38.100.120” o mediante un nombre DNS.

El cliente myPortal @work está conectado a la LAN dentro de una red doméstica o externa, que está conectada a Internet a través de un enrutador independiente. Se puede acceder al enrutador externo desde Internet con la dirección IP pública “82.69.132.24”.

Pasos de configuración

Para utilizar el cliente myPortal @work en OpenScape Business a través de Internet, se deben configurar los siguientes componentes en consonancia.

OpenScape Business dentro de la oficina

Soporte activo de STUN en el sistema si aún no lo ha hecho para un ITSP.

Configurar el usuario de myPortal @work (el flag SBC no es necesario para VoIP)

Enrutador de oficina

Dado que el cliente myPortal @work debe acceder a OpenScape Business desde Internet y viceversa, se debe configurar lo siguiente en el enrutador de la oficina para lograr esto:

- Reenvío de puerto HTTPS desde el puerto externo (el predeterminado es 8802) al puerto interno 8802 del sistema
  - Puerto externo (el predeterminado es 8802) -> Enrutador de oficina -> 192.168.1.30:8802

Para más información, véase también el capítulo. Configuración de puertos y firewall en la página 512

myPortal @work / enrutador externo

El cliente myPortal @work necesita conectarse a la dirección IP pública o DNS del enrutador de Internet de la oficina en el puerto externo, que de forma predeterminada es 8802 (debido al reenvío de puertos configurado

previamente, lo que apuntará a OpenScape Business dentro de la red de la oficina).

En la mayoría de los casos, no es necesario configurar nada más en el enrutador externo, pero en caso de problemas, consulte el capítulo Configuración de puertos y firewall en la página 512.

12.2.1.4 Otras recomendaciones & ajustes de configuración

Ajustes del servidor STUN

Para obtener más información sobre cómo configurar el servidor STUN, consulte el capítulo "Configuración de STUN" en la guía "Cómo configurar el sistema device@home" y la sección de la guía del usuario "Cómo añadir un servidor STUN" de OpenScape Business V3, my Portal @work.

Auriculares

Se pueden utilizar todos los dispositivos de sonido / micrófonos detectados que se encuentran en el sistema operativo.

Integración de auriculares Jabra/Plantronics

En caso de problemas con la integración de auriculares Jabra, ejecute la aplicación con derechos de administrador.

Para utilizar la integración de auriculares Jabra, el dispositivo Jabra debe configurarse como el dispositivo de micrófono principal en myPortal @work.

Para la integración de Plantronics, debe instalarse el conmutador Plantronics.

Configuración de puertos y firewall

Básicamente, se deberán configurar los siguientes puertos para la señalización de myPortal @work:

- Funcionalidad UC & señalización WebRTC / VoIP: 8802
- Puerto de servidor STUN predeterminado: 3478. Si se configura un servidor STUN personalizado, puede que sea necesario usar un puerto distinto.

La configuración de los puertos para la carga útil de WebRTC / VoIP depende del tipo de firewall utilizado en el entorno del cliente. Para ejecutar myPortal @work en un entorno de red de cliente, es fundamental comprender y verificar el tipo de firewall utilizado, ya sea con estado o sin estado, y configurar los ajustes del firewall junto con el administrador de TI responsable.

Para comprender mejor las diferencias entre ambos tipos de firewall, lea lo siguiente:

- Los firewall sin estado están diseñados para proteger redes basadas en información estática, como origen y destino.
- Un firewall con estado es un firewall que supervisa el estado completo de las conexiones de red activas, lo que significa que los firewalls con estado analizan constantemente el contexto completo del tráfico y los paquetes de datos.

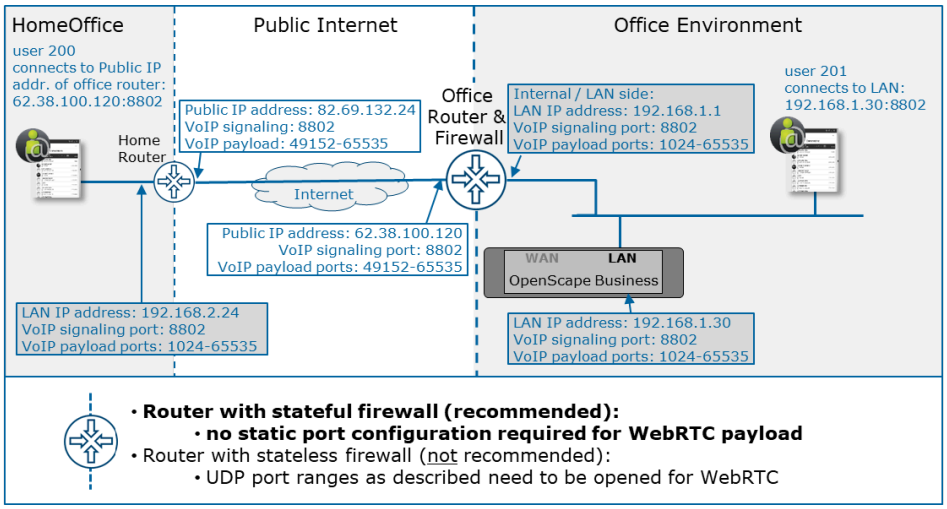
Para obtener más información sobre esos tipos de firewall, consulte Internet o la bibliografía técnica pertinente como fuente de información.

Se asume que se utilizará un dispositivo de firewall / NAT con estado para proteger mejor las redes privadas de los clientes, lo que significa que este dispositivo debe permitir conexiones salientes internas hacia su destino.

El dispositivo de firewall / NAT bloqueará cualquier paquete en la dirección entrante, a menos que pertenezca a una sesión ya establecida (en un puerto efímero / dinámico) que se configuró anteriormente como saliente.

En cuanto al uso del puerto, no es necesario configurar nada dentro del firewall / dispositivo NAT, ya que gestionará y negociará automáticamente cuando se utilice un firewall con estado.

El uso de un firewall con estado es la ruta recomendada y más segura para ejecutar soluciones VoIP basadas en WebRTC.



En cuanto a un firewall sin estado (que no se recomendará para VoIP), el siguiente rango de puertos de origen UDP para dispositivos dentro de la red del cliente debe abrirse para el tráfico de carga útil interno: 1024-65535.

Para todo el tráfico de carga útil que se intercambia a través de Internet, la tecnología WebRTC utiliza puertos del rango de puertos UDP de 49152-65535. Para obtener más información, consulte la bibliografía técnica pertinente como fuente de información.

Cada dispositivo de red en la ruta entre los puntos finales de carga útil involucrados debe configurarse en consonancia (por ejemplo, enrutador, firewall, NAT, proxy, etc.).

Debido al amplio rango de puertos que deben abrirse, no se puede recomendar un firewall sin estado para VoIP.

Tabla 4:

	Firewall con estado	Firewall sin estado que debe abrirse estáticamente
Puerto de señalización WebRTC / VoIP	8802	8802

	Firewall con estado	Firewall sin estado que debe abrirse estáticamente
Carga útil de WebRTC / VoIP Rango de puertos UDP dentro de la LAN local, es decir, dentro del entorno del cliente	dinámica[4]	1024-65535
Carga útil de WebRTC / VoIP Intervalo de puertos UDP utilizado en la Internet pública	dinámica[4]	49152-65535

Restricciones de VoIP

- En escenarios con múltiples llamadas (por ejemplo, transferencia, conferencia, en espera), recomendamos desactivar la integración de auriculares en caso de error. Al desactivar el indicador de integración de auriculares dentro de myPortal @work, solo no se puede usar la función de control de llamadas de los auriculares, pero estos aún se pueden usar como dispositivo de audio.
- La funcionalidad de “plaza libre” de myAgent (el agente puede seleccionar el teléfono que se utilizará a través de un menú desplegable durante el proceso de inicio de sesión), es decir, no se admite la selección libre de un dispositivo físico por parte de un agente en combinación con myPortal @work.
- La configuración NAT simétrica no es compatible.
- No se admiten firewall estrictos.

12.2.1.5 Guía para la resolución de problemas

Tiempo de conexión agotado

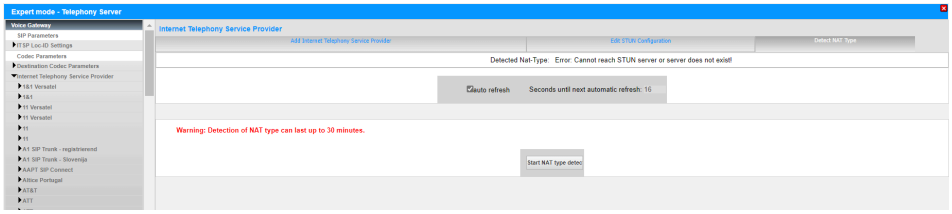
- Como usuario doméstico con conexión VPN, debe asegurarse de que el usuario pueda acceder a la dirección LAN del sistema y conectarse a la dirección LAN: Puerto 8802. Mensaje de resolución de problemas: Mensaje de error "tiempo de conexión agotado", Acción: compruebe si el usuario cuando está conectado a través de VPN tiene una IP local de la red VPN.
- Como usuario independiente, asegúrese de que no haya ningún otro dispositivo o cliente VoIP myPortal @work registrado con el mismo número de extensión. Compruebe también en **WBM> Modo experto> Web Services Assistant** en caso de conexiones abiertas.

Sin carga útil

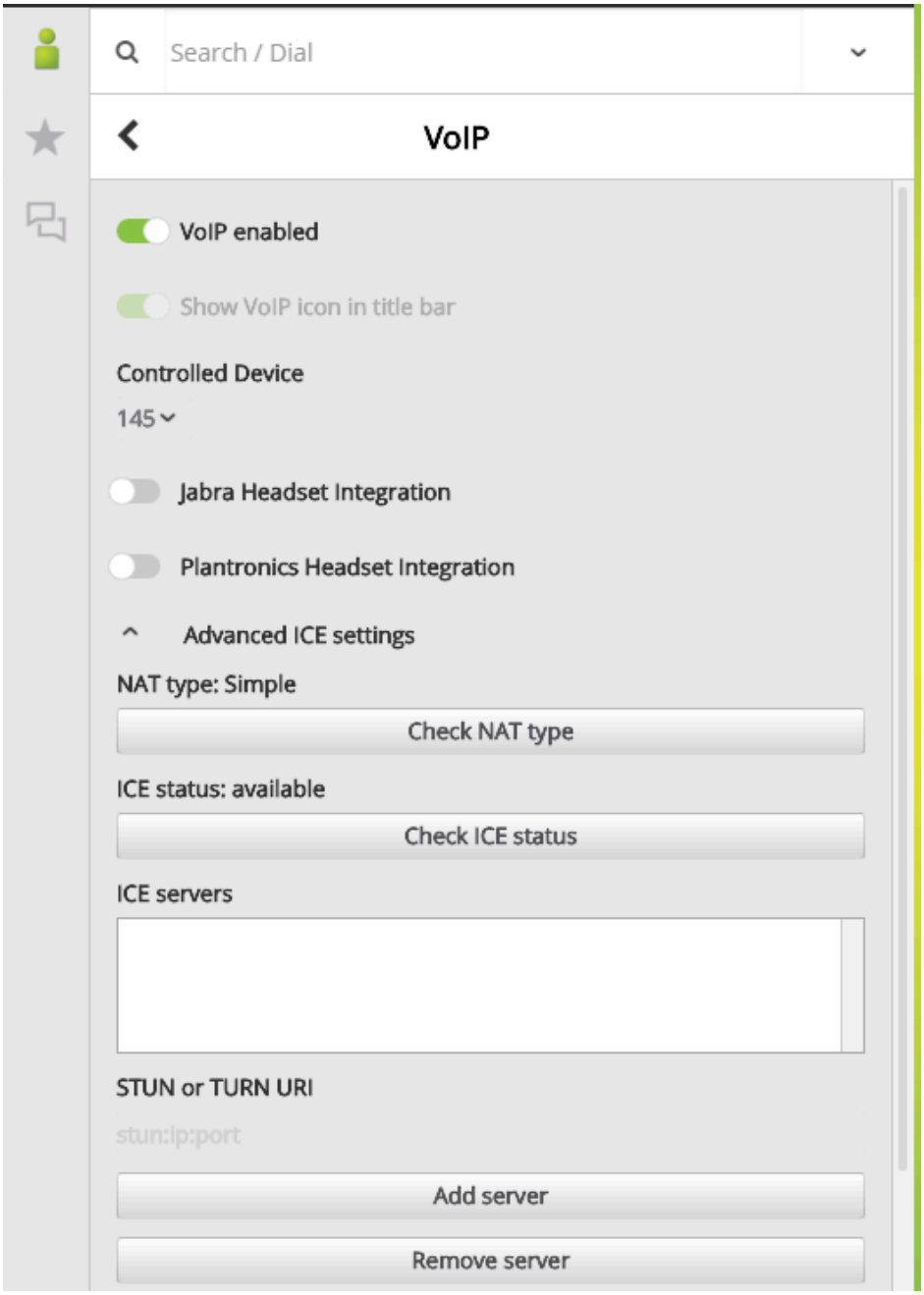
En caso de que no haya un problema permanente de carga útil:

[4] No se necesita ninguna acción de configuración; los puertos se adoptarán dinámicamente del mismo rango de puertos UDP que se enumeran para el firewall sin estado

- Verifique que los puertos permitidos estén abiertos en el firewall. Para obtener más información, consulte el capítulo Configuración de puertos y firewall en la página 512.
- Verifique la configuración del firewall NAT. La configuración NAT simétrica no es compatible.
- Puede detectar el tipo de NAT del sistema en **WBM> Modo experto> Gateway voz> Detección tipo NAT**.
- Verifique la conectividad del servidor STUN en el sistema.



- Verifique la conectividad de ICE en myPortal @work: **Configuración> VoIP> Configuración avanzada de ICE**. En caso de que el “tipo NAT” o el “Estado de ICE” no sean los que se muestran a continuación, su administrador debe verificar la configuración de la red / firewall.



Ejecute "Comprobar tipo NAT"> Tipo NAT: Simple

Ejecute "Comprobar el estado de ICE"> Estado de ICE: disponible

- Desactive la integración de auriculares desde myPortal @work y vuelva a realizar el escenario.
- Vuelva a seleccionar los dispositivos de audio de la configuración de VoIP.

12.2.1.6 Más sugerencias

SIP ALG (Gateway de capa de aplicación)

Si experimenta uno de los siguientes problemas, verifique si hay un SIP ALG activado en uno de los enrutadores involucrados. Hay algunas categorías de síntomas que SIP ALG podría afectar a las conexiones VoIP. No siempre es evidente, especialmente porque estos problemas suelen ocurrir de forma silenciosa y sin que los usuarios lo sepan.

- Audio unidireccional (solo una persona puede escuchar a la otra)
- El cliente no suena cuando se le llama
- Las llamadas se cortan después de conectarse
- Llamadas que van directamente al buzón de voz sin motivo conocido

12.3 Usuarios de UC Smart

Los usuarios de UC Smart son extensiones que usan clientes UC de UC Smart.

En UC Smart Assistant están disponibles los siguientes ajustes para clientes UC Smart:

Configuración	Explicación
Configuración	
Usuarios	Se muestra la configuración.
Nombre	Se muestra la configuración.
Contraseña	Contraseña para clientes UC Smart y UC Smart Assistant.
Idioma	Idioma de la interfaz de usuario.
El usuario debe asignar una contraseña nueva	Se muestra la configuración.
Acceso a UC Smart Assistant	Autorización para usar UC Smart Assistant en el navegador Web para tareas de configuración por parte del usuario.
Configurado como extensión Mobility	Se muestra la configuración.
Licencia de buzón de voz	Se muestra la configuración.
Servicios asociados	Se muestra la configuración.
Detalles de perfil	
Número de teléfono móvil	Número de teléfono móvil de la extensión en formato canónico (p.ej. `+49 173 1234567`).
Número de teléfono privado/ externo	Número de teléfono adicional de la extensión en formato canónico (p.ej. `+49 89 987654321`).
Dirección e-mail	Dirección de email del usuario.
Buzón de voz a correo electrónico	Activación/Desactivación de la notificación por correo electrónico cuando se recibe un mensaje de voz nuevo.

Configuración	Explicación
Visibilidad de presencia	Permite configurar si las extensiones internas y externas podrán ver el estado de presencia, si solo podrán verlo las extensiones internas o si nadie podrá verlo.
Información de licencia	
Visualización de las licencias asignadas al usuario	

12.3.1 Cómo configurar un usuario de UC Smart

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

En **Selección de aplicación** del modo experto, la opción **Paquete con UC Smart** está activada.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Smart**.
3) Haga clic en **Editar** para abrir el asistente **UC Smart**.
4) En el grupo de menús, haga clic en **Administración** > **Administración de usuarios**.
5) En la lista **Usuarios**, seleccione el usuario deseado.
6) En el área **Configuración** y en **Detalles de perfil**, introduzca los datos del usuario.
7) Haga clic en **Aplicar**.
8) Si desea configurar otro usuario, repita los pasos 5 a 7.

12.3.2 Cómo cambiar la contraseña de un usuario de UC Smart

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

En **Selección de aplicación**, en el modo experto, la opción **Paquete con UC Smart** está activada.

Nota: Tenga en cuenta que, de forma predeterminada, los usuarios UC Smart deben modificar su contraseña de nuevo si la ha modificado el administrador. Si no desea que sea así, después de modificar la contraseña desactive el flag "El usuario debe cambiar la contraseña".

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Smart**.

3) Haga clic en **Editar** para abrir el asistente **UC Smart**.
4) En el grupo de menús, haga clic en **Administración** > **Administración de usuarios**.
5) En el área **Usuarios** seleccione el usuario correspondiente.

> **Nota:** Por motivos de seguridad, el sistema no aceptará contraseñas que consistan en 5 asteriscos (*****).

6) En el área **Configuración**, en la sección **Contraseña**, indique la nueva contraseña.
7) Haga clic en **Aplicar**.
8) Si desea restablecer la contraseña de otro usuario, repita los pasos 5 a 7.

Pasos siguientes

Comunique la nueva contraseña a los usuarios correspondientes.

12.4 Presencia

El estado de presencia ofrece información en el directorio interno sobre la disponibilidad de una extensión interna (o una extensión Mobility Entry). Además, el estado de presencia controla la accesibilidad de las extensiones internas con el desvío de llamadas relativo al estado.

En calidad de usuario, puede modificar su estado de presencia en myPortal @work myPortal to go. Cada vez que se modifica el estado de presencia (excepto en **Oficina**) se establece el momento del regreso programado a **Oficina**, si es necesario.

En calidad de usuario, puede seleccionar los siguientes estados:

- **En la oficina**
- **Reunión**
- **Enfermo**
- **Pausa**
- **Fuera de oficina**
- **Vacaciones**
- **Pausa de mediodía**
- **Gone Home**
- **No molestar**

> **Nota:** El administrador del sistema puede activar/desactivar la visibilidad del estado “enfermo” dentro de la administración del sistema. Ver OpenScape Business UC Suite> Servidor

Con el desvío de llamadas relativo al estado, las llamadas se pueden desviar al buzón de voz personal (entre otras opciones). Si un usuario no tiene buzón de voz personal, puede desviar llamadas a un buzón de grupo o del sistema.

12.5 Directorios y diario

Los directorios y el diario organizan los contactos y las llamadas.

12.5.1 Directorios

Los directorios organizan los contactos de las extensiones. Las extensiones pueden acceder a los contactos con clientes UC Smart.

El sistema proporciona los directorios siguientes, compatibles con las funciones siguientes y con la prioridad siguiente para número de búsqueda (el número de búsqueda solo será compatible con llamadas externas y si la línea urbana/ITSP no suministra el número):

Directorio	Clientes de UC Smart	Teléfono de sistema con display
Directorio personal	Contactos de Outlook importados mediante el asistente personal.	
Directorio interno	Incluye todas las extensiones y todos los grupos internos (en su caso, con números de teléfono adicionales) que tienen activada la visualización en el sistema. Las extensiones internas con teléfono del sistema se muestran con estado de presencia. Para mostrar el estado de presencia de una extensión es necesario que el usuario en cuestión lo autorice.	Incluye todas las extensiones y todos los grupos internos que tienen activada la visualización en el sistema.
Lista de favoritos	Incluye contactos seleccionados por el usuario del directorio personal e interno. Las extensiones internas con teléfono del sistema se muestran también con el estado de presencia. Para mostrar el estado de presencia de una extensión es necesario que el usuario en cuestión lo autorice.	
Directorio del sistema	Incluye todos los números de marcación abreviada central.	

Nota: Si es posible, introduzca los números de teléfono en los directorios siempre con el formato canónico.

Nota: Al añadir o eliminar un contacto UC, pueden pasar varios minutos (**y** hasta 30') hasta que los cambios se apliquen en todos los clientes y dispositivos, debido a los mecanismos de almacenamiento en caché que se utilizan. También se

puede reiniciar el sistema para que los cambios surtan efecto **inmediatamente**.

12.5.1.1 Cómo configurar directorios para teléfonos de sistema

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Puede seleccionar qué directorios están disponibles en los teléfonos de sistema con display.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema** > **Display**.
4) En la lista desplegable **Listín**, seleccione una de estas opciones:
   - Si desea habilitar los contactos personales, los directorios interno, externo y de red, y el directorio de LDAP, seleccione **Todo**.
   - Si solamente desea habilitar los contactos personales y los directorios interno, externo y de red, seleccione **Interno**.
   - Si solo desea que esté disponible el directorio offline externo, seleccione **LDAP**.
   - Si no desea que esté disponible ningún directorio, seleccione **No**.

   Nota: El usuario puede activar las solicitudes de búsqueda que se gestionarán como solicitudes para el Directorio Unificado, seleccionando **Agenda interna mediante Directorio Unificado**. Si el flag está desactivado y no hay acceso al Directorio Unificado, no estará disponible la vista de lista del menú de agenda, implementado para OpenScape Desk Phone CP 200/205/210.
5) Haga clic en **Aplicar**.

Pasos siguientes

Si ha seleccionado **Todos** o **LDAP**, asegúrese de que hay disponible un directorio LDAP (p. ej. Open Directory Service) para los teléfonos del sistema.

12.5.2 Directorio interno

El directorio interno incluye los datos de contacto de las extensiones internas y de los grupos MULAP del sistema de comunicación. Los clientes de UC Smart pueden acceder al directorio interno.

En calidad de administrador tiene acceso ilimitado a todos los datos del directorio interno. En calidad de usuario puede marcar desde el directorio interno.

El parámetro de extensión **Registro del listín telefónico** (configurable en la Gestión basada en Web (WBM) mediante los asistentes de extensión) determina si se mostrarán grupos y extensiones internos en el directorio interno.

En la interred, el directorio interno se puede utilizar entre nodos.

Conceptos relacionados

Llamada de grupo en la página 699

12.5.2.1 Cómo activar o desactivar la indicación de una extensión en el directorio interno

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el grupo de menús, bajo **Extensiones** > **Extensión** > **…**, navegue hasta la extensión deseada (Índice - N.º de llamada - Nombre).
4) Haga clic en la pestaña **Editar flags exten.**
5) Elija una de estas opciones:
   - Si desea mostrar el nombre de la extensión en el directorio interno, active la casilla de verificación **Registro del listín telefónico**.
   - Si no desea mostrar el nombre de la extensión en el directorio interno, desactive la casilla de verificación **Registro del listín telefónico**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

12.5.3 Lista de favoritos

La lista de favoritos incluye los contactos seleccionados por el usuario de su directorio interno y personal. Los clientes de UC Smart pueden acceder a la lista de favoritos.

Los usuarios UC Smart pueden llamar a los contactos directamente desde la lista de favoritos. Si una extensión interna recibe una llamada, se indica en el estado de llamada. El usuario UC Smart puede capturar esta llamada. Se muestra además el estado de presencia de las extensiones internas.

12.5.4 Listín del sistema

El listín del sistema incluye todos los números de marcación abreviada centrales (siempre que tengan un nombre asignado). Los clientes de UC Smart pueden acceder al listín del sistema.

El administrador puede desactivar la indicación de cada extensión o de cada número de marcación abreviada con nombre por separado.

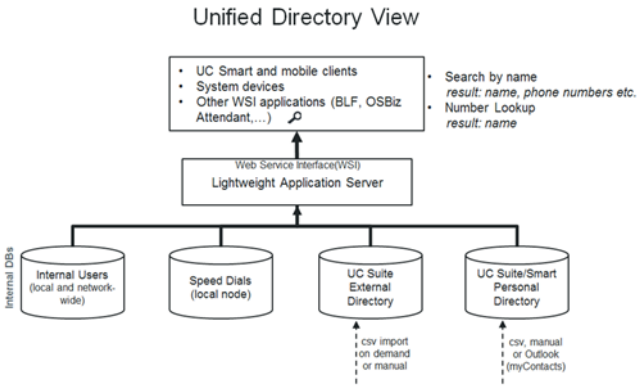
12.5.5 Directorio Unificado

OpenScape Business proporciona diferentes fuentes de datos para guardar y recuperar datos relacionados con usuarios y contactos, desde los datos de usuario interno de la configuración de usuario interno o la lista de marcación abreviada interna, hasta los diferentes directorios de las aplicaciones de UC.

Cada fuente de datos de OpenScape Business se utiliza desde una aplicación de cliente determinada localizada en el propio software del sistema de los dispositivos de teléfono o en una aplicación cliente de UC. Los datos recuperados y su presentación dependen de las fuentes de datos y de los clientes en uso.

El servicio "Directorio Unificado" de OpenScape Business incluye las fuentes de datos OpenScape Business actuales para las funciones de búsqueda común y de resolución de nombres. Proporciona los mismos resultados de búsqueda o información de resolución de nombres a todos los dispositivos de sistema y clientes OpenScape Business.

Se puede acceder al servicio Directorio Unificado a través de la interfaz de WebServices (WSI) desde clientes ubicados externamente como myPortal to go o internamente a través de mecanismos de procesamiento de llamadas (por ejemplo, desde teléfonos OpenStage).



Directorio Unificado utiliza las bases de datos internas y los directorios de OpenScape Business siguientes:

- Directorio de usuario interno (a nivel de red)
- Listas de marcación abreviada
- Directorio personal de UC Smart (opcional)
- UC SuiteDirectorio externo) (opcional)
- Contactos personales de Outlook (si se han importado mediante myContacts)

El servicio Directorio Unificado está disponible en todos los sistemas OpenScape Business a partir de la versión V2R2. No tiene requisitos concretos de licencia, hardware o software.

Para obtener unos resultados idóneos al utilizar el Directorio Unificado, se deben seguir algunas reglas relativas a formatos de números de teléfono y escritura de nombres.

12.5.5.1 Prestaciones

Clientes/Dispositivos compatibles

El servicio de Directorio Unificado proporciona:

- Búsqueda de directorio en varias fuentes de datos internas de OpenScape Business
- Presentación unificada de los resultados de la búsqueda para todos los clientes compatibles
- Búsqueda de número de teléfono/Resolución de nombres en varias fuentes de datos internas
- Presentación unificada de los resultados de resolución de nombres para todos los clientes compatibles
- Acceso a datos externos mediante la interfaz de WebServices (WSI)

Las prestaciones están disponibles para los sistemas de nodo único, tal y como se detalla a continuación. En redes OpenScape Business, la disponibilidad de las prestaciones depende principalmente del tipo de conexión de las líneas, los dispositivos y los clientes de la red.

Directorio Unificado es compatible con los clientes/dispositivos de sistema de Unify siguientes con las interfaces indicadas:

Dispositivo/Cliente	Protocolo/Interfaz en uso	Observaciones
Teléfonos OpenStage	Procesamiento de llamadas/Protocolo CorNet	WSI / HTTP(S) es opcional en OpenStage 60/80 para las imágenes de llamante
OpenScape Deskphone IP	Procesamiento de llamadas/Protocolo CorNet	WSI / HTTP(S) es opcional en DeskPhone IP 55 para las imágenes de llamante
Dispositivos inalámbricos (CMI)	Procesamiento de llamadas/Protocolo CMI	
CP 100/110 /200/205/210/ 405	Procesamiento de llamadas/Protocolo CorNet	
DeskPhone CP400/ 600/600E/ 700/700X/710	WSI / HTTP(S)	
myPortal @work	WSI / HTTP(S)	
myPortal to go	WSI / HTTPS	
OpenScape Business Attendant / BLF	Procesamiento de llamadas/Protocolo CorNet	WSI / HTTP(S) es opcional

Nota: Los clientes myPortal, myAttendant y myAgent de UC Suite utilizan sus mecanismos propios para la resolución de nombres y la búsqueda de directorio.

Función de búsqueda

La búsqueda de Directorio Unificado siempre se realiza con la interfaz de usuario del cliente o dispositivo en cuestión. Los criterios de búsqueda y el conjunto de caracteres utilizado podrían estar restringidos, en función de los clientes en uso.

Después de introducir el criterio de búsqueda, la búsqueda se realiza en directorios posteriores

- Directorio de usuario interno (a nivel de red)
- Listas de marcación abreviada
- Directorio personal de UC Smart (opcional)
- UC SuiteDirectorio externo) (opcional)
- Contactos personales de Outlook (si se han importado mediante myContacts)

Todas las coincidencias que se encuentren en los directorios anteriores aparecen como resultados de búsqueda junto con su origen. Las coincidencias incluyen el conjunto de datos completo del contacto o algunas partes. El volumen de información de los resultados depende de la fuente de los datos.

Nota: La búsqueda de nombres de grupo en myportal @work no se admite en el modo UC Suite. Solo se admite la búsqueda de usuarios con licencia (licencia básica) y grupos MULAP con licencia (entradas UC).

Las coincidencias se presentan en los dispositivos o los clientes, en función de las capacidades de visualización.

	Directorio de usuario interno	**Marcaciones abreviadas**	**Directorio Personal UC Smart**	**Directorio externo de UC Suite**	**Contactos Outlook personales (a través de my Contacts)**
Apellidos	X	---	X	X	X
Nombre	X	---	X	X	X
Nombre para mostrar/ abreviado	X	X	---	---	---
№ teléfono oficina	---	---	X	X	X
Privado/ ext. N.° de teléfono	---	---	X	---	X

	Directorio de usuario interno	Marcaciones abreviadas	Directorio Personal UC Smart	Directorio externo de UC Suite	Contactos Outlook personales (a través de my Contacts)
Núm. teléfono móvil	---	---	X	X	X
Dirección de correo electrónico	---	---	X	X	X
Nombre de compañía	---	---	X	X	X
Ciudad	---	---	---	---	---
Imagen de contacto	---	---	X	---	X
Vista previa de imagen de contacto	---	---	X	---	X

Búsqueda de número de teléfono

La búsqueda de número de teléfono de Directorio Unificado resuelve el llamante transferido (CLI) buscando el número en todas las fuentes de datos internas admitidas. La búsqueda se realiza en los siguientes campos de número de teléfono:

- Número de oficina
- Número de móvil
- Número privado

La búsqueda de número de teléfono se activa cuando se producen llamadas entrantes o salientes en general; las prestaciones específicas de desvío y encaminamiento se toman en consideración de forma adicional.

Para obtener el resultado lo más rápido posible, se implementa una priorización fija de las fuentes de datos que se utilizan para la búsqueda de número de teléfono. El resultado solo incluye el apellido, el nombre, el nombre para mostrar o, si está disponible, los datos de contacto relacionado completos.

Tabla 5: Fuentes de datos compatibles y prioridades

Prioridad	Fuentes de datos	Observación
1	Nombre CO/ITSP (como lo haya enviado el proveedor)	Previamente se debe activar el flag "Nombre en CO".
2	Lista de marcación abreviada	
3	Contactos personales	
4	Detalle de usuario de UC	

Los datos recuperados se presentan en el dispositivo del usuario y/o en el cliente de UC. El volumen de información depende de las capacidades de visualización.

- **Llamadas entrantes**

  Escenario compatible para sistemas de nodo único:

  – Basic Call
  – Llamada de grupo/Llamada MULAP
  – Timbre adicional
  – Transferencia de llamada de un solo paso (SSCT)
  – Transferencia por consulta/de consulta/asistida
  – Desvío de llamada directo (CFU = Call Forwarding Unconditional)
  – Desvío de llamada diferido (CFNR = Call Forwarding No Reply)
  – Desvío de llamada en caso de ocupado (CFB = Call Forwarding Busy)
  – Transferencia ciega
  – Telecaptura de llamadas

  Nota: Captura de llamada es diferente de Grupo de telecaptura. En Grupo de telecaptura, si un número externo se guarda en el Directorio Unificado, el nombre del llamante no se muestra en los miembros del grupo.

  El escenario compatible para entornos de varios nodos (red) es una llamada de gateway.
- **Llamada saliente**

  En el caso de una llamada saliente, la búsqueda del número de teléfono del interlocutor llamado se realiza solo una vez.

  El escenario admitido para sistemas de nodo único es una llamada básica a un número externo.

La forma en que se presente el resultado de la búsqueda de número de teléfono depende de las capacidades de visualización de los teléfonos.

12.5.5.2 Reglas y convenciones

Se deberán seguir las mismas convenciones de formato de nombre y de número para obtener unos resultados óptimos al usar el servicio de Directorio Unificado.

Formato de números admitido

Todos los números de teléfono externos de las fuentes de datos se deben introducir en formato canónico, incluidos el prefijo de país y el código de red; p. ej., +4989700712345.

La lista de marcación abreviada admite solo el formato de marcación del sistema; p. ej., 0089700712345 o 0004989700712345.

Cuando los números de marcación abreviada se configuren para estar accesibles a través de LDAP, deberá activar la opción Conversión de número para que se muestra el nombre del contacto cuando el número esté en formato canónico. Para obtener más información sobre cómo activar la opción

Conversión de número, véase Cómo añadir una fuente de datos externa para Open Directory Service en la página 1209.

Formatos de nombre admitidos

Se deberán seguir las siguientes convenciones de formato de nombres y juego de caracteres:

- **Formato de nombre de marcación abreviada**

  La búsqueda de nombre en la lista de marcación abreviada solo se admite con determinadas reglas de configuración. Los nombres y los apellidos se deben introducir en el campo de nombre existente con el siguiente patrón:

  <Apellido>, <Nombre> (separados por comas)
- **Usuarios internos en caso de migraciones**

  La migración a V2R1 y siguientes con usuarios internos que no atiendas a estas reglas de configuración no se realizará según lo previsto. Esto significa que el administrador deberá convertir los nombres internos al siguiente patrón antes de efectuar la migración:

  <Apellido>, <Nombre> (separados por comas)

Disponibilidad de los cambios de directorio

Después de crear, actualizar o eliminar contactos en las distintas fuentes de datos, podría llevar hasta 10 minutos que todos los cambios aparezcan en los resultados de búsqueda de número de teléfono.

12.5.5.3 Capítulo 11.5.5.3 Límites funcionales

Los siguientes límites funcionales no se aplican a Directorios Unificados:

Búsqueda por nombre

- Compatibilidad para nombre de grupo

  Los nombres de grupo (no los nombres MULAP) no se pueden buscar en todo tipo de configuraciones
- Compatibilidad de caracteres especiales

  En la mayoría de los dispositivos telefónicos, el usuario puede buscar caracteres estándar “a-z”. Los caracteres especiales (diacríticos), como los caracteres españoles “Áá, Ée, Íi, Óó, Úú, Üü y ñÑ” no están disponibles a través de la interfaz de usuario del teléfono.

  Por lo tanto, un resultado de búsqueda de caracteres comunes incluye también caracteres especiales. Una búsqueda de cualquiera de los caracteres “acdegilnorstuyz” también encuentra los caracteres especiales correspondientes “àáâãåä ąăäçćčďđ èéêë ęě# ìíîï ĺľł ñ ńň òóô ő õö řŕšßşť ùúû ůűüý ÿžý źž½ź”

  en el resultado de la búsqueda.

Nota: La búsqueda en la guía telefónica con el carácter comodín al principio de la cadena de búsqueda, por ejemplo, <*jo*>, solo se admite para usuarios internos.

- Compatibilidad del formato de nombre de marcación abreviada

  La búsqueda de nombre en la lista de marcación abreviada solo se admite con determinadas reglas de configuración. Los nombres y los apellidos se deben introducir en el campo de nombre existente con uno de los patrones siguientes

  – <Apellido>, <Nombre> (separados por comas)
  – <Nombre> <Apellido> (en este caso, separador de espacio)

Presentación del nombre

Los contactos personales de UC Smart y del directorio offline externo, en los que el nombre y el apellido superen en conjunto los 24 caracteres, se truncarán hasta los 24 caracteres, para adaptarse a la longitud de visualización de los dispositivos.

Búsqueda de número de teléfono

La prestación Búsqueda de número de teléfono (nombre de contacto recuperado del número de llamante) no se admite en el Directorio Unificado con dispositivos SIP y S0.

12.5.5.4 Directorio Unificado en sistemas interconectados

El servicio Directorio Unificado está activo en todos los nodos de una red OpenScape Business y utiliza las fuentes de datos del sistema propio. El cliente y los dispositivos de teléfono siempre utilizan el servicio Directorio Unificado en su propio nodo.

Por tanto, dependerá del tipo de contenido de fuente de datos si hay disponibles contactos a nivel de red.

Tabla 6: Fuente de datos local y a nivel de red

Fuente de datos	Datos locales	Datos a nivel de red
Directorio de usuario interno	X	X
Listas de marcación abreviada	X	---
Directorio personal de UC Smart	X	---
Directorio personal de UC Smart	X	---
Contactos personales de Outlook (mediante myContacts)	X	---

Búsqueda de número de teléfono

En escenarios de interconexión no se utiliza la funcionalidad Búsqueda de número de teléfono. En esos escenarios, el nombre de transmite a través de mecanismos de interconexión normales entre los nodos de red.

Con los usuarios internos, se utiliza el Nombre para mostrar configurado, por lo que no se necesita la búsqueda.

12.5.6 Diario

El diario es la lista de todas las llamadas entrantes y salientes de una extensión. El usuario permite acceder rápida y fácilmente a los contactos de las extensiones, llamarles fácilmente o responder a las llamadas perdidas.

El usuario UC Smart puede visualizar como máx. las 100 últimas llamadas.

Carpetas para tipos de llamada

Las llamadas pueden reunirse en los siguientes grupos:

- **Pendientes**
- **Perdidas**
- **Contestadas**
- **Todas las llamadas**

Detalles de llamada

Cada llamada se muestra con la fecha y hora correspondientes y, si está disponible la información, con el número de teléfono. Si un directorio contiene más información sobre un número de teléfono (por ejemplo, **Apellidos** y **Nombre**), aparece también indicada. Se muestra además la **Ruta** de la llamada y la **Duración** así como desvíos y capturas realizados.

12.6 Llamadas

Para las llamadas es especialmente importante el formato de números de teléfono.

12.6.1 Formatos de números de teléfono

Para introducir números de teléfono se pueden utilizar distintos formatos.

Formato	Descripción	Ejemplo
canónico	Comienza por + e incluye siempre el código de país, el código local y el número de teléfono completo. Se admiten espacios en blanco y los caracteres especiales + ( ) / - : ;.	+49 (89) 7007-98765

Formato	Descripción	Ejemplo
marcación	Exactamente como marcaría el número en el teléfono del sistema en la oficina, siempre con código de línea urbana.	• 321 (interno) • 0700798765 (red local propia) • 0089700798765 (red local no propia) • 0004989700798765 (extranjero)

Consejo: Siempre que sea posible, utilice el formato de números de teléfono canónico. De esta forma, los números de teléfono serán siempre únicos, completos y consistentes para la interconexión y las extensiones móviles.

Al marcar de forma manual (formato de marcación) un número de teléfono externo, se debe marcar también el código de acceso a línea urbana.

Al marcar un número de teléfono externo en formato de marcación desde un directorio (y, con ciertos clientes de UC, con la marcación de escritorio y con la marcación clipboard), el sistema de comunicación completa automáticamente el código de acceso a línea urbana (ruta 1).

Nota: Al llamar dentro de los EE.UU. mediante CSTA a un número de teléfono en formato canónico, el número de teléfono se convierte a formato de marcación.

12.6.2 Requisitos previos para recibir llamadas a través de VoIP en myPortal to go para usar CallKit en su iPhone

Las notificaciones de llamadas a través de VOIP de iOS se basan en el mecanismo APNS de Apple.

Este servicio requiere lo siguiente:

- Un servidor DNS configurado que resuelva nombres de dominio público de Internet.
- Acceso a Internet para el sistema OpenScape Business (puerto TCP/443 saliente) para enviar notificaciones de llamadas APNS.
- El software del sistema debe estar actualizado con la última versión superior/inferior/corregida publicada. La última versión del sistema es importante porque el servicio APNS requiere certificados específicos que caducan cuando se ejecuta un software de sistema más antiguo.

12.7 Conferencias

En una conferencia varios usuarios (también externos) pueden comunicarse entre sí al mismo tiempo. La función de gestión de conferencias permite alojar o planificar de antemano conferencias, de forma rápida y sencilla.

Conferencias controladas por teléfono o por aplicación

En calidad de participante, puede iniciar conferencias mediante el teléfono o mediante las aplicaciones UC Smart.

Puede iniciar una conferencia controlada por teléfono de las siguientes formas y, a continuación, controlarla en su teléfono:

- Llame a los participantes que quiera y conéctelos con la conferencia
- Amplíe una llamada de consulta para una conferencia
- Amplíe una segunda llamada para una conferencia

Las conferencias controladas por aplicación se pueden iniciar, controlar y administrar mediante la gestión de conferencia. Para utilizar la gestión de conferencias se requiere una licencia de conferencia.

Diferencias entre tipos de conferencias:

	Conferencia controlada por teléfono	**Conferencia controlada por aplicación**
Dirección del establecimiento de conexión desde el sistema	• Saliente	• Entrante (acceso telefónico por el participante)
Autenticación de los participantes de la conferencia	-	• PIN personal (ID de conferencia) • PIN de invitado (opcional)
Invitación predefinida a los participantes de la conferencia	-	• Nombre de conferencia • Número de acceso telefónico (MeetMe) • PIN personal (ID de conferencia) • PIN de invitado (opcional)
Cantidad máx. de participantes por conferencia	8	16

Conferencia programada

Las conferencias programadas se crean como conferencias permanentes. La conferencia se puede utilizar según se requiera, en cualquier momento, sin planificación extra. Las conferencias programadas no ocupan canales de conferencia mientras no acceda a ellas ningún participante. El orden de acceso determina la asignación de los canales de conferencia.

Durante la configuración inicial, los administradores pueden modificar el número de acceso telefónico predefinido (MeetMe) para conferencias mediante la Gestión basada en Web (WBM). Los participantes pueden ver el número de acceso telefónico que pueden usar para unirse a la conferencia. Después de usarlo, tendrán que autenticarse con su PIN personal o, si se permite, con un PIN de invitado general.

Moderadores

La persona que inicia una conferencia se convierte automáticamente en moderador y puede hacer lo siguiente:

- Crear, editar y borrar conferencias programadas.
- Agregar y eliminar participantes.

  Los participantes eliminados no permanecen en la conferencia.

- Desconectar a los participantes de conferencia.

  Los participantes desconectados pueden acceder de nuevo a la conferencia.
- Definir a otro participante interno del mismo nodo como moderador.
- Abandonar la conferencia sin finalizarla inmediatamente.

  Si el último moderador abandona la conferencia, esta finaliza al cabo de 5 minutos.
- Finalizar conferencias activas.
- Iniciar una sesión de Web Collaboration en una conferencia activa.
- Enviar invitaciones predefinidas a todos los participantes de la conferencia o a cada participante por separado.

Todos los participantes internos de un nodo pueden ser moderadores. Pero para ello se requiere una licencia de conferencia.

Los participantes de conferencia cuyos datos de contacto se hayan introducido manualmente, se consideran participantes externos y no se pueden definir como moderadores.

Participantes de conferencia

Los participantes de una conferencia pueden salir de ella y regresar de nuevo mediante acceso telefónico. Además, pueden participar en una sesión de Web Collaboration que ya esté iniciada. Mientras solo haya un participante en la conferencia, este oirá la música de espera. El número máximo de participantes externos está limitado, entre otros factores, por el número de líneas urbanas disponibles.

Finalización automática sin moderador

Si el último moderador abandona la conferencia, un mensaje de texto notifica a los participantes que la conferencia finalizará al cabo de 5 minutos.

Notificación a los participantes de conferencia

El moderador puede enviar una invitación por correo electrónico a todos los participantes de la conferencia o a cada uno de ellos por separado. Para ello se requiere que haya instalado un programa de correo electrónico en el PC de cliente. Las direcciones de correo electrónico conocidas se añaden automáticamente a la lista de distribución. Si se envía una invitación a todos los participantes, solo se incluye el PIN de invitado general (si se permite); si las invitaciones son individuales, se envía además el PIN personal.

Como alternativa, se puede copiar en el portapapeles un texto de invitación predefinido, que se podrá utilizar en otros programas (por ejemplo, en un chat).

12.8 Web Collaboration

myPortal admite la integración del producto independiente Web Collaboration durante llamadas telefónicas y conferencias, para la colaboración simultánea y multimedia. Este producto permite acceder rápidamente a funciones como publicación de aplicaciones y de uso de escritorio, publicación de archivos, navegación simultánea, whiteboarding, push de URL, y chat de IM o de vídeo con varios participantes.

Un usuario puede iniciar Web Collaboration durante una llamada en la ventana de llamada del cliente de PC de UC; también puede iniciarla el moderador

de una conferencia activa. Se abre una página web donde se puede iniciar la descarga del cliente de Web Collaboration. Los participantes de la conferencia no necesitan hacer una instalación local de Web Collaboration. Si en el cliente de PC de UC hay un programa de correo electrónico, se puede enviar a los interlocutores un correo electrónico con un enlace al cliente de Web Collaboration. Encontrará información sobre Web Collaboration en la documentación del producto Web Collaboration.

Al borrar o finalizar una conferencia, se borra automáticamente la sesión de Web Collaboration correspondiente.

Integración de Web Collaboration

Para la integración de Web Collaboration, el administrador debe introducir en la Gestión basada en Web (WBM) el número de licencia y la contraseña de la conexión de Web Collaboration alojada. El fabricante ofrece el servidor de Web Collaboration en Internet como servicio (Pubic Server). Mediante una conexión segura https se transmiten el número de licencia y la contraseña. De forma predeterminada se utiliza el puerto TCP 5100. No se admiten los servidores locales de Web Collaboration.

Nota: Para el uso de Web Collaboration, los clientes de PC de UC y el sistema de comunicación requieren una conexión a Internet. El sistema de comunicación no admite conexiones mediante proxy.

Mensajería instantánea y Web Collaboration

Las funciones de Instant Messaging (mensajería instantánea) del sistema y de Web Collaboration (colaboración web) son independientes entre sí: los mensajes instantáneos de un cliente de PC de UC no aparecen en una sesión de Web Collaboration del mismo participante, y a la inversa.

12.8.1 Cómo configurar la conexión con el servidor de Web Collaboration (Public Server)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Hay disponible un acceso a Internet.

Para una conexión protegida con el servidor de Web Collaboration (Public Server) se requiere un número de licencia y una contraseña.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **Web Services**.
3) En el grupo de menús, desplácese a **Web Services** > **Web Collaboration**.
4) Active el campo de opción **Public Server**.
5) En el campo **Número de licencia** introduzca el número de licencia para la conexión con el servidor de Web Collaboration (Public Server).

6) En el campo **Contraseña** introduzca la contraseña para la conexión protegida con el servidor de Web Collaboration (Public Server).

Nota: Si desea probar Web Collaboration durante 5 minutos, puede activar el campo de opción **Public Server (Demo Mode/Evaluation Mode)**. Para ello no requiere número de licencia ni contraseña.

---

7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

12.8.2 Cómo desactivar la conexión con el servidor de Web Collaboration

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **Web Services**.
3) En el grupo de menús, desplácese a **Web Services** > **Web Collaboration**.
4) Active el campo de opción **Ningún servidor de Web Collaboration**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**. La opción para iniciar una sesión de Web Collaboration está desactivada en los clientes de Unified Communications.

12.9 Mensajería instantánea

Mensajería instantánea ("Instant Messaging") es la comunicación mediante mensajes instantáneos (Chat).

12.9.1 Mensajería instantánea

Con los mensajes instantáneos puede chatear con otros usuarios de UC Smart.

Los mensajes instantáneos enviados y recibidos se muestran a ambos interlocutores en forma de diálogo. Al seleccionar un destinatario, el cliente indica si en ese momento el interlocutor está conectado. Si el interlocutor está fuera de línea, no se le pueden enviar mensajes instantáneos. La página de resumen de los mensajes instantáneos muestra los últimos hilos. El sistema guarda un número limitado de mensajes instantáneos. Se muestran como máximo los 100 últimos mensajes instantáneos de un usuario.

12.10 Buzón de voz (SmartVM)

El buzón de voz (también denominado SmartVM) reproduce a los llamantes un saludo y les da la posibilidad de dejar un mensaje o de ser transferidos. Los usuarios internos pueden acceder al buzón de voz a través de un teléfono

con el cliente de UC Smart. Los usuarios que deseen utilizar un buzón de voz necesitan una licencia VoiceMail.

Tipos de buzón de voz

Estos son los tipos de buzón de voz:

- Buzón estándar:

  El buzón estándar es el buzón de voz personal de una extensión. Acepta la llamada, saluda al llamante con un anuncio grabado personal o un anuncio grabado estándar y le da posibilidad de dejar un mensaje. El usuario configura el buzón estándar a través del teléfono o a través del clientes de UC Smart (p.ej. grabando un saludo personalizado).
- Buzón de grupo:

  El buzón de grupo tiene las mismas características que el buzón estándar, con la diferencia de que no está asignado a un único usuario si no a un grupo de usuarios. Solo se pueden grabar mensajes para un buzón de grupo si al menos uno de los miembros del grupo tiene una licencia VoiceMail. La información del buzón de voz se muestra a todos los miembros del grupo con licencia VoiceMail. Los mensajes se pueden escuchar a través del menú telefónico del buzón de voz personal de los miembros del grupo.
- Buzón de puesto de operadora (AutoAttendant / Company AutoAttendant):

  El buzón de puesto de operadora da a los llamantes un saludo, con o sin opción de conmutación. Una forma especial de buzón de puesto de operadora es el Company AutoAttendant. Este buzón permite transferir a los llamantes automáticamente (p.ej. al puesto e operadora) o los transfiere a una extensión (p.ej. al departamento de atención al cliente o a la línea de ayuda) mediante la marcación de un número de teléfono interno o de un número de marcación abreviada (dígitos 0-9). Naturalmente, deberá emitirse el correspondiente anuncio que informe de las posibilidades de marcación. Además se pueden configurar un destino de interceptación, al que el llamante será transferido si no pulsa ningún número o pulsa un número equivocado (que no esté ocupado). El administrador puede configurar hasta 100 buzones de puesto de operadora.
- Buzón de anuncio grabado:

  Al asignar un índice de anuncio grabado a un puerto de anuncios grabados y configurar un buzón de voz con el número de teléfono del puerto de anuncios grabado, se configura la función de anuncio grabado. Como anuncio grabado se utiliza el saludo del buzón de voz. La reproducción puede hacerse una vez (anuncio grabado) o de forma cíclica (música), según el tipo de anuncio grabado configurado. El menú telefónico de un buzón de anuncio grabado solo se puede utilizar desde otro teléfono, ya que no hay teléfono propio. Por ello, para el buzón de anuncio grabado hay que utilizar otro PIN que para el buzón de voz del teléfono utilizado.
- Buzón del sistema:

  Como buzón del sistema se utiliza el buzón de voz con el número de teléfono de la línea colectiva del SmartVM. El buzón del sistema debe ser un buzón estándar (no un AutoAttendant) que tenga activada la grabación de voz. La información del buzón de voz se muestra al dueño del buzón con el índice 1 y también se puede consultar ahí. El primer buzón de voz no debe ser un buzón de grupo, un buzón de puesto de operadora ni un buzón de anuncio grabado. Si no se va a utilizar el buzón del sistema, no hay que

configurar un buzón de voz con el número de teléfono de la línea colectiva del SmartVM.

Funciones del buzón de voz

- Consulta y control por teléfono

  (Externamente: se requiere un número de teléfono propio)
- Selección manual o automática de diferentes saludos
- Menú telefónico (Telephone User Interface, TUI) con estructura de menús conmutable a nivel de sistema:
  - Menú del teléfono, UC Smart: **SmartVM** (similar a EVM)
  - Menú del teléfono, UC Suite: **OSO** (similar a UC Suite)
- Se pueden configurar hasta 320 buzones de voz por sistema
- Hasta 32 horas de capacidad de grabación de voz por sistema
- Hasta 100 mensajes memorizados por buzón de voz
- Hasta 2 min de grabación de mensaje de voz por buzón de voz
- Hasta 10 procesos de respuesta o de conmutación simultáneos posibles
- Anuncio grabado/inserción de música antes de contestar
- Reproducción de anuncios grabados individuales
- Transferencia de llamadas de fax mediante detección automática de tono de fax a un destino de fax previamente configurado

---

Nota: Puede consultar información sobre el menú telefónico en las dos instrucciones de uso breves UC Smart Telephone User Interface (TUI) y UC Suite Telephone User Interface (TUI).

Configuración de número de código

Antes de utilizar por primera vez el buzón de voz, los usuarios deben modificar el número de código preestablecido (valor predeterminado: `123456`).

El número de código consta de una serie de seis dígitos. No puede constar de dígitos repetidos (p.ej. `333333`) ni de una secuencia de números ascendente o descendente (p.ej. `987654`). Si se introduce un número de código erróneo seis veces, se bloquea el acceso al buzón de voz correspondiente hasta que el administrador restablezca la contraseña. Si se introduce una contraseña errónea dos veces en el menú telefónico, se desconecta la conexión.

Puertos

El buzón de voz utiliza los puertos S_0 500-509 con los números de teléfono asignados correspondientes 739-748. Los puertos 504 y 505 están asignados de forma predeterminada al Company AutoAttendant (número de teléfono 352), los demás 8 puertos, a la línea colectiva del buzón de voz (número de teléfono 351). El número de teléfono 351 es el número de teléfono general del buzón de voz con el que se puede acceder al menú telefónico.

Acceso a la red urbana

Por motivos de seguridad, los puertos del buzón de voz solo tienen acceso indirecto a la red urbana de forma predeterminada. Estas prestaciones requieren la asignación de un grupo de clase de servicio con acceso a la red urbana:

- Cómo llamar al remitente de un mensaje de voz

- Escucha de mensajes de voz de usuarios Mobility mediante devolución de llamada
- Transferencia a destino externo mediante Company AutoAttendant

Saludos/Anuncios grabados

Los saludos individuales (=anuncios grabados) se graban con un teléfono o se cargan en el sistema con la Gestión basada en Web (WBM). Al hacer la configuración con el teléfono se marca el número de teléfono del buzón de voz y siguiendo las indicaciones del buzón de voz se puede grabar un saludo nuevo mediante el teléfono.

Mediante el modo Experto, también se pueden cargar, guardar y borrar saludos en el sistema por separado para cada buzón de voz.

Nota: Para reproducir correos de voz desde números de teléfono externos (p. ej., reproducción a través de un teléfono móvil usando myPortal to go), se debe ajustar la clase de servicio de los puertos Smart VM. Se recomienda utilizar una "lista de números permitidos" para estos casos.

12.10.1 Configuración del buzón de voz (SmartVM)

La configuración del buzón de voz (SmartVM) incluye la configuración de los buzones estándares/buzones de grupo y de los buzones de puesto de operadora.

Los ajustes generales del buzón de voz (SmartVM) se realizan con el asistente **SmartVM**, por ejemplo, el ajuste del número de teléfono del buzón de voz a un plan de numeración de 4 posiciones.

Los ajustes de configuración especiales del buzón de voz (SmartVM) y la configuración de los buzones estándares/buzones de grupo y de los buzones de puesto de operadora se realizan mediante el modo Experto.

Nota: Al cambiar el número de teléfono se restablece el buzón de voz de la extensión en cuestión. Todos los mensajes de voz, saludos y anuncios grabados personales se pierden y se restablece la contraseña.

Puede cargar, guardar y borrar también saludos individuales en el SmartVM; también puede guardar y recuperar saludos y mensajes para los distintos buzones de voz o para todos. Además, se pueden consultar los idiomas cargados para la interfaz del usuario y visualizar los 10 buzones de voz con más mensajes y la memoria ocupada por mensajes y saludos.

Puede consultar la configuración de buzones de puesto de operadora en el capítulo Attendants - AutoAttendants - Company AutoAttendant (UC Smart).

Asignación del buzón a las extensiones

Si el buzón de voz (SmartVM) está configurado, se pueden asignar buzones estándares a las extensiones. Se puede realizar mediante

- una transferencia automática diferida para la extensión mediante una lista de destinos de llamada (que configura el administrador). En este caso, la

llamada se transfiere por orden a los destinos de llamada seleccionados (p.ej., primero a la extensión y, al cabo de un tiempo configurable, al buzón).

- un desvío de llamadas al teléfono de la extensión (lo puede ejecutar el propio usuario). En este caso, la llamada pasa automáticamente al buzón.

  Si la extensión es miembro de una línea colectiva y se llama a dicha línea colectiva, la llamada no se desvía al buzón de voz de la línea colectiva.

12.10.1.1 Cómo activar o desactivar el buzón de voz

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

UC Smart está activado.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Conexiones**.
3) En el grupo de menús, haga clic en **Conexiones** > **SmartVM**.
4) Haga clic en la pestaña **Editar parámetros SmartVM**.
5) Si desea desactivar el buzón de voz, active la casilla de verificación **Desactivación de EVM**.
6) Si desea activar el buzón de voz, desactive la casilla de verificación **Desactivación de EVM**.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

12.10.1.2 Cómo configurar el buzón de voz (SmartVM)

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **SmartVM**.
4) Active la casilla de verificación **Activar SmartVM**.
5) Si es necesario, modifique los ajustes generales del buzón del sistema en la columna **Buzón de voz**:
   a) Si es necesario, en el campo **Número de llamada** modifique el número de teléfono del buzón de voz (valor predeterminado: `351`), por ejemplo para adaptarlo a un plan de numeración de 4 dígitos.
   b) Si es necesario, en el campo **Marc. dir.** modifique el número de marcación directa del buzón de voz (valor predeterminado: `351`), por ejemplo para adaptarlo a un plan de numeración de 4 dígitos.
   c) Si es necesario, en el campo **Nombre** modifique el nombre del buzón de voz (valor estándar: `VOICEMAIL`).

6) Si es necesario, modifique los ajustes generales del buzón del puesto de operadora en la columna **AutoAttendant**:
   a) Si es necesario, en el campo **Número de llamada** modifique el número de teléfono del buzón de voz (valor predeterminado: `352`), por ejemplo para adaptarlo a un plan de numeración de 4 dígitos.
   b) Si es necesario, en el campo **Marc. dir.** modifique el número de marcación directa del buzón de voz (valor predeterminado: `352`), por ejemplo para adaptarlo a un plan de numeración de 4 dígitos.
   c) Si es necesario, en el campo **Nombre** modifique el nombre del buzón de voz (valor predeterminado: `AutoAttendant`).
7) Haga clic en **OK & Continuar**.
8) Si es necesario, en el campo **N° llam.** de la línea del puerto deseado, modifique el número de teléfono del puerto (valor predeterminado: `739-748`), por ejemplo para adaptarlo a un plan de numeración de 4 dígitos.
9) Si es necesario, en el campo **Nombre** de la línea del puerto deseado, modifique el nombre del puerto (valor predeterminado: `SmartVM 1-10`).
10) Si es necesario, en la lista desplegable **Tipo** de la línea del puerto deseado, modifique el tipo del puerto:
    - **Phone Mail (n.º de 5 dígitos)**: el puerto está asignado a los buzones estándar y a los buzones de puesto de operadora del tipo AutoAttendant. Los puertos de este tipo se toman automáticamente en la línea colectiva 351.
    - **Estándar**: el puerto está asignado a los buzones de puesto de operadora del tipo Company AutoAttendant y a los buzones de anuncio grabado. Los puertos de este tipo se toman automáticamente en la línea colectiva 352.
11) Si es necesario, en la lista desplegable **Modo** de la línea del puerto deseado modifique el modo del puerto:
    - **Anuncio grabado**: se reproduce una vez un saludo/anuncio grabado.
    - **Música en espera**: se reproduce un saludo, un anuncio grabado o una música en un bucle infinito.
    - **Company AutoAttendant**: después de reproducir un saludo o anuncio grabado, existe la opción de transferir la llamada.
12) Haga clic en **OK & Continuar**.
13) En la lista desplegable **Selección de buzón** seleccione el buzón deseado. A continuación aparecen campos para configurar los saludos.
14) Si desea utilizar saludos propios para el buzón seleccionado, haga clic en **Examinar**, desplácese hasta el lugar donde están guardados los archivos (formato: wave, PCM, 16 bit, 8kHz, mono) y haga clic en **Cargar**. Los saludos seleccionados se cargan en el sistema.

Nota: Una vez cargados, puede guardar y borrar los saludos.

---

15) Si desea configurar saludos para más buzones, repita los pasos 13 y 14.
16) Haga clic en **OK & Continuar**.
17) Los parámetros generales solo se deben modificar si es necesario. Puede consultar una descripción de los parámetros generales en Conexiones>SmartVM .
18) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

12.10.1.3 Cómo añadir un buzón estándar para una extensión

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

La extensión en cuestión tiene asignada una licencia Voicemail.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Conexiones**.
3) En el grupo de menús, haga clic en **Conexiones** > **SmartVM**.
4) Haga clic en la pestaña **Editar buzones SmartVM**.
5) En el campo **Nº llam. buz. voz**, introduzca el número de teléfono de la extensión para la que desea añadir el buzón.
6) En la lista desplegable **Saludo** introduzca un saludo.
7) Si desea que los llamantes puedan dejar mensajes en el buzón de voz, active la casilla de verificación **Grabación**.
8) Compruebe que la casilla de verificación **AutoAttendant** está desactivada.
9) La casilla de verificación **Reponer contraseña** no debe estar marcada al cambiar la configuración de un buzón de voz. Hace que se restablezca la contraseña del buzón de voz. Al cambiar la configuración, el usuario ya debe modificar la contraseña inicial al acceder por primera vez al buzón de voz.
10) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

12.10.1.4 Cómo modificar el grupo de clases de servicio de un puerto de buzón de voz

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

UC Smart ha sido activado.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) Haga clic en **Servidor de telefonía** > **Clases de servicio** en el árbol de navegación.
3) Haga clic en el árbol del menú en **Clases de servicio** > **Estación** > **EVM** y luego en el puerto del buzón de voz deseado.
4) Seleccione los grupos COS deseados para el servicio diurno y nocturno en la pestaña **Editar grupo COS** pestaña del **Clase de servicio Día del grupo** y las listas desplegables **Clase de Servicio Noche Grupal**, respectivamente.
5) Haga clic en **Aplicar**, seguido de **Aceptar**.

Nota: Los textos del puerto EVM se generan según el Asistente de **configuración básica** > **Código de país del sistema**.

12.10.1.5 Cómo modificar la estructura del menú telefónico del buzón de voz

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

UC Smart está activado.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) Haga clic en **Telefonía** > **Equipo auxiliar** en el árbol de navegación.
3) Haga clic en **Equipo auxiliar** > **SmartVM** en el árbol del menú.
4) Haga clic en la pestaña **Editar parámetros de SmartVM**.
5) Si desea que la estructura del menú del teléfono sea similar a OpenScape Office, seleccione la entrada **OSO** en la lista desplegable **Interfaz de usuario del teléfono**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

12.10.1.6 Cómo cargar, guardar y borrar saludos sueltos

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

UC Smart está activado.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Configuración**.
3) En el grupo de menús, haga clic en **Configuración** > **Configuración de SmartVM** > **Operaciones en archivo**.
4) Haga clic en la pestaña **Datos de anuncios grabados**.
5) En la lista desplegable **Selección de buzón**, seleccione el buzón de voz deseado.
6) Si desea cargar un saludo que haya grabado previamente o un archivo Wave en el SmartVM, en el saludo deseado haga clic en **Examinar** y desplácese hasta el lugar donde está guardado el saludo. A continuación, haga clic en **Cargar**.

   Nota: El archivo Wave de carga debe tener el siguiente formato: PCM, 16 bits, 8 kHz, monoaural. Al realizar la carga, el archivo wave se convierte. Esto puede tardar bastante, dependiendo del tamaño del archivo wave.

7) Si desea guardar un saludo existente, en el saludo deseado haga clic en **Guardar** y guarde el archivo vma en el lugar que desee.
8) Si desea borrar un saludo existente, en el saludo deseado haga clic en **Borrar** y confirme la acción con **Aceptar**.

12.10.1.7 Cómo guardar y recuperar saludos y mensajes

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

UC Smart está activado.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Mantenimiento** > **Configuración**.

3) En el grupo de menús, haga clic en **Configuración** > **Configuración de SmartVM** > **Operaciones en archivo**.

4) Si desea hacer una copia de seguridad de saludos y mensajes:

a) Haga clic en la pestaña **Copia de seguridad**.

b) Active la casilla de verificación **Mensajes**, si además de los saludos también desea hacer una copia de seguridad de los mensajes.

c) Incluya los buzones de voz de los que desee hacer una copia de seguridad desde la lista **Buzones disponibles** en la lista **Buzones para copia de seguridad**.

d) Haga clic en **Aplicar**. Los saludos (y los mensajes, si el flag **Mensajes** está activado) de los buzones de voz para copia de seguridad se guardan en un archivo de copia de seguridad (*.tar). Guarde el archivo en el lugar que usted elija.

5) Si desea restaurar saludos y mensajes:

a) Haga clic en la pestaña **Restaurar**.

b) Haga clic en **Examinar**, desplácese hasta el lugar de almacenamiento del archivo de seguridad (*.tar) y haga clic en **Abrir**.

c) Haga clic en **Cargar** y, a continuación, en **Aceptar**. Se muestran los buzones de voz incluidos en el archivo de copia de seguridad.

d) Incluya los buzones de voz que desee restaurar desde la lista **Buzones disponibles** en la lista **Buzones para recuperación**.

e) Active la casilla de verificación **Mensajes**, si desea restablecer los saludos y los mensajes de los buzones de voz seleccionados.

f) Si la casilla de verificación **Intercalación** está desactivada, solo se sobrescriben los saludos de los buzones de voz seleccionados que estén incluidos en los datos de copia de seguridad. Si además está activada la casilla de verificación **Mensajes** también se añaden los mensajes incluidos en los datos de copia de seguridad. Los mensajes ya existentes no se pierden.

g) Si la casilla de verificación **Intercalación** está activada, antes de la restauración se borran todos los saludos y los mensajes de los buzones de voz seleccionados del SmartVM. Si se seleccionan buzones de voz que no están incluidos en los datos de copia de seguridad, también se borran. Los saludos incluidos en los datos de seguridad se transfieren. Si además está activada la casilla de verificación **Mensajes**, también se transfieren los mensajes contenidos en los datos de copia de seguridad.

h) Haga clic en **Cargar** y, a continuación, en **Aceptar**. Los saludos y los mensajes de los buzones de voz seleccionados se restauran.

12.10.2 Servicio de notificación de nuevos mensajes

El sistema puede informar a un usuario de UC Smart por correo electrónico cuando se reciba un nuevo mensaje de voz.

Requisito para el servicio de notificaciones

- El envío de correo electrónico (transferencia de correos electrónicos) debe estar configurado en el sistema por el administrador.
- El sistema debe conocer la dirección de correo electrónico del usuario. Durante la instalación inicial, el administrador puede importar todas las direcciones de correo electrónico de la administración basada en web (WBM) mediante un archivo XML. O bien, puede registrar una dirección de correo electrónico por usuario en el UC Smart Assistant (véase Cómo configurar un usuario de UC Smart). Como alternativa, el propio usuario puede indicar su dirección de correo electrónico en su cliente de UC Smart.
- El usuario tiene asignada una licencia de buzón de voz (VoiceMail).
- La prestación **Buzón de voz a correo electrónico** está activada. El administrador puede activar la prestación para todos los usuarios en el UC Smart Assistant (Cómo activar o desactivar las notificaciones de email). Como alternativa, el propio usuario puede activar la prestación en su cliente de UC Smart.

El usuario de UC Smart recibe un correo electrónico con el mensaje de voz como archivo WAV adjunto (16 bits, mono), la fecha y hora de recepción, la duración del mensaje de voz y (si están disponibles) el número de teléfono y el nombre del remitente.

12.10.2.1 Cómo activar o desactivar las notificaciones de email

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

En **Selección de aplicación** del modo experto, la opción **Paquete con UC Smart** está activada.

La dirección de correo electrónico del usuario está registrada en sus datos de perfil.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Smart**.
3) Haga clic en **Editar** para abrir el asistente **UC Smart**.
4) En el grupo de menús, haga clic en **Administración** > **Administración de usuarios**.
5) En la lista **Usuarios**, seleccione el usuario deseado.

6) Elija una de estas opciones:
   a) Si desea activar el servicio de notificación para nuevos mensajes, en el área **Datos de perfil**, active la casilla de verificación **Buzón de voz a correo electrónico**.
   b) Si desea desactivar el servicio de notificación para nuevos mensajes, en el área **Datos de perfil**, desactive la casilla de verificación **Buzón de voz a correo electrónico**.
7) Haga clic en **Aplicar**.
8) Si desea configurar otro usuario, repita los pasos 5 a 7.

13 UC Suite

UC Suite ofrece prestaciones de Comunicaciones Unificadas como, por ejemplo, estado de presencia y CallMe, Conferencias y mensajes de voz y de fax en los clientes myPortal for Desktop y myPortal for Outlook. myAttendant ofrece además funciones de puesto de operadora.

Nota: Para los modelos de hardware OpenScape Business X3/X5/X8, la solución de Comunicaciones Unificadas UC Suite, requiere el hardware UC Booster (UC Booster Card o UC Booster Server). En OpenScape Business S (softswitch), ya está integrada la solución de Comunicaciones Unificadas UC Suite.

Nota: Después de modificar la configuración de extensiones, grupos, Mobility u otros parámetros del sistema, como códigos de acceso a línea urbana, hay que sincronizar los datos UC para UC Smart o UC Suite. La sincronización se produce cinco minutos después del último cambio de configuración. Si se modifica la configuración antes de que termine el temporizador de 5 minutos, se reinicia el reloj. Los datos UC pueden estar desactualizados hasta que comience la sincronización. Durante la sincronización, la aplicación UC y la API de Interfaz de Web Services no están disponibles; además, los clientes UC conectados pierden la conexión hasta que termina la sincronización de los datos UC. Las conexiones se restauran automáticamente cuando ha terminado la sincronización de datos UC.

13.1 Configuración básica para la UC Suite

Los ajustes básicos de la UC Suite se pueden modificar.

UC Suite se puede activar o desactivar. Si se utiliza la UC Suite, hay que desactivar UC Smart.

Además, en todas las llamadas de UC iniciadas por el sistema (p.ej. mediante el servicio CallMe), antes de marcar se puede comprobar si el usuario de UC que solicita la llamada tiene autorización para ello. Si el usuario UC no está autorizado, no se realiza la llamada.

Nota: Si se utilizan aplicaciones CSTA, se debe establecer el parámetro de código para todas las líneas activas.

Tareas relacionadas

Cómo determinar las direcciones IP de los componentes del sistema en la página 498

13.1.1 Cómo activar la UC Suite

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **Selección de aplicación**.
3) En el grupo de menús, haga clic en **Selección de aplicación** > **Servicios Web**.
4) Elija una de estas opciones:
   - Si quiere utilizar la UC Suite con UC Booster Card, haga clic en **Paquete con UC Suite**.
   - Si quiere utilizar UC Suite con UC Booster Servidor, haga clic en **Paquete con UC Suite en OSBiz UC Booster-Server** y en el campo **Dirección IP del OSBiz UC Booster-Server**, introduzca la dirección IP del servidor Linux externo.
5) Haga clic en **Aplicar**.

13.1.2 Cómo restringir la clase de servicio de las llamadas UC iniciadas por parte del sistema

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **Flags del sistema**.
4) Si antes de marcar llamadas de UC iniciadas por el sistema desea comprobar si el usuario de UC Suite que hace la solicitud está autorizado para realizar la llamada, en el área **Restricción de llamadas UC** active la casilla de verificación **Restricción de llamadas UC**.
5) Si antes de marcar llamadas de UC iniciadas por el sistema no desea comprobar si el usuario de UC Suite que hace la solicitud está autorizado para realizar la llamada, en el área **Restricción de llamadas UC** desactive la casilla de verificación **Restricción de llamadas UC**.
6) Haga clic en **Aplicar**.

13.2 Clientes de UC Suite

Los clientes de la UC Suite ofrecen interfaces cómodas para un amplio abanico de funciones de Comunicaciones Unificadas.

El sistema ofrece los siguientes clientes de UC para los siguientes dispositivos:

Tipo de cliente	Cliente	Tipo de equipo
Cliente de comunicaciones	myPortal for Desktop	PC
	myPortal for Outlook	
	myPortal @work	
	Fax Printer	
	myAttendant	
Cliente Mobile	myPortal to go (UC Suite) (véase Mobility)	Smartphone, tableta
Cliente de Contact Center	myAgent (véase Multimedia Contact Center)	PC
	myReports (véase Multimedia Contact Center)	

Los usuarios con dirección correo electrónico reciben correo de bienvenida con introd. primeros pasos.

Config. person.

Los ajustes de configuración personalizada de usuario para myPortal for Desktop se almacenan en archivos .ini en el PC. Se crea un archivo .ini para cada usuario. Los ajustes de configuración personalizada de usuario para myPortal for Outlook, myAttendant y Fax Printer se almacenan en el registro del PC. De esta forma, los distintos usuarios pueden utilizar a través de un PC las aplicaciones myPortal for Desktop, myPortal for Outlook, myAttendant y Fax Printer (Desk Sharing). Permite el uso en entornos Windows Terminalserver y Citrix-Server. De esta forma, distintos usuarios pueden utilizar las aplicaciones desde sus propios PC, sin necesidad de instalación local.

13.2.1 myPortal for Desktop

myPortal for Desktop es un cliente para Comunicaciones Unificadas en su PC. Además de a información sobre el estado de presencia de otros usuarios y a las cómodas ayudas de marcado a través de favoritos y directorios, el usuario puede acceder, por ejemplo, a mensajes de voz y faxes.

myPortal for Desktop ofrece las siguientes prestaciones:

- Directorios
- Lista de favoritos
- Diario
- Marcación de escritorio
- Ventanas emergentes
- Estado de presencia
- Servicio CallMe con ONS (One Number Service o Servicio de número único)

- Desvío de llamadas basado en el estado
- AutoAttendant personal
- Gestión de conferencias
- Grabar conferencias
- Grabación de llamadas
- Mensajería instantánea
- Mensajes de voz y de fax

13.2.2 myPortal @work

myPortal @work es una aplicación de comunicaciones unificadas que combina todas las funciones y servicios necesarios, como la práctica marcación mediante directorios telefónicos, favoritos, conversaciones e información sobre el estado de presencia de compañeros de trabajo. Todo, en un diseño de solución única para agilizar la comunicación diaria, mejorar el trabajo en equipo y establecer contacto rápidamente con compañeros, clientes y socios.

Nota: Cuando el cliente VoIP myportal@work se utiliza en combinación con otros clientes UC Suite se recomienda utilizar la retención de consulta de myportal@work en lugar de la retención común de los clientes UC Suite.

---

myPortal @work se puede utilizar con la soluciones de UC Smart y UC Suite. Para más información, véase myPortal @work.

13.2.3 myPortal for Outlook

myPortal for Outlook es el cliente para Unified Communications en Microsoft Outlook (plugin), similar a myPortal for Desktop.

myPortal for Outlook ofrece, además de myPortal for Desktop, las siguientes prestaciones:

- Cómo llamar a un contacto Outlook
- Cómo crear un contacto Outlook con el remitente de un mensaje de voz
- Cómo enviar un mensaje de voz como correo electrónico
- Cómo enviar un mensaje de fax como correo electrónico

13.2.4 Fax Printer

Fax Printer (Impresora de fax) es una aplicación Windows para el envío de mensajes de fax desde otras aplicaciones Windows (como, por ejemplo, Microsoft Word) con portadas personalizadas.

Fax Printer incluye los siguientes componentes:

- Fax Printer Cover Editor

- Fax Printer Driver - con las siguientes prestaciones:
  - Envío de fax a destinatarios individuales
  - Directorios
  - Uso de portadas centrales
  - Uso de líneas de encabezado predefinidas
  - Fax de serie
  - Control mediante la interfaz de usuario
  - Control mediante la línea de comandos

13.2.5 myAttendant

myAttendant es una aplicación de Unified Communications para funciones de conmutación. Además de cómodas funciones de conmutación, ayudas de marcación a través de directorios e información sobre el estado de presencia de las extensiones, también permite el acceso a mensajes de voz y de fax. La mensajería instantánea admite la comunicación con extensiones internas.

myAttendant ofrece las siguientes prestaciones:

- Funciones de conmutación
- Directorios
- Diario
- Ventana emergente
- Modificar el estado de presencia de las extensiones
- Grabación de llamadas
- Centro de mensajes
- Botones de extensión
- Gestión de mensajes de voz y de fax
- Mensajería instantánea
- Funciones Team
- Gestión de conferencias

13.2.6 Requisitos para los clientes de PC de UC Suite

Para utilizar los clientes de PC de UC Suite, el cliente PC debe estar equipado con las configuraciones de hardware y software adecuadas. Para la instalación y actualización automática se requieren derechos de administrador dependientes de la configuración. El abanico de funciones disponible depende de las licencias en uso.

Nota: Siga siempre las indicaciones del archivo `Readme first`, que puede encontrar en el directorio de almacenamiento de los archivos de instalación.

Teléfonos

Los clientes de PC de la UC Suite se pueden utilizar junto con los teléfonos siguientes:

- OpenStage HFA y SIP
- OpenScape Desk Phone IP 35G/55G HFA y SIP

- OpenScape Desk Phone IP 35G Eco HFA y SIP
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA y SIP
- OpenScape Desk Phone CP 110/210/410/710 HFA and SIP
- Teléfonos SIP compatibles con 3PCC
- Terminales analógicos
- Teléfonos RDSI
- OpenScape Personal Edition HFA y SIP
- OpenStage M3 (OpenScape Business inalámbrico)
- Teléfono OpenScape DECT S6/SL6/R6 (OpenScape Business inalámbrico)
- optiPoint WL3 professional SIP

Se admiten dispositivos más antiguos (como optiPoint 410/420/500, Gigaset M2/SL3/S4/SL4/S5 y optiPoint WL2 SIP). No se pueden operar dispositivos Optiset E. En las notas de la versión puede consultar cuáles son los dispositivos comprobados y autorizados.

Nota: El cliente integrado OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA no tiene ningún requisito previo especial, aparte de la configuración y licencia estándar del cliente.

"Favoritos" en el menú del teléfono contiene teclas programables libres y no está relacionado con los favoritos de UC. Los detalles de esas teclas y cómo programarlas están disponibles en la documentación del dispositivo.

Nota: Los teléfonos analógicos y DECT no admiten el indicador de buzón. Asimismo, la indicación de informaciones en la pantalla solo tiene compatibilidad restringida.

Sistemas operativos

Los clientes de PC de la UC Suite se pueden utilizar con los siguientes sistemas operativos:

- Microsoft Windows 11 (64 bits) todas las versiones
- Microsoft Windows 10 (64 bits) todas las versiones
- Apple macOS 13 / 14 / 15.1 a 15.4

Consejo: El sistema operativo utilizado requiere siempre la última versión de todas las actualizaciones disponibles (Service Packs y parches).

El soporte de los clientes de PC de la UC Suite para Microsoft Office 2003, Microsoft Windows XP y Microsoft Windows Server 2003 terminará al mismo tiempo que la asistencia de Microsoft. El producto seguirá soportado, pero ya no se harán pruebas exhaustivas.

La instalación en Windows requiere derechos de administrador locales en un PC cliente, pero no requiere actualizaciones automáticas. La interfaz de usuario en ruso o chino de myPortal for Outlook requiere una instalación del sistema operativo Windows en esos idiomas.

myPortal for Desktop para Mac de Apple está disponible con la misma interfaz que para Microsoft Windows. Debido a la arquitectura del sistema operativo de los Mac de apple, por el momento no son compatibles las siguientes funciones:

- Envío de faxes
- Integración de Entourage, Outlook

myPortal for Outlook es compatible con entornos Microsoft Office 365. Microsoft Office 365 es una aplicación en la nube. Se incluyen, entre otros un servidor de Exchange para la distribución central de correos electrónicos y los productos clásicos de Microsoft Office. OpenScape Business es compatible con Microsoft Office 365.

Con Microsoft Office 365 se pueden utilizar las siguientes funciones:

- Integración de calendarios de Exchange
- Transferencia de correos electrónicos

Navegador Web

Para programar las teclas de los teléfonos mediante los clientes UC, se pueden utilizar los siguientes navegadores Web:

- Microsoft Internet Explorer Versión 10 (o superior)
- Microsoft Edge
- Mozilla Firefox 19 (o superior)
- Google Chrome

Software adicional

Software adicional	myPortal for Deskto	myAttendant	myPortal for Outlook
Oracle Java JRE 1.8.x o superior (32 bits / 64 bits) OpenJDK V8 o superior (32 bits / 64 bits)	X	X	
Microsoft Outlook / Office • 2021 (32 bit / 64 Bit) + Office 365 • 2019 (32 bits / 64 bits) • 2016 (32 bits / 64 bits) - compatible, pero ya no forma parte de las pruebas del sistema - en caso de error no se proporcionará ninguna corrección de software (fin del soporte por parte de OpenScape Business)			X
Acceso a Microsoft Exchange Server (para contactos y citas de Outlook) Exchange 2015 / 2013 / 2010 (64 bits)	X		X
Microsoft .NET Framework >= 4.0 (a partir de Outlook 2010)			X

Nota: Para utilizar la integración del Calendario de Exchange con Microsoft Small Business Server, puede ser necesario deshabilitar la autenticación basada en formularios (FBA) en algunas circunstancias.

Indicación sobre Java 32 o 64 bits

Para utilizar la función "Importar contactos de Outlook al inicio" de myPortal for Desktop junto con la versión de 64 bits de Microsoft Office 2013, se requiere la instalación de la variante de 64 bits de Java. Si no se utiliza esta función, es recomendable utilizar la versión de 32 bits de Java, ya que requiere mucha menos memoria. Por este motivo, en todas las demás instalaciones se recomienda por norma general la versión de 32 bits de Oracle Java u OpenJDK.

Nota: El uso continuo de Oracle Java existente con OpenScape Business no requiere ningún cambio. Si se requiere una modificación de la versión de Java (por ejemplo, actualización de Oracle Java 7 a Oracle Java 8 o a OpenJDK V8), es necesaria una reinstalación del cliente de comunicaciones.

Requisitos mínimos de hardware

- 2 GHz CPU
- RAM: 2GB
- LAN de 100 Mbit/s (LAN de 1 Gbit/s recomendada)
- Resolución de pantalla XGA (1024x768), myPortal for Outlook: Resolución de pantalla SVGA (800x600)

Nota: Los monitores 4K no son compatibles con myPortal y myAttendant.

Microsoft Terminal Server, Citrix XenApp Server

Los clientes de PC de la UC Suite se pueden utilizar en entornos Microsoft Terminal Server y Citrix Server si se cumplen las condiciones siguientes:

Consejo: Los entornos de Terminal Server y CitrixServer (incluidos entornos virtuales y de Hosted Services) son responsabilidad del cliente.

Consejo: Los entornos Citrix-Server no pueden decodificar correctamente algunos caracteres regionales (p.ej., las diéresis del alemán).

Sistemas operativos:

- Microsoft Windows Server 2022 de 64 bits
- Microsoft Windows Server 2019 de 64 bits
- Microsoft Windows Server 2016 de 64 bits
- Microsoft Windows Server 2025 de 64 bits

Aplicaciones Office:

Microsoft Outlook / Office

- 2021 (32 bit / 64 Bit) + Office 365
- 2019 (32 bits / 64 bits)

- 2016 (32 bits / 64 bits) - compatible, pero ya no forma parte de las pruebas del sistema - en caso de error no se proporcionará ninguna corrección de software (fin del soporte por parte de OpenScape Business)

Requisitos de hardware:

El número de clientes que se pueden instalar depende del rendimiento del servidor y de la memoria de trabajo disponible. Si en el servidor se utilizan otras aplicaciones hay que atender a su consumo de memoria de trabajo.

Archivos de instalación

Para poner los archivos de instalación a disposición de los usuarios existen las siguientes opciones:

- El administrador descarga los archivos de instalación desde el **Centro de servicios** y los pone a disposición de los usuarios a través de, por ejemplo, una unidad.
- El administrador descarga también el repositorio del instalador en modo sin conexión, por ejemplo.
- El administrador también puede descargar el repositorio del instalador en modo sin conexión desde el **Centro de servicios** y los clientes se pueden instalar sin conexión.

13.2.7 Instalación/desinstalación silenciosa para clientes de PC de la UC Suite

La instalación/desinstalación silenciosa utiliza líneas comandos para instalar, desinstalar o modificar automát. clientes PC UC Suite en equipos sin tener que hacer ninguna entrada.

Nota: Siga siempre las indicaciones del archivo `ReadMe first.rtf`.

La instalación/desinstalación está requiere derechos de administración locales en el PC correspondiente. La instalación/desinstalación silenciosa permite la protocolización del proceso en un archivo.

Para la instalación/desinstalación silenciosa estás disponibles los siguientes parámetros:

Parámetros	Componentes
`/quiet`	Inicia el procedimiento de instalación sin intervención del usuario y sin una interfaz de usuario. Este parámetro requiere la existencia del repositorio.
`/repository`	Establece la dirección IP o el nombre de host para utilizar durante la instalación. Por ejemplo: `/repository=192.168.50.50`

Parámetros	Componentes
`/installpath`	Establece la ruta de los clientes instalados. El valor preestablecido es: `C:\Program Files(x86)\communicationsclients\`
`/autostart`	Inicia el procedimiento de instalación sin intervención del usuario. Este parámetro requiere la existencia del repositorio.
`/i`	Selecciona un producto para instalar. Los valores disponibles son `OLI`, `myPortal`, `myAgent`, `FPD`, `myReports` y `all`. Por ejemplo: `/i="OLI,FPD"`
`/u`	Selecciona un producto para quitar. Por ejemplo: `/u="OLI,FPD"`
`/set`	Selecciona los productos que se deben instalar en el sistema. Este control instala los productos seleccionados o los modifica si es que ya están instalados. Además quita los productos instalados que no figuren en el conjunto provisto. Por ejemplo: `/set="OLI,FPD"`
`/repair`	Repara los productos especificados. Por ejemplo: `/repair="OLI,FPD"`

13.2.7.1 Cómo realizar la instalación silenciosa

Requisitos previos

Su PC cumple con los Requisitos para los clientes de PC de UC Suite.

Dispone de derechos de administración en el PC cliente.

El archivo `CommunicationsClients.exe` está disponible en el PC cliente.

Nota: Siga siempre las indicaciones del archivo `ReadMe first`.

Utilice líneas de comando según los siguientes modelos en un archivo por lotes o en una ventana de símbolo del sistema DOS.

Paso a paso

1) Si no desea registrar el proceso, ejecute el siguiente comando:

   ```
   CommunicationsClients.exe /repository=<IP-address> /
   i=all /quiet
   ```

   Donde `<IP-address>` debe reemplazarse por la dirección IP de los clientes de UC.

2) Si desea registrar el proceso, por ejemplo en un archivo como `C:\ccinstall.log`, ejecute uno de los siguientes comandos:

   ```
   CommunicationsClients.exe /repository=<IP-address> /
   i="myPortal,FPD" /quiet /l="C:\ccinstall.log"
   ```

   Donde `<IP-address>` debe reemplazarse por la dirección IP de los clientes de UC. El comando de arriba instala únicamente myPortal for Desktop y FaxPrinter. Puede modificarlo para instalar los clientes que desee.

13.2.7.2 Cómo realizar la desinstalación silenciosa

Requisitos previos

Su PC cumple con los Requisitos para los clientes de PC de UC Suite.

Dispone de derechos de administración en el PC cliente.

El archivo `CommunicationsClients.exe` está disponible en el PC cliente.

Nota: Siga siempre las indicaciones del archivo `ReadMe first`.

Utilice líneas de comando según los siguientes modelos en un archivo por lotes o en una ventana de símbolo del sistema DOS.

Paso a paso

1) Si después de la última instalación silenciosa se ha actualizado el sistema, con el nuevo archivo `CommunicationsClients.exe` repita las líneas de comandos ejecutadas con el archivo `CommunicationsClients.exe` anterior (como si deseara reinstalar los componentes ya instalados con el nuevo archivo `CommunicationsClients.exe`). Solo entonces se puede realizar la desinstalación silenciosa.
2) Si no desea registrar el proceso, seleccione una de las siguientes líneas de comandos:
   - Si desea desinstalar todos los componentes:

     ```
     CommunicationsClients.exe /quiet /u=all
     ```
   - Si desea desinstalar varios componentes, introduzca los parámetros correspondientes en forma de enumeración, separados por comas,

después de `/u=`, por ejemplo, myPortal for Desktop / myAttendant y Fax Printer:

```
CommunicationsClients.exe /quiet /u="myPortal,FPD"
```

- Si solo desea desinstalar un componente, introduzca el parámetro correspondiente después de `/u=` por ejemplo, myPortal for Desktop / myAttendant:

```
CommunicationsClients.exe /quiet /u=myPortal
```

3) Si desea registrar el proceso, por ejemplo en un archivo como `C:\ccuninstall.log`, seleccione una de las siguientes líneas de comandos:

- Si desea desinstalar todos los componentes:

```
CommunicationsClients.exe /quiet /l="C:
\ccuninstall.log" /u=all
```

- Si desea desinstalar varios componentes, introduzca los parámetros correspondientes en forma de enumeración, separados por comas, después de `/u=`, por ejemplo, myPortal for Desktop / myAttendant y Fax Printer:

```
CommunicationsClients.exe /quiet /l="C:
\ccuninstall.log" /u="myPortal,FPD"
```

- Si solo desea desinstalar un componente, introduzca el parámetro correspondiente después de `/u=` por ejemplo, myPortal for Desktop / myAttendant:

```
CommunicationsClients.exe /quiet /l="C:
\ccuninstall.log" /u=myPortal
```

13.2.8 Actualizaciones automáticas

Las actualizaciones automáticas mantienen los clientes de UC siempre actualizados.

Si hay disponible una versión nueva, se actualiza automáticamente o se informa al usuario de que hay disponible una actualización. Si es preciso, aparece un mensaje para indicar que se deben cerrar una o varias aplicaciones para poder realizar la actualización.

Nota: Es aconsejable realizar siempre las actualizaciones sugeridas. Lo mismo se recomienda para software necesario para determinados clientes UC.

Nota: MacOS no admite la actualización automática de myPortal @work.

13.3 Usuarios y perfiles de usuario de la UC Suite

Los usuarios de la UC Suite son extensiones que utilizan clientes de UC de la UC Suite. Los perfiles de usuario guardan ajustes de configuración de usuarios de la UC Suite.

13.3.1 Usuarios de UC Suite

Los usuarios de UC Suite usan los clientes UC de la UC Suite. Los ajustes de los usuarios de UC Suite se pueden configurar en el directorio de usuario.

El directorio de usuario incluye todas las extensiones del sistema. Para utilizar los clientes UC hay que configurar datos de usuario adicionales en el directorio de usuario.

En el directorio de usuario se muestra la siguiente información por cada usuario:

- Símbolo de presencia

  El administrador puede modificar este estado de presencia para cada usuario.
- **Extensión**
- **Nombre de usuario**

  Nota: Si bien UCSuite permite y admite el cambio de nombres de usuario para sus propios clientes, dichos cambios podrían afectar el inicio de sesión de clientes que no son de UCSuite como myPortalToGo/myPortal@Work (cuando corresponda), por lo que no se recomiendan en tales situaciones.
- **Nombre**

  Nombre y apellidos, tal y como están configurados para la extensión.
- **Departamento**

  Si el usuario está asignado a un departamento.
- **Correo electrónico**

  Dirección de correo electrónico
- **Es agente**

  Nivel de agente en el Multimedia Contact Center.
- **Buzón de voz**

  El usuario puede recibir mensajes de voz.
- **Desvíos de llamadas**

  El usuario tiene configurado un desvío de llamadas.

La funcionalidad de búsqueda también está disponible para los campos del directorio de usuario.

Se pueden configurar los siguientes ajustes:

Valores y configuración	Palabras clave
Detalles personales	
Mis detalles personales	Nombre propio, nombre de usuario, contraseña, dirección de correo electrónico, departamento, número de teléfono adicional

Valores y configuración	Palabras clave
Mi foto	Mi foto Formatos de archivo admitidos: BMP, JPG/ JPEG/JFIFI, PNG. Tamaño máximo de archivo: 10MB
Nivel de usuario	Recepción de mensajes de voz: véase Extensiones Usuarios como puesto de operadora: véase Extensiones Usuarios como agentes: véase Extensiones
Mis preferencias	
Presentación	Colores de aspecto, idioma de la interfaz de usuario
Notificaciones	Ventanas emergentes
Conexión del calendario	Creación automática de citas Outlook en caso de ausencia, Actualización automática del estado de presencia mediante citas Outlook/iCal
Teclas de acceso rápido	Tecla de acceso rápido para funciones
Varios	Restablecimiento automático del estado de presencia, Método de transferencia, Tiempo de retención para entradas de diario, Dirección de servidor, Teclas de función del teléfono
Reglas de llamada	
Destinos de reenvío	Desvío de llamadas basado en el estado
Módulo de reglas	Desvío de llamadas basado en reglas
Comunicaciones	
Ajustes del buzón de voz	Modo de anuncio o grabación, Idioma del buzón de voz
Notificación de buzón de voz	Servicio de notificación de nuevos mensajes
Notificación de fax	Servicio de notificación de nuevos mensajes
Perfiles	
Ocupado, No contesta, Reunión, Enfermo, Pausa, Fuera de oficina, Vacaciones, Pausa de mediodía, Domicilio	Perfil para AutoAttendant personal
Sensibilidad	
Seguridad y acceso	Consulta de mensajes de voz y fax mediante el puesto de operadora, consulta de contraseña del buzón de voz
Visibilidad de presencia	Visibilidad del estado de presencia para otros usuarios

Valores y configuración	Palabras clave
Presencia de buzón de voz	Indicación del estado de presencia para llamantes externos, Indicación del estado de presencia para determinados llamantes
Permitir que otros usuarios copien mi diseño de BLF	Permitir que otros usuarios copien los grupos y botones de BLF Esta opción no está disponible para los perfiles que ya se hayan creado.
myAttendant	
Mensajes LAN	Módulos de texto para mensajes instantáneos
Números de llam. de marcación directa	MSN
Comunicaciones	Transferencias de llamadas

Puede consultar información más detallada sobre los ajustes de configuración de los usuarios en las instrucciones de manejo de los clientes de UC, bajo las palabras clave indicadas en la tabla.

De forma predeterminada, la contraseña para los clientes UC tiene seis posiciones. La longitud de la contraseña se puede adaptar a las necesidades (de 6 a 10 posiciones). La cantidad máxima de caracteres repetidos es dos y la cantidad máxima de caracteres secuenciales es tres. El nombre de la cuenta (invertido o no) no puede formar parte de la contraseña, y el cambio de contraseña requiere el conocimiento de la contraseña anterior. Se obliga al usuario a cambiar la contraseña predeterminada después del primer uso. La cantidad máxima de intentos de inicio de sesión erróneos es cinco. Los administradores con el perfil **Avanzado** pueden cambiar la contraseña de un usuario (por ejemplo, si ha olvidado la contraseña).

Nota: El nombre y apellidos de un usuario se sobrescriben en el directorio de usuario si se modifican mediante un asistente o mediante el modo Experto. Si, por el contrario, el nombre y apellidos de un usuario se modifican en el directorio de usuario, los datos del usuario (tal y como aparecen mediante un asistente o a través del modo Experto) no se sobrescriben. En este caso, hay dos nombres de usuario diferentes para el mismo usuario. Además, si el nombre o el apellido tienen más de 16 caracteres en total, se cortarán a 16, para ajustarse a la pantalla del dispositivo.

Las extensiones que tienen configurada una dirección de correo electrónico y que utilizan myPortal for Desktop, reciben un correo electrónico de bienvenida con una indicación de los primeros pasos.

Restablecer los datos de usuario

Los ajustes de un usuario se pueden restablecer a los valores estándar. Si restablece los datos de usuario, se borrarán todos sus datos, incluidos el nombre, apellidos y nombre de usuario.

Si el usuario tiene o no establecido el nombre o los apellidos mediante **WBM** > **Modo Experto** > **Servidor de telefonía** > **Extensión**, el restablecimiento de

este usuario mediante UC Suite asignará eventualmente el número que está almacenado como extensión también en el campo **Nombre**.

13.3.1.1 Cómo configurar un usuario de la UC Suite

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Directorio de usuario**. Se muestran todos los usuarios.
4) Marque el usuario deseado y haga clic en **Editar**.
5) Modifique los datos del usuario.
6) Haga clic en **Guardar**. La ventana se cierra automáticamente. Se muestran todos los usuarios.
7) Si desea configurar otro usuario, repita los pasos 4 a 6.

13.3.1.2 Cómo restablecer un usuario de la UC Suite

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Directorio de usuario**. Se muestran todos los usuarios.
4) Marque el usuario deseado y haga clic en **Restablecer usuario**.
5) Haga clic en **Guardar**. La ventana se cierra automáticamente. Se muestran todos los usuarios.
6) Si desea restablecer otro usuario, repita los pasos 4 a 5.

13.3.1.3 Cómo configurar un usuario de la UC Suite como agente (myAgent)

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Directorio de usuario**. Se muestran todos los usuarios.
4) Haga clic en la línea del usuario correspondiente.
5) Haga clic en **Editar**.
6) Haga clic en **Detalles personales** > **Nivel de usuario**.
7) Elija una de estas opciones:

   Si desea que el agente esté disponible de forma permanente, active la casilla de verificación **Agente disponible de forma permanente**. De esta forma, el agente también permanecerá disponible para llamadas, faxes y correos electrónicos aunque no acepte una llamada, un fax o un correo electrónico.

   Si no desea que el agente esté disponible de forma permanente, desactive la casilla de verificación **Agente disponible de forma permanente**. El agente deja de estar disponible si no acepta una llamada, un fax o un correo electrónico.
8) En la lista desplegable **Nivel** del agente, seleccione el rol deseado: **Agente**, **Supervisor** o **Administrador**.
9) Haga clic en **Guardar**.
10) Si desea configurar otro usuario como agente, repita los pasos 4 a 9.

13.3.1.4 Cómo modificar el estado de presencia de un usuario de la UC Suite

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Directorio de usuario**. Se muestran todos los usuarios.
4) Marque el usuario deseado.
5) Haga clic en el icono de estado de presencia y seleccione el estado de presencia correspondiente en la lista desplegable. Si es necesario, introduzca la hora de devolución en el formato `aaaa/mm/dd hh:mm`, por ejemplo, `2012/12/12 12:00`.
6) Haga clic en **Guardar**.
7) Si desea modificar el estado de presencia de otro usuario, repita los pasos 4 a 6.
8) Cierre la ventana.

13.3.1.5 Cómo modificar la contraseña para un usuario de UC Suite

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Directorio de usuario**. Se muestran todos los usuarios.
4) Marque el usuario que corresponda y haga clic en **Editar** > **Detalles personales** > **Mis detalles personales**.
5) En **Contraseña**, haga clic en **Cambiar**.
6) Introduzca la nueva contraseña en **Nueva**.
7) Introduzca la nueva contraseña en **Confirmar**.
8) Haga clic en **Aceptar**. La ventana se cierra automáticamente. Se muestran todos los usuarios.
9) Si desea cambiar la contraseña de otro usuario, repita los pasos del 4 al 8.

Pasos siguientes

Comunique la nueva contraseña a los usuarios correspondientes.

13.3.1.6 Cómo modificar la longitud de la contraseña un usuario de la UC Suite

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor**.
4) Clic **Ajustes generales**.
5) Introduzca la longitud mínima requerida de la contraseña (6-10) para el futuro en el campo **Longitudes**, en la sección **Longitud de la contraseña**.
6) Haga clic en **Guardar**.

13.3.2 Perfil de usuario de UC Suite

Los perfiles de usuario de la UC Suite guardan ajustes de configuración de usuarios de la UC Suite. Se pueden asignar varios usuarios (miembros) a un perfil de usuarios. Todos los miembros del perfil comparten los ajustes de configuración.

Todos los usuarios solo pueden formar parte de un perfil de usuarios. Si se hacen cambios directamente en un usuario (no a través del perfil asignado), el usuario se borra automáticamente del perfil.

Si se anula la asignación de un usuario a un perfil, conserva la configuración que representa este perfil.

Cuando un usuario ya está asignado a un perfil, los únicos cambios que se aplican a dicho usuario son los elementos del perfil bloqueado. Si el símbolo de bloqueo está desbloqueado, los cambios no se aplicarán.

Si se elimina un perfil completo, los usuarios que se asignaron a este perfil también conservan la configuración del perfil.

Se pueden configurar los siguientes valores y propiedades:

Opciones de menú	Valores y ajustes de configuración de
Detalles personales	
Mis detalles personales	Visibilidad de números de teléfono
Mis preferencias	
Apariencia	Colores de aspecto, idioma de la interfaz de usuario
Notificaciones	Ventanas emergentes
Conectividad de Outlook	Creación automática de citas Outlook en caso de ausencia, Actualización automática del estado de presencia mediante citas Outlook/iCal
Teclas de acceso rápido	Activación y configuración de combinaciones de teclas para acceder a varias funciones de uso habitual a través del teclado. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Varios	Restablecimiento automático del estado de presencia, Método de transferencia, Tiempo de retención para entradas de diario, Dirección de servidor
Reglas de llamada	
Destinos de reenvío	Desvío de llamadas basado en el estado
Comunicaciones	
Ajustes del buzón de voz	Modo de anuncio o grabación, Idioma del buzón de voz
Notificación de buzón de voz	Servicio de notificación de nuevos mensajes
Notificación de fax	Servicio de notificación de nuevos mensajes
Notificaciones de llamadas perdidas	Servicio de notificación de llamadas perdidas
Perfiles	
Perfiles	Perfil para AutoAttendant personal Estado disponible: Ocupado, No contesta, Reunión, Enfermo, Pausa, Fuera de la oficina, Vacaciones, Pausa de mediodía, En casa.
Sensibilidad	

Opciones de menú	Valores y ajustes de configuración de
Seguridad y acceso	Consulta de mensajes de voz y fax mediante el puesto de operadora, consulta de contraseña del buzón de voz
Visibilidad de presencia	Visibilidad del estado de presencia para otros usuarios
Presencia de buzón de voz	Indicación del estado de presencia para llamantes externos, Indicación del estado de presencia para determinados llamantes
Favoritos	
Favoritos	Grupos favoritos con una lista de contactos que se pueden asignar al usuario.

Puede consultar información más detallada sobre los ajustes de configuración de los perfiles de usuarios en las instrucciones de manejo de los clientes de UC, bajo las palabras clave indicadas en la tabla.

13.3.2.1 Cómo añadir un perfil de usuario de la UC Suite

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Perfil**. Se muestran todos los perfiles de usuarios y sus miembros.
4) Haga clic en **Agregar**.
5) En **Nombre** introduzca el nombre deseado para el perfil.
6) Haga clic en **Guardar**.
7) Configure los ajustes deseados del perfil de usuario.
8) Haga clic en **Guardar** y cierre la ventana.

13.3.2.2 Cómo modificar un perfil de usuario de UC Suite

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Perfil**. Aparecen todos los perfiles y sus usuarios.

4) Marque el perfil deseado.
5) Haga clic en **Editar**.
6) Modifique los valores y ajustes de configuración deseados.

Nota: Haga clic en **Guardar** antes de pasar a otra opción de menú para que se apliquen los cambios.

7) Para finalizar, haga clic en **Guardar** y cierre la ventana.

13.3.2.3 Cómo mostrar los perfiles de usuario de la UC Suite

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Perfil**. Se muestran todos los perfiles de usuarios y sus miembros.

13.3.2.4 Cómo añadir miembros a un perfil de usuario de UC Suite

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Perfil**. Se muestran todos los perfiles de usuarios y sus miembros.
4) Marque el perfil de usuarios deseado y haga clic en **Asignar usuarios**.
5) En la lista **Usuarios disponibles**, seleccione los miembros deseados.
6) Haga clic en **<-** para añadirlos a la lista **Usuarios asignados**.

   Se muestran todos los perfiles de extensiones existentes y sus miembros.
7) Cierre la ventana.

13.3.2.5 Cómo borrar miembros de un perfil de usuarios de la UC Suite

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Perfil**. Se muestran todos los perfiles de usuarios y sus miembros.
4) Marque el perfil de usuarios deseado y haga clic en **Asignar extensión**.
5) En la lista **Usuarios asignados**, seleccione los miembros correspondientes.
6) Haga clic en **->** para incluirlos en la lista **Usuarios disponibles**.

   Se muestran todos los perfiles de extensiones existentes y sus miembros.
7) Cierre la ventana.

13.3.2.6 Cómo borrar un perfil de usuario de la UC Suite

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Perfil**. Se muestran todos los perfiles de usuarios y sus miembros.
4) Marque el perfil de usuario deseado.
5) Haga clic en **Eliminar**.
6) Confirme con **Aceptar**. Se muestran todos los perfiles de extensiones existentes y sus miembros.
7) Cierre la ventana.

13.4 Estado de presencia y servicio CallMe

El estado de presencia y el servicio CallMe muestran y optimizan la accesibilidad de los usuarios. El estado de presencia permite realizar un desvío de llamadas relativo al estado y un desvío de llamadas basado en reglas de configuración flexible con myPortal for Desktop o myPortal for Outlook.

13.4.1 Presencia

El estado de presencia ofrece información sobre la disponibilidad de las extensiones internas (incluidas las extensiones móviles) en la lista de favoritos, en el directorio interno, en la sala de conferencias virtual y a través de anuncios grabados del buzón de voz. Además, la presencia controla la accesibilidad de las extensiones internas con desvío de llamadas relativo al estado, con desvío de llamadas basado en reglas y con el AutoAttendant personal.

En calidad de usuario, puede modificar su estado de presencia en myPortal for Desktop, myPortal for Outlook o a través del control de menús del buzón de

voz. Al desactivar el desvío de llamadas en el teléfono, se regresa al estado de presencia **Oficina**. Cada vez que se modifica el estado de presencia (excepto en **Oficina** y **CallMe**) puede establecer el momento del regreso programado a **Oficina** o **CallMe**.

En calidad de usuario, puede seleccionar los siguientes estados:

- **En la oficina**
- **Reunión**
- **Enfermo**
- **Pausa**
- **Fuera de oficina**
- **Vacaciones**
- **Pausa de mediodía**
- **En casa**
- **No molestar**

Nota: El administrador del sistema puede activar/desactivar la visibilidad del estado “enfermo” dentro de la administración del sistema. Ver OpenScape Business UC Suite> Servidor

---

Desvío al buzón de voz

Si el estado de presencia no es **Oficina** ni **CallMe**, el sistema de comunicación desvía las llamadas de forma predeterminada al buzón de voz. Mediante anuncios grabados relativos al estado informa del tipo de ausencia y del momento programado de regreso.

Texto de información

Puede introducir un texto de información relativo a su estado de presencia actual. Por ejemplo, si está en una reunión: "Estoy en la sala...". El texto de información aparece en la lista de favoritos, en el directorio interno y en la sala de conferencias virtual. El texto de información se borra al modificar su estado de presencia.

Restablecimiento automático del estado de presencia

En calidad de usuario, puede restablecer automáticamente el estado de presencia a **Oficina** una vez alcanzado el momento programado de final de la ausencia. De lo contrario, el sistema amplía el estado de presencia actual en intervalos de 15 minutos, hasta que usted mismo modifique el estado.

Visibilidad del estado de presencia

En calidad de usuario, puede establecer de forma individualizada si las distintas extensiones del directorio interno pueden ver un estado de presencia que no sea **Oficina** o **CallMe**, el momento programado de regreso y el texto de información que haya podido introducir.

Nota: Los ajustes de visibilidad no se aplican a los usuarios de myAttendant, ya que siempre pueden ver el estado de presencia de otros usuarios.

Actualización automática del estado de presencia mediante citas Outlook/ iCal

En calidad de usuario, puede controlar su estado de presencia mediante citas (no canceladas ni propuestas) con determinadas palabras clave en el asunto. Puede elegir entre los siguientes calendarios:

- Calendario Exchange (en el Microsoft Exchange Server)

  La actualización automática del estado de presencia mediante citas Outlook se realiza esté o no el PC en servicio. Para esta función, el administrador debe configurar la integración del calendario de Exchange.

  Nota: Encontrará información detallada sobre el uso de las distintas versiones de Microsoft Exchange Server en la wiki de expertos de Unify, en: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

- Calendario Oulook

  Para realizar una actualización automática del estado de presencia mediante citas Outlook es necesario iniciar myPortal for Desktop o myPortal for Outlook en el PC.
- Calendario iCal (myPortal for Desktop)

Puede utilizar las siguientes palabras clave:

- **Reunión**
- **Enfermo**
- **Pausa**
- **Fuera de oficina**
- **Vacaciones**
- **Pausa de mediodía**
- **En casa**

Las palabras clave dependen del idioma de tratamiento posterior de la interfaz de usuario configurado. Las palabras clave pueden estar en cualquier posición del asunto. Si el asunto contiene varias de estas palabras clave, sólo se aplica la primera. Si esta función está activada, el estado de presencia se modifica automáticamente en la hora de inicio y en la hora de fin de la cita correspondiente. Cada 30 segundos se comprueba si hay citas en el calendario.

Nota: Si activa esta función, tenga en cuenta que una cita que incluya cualquiera de estas palabras clave en la línea de asunto podría modificar de forma no deseada su estado de presencia. Si es necesario, modifique el asunto.

Nota: El estado de presencia “enfermo” puede no estar disponible, según la configuración del sistema realizada por el administrador.

Creación automática de citas Outlook en caso de ausencia (Windows)

En calidad de usuario, puede crear automáticamente citas Outlook para estado ausente. Para ello, modifique su estado de presencia. El asunto de la cita

Outlook correspondiente consta de su estado de presencia y del texto "(Auto)", por ejemplo: "Reunión (Auto)". La hora de inicio y la hora de fin de la cita en cuestión se corresponden con la información incluida en myPortal for Desktop o myPortal for Outlook. La hora de fin de la cita Outlook no se modifica en caso de que se retrase el regreso. Es posible establecer si las citas Outlook se guardarán en el archivo PST local o en el servidor de Exchange. Si se utiliza el archivo PST local, Outlook deberá estar abierto en el momento de creación de las citas Outlook. Si se utiliza el servidor de Exchange, las citas Outlook se generan esté abierto o no Outlook. Para esta función, el administrador debe configurar la integración del calendario de Exchange.

Nota: Encontrará información detallada sobre el uso de las distintas versiones de Microsoft Exchange Server en la wiki de expertos de Unify, en: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

Ventanas emergentes en caso de modificación del estado de presencia

En calidad de usuario, puede mostrar las modificaciones del estado de presencia mediante ventanas emergentes.

13.4.2 Servicio CallMe

El servicio CallMe permite a los usuarios definir cualquier teléfono de un puesto de trabajo alternativo como destino CallMe y estar disponible en él con su número de teléfono interno. Los usuarios pueden utilizar myPortal for Desktop o myPortal for Outlook en su puesto de trabajo alternativo como desde la oficina y, de esta forma, realizar llamadas salientes desde el destino CallMe.

Llamadas entrantes

Las llamadas entrantes dirigidas a su número de teléfono interno se desvían al destino CallMe. Los llamantes pueden ver el número de teléfono interno del usuario llamado. Las llamadas no aceptadas se transfieren al buzón de voz al cabo de 60 segundos.

Llamadas salientes

En el caso de las llamadas salientes con myPortal for Desktop o myPortal for Outlook, el sistema de comunicación establece dos conexiones. En primer lugar, el sistema de comunicación llama al usuario a su destino CallMe. Si contesta a la llamada, el sistema de comunicación llama al destino deseado y conecta ambas llamadas. En el destino se muestra el número de teléfono interno de llamante (One Number Service o "Servicio de número único").

Presencia

Si el servicio CallMe está activado, en la pantalla del teléfono correspondiente aparece "`CallMe activo`" (no en el caso de los teléfonos analógicos y de los teléfonos DECT). Los demás usuarios ven el estado de presencia **Oficina**.

Activación

En calidad de usuario puede activar el servicio CallMe de forma manual. Además, el servicio CallMe también se reactiva cuando el estado de presencia

se restablece automáticamente tras una ausencia, siempre que estuviera previamente activado. No se admiten los siguientes tipos de destinos CallMe:

- Grupo
- Teléfono transferido

Indicación del destino CallMe en la lista de favoritos

En calidad de usuario, en lugar de su número de teléfono puede mostrar el número de teléfono de su destino CallMe en la lista de favoritos de otras extensiones.

Desactivación

El servicio CallMe permanece activo hasta que se modifica el estado de presencia.

Nota: La función CallMe no debe utilizarse al acceder o participar en una conferencia abierta.

13.4.3 Desvío de llamadas relativo al estado

Con el desvío de llamadas relativo al estado, el usuario puede desviar a los llamantes a uno de sus números de teléfono adicionales o al buzón de voz, en función del estado de presencia.

Los usuarios pueden configurar el desvío de llamadas relativo al estado para cualquier estado de presencia, excepto: **Oficina**, **CallMe** y **No molestar**. Si modifica su estado de presencia, el sistema de comunicación activa el desvío de llamadas al destino definido para el nuevo estado (por ejemplo, si está fuera de casa a un teléfono móvil y si está de vacaciones a su representante.

13.4.4 Desvío de llamadas basado en reglas

Con el desvío de llamadas basado en reglas, los usuarios pueden desviar a las personas que llaman según unas condiciones o excepciones muy distintas. Es un desvío más flexible que el basado en estado.

Además, el desvío de llamadas basado en reglas admite:

- Cualquier destino
- El estado de presencia **Oficina**, **, reunión, enfermo, pausa, fuera de oficina, vacaciones, pausa de mediodía, en mi domicilio**

Nota: CallMe y **DND** no son válidos para el desvío de llamadas basados en reglas.

En calidad de usuario, puede utilizar el asistente de reglas para establecer reglas y activarlas o desactivarlas en cualquier momento. Una regla solo está activa cuando el teléfono no está desviado. Los desvíos de llamadas basados en estado (excepto al buzón de voz) anulan el desvío de llamadas basado en reglas.

Si hay activa una regla para el desvío de llamadas, el display del teléfono muestra **"Regla activa"**.

Si hay una llamada entrante, el sistema de comunicación comprueba la capacidad de aplicación de las reglas activas según su orden en el asistente de reglas. Solo se ejecuta la primera regla aplicable. En tal caso, el teléfono suena una vez y, a continuación, el sistema de comunicación desvía la llamada al destino establecido.

En una regla, se pueden definir varios tipos de condiciones y excepciones (excepto...). Sin embargo, no se pueden definir condiciones con excepciones del mismo tipo. Por ejemplo, no se puede establecer una condición del tipo "en determinados días de la semana" junto con una excepción del tipo "excepto determinados días de la semana".

Tipos de condiciones y excepciones

- (excepto) con determinada presencia
- (excepto) de determinadas personas (del directorio interno, del directorio externo, del directorio personal o de un número de teléfono concreto)
- (excepto) si se le transfiere desde determinadas personas (del directorio interno, del directorio externo, del directorio personal o de un número de teléfono concreto)
- (excepto) de un tipo determinado, es decir. **interno**, **externo** o **Contacto desconocido**
- (excepto) en una fecha determinada (o varias)
- (excepto) en determinados días de la semana
- (excepto) entre una determinada fecha de inicio y de fin
- (excepto) entre una determinada hora de inicio y de fin

13.5 Directorios y diario

Los directorios, la lista de favoritos y el diario organizan los contactos y llamadas.

13.5.1 Directorios

Los directorios organizan los contactos de las extensiones. Las extensiones pueden acceder a contactos con clientes de la UC Suite o con teléfonos de sistema con pantalla.

El sistema proporciona los directorios siguientes, compatibles con las funciones siguientes y con la prioridad siguiente para número de búsqueda (el número de búsqueda solo será compatible con llamadas externas y si la línea urbana/ITSP no suministra el número):

Directorio	myPortal for Desktop, myAttendant, myAgent, FaxPrinter	myPortal for Outlook	Teléfono de sistema con display
Contactos Outlook Contactos de Mac OS (myPortal for Desktop)	Si es necesario, los usuarios pueden importar los contactos de Outlook/Mac OS al iniciar myPortal for Desktop en Windows.	Contiene los contactos personales de Outlook de una extensión. Solo tiene derecho de escritura en estos datos el usuario en cuestión.	Contiene los contactos personales de Outlook de una extensión. Solo tiene derecho de escritura en estos datos el usuario en cuestión.
Directorio personal	Los usuarios pueden importar los contactos de Outlook o de Mac OS al iniciar myPortal for Desktop o administrar los contactos personales de forma manual. No se pueden modificar los contactos importados.	-	Contactos de Outlook importados mediante el asistente personal.
Directorio interno	El directorio interno de UC Smart ofrece prestaciones adicionales con la UC Suite. Contiene: • Todas las extensiones • Grupos internos que tienen activada la visualización en el sistema • Números de teléfono adicionales, si el usuario de la extensión ha dejado esta información visible para otras extensiones internas Las extensiones internas con teléfono del sistema se presentan con indicación del estado de presencia. Se puede establecer contacto con ellas por mensajería instantánea. Para mostrar el estado de presencia de una extensión es necesario que el usuario en cuestión lo autorice. En caso necesario, se muestra un momento de regreso planificado. Además, se muestra el texto de información que haya podido introducir el usuario. Un usuario solo tiene acceso de lectura a este directorio. El directorio interno incluye el directorio de sistema. Pero las búsquedas que se realicen en el directorio interno no incluirán resultados del directorio de sistema, sino tan solo entradas del propio directorio interno.		Incluye todas las extensiones y todos los grupos internos que tienen activada la visualización en el sistema.
Directorio externo	Contiene contactos de un directorio de empresa y lo configura el administrador. Un usuario solo tiene acceso de lectura a este directorio.		-
Carpeta Exchange pública (no se puede usar con Office 365)	Incluye los contactos de la carpeta Exchange pública, si el administrador ha configurado una. Se muestran en el directorio externo. Encontrará información detallada sobre el uso de las distintas versiones de Microsoft Exchange Server en la wiki de expertos de Unify, en: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.		-

Directorio	myPortal for Desktop, myAttendant, myAgent, FaxPrinter	myPortal for Outlook	Teléfono de sistema con display
Directorio offline externo (LDAP)	Contiene contactos del directorio de empresa LDAP y lo configura el administrador. El directorio offline externo solo se puede utilizar para búsquedas. El administrador puede activar y desactivar la indicación del directorio offline externo para los teléfonos de sistema.		
Directorio del sistema	Contiene números sistema, CU y usuarios no CU. Los usuarios no UC incluyen extensiones con licencias que no sean de UC y extensiones virtuales como Fax o AutoAttendant. El listín del sistema no es válido para Fax Printer		Incluye todas las extensiones internas y los números de marcación abreviada central. El administrador puede activar y desactivar la indicación de una extensión en el listín del sistema.

Nota: Los números de teléfono almacenados en la configuración del usuario y los todos los directorios (internos, externos, personales, Outlook, Exchange) deben indicarse en formato canónico para que pueda accederse a ellos desde la CU y desde el dispositivo.

El código de acceso no debe estar en el número.

Nota: Al añadir o eliminar un contacto UC, pueden pasar varios minutos (**y** hasta 30') hasta que los cambios se apliquen en todos los clientes y dispositivos, debido a los mecanismos de almacenamiento en caché que se utilizan. También se puede reiniciar el sistema para que los cambios surtan efecto **inmediatamente**.

Búsqueda sencilla

En calidad de usuario, puede realizar búsquedas en los directorios por **Nombre**, **Apellidos** o número de teléfono. Los directorios se examinan en el mismo orden que en la tabla. La búsqueda se puede realizar por palabra completa o por término de búsqueda incompleto (por ejemplo, parte de un número de teléfono). Las opciones de búsqueda configuradas se mantienen hasta que se realice una nueva búsqueda. Se guardan todos los términos de búsqueda utilizados. Puede borrar la lista de términos de búsqueda utilizados.

Búsqueda avanzada

Puede realizar búsquedas selectivas por los campos **Título**, **Nombre**, **Apellido**, **Compañía**, **Extensión**, **Tel. compañía**, **Tel. empresa 1**, **Tel. empresa 2**, **Tel. domicilio 1**, **Tel. domicilio 2**, **Número de móvil** y **Correo electrónico** y limitar el número de resultados máximo. La interfaz de usuario moderna de myPortal for Desktop no es compatible con la búsqueda avanzada. En un dispositivo tan solo se admiten **Tel. empresa 1**, **Tel. domicilio 1** o **Número de móvil.**

Orden

Los contactos de un directorio de myPortal for Desktop y myPortal for Outlook se pueden ordenar por columnas, en orden alfanumérico ascendente o descendente. La interfaz de usuario moderna de myPortal for Desktop no es compatible con la función de orden.

13.5.1.1 Cómo configurar directorios para teléfonos de sistema

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Puede seleccionar qué directorios están disponibles en los teléfonos de sistema con display.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema** > **Display**.
4) En la lista desplegable **Listín**, seleccione una de estas opciones:
   - Si desea habilitar los contactos personales, los directorios interno, externo y de red, y el directorio de LDAP, seleccione **Todo**.
   - Si solamente desea habilitar los contactos personales y los directorios interno, externo y de red, seleccione **Interno**.
   - Si solo desea que esté disponible el directorio offline externo, seleccione **LDAP**.
   - Si no desea que esté disponible ningún directorio, seleccione **No**.

   Nota: El usuario puede activar las solicitudes de búsqueda que se gestionarán como solicitudes para el Directorio Unificado, seleccionando **Agenda interna mediante Directorio Unificado**. Si el flag está desactivado y no hay acceso al Directorio Unificado, no estará disponible la vista de lista del menú de agenda, implementado para OpenScape Desk Phone CP 200/205/210.
5) Haga clic en **Aplicar**.

Pasos siguientes

Si ha seleccionado **Todos** o **LDAP**, asegúrese de que hay disponible un directorio LDAP (p. ej. Open Directory Service) para los teléfonos del sistema.

13.5.2 Directorio interno

El directorio interno incluye los detalles de contacto de las extensiones internas del sistema de comunicación. Los clientes de la UC Suite pueden acceder al listín del sistema.

En calidad de administrador tiene acceso ilimitado a todos los datos del directorio interno. En calidad de usuario puede marcar desde el directorio interno.

El administrador puede desactivar la indicación para todas las extensiones analógicas o para las extensiones analógicas sin nombre. En este último caso, no se muestran las extensiones cuyo nombre empiece por "-".

13.5.2.1 Cómo activar o desactivar la indicación de extensiones analógicas en el directorio interno

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) En el grupo de menús, haga clic en **Servidor**.
4) Haga clic en la pestaña **Ajustes generales**.
5) En el área **Extensiones analógicas**, y en la lista desplegable **Modo de usuario analógico**, seleccione una de estas opciones:
   - Si desea mostrar todas las extensiones analógicas del directorio interno, seleccione **Mostrar todo**.
   - Si solo desea mostrar extensiones analógicas con nombre en el directorio interno, seleccione **Mostrar solo con nombre**.

     Nota: Con esta configuración no se muestran las extensiones analógicas cuyo nombre comience con "-".
   - Si no desea mostrar ninguna extensión analógica, seleccione **Sin muestra**.
6) Haga clic en **Guardar**.

13.5.2.2 Cómo activar o desactivar la búsqueda en el directorio interno únicamente

Al marcar por nombre, puede configurar que la búsqueda se limite exclusivamente al directorio interno, o examinar todos los directorios en el entorno de red. De forma predeterminada, el sistema está configurado para buscar únicamente en el directorio interno.

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en Aplicaciones > OpenScape Business UC Suite.

3) En el grupo de menús, haga clic en Servidor.
4) Haga clic en la pestaña Ajustes generales.
5) Para activar la búsqueda únicamente en el directorio interno, seleccione la casilla de verificación Marcar por nombre - Buscar solo extensión local.

   Nota: La casilla Marcar por nombre - Buscar solo extensión local está activada de forma predeterminada.

   Ahora, el sistema solo busca el directorio interno al marcar por nombre. Al llegar a la extensión local, el sistema reproduce el nombre del receptor (si se ha grabado previamente).
6) Para desactivar la búsqueda únicamente en el directorio interno, anule la selección de la casilla Marcar por nombre - Buscar solo extensión local.

   Ahora, el sistema busca en todos los directorios del entorno de red al marcar por nombre.

13.5.3 Directorio externo

El directorio externo incluye contactos de fuera del sistema de comunicación.

Todos los usuarios pueden acceder a los datos del directorio externo en todos los clientes de la UC Suite y a través de teléfonos con pantalla. Los usuarios pueden marcar desde el directorio externo. Los usuarios de los clientes de la UC Suite myAttendant y myAgent pueden editar datos del directorio externo.

Importar un archivo CSV

En calidad de administrador puede importar contactos al directorio externo desde un recurso compartido de red o desde el sistema de archivos local en un archivo CSV en codificación UTF-8.

Un encabezado del archivo CSV permite asignar los nombres de campo del archivo CSV a los campos del sistema. El archivo CSV puede tener, por ejemplo, la siguiente estructura:

- Encabezado:

  "ID de cliente","Apellido","Nombre","Número de teléfono de empresa","Nombre compañía"
- Línea de datos:

  "987654","Dubios","Natalie","+498977712345","Company"

Al realizar la importación puede asignar los datos del archivo CSV a los siguientes campos:

- ID de cliente
- Título
- Nombre
- Apellidos
- Empresa
- Tel. empresa
- Tel2. empresa
- Tel. móvil
- En casa

- Tel. fax
- Correo electrónico
- Ciudad

Nota: El nombre del contacto se mostrará en el historial de llamadas, solo si rellena los campos Nombre y Apellidos.

Después de editar la plantilla CSV hay que guardar el archivo en formato UTF-8 para que los posibles caracteres especiales se puedan importar correctamente.

Si al realizar la importación desea sobrescribir los datos, el **ID de cliente** correspondiente debe ser idéntico.

Nota: Encontrará una plantilla CSV y una descripción de la sintaxis necesaria para importar datos al directorio externo en **Centro de servicios** > **Documentos** > **Plantillas CSV**.

13.5.3.1 Cómo importar un archivo CSV desde el sistema de archivos local en el directorio externo

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

En el sistema de archivos local hay un archivo CSV adecuado con la codificación UTF-8 y con datos para el directorio externo.

Existen ciertas limitaciones en cuanto a la longitud de los campos en las plantillas CSV. Estas limitaciones de longitud se enumeran a continuación:

- Carácter customer_business variable(50)
- Carácter customer_business2 variable(50)
- Carácter customer_home variable(50)
- Carácter customer_mobile variable(50)
- Carácter customer_title variable(20)
- Carácter customer_firstname variable(50)
- Carácter customer_surname variable(50)
- Carácter customer_company variable(255)
- Carácter customer_id variable(255)
- Carácter customer_xmppid variable(256)
- Carácter customer_fax variable(50)
- Carácter customer_email variable(255)
- Carácter customer_city variable(255)
- Carácter customer_street_address variable(2048)
- Carácter customer_import_source variable(256)

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) Haga clic en el árbol de navegación en **Asistentes** > **UC Suite**.

3) Haga clic en **Editar** para iniciar el asistente **Directorio externo**.

4) Haga clic en la pestaña **Importar directorio externo**.
5) Elija una de estas opciones:
   - Si desea cargar el archivo CSV desde un sistema de archivos local, active el campo de opción **Archivo local** y en el área **Cargar archivo**, desplácese hasta el archivo CSV.
   - Si desea cargar el archivo CSV desde un recurso compartido de red, seleccione el botón de opción **Carpeta pública de Windows** e ingrese los datos de acceso al recurso compartido de red (nombre del archivo CSV, nombre de dominio, así como nombre de usuario y contraseña para el recurso compartido) en el área **Carpeta pública de Windows**.

     Con **Prueba** puede comprobar si los datos son correctos.
6) Haga clic en el área **Carga de archivos** en **Elegir archivo** y seleccione el archivo deseado.
7) En el campo **Filas de encabezado**, indique el número de líneas de encabezado del archivo CSV.
8) Indique el **Separador de campos** utilizado en el archivo CSV.
9) Elija una de estas opciones:
   - Si desea eliminar los datos existentes del directorio externo, seleccione la casilla de verificación **Eliminar datos antes de importar**.
   - Si no desea eliminar los datos existentes del directorio externo, desactive la casilla de verificación **Eliminar datos antes de importar**.

     Nota: La bandera **Eliminar datos antes de importar** no eliminará registros si ya se utilizan en otras funciones, como llamadas VIP, etc.

     Nota: La marca **Eliminar datos antes de importar** solo elimina los datos que se importan desde la importación CSV. Los datos importados manualmente no se eliminan para evitar pérdidas inesperadas de datos. La única forma de eliminar los datos ingresados manualmente es eliminarlos manualmente.
10) En la sección **ID de cliente duplicado**, indique la forma de respuesta del sistema ante los intentos de importación de datos con ID de cliente ya existentes:
    - Si desea que los datos del archivo CSV sobrescriban los datos actuales, seleccione **Actualizar contactos**.

      Nota: CustomerID es el identificador que determina si dos registros están duplicados. Así, se considera que los registros importados con un CustomerID existente se refieren a un cliente existente y serán actualizados. El indicador **Actualizar cliente existente** solo funciona cuando se asigna CustomerID durante la importación. Se recomienda encarecidamente que confíe en la plantilla proporcionada y adapte los datos sobre ella, sin omitir identificadores únicos.
    - Si desea conservar los contactos, seleccione **Mantener contactos presentes**.

11) Haga clic en **Continuar**.
12) En las listas desplegables y en orden, seleccione la asignación de los campos del archivo CSV con los campos correspondientes del sistema. Si dichos campos no existen o no desea importar los datos, haga clic en la opción en blanco.
13) Haga clic en **Continuar**.
14) Haga clic en **Importar**. No cierre esta ventana mientras los datos aún se estén importando. Una vez finalizada la importación, se muestra el número de los registros de datos importados.

13.5.3.2 Cómo añadir acceso a una base de datos externa para el directorio externo

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Tiene a su disposición los datos para acceder a la base de datos externa.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Directorio externo**.
4) Haga clic en la pestaña **Importar directorio externo**.
5) Haga clic en la sección **Carga de archivo**, en **Seleccionar archivo**, y seleccione el archivo deseado.

13.5.3.3 Cómo exportar un archivo CSV desde el directorio externo

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en la pestaña **Exportar directorio externo**.
4) Elija una de estas opciones:
   - Si desea exportar un archivo CSV del sistema de archivos local, seleccione el botón **Archivo local** y haga clic en el botón **Inicio**.
   - Si desea exportar en una carpeta pública de Windows, seleccione el botón **Carpeta Público de Windows**. Introduzca los valores requeridos en los siguientes campos:

     - **Nombre de archivo**

     - **Nombre usuario**

     - **Dominio**

     - **Contraseña**

     Y haga clic en el botón **Inicio**.

13.5.4 Directorio offline externo (LDAP)

El directorio offline externo (LDAP) incluye contactos de un servidor LDAP para myPortal for Desktop, myAgent, Fax Printer, myPortal for Outlook y para teléfonos de sistema con display.

El sistema admite LDAP Versión 2 con autenticación.

LDAP (Lightweight Directory Access Protocol) es un protocolo de acceso a directorios basado en TCP/IP que permite acceder a los servicios de directorio en red. LDAP tiene un formato único a nivel mundial que permite la representación de cualquier nombre. Ofrece distintos diseños y una asignación exclusiva entre el nombre y su representación interna. El administrador, junto con el administrador de TI del cliente, define estos datos en una reunión de toma de decisiones de proyecto. LDAP se puede utilizar en los sistemas operativos MS Windows y Linux.

En un entorno Microsoft, el servidor ADS (Active Directory Server) o el servidor Exchange Server actúan también, al mismo tiempo, como servidor LDAP. En Microsoft Windows, los datos de usuario se pueden administrar con la aplicación Active Directory o ESTOS Metadir, por ejemplo. Por norma general, el encargado de administrar estos datos es el administrador de TI del cliente.

En Linux se pueden administrar los datos de usuario, por ejemplo, con OpenLDAP.

Un navegador LDAP (por ejemplo, Freeware de Softerra), simplifica la configuración de un servicio de directorio LDAP.

Los números de teléfono del servidor LDAP solo pueden incluir como delimitador el carácter "-" y espacios en blanco. El sistema no puede filtrar otros delimitadores.

Al configurar un directorio offline externo, en calidad de administrador puede adaptar la asignación de campos a los nombres del servidor LDAP utilizado. Los campos borrados se omiten al realizar búsquedas de nombre mediante número de teléfono. La búsqueda se realiza siempre con los últimos 4 dígitos del número de teléfono con el comodín preestablecido. Puede desactivar la búsqueda de nombre mediante número de teléfono en las llamadas entrantes.

Si el puerto 389 utilizado de forma predeterminada está asignado, hay que configurar otro puerto.

Nota: Encontrará más información en Internet, en la dirección: `http://wiki.unify.com`.

Los usuarios pueden acceder a los datos del directorio externo a través de myPortal for Desktop, myAttendant, Fax Printer y myPortal for Outlook durante la búsqueda.

Teléfonos de sistema con display

En calidad de usuario puede seleccionar en el menú entre el directorio interno y el directorio LDAP, siempre que estén configurados para los teléfonos de sistema. El directorio LDAP admite la búsqueda en los contactos correspondientes y permite llamar a un contacto una vez ejecutada la búsqueda.

La información de nombres aportada por el servidor LDAP no se utiliza para la indicación en display en el estado de llamada o de comunicación. Igualmente, los números de llamada de las llamadas entrantes tampoco son sustituidos por la información de nombres aportada por el servidor LDAP (como por ejemplo la sustitución de números de teléfono por nombres de marcación abreviada).

Una extensión del sistema solo está accesible a través del directorio LDAP si se ha configurado para ella un número de marcación directa y siempre que este coincida con el registro de la base de datos LDAP. Los números de llamada aportados por el servidor LDAP solo pueden encaminarse de forma interna en la red si el número de llamada interno y el número de marcación directa son idénticos.

13.5.4.1 Cómo añadir un Directorio offline externo (LDAP) para clientes PC

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Dispone de los datos de acceso para el servidor LDAP.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en la pestaña **Configuración de proveedores externos**.
4) Elija una de estas opciones:
   - Si en el diario de llamadas externas entrantes desea activar la resolución de números de teléfono en nombres, active la casilla de verificación **Buscar por número de teléfono**.
   - Si en el diario de llamadas externas entrantes desea desactivar la resolución de números de teléfono en nombres, desactive la casilla de verificación **Buscar por número de teléfono**.
5) Haga clic en **Agregar**.
6) Indique los datos de acceso del servidor LDAP:
   a) En **Nombre** indique un nombre para el directorio offline externo.
   b) En **Servidor** indique el nombre o la dirección IP del servidor LDAP.
   c) En **Puerto**, introduzca el número de puerto del servidor LDAP.
   d) En **Nombre distintivo de base (BaseDN) LDAP**, introduzca dicho nombre, por ejemplo, `dc=ejemplo-de-dominio, dc=net`.
   e) Indique el **Nombre de usuario**.
   f) Introduzca la **Contraseña**.
7) Introduzca la designación de campo correspondiente del servidor LDAP para los siguientes campos: **Título**, **Nombre**, **Apellidos**, **Tel. empresa 1**, **Tel. empresa 2**, **Domicilio**, **Móvil**, **Empresa**, **Teléfono de la empresa**, **Dirección postal**, **Estado, provincia o condado**, **País**, **Código postal**, **Correo electrónico**, **Localizador**, **Número de fax** y **Ciudad**.
8) Haga clic en **Guardar**.

13.5.4.2 Cómo borrar un Directorio offline externo (LDAP) para clientes PC

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en la pestaña **Configuración de proveedores externos**.
4) Haga clic en el Directorio offline externo que desee borrar.
5) Haga clic en **Eliminar**.

13.5.4.3 Cómo añadir un directorio offline externo (LDAP) para teléfonos de sistema

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Dispone de los datos de acceso para el servidor LDAP.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **System** > **LDAP** (Sistema > LDAP).
4) Indique la **Dirección IP del servidor LDAP**.
5) Indique el **Número de puerto del acceso LDAP**.
6) Indique el **Nombre de usuario**.
7) Introduzca la **Contraseña**.
8) En **Confirmar clave**, introduzca la contraseña.
9) En **DN base**, introduzca el nombre distintivo LDAP BASE del servidor LDAP, por ejemplo, `dc=ejemplo-de-domino, dc=net`.
10) En **Búsqueda**, introduzca la cadena de búsqueda para el servidor LDAP, por ejemplo, `cn=$*`.
11) Introduzca el **Atributo de resultado Nombre** para el servidor LDAP, por ejemplo, `cn`.
12) Introduzca el **Atributo de resultado Nº llamada** para el servidor LDAP, por ejemplo, `telephoneNumber`.
13) Para organizar los resultados de la búsqueda, seleccione una de estas opciones:
    - Si desea ordenar los resultados de la búsqueda, active la casilla de verificación **Clasificación de resultados de búsqueda**.
    - Si no desea ordenar los resultados de la búsqueda, desactive la casilla de verificación **Clasificación de resultados de búsqueda**.
14) Indique el **Código de ocupación LDAP**.
15) Indique el **Prefijo de nº llamada LDAP:**.
16) Haga clic en **Aplicar**.

13.5.5 Listín del sistema

En relación con los clientes de UC Suite, el listín del sistema contiene todos los números del sistema, usuarios de CU y no usuarios de CU. Los usuarios no CU incl. ext. con licencias no CU y ext. virtuales como Fax o AutoAttendant. En lo concerniente a los dispositivos, el listín del sistema contiene todas las extensiones internas y todos los números de marcación abreviada central.

El administrador puede desactivar la indicación de cada extensión o de cada número de marcación abreviada con nombre por separado.

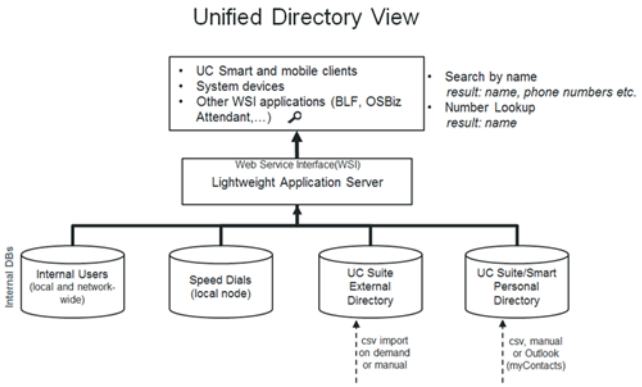
13.5.6 Directorio Unificado

OpenScape Business proporciona diferentes fuentes de datos para guardar y recuperar datos relacionados con usuarios y contactos, desde los datos de usuario interno de la configuración de usuario interno o la lista de marcación abreviada interna, hasta los diferentes directorios de las aplicaciones de UC.

Cada fuente de datos de OpenScape Business se utiliza desde una aplicación de cliente determinada localizada en el propio software del sistema de los dispositivos de teléfono o en una aplicación cliente de UC. Los datos recuperados y su presentación dependen de las fuentes de datos y de los clientes en uso.

El servicio "Directorio Unificado" de OpenScape Business incluye las fuentes de datos OpenScape Business actuales para las funciones de búsqueda común y de resolución de nombres. Proporciona los mismos resultados de búsqueda o información de resolución de nombres a todos los dispositivos de sistema y clientes OpenScape Business.

Se puede acceder al servicio Directorio Unificado a través de la interfaz de WebServices (WSI) desde clientes ubicados externamente como myPortal to go o internamente a través de mecanismos de procesamiento de llamadas (por ejemplo, desde teléfonos OpenStage).



Directorio Unificado utiliza las bases de datos internas y los directorios de OpenScape Business siguientes:

- Directorio de usuario interno (a nivel de red)
- Listas de marcación abreviada
- Directorio personal de UC Smart (opcional)
- UC SuiteDirectorio externo) (opcional)

- Contactos personales de Outlook (si se han importado mediante myContacts)

El servicio Directorio Unificado está disponible en todos los sistemas OpenScape Business a partir de la versión V2R2. No tiene requisitos concretos de licencia, hardware o software.

Para obtener unos resultados idóneos al utilizar el Directorio Unificado, se deben seguir algunas reglas relativas a formatos de números de teléfono y escritura de nombres.

13.5.6.1 Prestaciones

Clientes/Dispositivos compatibles

El servicio de Directorio Unificado proporciona:

- Búsqueda de directorio en varias fuentes de datos internas de OpenScape Business
- Presentación unificada de los resultados de la búsqueda para todos los clientes compatibles
- Búsqueda de número de teléfono/Resolución de nombres en varias fuentes de datos internas
- Presentación unificada de los resultados de resolución de nombres para todos los clientes compatibles
- Acceso a datos externos mediante la interfaz de WebServices (WSI)

Las prestaciones están disponibles para los sistemas de nodo único, tal y como se detalla a continuación. En redes OpenScape Business, la disponibilidad de las prestaciones depende principalmente del tipo de conexión de las líneas, los dispositivos y los clientes de la red.

Directorio Unificado es compatible con los clientes/dispositivos de sistema de Unify siguientes con las interfaces indicadas:

Dispositivo/Cliente	Protocolo/Interfaz en uso	Observaciones
Teléfonos OpenStage	Procesamiento de llamadas/Protocolo CorNet	WSI / HTTP(S) es opcional en OpenStage 60/80 para las imágenes de llamante
OpenScape Deskphone IP	Procesamiento de llamadas/Protocolo CorNet	WSI / HTTP(S) es opcional en DeskPhone IP 55 para las imágenes de llamante
Dispositivos inalámbricos (CMI)	Procesamiento de llamadas/Protocolo CMI	
CP 100/110 /200/205/210/ 405	Procesamiento de llamadas/Protocolo CorNet	
DeskPhone CP400/ 600/600E/ 700/700X/710	WSI / HTTP(S)	
myPortal @work	WSI / HTTP(S)	

Dispositivo/Cliente	Protocolo/Interfaz en uso	Observaciones
myPortal to go	WSI / HTTPS	
OpenScape Business Attendant / BLF	Procesamiento de llamadas/Protocolo CorNet	WSI / HTTP(S) es opcional

Nota: Los clientes myPortal, myAttendant y myAgent de UC Suite utilizan sus mecanismos propios para la resolución de nombres y la búsqueda de directorio.

Función de búsqueda

La búsqueda de Directorio Unificado siempre se realiza con la interfaz de usuario del cliente o dispositivo en cuestión. Los criterios de búsqueda y el conjunto de caracteres utilizado podrían estar restringidos, en función de los clientes en uso.

Después de introducir el criterio de búsqueda, la búsqueda se realiza en directorios posteriores

- Directorio de usuario interno (a nivel de red)
- Listas de marcación abreviada
- Directorio personal de UC Smart (opcional)
- UC SuiteDirectorio externo) (opcional)
- Contactos personales de Outlook (si se han importado mediante myContacts)

Todas las coincidencias que se encuentren en los directorios anteriores aparecen como resultados de búsqueda junto con su origen. Las coincidencias incluyen el conjunto de datos completo del contacto o algunas partes. El volumen de información de los resultados depende de la fuente de los datos.

Nota: La búsqueda de nombres de grupo en myportal @work no se admite en el modo UC Suite. Solo se admite la búsqueda de usuarios con licencia (licencia básica) y grupos MULAP con licencia (entradas UC).

Las coincidencias se presentan en los dispositivos o los clientes, en función de las capacidades de visualización.

	Directorio de usuario interno	Marcaciones abreviadas	Directorio Personal UC Smart	Directorio externo de UC Suite	Contactos Outlook personales (a través de my Contacts)
Apellidos	X	---	X	X	X
Nombre	X	---	X	X	X

	Directorio de usuario interno	Marcaciones abreviadas	Directorio Personal UC Smart	Directorio externo de UC Suite	Contactos Outlook personales (a través de my Contacts)
Nombre para mostrar/ abreviado	X	X	---	---	---
№ teléfono oficina	---	---	X	X	X
Privado/ ext. N.° de teléfono	---	---	X	---	X
Núm. teléfono móvil	---	---	X	X	X
Dirección de correo electrónico	---	---	X	X	X
Nombre de compañía	---	---	X	X	X
Ciudad	---	---	---	---	---
Imagen de contacto	---	---	X	---	X
Vista previa de imagen de contacto	---	---	X	---	X

Búsqueda de número de teléfono

La búsqueda de número de teléfono de Directorio Unificado resuelve el llamante transferido (CLI) buscando el número en todas las fuentes de datos internas admitidas. La búsqueda se realiza en los siguientes campos de número de teléfono:

- Número de oficina
- Número de móvil
- Número privado

La búsqueda de número de teléfono se activa cuando se producen llamadas entrantes o salientes en general; las prestaciones específicas de desvío y encaminamiento se toman en consideración de forma adicional.

Para obtener el resultado lo más rápido posible, se implementa una priorización fija de las fuentes de datos que se utilizan para la búsqueda de número de teléfono. El resultado solo incluye el apellido, el nombre, el nombre para mostrar o, si está disponible, los datos de contacto relacionado completos.

Tabla 7: Fuentes de datos compatibles y prioridades

Prioridad	Fuentes de datos	Observación
1	Nombre CO/ITSP (como lo haya enviado el proveedor)	Previamente se debe activar el flag "Nombre en CO".
2	Lista de marcación abreviada	
3	Contactos personales	
4	Detalle de usuario de UC	

Los datos recuperados se presentan en el dispositivo del usuario y/o en el cliente de UC. El volumen de información depende de las capacidades de visualización.

- **Llamadas entrantes**

  Escenario compatible para sistemas de nodo único:

  – Basic Call
  – Llamada de grupo/Llamada MULAP
  – Timbre adicional
  – Transferencia de llamada de un solo paso (SSCT)
  – Transferencia por consulta/de consulta/asistida
  – Desvío de llamada directo (CFU = Call Forwarding Unconditional)
  – Desvío de llamada diferido (CFNR = Call Forwarding No Reply)
  – Desvío de llamada en caso de ocupado (CFB = Call Forwarding Busy)
  – Transferencia ciega
  – Telecaptura de llamadas

  Nota: Captura de llamada es diferente de Grupo de telecaptura. En Grupo de telecaptura, si un número externo se guarda en el Directorio Unificado, el nombre del llamante no se muestra en los miembros del grupo.

  El escenario compatible para entornos de varios nodos (red) es una llamada de gateway.
- **Llamada saliente**

  En el caso de una llamada saliente, la búsqueda del número de teléfono del interlocutor llamado se realiza solo una vez.

  El escenario admitido para sistemas de nodo único es una llamada básica a un número externo.

La forma en que se presente el resultado de la búsqueda de número de teléfono depende de las capacidades de visualización de los teléfonos.

13.5.6.2 Reglas y convenciones

Se deberán seguir las mismas convenciones de formato de nombre y de número para obtener unos resultados óptimos al usar el servicio de Directorio Unificado.

Formato de números admitido

Todos los números de teléfono externos de las fuentes de datos se deben introducir en formato canónico, incluidos el prefijo de país y el código de red; p. ej., +4989700712345.

La lista de marcación abreviada admite solo el formato de marcación del sistema; p. ej., 0089700712345 o 0004989700712345.

Cuando los números de marcación abreviada se configuren para estar accesibles a través de LDAP, deberá activar la opción Conversión de número para que se muestra el nombre del contacto cuando el número esté en formato canónico. Para obtener más información sobre cómo activar la opción Conversión de número, véase Cómo añadir una fuente de datos externa para Open Directory Service en la página 1209.

Formatos de nombre admitidos

Se deberán seguir las siguientes convenciones de formato de nombres y juego de caracteres:

- **Formato de nombre de marcación abreviada**

  La búsqueda de nombre en la lista de marcación abreviada solo se admite con determinadas reglas de configuración. Los nombres y los apellidos se deben introducir en el campo de nombre existente con el siguiente patrón:

  <Apellido>, <Nombre> (separados por comas)
- **Usuarios internos en caso de migraciones**

  La migración a V2R1 y siguientes con usuarios internos que no atiendas a estas reglas de configuración no se realizará según lo previsto. Esto significa que el administrador deberá convertir los nombres internos al siguiente patrón antes de efectuar la migración:

  <Apellido>, <Nombre> (separados por comas)

Disponibilidad de los cambios de directorio

Después de crear, actualizar o eliminar contactos en las distintas fuentes de datos, podría llevar hasta 10 minutos que todos los cambios aparezcan en los resultados de búsqueda de número de teléfono.

13.5.6.3 Capítulo 11.5.5.3 Límites funcionales

Los siguientes límites funcionales no se aplican a Directorios Unificados:

Búsqueda por nombre

- Compatibilidad para nombre de grupo

  Los nombres de grupo (no los nombres MULAP) no se pueden buscar en todo tipo de configuraciones
- Compatibilidad de caracteres especiales

  En la mayoría de los dispositivos telefónicos, el usuario puede buscar caracteres estándar “a-z”. Los caracteres especiales (diacríticos), como los

caracteres españoles “Áá, Ée, Íi, Óó, Úú, Üü y ñÑ” no están disponibles a través de la interfaz de usuario del teléfono.

Por lo tanto, un resultado de búsqueda de caracteres comunes incluye también caracteres especiales. Una búsqueda de cualquiera de los caracteres “acdegilnorstuyz” también encuentra los caracteres especiales correspondientes “àáâãåä ąăäçćčďđ èéêë ęě# ìíîï ĺľł ñ ńň òóô ő öö řŕšśşť ùúû ůűüý ÿžý źž½ź”

en el resultado de la búsqueda.

Nota: La búsqueda en la guía telefónica con el carácter comodín al principio de la cadena de búsqueda, por ejemplo, <*jo*>, solo se admite para usuarios internos.

- Compatibilidad del formato de nombre de marcación abreviada

  La búsqueda de nombre en la lista de marcación abreviada solo se admite con determinadas reglas de configuración. Los nombres y los apellidos se deben introducir en el campo de nombre existente con uno de los patrones siguientes

  – <Apellido>, <Nombre> (separados por comas)
  – <Nombre> <Apellido> (en este caso, separador de espacio)

Presentación del nombre

Los contactos personales de UC Smart y del directorio offline externo, en los que el nombre y el apellido superen en conjunto los 24 caracteres, se truncarán hasta los 24 caracteres, para adaptarse a la longitud de visualización de los dispositivos.

Búsqueda de número de teléfono

La prestación Búsqueda de número de teléfono (nombre de contacto recuperado del número de llamante) no se admite en el Directorio Unificado con dispositivos SIP y S0.

13.5.6.4 Directorio Unificado en sistemas interconectados

El servicio Directorio Unificado está activo en todos los nodos de una red OpenScape Business y utiliza las fuentes de datos del sistema propio. El cliente y los dispositivos de teléfono siempre utilizan el servicio Directorio Unificado en su propio nodo.

Por tanto, dependerá del tipo de contenido de fuente de datos si hay disponibles contactos a nivel de red.

Tabla 8: Fuente de datos local y a nivel de red

Fuente de datos	Datos locales	Datos a nivel de red
Directorio de usuario interno	X	X
Listas de marcación abreviada	X	---

Fuente de datos	Datos locales	Datos a nivel de red
Directorio personal de UC Smart	X	---
Directorio personal de UC Smart	X	---
Contactos personales de Outlook (mediante myContacts)	X	---

Búsqueda de número de teléfono

En escenarios de interconexión no se utiliza la funcionalidad Búsqueda de número de teléfono. En esos escenarios, el nombre de transmite a través de mecanismos de interconexión normales entre los nodos de red.

Con los usuarios internos, se utiliza el Nombre para mostrar configurado, por lo que no se necesita la búsqueda.

13.5.6.5 Cómo importar contactos a un Directorio Unificado

El asistente de importación de contactos ofrece la opción de importar contactos a partir de un archivo CVS.

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Directorio Unificado**.
3) Haga clic en **Editar**, junto a **Importar contactos**, para poder agregar los contactos al Directorio General.
4) En la opción **Cargar archivos**, haga clic en **Elegir archivo** y seleccione el archivo CSV que desee cargar.

   Nota: La cantidad máxima de entradas por importación es de 100.000 (30.000 para sistemas integrados).

5) En la sección **Opciones**, pulse en **Separador de archivos**. «;» o «,» son entradas válidas.
6) Clic **OK & Cont.**.
7) El modo administrador procesa el archivo, lee los encabezados y los presenta junto con las categorías predeterminadas del directorio principal en la **página de asignación de encabezados CSV.** A continuación, el usuario puede cotejar las entradas de los archivos CSV para importar los datos correspondientes a otras categorías distintas a las predeterminadas.
8) Clic **OK & Cont.**.

9) En la página **Descripción general de la importación**:

a) Seleccione una de las siguientes opciones para el archivo CSV importado:

- Añadir contactos del directorio global
- Eliminar todos los contactos del directorio global importados a través del archivo CSV
- Eliminar todos los contactos del directorio global

b) En relación con el **identificador de cliente duplicado**, seleccione una de las siguientes opciones:

- Actualizar cliente existente
- Detener la importación del registro en curso

Las entradas que se van a añadir y las que no se han podido validar se encuentran en dos tablas diferentes.

Nota: Los datos duplicados se pueden identificar mediante los siguientes campos: nombre, apellidos, teléfono de trabajo y correo electrónico. Estos campos no se pueden actualizar automáticamente al seleccionar «**Actualizar cliente existente**». Para actualizar estos campos, deberá eliminar los registros antiguos siguiendo el paso 9a.

El flag **"Actualizar contactos"** solo funciona si ID de cliente se asigna durante la importación.

Solo se considerarán «clientes existentes» los que tengan el mismo **identificador de cliente** y se actualizarán.

El flag "**Eliminar directorio antes de importar**" no eliminará registros si ya se utilizan en otras funciones, por ejemplo las de llamante VIP, etc.

El identificador de cliente es el único criterio para determinar si el registro está duplicado. Si al cliente no se le asigna un identificador, es imposible evitar los duplicados.

Por lo tanto, se recomienda encarecidamente que los clientes confíen en la plantilla provista y adapten sus datos en ella sin omitir identificadores únicos.

---

10) Clic **OK & Cont.**. Este proceso puede durar varios minutos.

11) La página **Importación finalizada** informa del número de entradas que se han importado.

12) Haga clic en **Terminar**.

13.5.6.6 Cómo editar o agregar nuevos contactos al Directorio Unificado

El asistente de edición de contactos ofrece la función de editar los contactos que ya estén importados o agregar uno nuevo.

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Directorio Unificado**.
3) Haga clic en **Editar**, junto a **Editar contactos**, para poder editar los contactos del Directorio General.
4) Edite los campos que desee de los contactos. El botón **Aceptar** solo estará disponible cuando se haya editado algún campo.
5) Haga clic en **Agregar** para guardar un contacto nuevo manualmente.
6) Rellene los campos que desee del contacto nuevo y haga clic en el botón **Aceptar**.

13.5.7 Departamentos

Los departamentos agrupan a extensiones en el directorio interno según su pertenencia dentro de la organización. El directorio interno permite buscar o clasificar extensiones por departamentos.

13.5.7.1 Cómo agregar un departamento

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Departamentos**.
4) Haga clic **Agregar**.
5) Introduzca el **Nombre de departamento**.
6) Introduzca el identificador de la **Línea colectiva**.
7) Haga clic en **Guardar**.

13.5.7.2 Cómo asignar extensiones a un departamento

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Directorio de usuario**.
4) Seleccione la extensión correspondiente.
5) Haga clic en **Editar** > **Detalles personales** > **Mis detalles personales**.
6) Seleccione el departamento deseado en el cuadro de lista **Departamento**.
7) Haga clic en **Guardar**.

13.5.7.3 Cómo editar un departamento

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Departamentos**.
4) En la lista de departamentos haga clic en el departamento correspondiente.
5) Clic en **Edit.**.
6) Introduzca el **Nombre de departamento**.
7) Introduzca el identificador de la **Línea colectiva**.
8) Haga clic en **Guardar**.

13.5.7.4 Cómo eliminar un departamento

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Departamentos**.
4) En la lista de departamentos haga clic en el departamento correspondiente.
5) Haga clic en **Eliminar**.
6) Haga clic en **Aceptar**.

13.5.8 Lista de favoritos

La lista de favoritos ofrece a los usuarios una vista permanente de los contactos seleccionados. Con la lista de favoritos se puede llamar fácilmente a dichos contactos. Todas las extensiones internas con teléfono del sistema y los interlocutores de comunicación ven su estado de presencia y pueden ponerse en contacto con usted mediante mensajes instantáneos.

En calidad de usuario, puede agregar contactos de cualquier directorio a la lista de favoritos. En el caso de los favoritos que no proceden del directorio interno, en lugar del símbolo del estado de presencia aparece el símbolo que indica el origen del contacto.

La lista de favoritos gestiona los contactos en grupos. Los contactos de todos los grupos se pueden ordenar por Nombre, Apellidos o siguiendo el orden original.

En caso de ausencia de un usuario interno, se indica el momento programado de regreso. Para ello, coloque el puntero del ratón sobre la entrada (siempre que el usuario haya autorizado la visibilidad del estado de presencia).

En el caso de los favoritos con varios números de teléfono se puede consultar el número de teléfono de acceso estándar del contacto. El número de teléfono estándar de un favorito se puede reconocer porque el símbolo del menú contextual muestra la casilla de verificación activada.

13.5.9 Diario

El diario es la lista de todas las llamadas entrantes y salientes de un suscriptor. Permite que los suscriptores respondan rápidamente llamadas perdidas o llamen fácilmente a sus contactos desde el diario.

Carpeta para tipos de llamada

Las llamadas se organizan en estos grupos:

- **Pendientes**

  Incluye llamadas perdidas sin responder en las que se ha transmitido un número de llamada. En cuanto se responde una de estas llamadas, desaparecen todas las entradas con el número de llamada correspondiente.
- **Todas las llamadas**
- **Perdidas**
- **Contestadas**
- **Internas**
- **Externas**
- **Entrantes**
- **Salientes**
- **Programado**

  Incluye las llamadas que haya programado (como suscriptor) para fechas/horas específicas. La prestación de llamadas programadas no está a disposición de los agentes del Centro de contactos. Para que el sistema de comunicación realice una llamada programada, myPortal for Desktop o myPortal for Outlook debe estar abierto en el momento programado, el estado de presencia debe ser **Oficina** o **CallMe** y también debe confirmar la ejecución de la llamada en un cuadro de diálogo. Si está ocupado en el momento de la llamada programada, el sistema la aplaza hasta que usted esté disponible. Al salir del programa, myPortal for Desktop o myPortal for Outlook notifican si hay llamadas programadas pendientes. Al iniciarse la aplicación, myPortal for Desktop o myPortal for Outlook notifican si hay llamadas programadas cuya fecha u hora haya pasado. Puede borrarlas o guardarlas con una nueva fecha/hora.

En la interfaz de usuario moderna de myPortal for Desktop no están disponibles todas las carpetas para tipos de llamada.

Al iniciar la interfaz de usuario moderna myPortal for Desktop, solo se cargan 100 entradas de diario. Después de eso y cuando entren nuevas llamadas, el número en el historial de llamadas excederá los 100 registros.

Tiempo de retención

El sistema guarda un registro de las llamadas en el diario durante un tiempo limitado, que puede configurar el administrador. En calidad de suscriptor puede reducir ese tiempo. Una vez transcurrido el tiempo de retención, el sistema borra automáticamente las entradas asociadas.

Nota: El tiempo de retención también define el periodo máximo para las evaluaciones con myReports.

Grupos por periodo de tiempo

Las llamadas se agrupan de forma temporal en cada grupo, por ejemplo, Hoy, Ayer, etc., Semana pasada, Último mes y Anterior. El administrador puede configurar durante cuánto tiempo se conservarán las llamadas en el diario. Una vez transcurrido el tiempo establecido, las entradas se eliminan de forma automática. En la interfaz de usuario moderna de myPortal for Desktop no están disponibles los grupos por periodo de tiempo.

Detalles de llamada

Cada llamada se muestra con una fecha y una hora y, de haberlo, con el número de llamada. Si un directorio contiene más información sobre un número de teléfono (por ejemplo, **Apellidos**, **Nombre** y **Compañía**), también aparece indicada. Además, en casi todas las carpetas se muestran las columnas **Ruta**, **Duración** y **Llamada finalizada**. En la interfaz de usuario moderna de myPortal for Desktop no están disponibles todos los detalles de llamada.

Orden

Las llamadas del diario se pueden organizar en orden alfanumérico ascendente o descendente a partir de cualquier columna.

Puede saltar a la primera llamada del diario cuya entrada de la columna base de la ordenación comience por un carácter determinado (por ejemplo, al primer apellido que comience por "P"). A continuación, puede introducir otros caracteres para precisar los resultados de la búsqueda. En la interfaz de usuario moderna de myPortal for Desktop no está disponible la función de ordenación.

Exportar

En calidad de suscriptor puede exportar el diario como archivo CSV con myPortal for Desktop o myPortal for Outlook:

13.5.9.1 Cómo modificar el tiempo máximo de retención para el diario.

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor**.
4) Haga clic en **Mantenimiento**.

5) Introduzca la duración deseada en días en el campo **Conservar el historial de llamadas durante**, en la sección **Mantenimiento de información de llamadas**.

> **Nota:** El tiempo de retención también define el periodo máximo para las evaluaciones con myReports.

6) Haga clic en **Guardar**.

13.6 Llamadas

Los usuarios disponen de cómodas prestaciones para llamadas como, por ejemplo, marcación de escritorio, ventanas emergentes y la grabación de llamadas y conferencias.

13.6.1 Marcación de escritorio y clipboard

Marcación de escritorio y Marcación clipboard permiten a los usuarios con myPortal for Desktop (Windows) o myPortal for Outlook llamar a un destino seleccionado o a un destino del portapapeles de Windows desde muchas aplicaciones de Windows (p. ej., un correo electrónico de Outlook) mediante una combinación de teclas.

En función del tipo de secuencia de caracteres utilizada, la marcación funciona como sigue:

- Se marca un número de teléfono en formato canónico.
- Un número de teléfono en formato canónico se marca en cuanto el sistema de comunicación puede determinar si se trata de un destino externo o interno. De lo contrario, se solicita al usuario que haga la selección correspondiente.
- En los directorios, se busca una secuencia de caracteres que incluya letras como Nombre o Apellido.

La marcación de escritorio y la marcación clipboard se ejecutan tras un tiempo que puede configurar el usuario. En este tipo se puede interrumpir la marcación. Si el valor predefinido cambia de 3 s a 0 s, la marcación se ejecuta inmediatamente. El valor se cambia en los ajustes de los clientes UC Suite.

Por norma general, las aplicaciones de Windows que se hayan implementado mediante componentes estándar de Windows admiten la marcación de escritorio y la marcación clipboard. No así las aplicaciones de 16 bits. La marcación de escritorio solo es compatible con aplicaciones de 32 bits.

13.6.2 Ventanas emergentes

Las ventanas emergentes de los clientes de la UC Suite permiten responder de forma cómoda con un solo clic, por ejemplo, en caso de llamadas entrantes o de nuevos mensajes de voz.

Las ventanas emergentes aparecen en la esquina inferior derecha de la pantalla. Hay diferentes tipos de ventanas emergentes. Las ventanas emergentes de llamadas y mensajes muestran el número de teléfono, el

nombre y la imagen del llamante (si están disponibles). Los botones de las ventanas emergentes varían en función del contexto.

Las ventanas emergentes se pueden minimizar como iconos de bandeja del sistema. Si hay abiertas más de tres ventanas emergentes de llamadas, aparecen minimizadas automáticamente en la bandeja del sistema.

13.6.3 Grabación de llamadas

Los usuarios pueden grabar llamadas. Las llamadas grabadas aparecen en el buzón de voz.

Consejo: Es obligatorio informar al interlocutor de que la llamada va a ser grabada. En determinados países (como Francia), el sistema informa al interlocutor de forma automática.

En calidad de administrador, puede autorizar o prohibir la grabación de llamadas y conferencias a nivel de sistema. De forma opcional, al comienzo de la grabación puede configurar la reproducción de un anuncio grabado o de un tono de aviso.

En calidad de usuario puede controlar la grabación de llamadas a través de myPortal for Desktop o de myPortal for Outlook. Las llamadas grabadas están identificadas en el buzón de voz mediante un punto rojo y muestran (si la información está disponible) el número de teléfono del interlocutor.

La grabación en curso se interrumpe mediante los procedimientos de Consulta, Retener, Transferir e Iniciar una conferencia.

Nota: No se admite DTFM durante la grabación de llamadas.

13.6.3.1 Cómo activar o desactivar la grabación de llamadas

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor**.
4) Haga clic en **Grabación de la llamada**.
5) Elija una de estas opciones:
   - Si desea permitir la grabación de llamadas, seleccione la casilla de verificación **Grabación de la llamada**.
   - Si desea impedir la grabación de llamadas, desactive la casilla de verificación **Grabación de la llamada**.

6) Haga clic en **Guardar**.

Nota: Las llamadas que tienen esta funcionalidad activada no pueden ser transferidas ni retenidas.

13.6.3.2 Cómo activar o desactivar el anuncio grabado de una grabación

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor**.
4) Haga clic en **Grabación de la llamada**.
5) Elija una de estas opciones:
   - Si desea reproducir un anuncio grabado al comienzo de una grabación, seleccione la casilla de verificación **Reproducir indicación antes de la grabación**.
   - Si no desea reproducir un anuncio grabado al comienzo de una grabación, desactive la casilla de verificación **Reproducir indicación antes de la grabación**.
6) Haga clic en **Guardar**.

13.6.3.3 Cómo activar o desactivar el tono de aviso para la grabación

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor**.
4) Haga clic en **Grabación de la llamada**.
5) Elija una de estas opciones:
   - Si desea reproducir un tono de aviso antes de una grabación, active la casilla de verificación **Reproducir tono de aviso antes de la grabación**.
   - Si no desea que se reproduzca un tono de aviso antes de una grabación, desactive la casilla de verificación **Reproducir tono de aviso antes de la grabación**.
6) Haga clic en **Guardar**.

Nota: Este proceso solo es válido para **Openscape Business S**. La activación del tono de aviso de grabación en **Openscape Business X** lo controla el flag **Tono de aviso durante grabación de voz** ubicado en **Modo Experto** > **Ajustes básicos** > **Flags del sistema**.

13.7 Conferencias

En una conferencia varios usuarios (también externos) pueden comunicarse entre sí al mismo tiempo.

13.7.1 Gestión de conferencias

La gestión de conferencias permite a los usuarios utilizar distintos tipos de conferencias.

Tipos de conferencias

Los distintos tipos de conferencias ofrecen las siguientes opciones:

	Ad-hoc	Programado	Permanente	Pendientes
Uso	• Controlada por teléfono • Controlada por aplicación	• Controlada por aplicación	• Controlada por aplicación	• Controlada por aplicación
Inicio	• Manual	• Según plan horario	• Manual	• Manual
Fin	• Manual	• Según plan horario • Manual	• Manual	• Manual
Duración de la reserva de canales de conferencia	• Valor estándar: 1 hora	• Según plan horario	• Hasta la desactivación o borrado de la conferencia	• Hasta la desactivación o borrado de la conferencia
Ampliación	x	x	-	-
Repetición	• Manual	• Según plan horario	-	-
Dirección del establecimiento de conexión desde el sistema	• Saliente	• Saliente • Entrantes	• Entrantes	• Entrantes
Participantes	• Fijo	• Fijo	• Fijo	• Pendientes

	Ad-hoc	Programado	Permanente	Pendientes
Autenticación del controlador de la conferencia	-	• ID de conferencia individual (opcional) • Contraseña (opcional)	• ID de conferencia individual (opcional) • Contraseña (opcional)	• ID de conferencia común (opcional)
Grabación, si está activa en el sistema	• manual (On Demand Conference Recording)	• automático (Auto Conference Recording) • manual (On Demand Conference Recording)	• automático (Auto Conference Recording) • manual (On Demand Conference Recording)	• automático (Auto Conference Recording) • manual (On Demand Conference Recording)
Invitación por correo electrónico con:	• Nombre de conferencia • Enlace para la sesión de Web Collaboration	• Nombre de conferencia • Número de acceso telefónico • ID de conferencia • Contraseña • Fecha y hora del comienzo y final de la conferencia • Enlace para la sesión de Web Collaboration	• Nombre de conferencia • Número de acceso telefónico • ID de conferencia • Contraseña • Enlace para la sesión de Web Collaboration	• Nombre de conferencia • Número de acceso telefónico • ID de conferencia • Contraseña
Cita de Outlook como anexo de correo electrónico (.ics)	-	x	-	-

Conferencia controlada por aplicación

En calidad de participante puede iniciar, controlar y administrar una conferencia con la gestión de conferencias de myPortal for Desktop o de myPortal for Outlook.

Conferencia controlada por teléfono

En calidad de participante puede iniciar una conferencia controlada por teléfono de las siguientes formas y, a continuación, controlarla a través del teléfono:

- llame a los participantes deseados y conéctelos con la conferencia
- amplíe una llamada de consulta para una conferencia
- amplíe una segunda llamada para una conferencia

Sala de conferencias virtual

La sala de conferencias virtual permite a los participantes de las conferencias controladas por aplicación seguir una conferencia y a sus participantes en un entorno gráfico en tiempo real. A su vez, los controladores también pueden controlar la conferencia. La sala de conferencias virtual muestra el número de

teléfono, el nombre y el estado de presencia del controlador de la conferencia, si la información está disponible.

Número de acceso telefónico

En calidad de administrador puede modificar los números de acceso telefónico para las conferencias establecidos en la instalación básica. En calidad de usuario puede mostrar el número de acceso telefónico de una conferencia.

Controlador de conferencia

El iniciador de la conferencia se convierte de forma automática, y hasta que se adopte una nueva configuración, en el controlador de conferencia. Puede hacer lo siguiente (en función del tipo de conferencia):

- Agregar o eliminar participantes (conferencia controlada por aplicación):

  Los participantes eliminados no permanecen en la conferencia.
- Desconectar o recuperar a participantes de conferencia:

  Las extensiones recuperadas pueden continuar en la conferencia. Mientras el controlador de conferencia conecta a un participante, éste escucha una música de espera y los demás participantes permanecen conectados entre sí.
- Grabar la conferencia

  Las conferencias grabadas aparecen identificadas en el buzón de voz con un punto rojo e indican, si la información está disponible, el número de teléfono del primer participante en la conferencia. No se pueden grabar las conferencias en las que hay un usuario en retención.
- Definir a otro participante interno del mismo nodo como controlador de conferencia.
- Ampliar la conferencia
- Abandonar la conferencia sin finalizarla:

  El participante interno que lleve más tiempo en la conferencia se convierte automáticamente en el controlador.
- Finalizar la conferencia.

Participante de conferencia

Los participantes pueden abandonar la conferencia o volver a acceder a ella (conferencia programada y permanente). Mientras haya un participante en la conferencia, este podrá escuchar la música de espera. En calidad de administrador puede establecer si pueden acceder a la conferencia varios participantes externos. El número máximo de participantes externos está limitado, entre otros factores, por el número de líneas urbanas disponibles.

Tono de conferencia

Al conectar o desconectar a un participante, los demás participantes escuchan el tono de conferencia. En calidad de administrador puede activar o desactivar este tono.

Finalización automática sin controlador de conferencia

Si en una conferencia solo permanecen participantes externos, transcurrido un determinado tiempo escucharán un tono de advertencia. Transcurrido un tiempo más, el sistema finaliza automáticamente la conferencia. En calidad de administrador puede modificar estos tiempos.

Notificación por correo electrónico o cita Outlook

El sistema puede notificar automáticamente a los participantes de la conferencia por correo electrónico y, en el caso de las conferencias programadas, mediante una cita de Outlook incluida en forma de adjunto (.ics) sobre lo siguiente:

Suceso	Participantes de la conferencia notificados	Cita de Outlook
Nueva conferencia	Todas	Creación automática
Borrado de la conferencia		Borrado automático
Aplazamiento de la conferencia		Actualización automática
Agregar participantes de la conferencia	Afectados	Creación automática (afectados)
Eliminar participantes de la conferencia		Borrado automático (afectados)

El requisito para ello es que el administrador haya configurado el envío de correo electrónico. Además, los participantes de conferencia internos deben haber definido su dirección de email. El usuario que ha iniciado la conferencia deberá introducir la dirección de email de los participantes externos.

Nota: Para las notificaciones por correo electrónico no se hace ningún aviso en caso de error de envío o sobre posibles notificaciones por ausencia, ya que debido a la integración de Web Collaboration el sistema envía directamente los correos electrónicos.

Otras llamadas

Durante la participación en una conferencia, la realización o aceptación de otra llamada supone la desconexión de la conferencia.

Aparcar, Alternar

En una conferencia no están disponibles las prestaciones Aparcar ni Alternar.

Tasas de llamada

Las tasas se asignan a la persona que ha establecido la comunicación sujeta a tasas. Si se produce una transferencia a otro controlador, se transfieren también a él las demás tasas.

Carga del sistema

En calidad de administrador puede visualizar tanto conferencias activas como guardadas. Las conferencias inactivas se pueden borrar.

Consejo: Las conferencias permanentes ocupan recursos del sistema de forma constante. En myPortal for Desktop o myPortal for Outlook, todos los usuarios pueden configurar

conferencias permanentes, por lo que se recomienda a los administradores comprobar con regularidad las conferencias guardas para evitar un consumo innecesario de recursos.

Transmisión de vídeo

Si hay una transmisión de vídeo en curso, debe finalizarse antes de participar en una conferencia.

13.7.1.1 Cómo modificar el número de acceso telefónico para la sala de conferencias virtual

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Extensiones**.
3) En el grupo de menús, desplácese hasta **Extensiones** > **UC Applications** > **Conferencia**.

   En el área de trabajo se muestran los números de teléfono de las salas de conferencias virtuales. El último de estos teléfonos es el de las conferencias programadas y permanentes.
4) En el grupo de menús, haga clic en la entrada correspondiente (Índice - Número de teléfono).
5) Haga clic en la pestaña **Editar parámetros exten.**.
6) En el campo **Número de teléfono** introduzca el nuevo número de acceso telefónico. El número de acceso telefónico solo puede incluir las cifras 0-9.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

13.7.1.2 Cómo autorizar o desaprobar la presencia de varios participantes de conferencia externos

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el árbol de navegación, desplácese hasta **Sistema** > **Flags del sistema**.

4) Elija una de estas opciones:
   - Si desea autorizar la presencia de varios participantes de conferencia externos, active la casilla de verificación **Más de 1 miembro de conferencia externo**.
   - Si desea impedir la presencia de varios participantes de conferencia externos, desactive la casilla de verificación **Más de 1 miembro de conferencia externo**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

13.7.1.3 Cómo activar o desactivar el tono de advertencia

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el árbol de navegación, desplácese hasta **Sistema** > **Flags del sistema**.
4) Elija una de estas opciones:
   - Si desea activar el tono de conferencia, active la casilla de verificación **Tono de conferencia**.
   - Si desea desactivar el tono de conferencia, desactive la casilla de verificación **Tono de conferencia**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

13.7.1.4 Cómo modificar el intervalo de tiempo para la finalización automática de conferencias

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el árbol de navegación, desplácese hasta **Sistema** > **Parámetros de tiempo**.
4) En la línea junto a **Tiempo hasta tono advertencia en enlaces de tránsito HKZ**, y en **Base** y **Factor**, seleccione el tiempo que debe transcurrir entre el momento en el que el último controlador abandone la conferencia y la emisión del tono de advertencia.
5) En la línea junto a **Tiempo desde tono de advertencia hasta activación...**, indique el tiempo que debe transcurrir entre la emisión del tono de advertencia y la finalización automática de la conferencia.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

13.7.1.5 Cómo consultar información detallada sobre una conferencia memorizada

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **En conferencia**.
4) Haga clic en la conferencia correspondiente.
5) Haga clic en **Mostrar**.

13.7.1.6 Cómo borrar una conferencia guardada

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **En conferencia**.
4) Haga clic en la conferencia correspondiente.
5) Haga clic en **Borrar** y confirme la consulta de seguridad.

13.7.1.7 Cómo configurar la grabación de conferencias

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor**.
4) Haga clic en **Grabación de la llamada**.
5) Elija una de estas opciones:
   - Si desea permitir la grabación de conferencias, seleccione la casilla de verificación **Disponibilidad de la grabación en directo de la conferencia**.
   - Si desea impedir la grabación de conferencias, desactive la casilla de verificación **Disponibilidad de la grabación en directo de la conferencia**.

6) Haga clic en **Guardar**.

Nota: Las conferencias que tienen esta funcionalidad activada no pueden ser transferidas ni retenidas.

13.7.2 Conferencia Ad-hoc

La conferencia Ad-hoc sucede de forma espontánea y la inicia de forma manual el controlador de conferencia (sin programación previa). El controlador de conferencia puede guardar las conferencias Ad-hoc para poder ejecutarlas en cualquier momento posterior.

Inicio de conferencia

En las extensiones de todos los participantes internos, el sistema abre de forma automática la ventana con la sala de conferencias virtual. El proceso se realiza siempre que los participantes hayan iniciado myPortal for Desktop con la interfaz de usuario clásica o myPortal for Outlook. El sistema llama de forma simultánea a todos los participantes. Al incorporarse a la conferencia, los participantes reciben un saludo de bienvenida que indica la identidad del controlador de conferencia.

Grabación de la conferencia

El controlador de la conferencia puede grabar la conferencia de forma manual para sí mismo y para todos los participantes internos conectados, siempre que la grabación de llamadas esté activa en el sistema. Los participantes del nodo propio recibirán la grabación en su buzón de voz y los participantes de otros nodos por correo electrónico. La duración de la grabación solo está limitada por la capacidad de memoria disponible del sistema.

Finalizar una conferencia

El controlador de conferencia puede finalizar la conferencia en el cliente o mediante la acción colgar. Como alternativa, la conferencia finaliza cuando todos los participantes han abandonado la conferencia.

Conversión de una llamada en una conferencia

Una extensión interna que esté realizando una llamada puede transferir la llamada a una conferencia ad-hoc y añadir otras extensiones. Para ello, el usuario debe tener una licencia de la UC Suite Conference. Esta prestación no está disponible con CallMe.

13.7.3 Conferencia programada

Las conferencias programadas (o conferencias MeetMe) tienen lugar en un momento futuro y con duración previamente establecida. Pueden repetirse de forma recurrente a la misma hora.

Las conferencias programadas permanecen activas durante todo el tiempo, haya conectadas o no extensiones. El controlador de conferencia guarda las conferencias programadas con un nombre propio.

Opciones de configuración de una conferencia permanente

El usuario que inicia la conferencia puede establecer estas propiedades:

- Momento de inicio y final
- Carácter recurrente de la conferencia
- Obligatoriedad de la presencia del controlador
- Obligatoriedad de la autenticación de los participantes para incorporarse a la conferencia (introduciendo el ID de la conferencia o una contraseña mediante el teclado del teléfono).

  Nota: Las extensiones Mobility Entry deben introducir el código para marcación posterior MF antes de proceder a la autenticación.

  La contraseña estándar para las conferencias es 123456. El controlador de conferencia puede modificar este ajuste para cada uno de los participantes de forma individual.
- Idioma de los anuncios grabados al comienzo de la conferencia
- Dirección del establecimiento de conexión para cada uno de los participantes (valor estándar: **Saliente**)

Inicio de conferencia

En las extensiones de todos los participantes internos y en el momento programado, el sistema abre de forma automática la ventana con la sala de conferencias virtual. El proceso se realiza siempre que los participantes hayan iniciado myPortal for Desktop con la interfaz de usuario clásica o myPortal for Outlook. Si se requiere la presencia del controlador de conferencia, el sistema le llama en primer lugar. Si la autenticación es correcta llama de forma simultánea a todos los demás participantes. Los participantes de conferencia que han establecido un desvío al buzón de voz o que han señalizado Ausente en el estado de presencia, no reciben ninguna llamada. En función del establecimiento de conexión que haya sido configurado, el sistema llama a los participantes de conferencia, o bien, son ellos los que pueden acceder telefónicamente a la conferencia. El sistema anuncia la incorporación de cada uno de los participantes mediante un anuncio grabado, del tipo: "… `participa en la conferencia`". Para ello es necesario que el usuario que ha iniciado la conferencia grabe de antemano el anuncio con su nombre.

Nota: Para que los participantes de una conferencia programada sin autenticación puedan oír el anuncio grabado con el nombre del controlador, éste debe haber iniciado previamente una conferencia con autenticación.

Acceso telefónico

Mediante un número de acceso telefónico, los participantes de conferencia pueden acceder a la conferencia en cualquier momento del horario programado, sea cual sea la dirección de establecimiento de conexión establecida. Si se accede fuera del tiempo programado, se emite un anuncio grabado. En el acceso telefónico mediante un ITSP, este debe admitir RFC 2833 (caracteres MF).

Autenticación forzosa con la tecla *

El controlador de conferencia puede configurar la conferencia de modo que cada participante deba autenticarse de algún modo (como mínimo pulsando la tecla *. Esto garantiza que solo se puedan conectar a la conferencia usuarios presentes, y ningún buzón de voz.

Ampliación de la conferencia

Diez minutos antes del final de conferencia programado, los participantes oyen un anuncio grabado en el que se les indica el próximo final de la conferencia y la posibilidad de ampliarla marcando un determinado dígito. Cualquier participante puede ampliar la conferencia marcando el dígito indicado. El controlador de la conferencia puede ampliar la conferencia en cualquier momento desde myPortal for Outlook.

Grabación de la conferencia

El controlador de la conferencia puede grabar la conferencia de forma automática o manual para sí mismo y para todos los participantes internos conectados, siempre que la grabación de llamadas esté activa en el sistema. Los participantes del nodo propio recibirán la grabación en su buzón de voz y los participantes de otros nodos por correo electrónico. La duración de la grabación solo está limitada por la capacidad de memoria disponible del sistema.

Finalizar una conferencia

La conferencia finaliza en el momento programado. El controlador también puede finalizarla antes de tiempo.

13.7.4 Conferencia permanente

Las conferencias permanentes no tienen límite de tiempo. Los participantes de conferencia pueden acceder telefónicamente a ella en cualquier momento.

El controlador de conferencia guarda las conferencias permanentes con un nombre propio. La conferencia se mantiene hasta que es eliminada.

Opciones de configuración de una conferencia permanente

El usuario que ha iniciado la conferencia puede establecer:

- Si los participantes de conferencia se deben autenticar al incorporarse a ella mediante la introducción de un ID de conferencia y una contraseña a través del teclado del teléfono.

  Nota: Las extensiones Mobility Entry deben introducir el código para marcación posterior MF antes de proceder a la autenticación.

  La contraseña estándar para las conferencias es 123456. El controlador de conferencia puede modificar este ajuste para cada uno de los participantes de forma individual.
- El idioma de los anuncios grabados al comienzo de la conferencia.

Inicio de conferencia

En cuanto accede el primer participante de conferencia, el sistema inicia automáticamente la sala de conferencias virtual en las extensiones de los participantes de conferencia internos, siempre que los participantes hayan iniciado myPortal xA0;for xA0;Desktop o myPortal xA0;for xA0;Outlook. Los participantes de conferencia deben acceder por sí mismos. El sistema anuncia a todos los participantes internos que se incorporan a la conferencia mediante un anuncio grabado: "… participa en la conferencia"

Acceso telefónico

Los participantes de conferencia pueden acceder a ella en cualquier momento mediante un número de acceso telefónico. En el acceso telefónico mediante un ITSP, este debe admitir RFC 2833 (caracteres MF).

Grabación de la conferencia

El controlador de la conferencia puede grabar la conferencia para sí mismo y para todos los participantes internos conectados, siempre que la grabación de llamadas esté activa en el sistema. Los participantes del nodo propio recibirán la grabación en su buzón de voz y los participantes de otros nodos por correo electrónico. La duración de la grabación solo está limitada por la capacidad de memoria disponible del sistema.

La grabación automática de una conferencia permanente se inicia cuando hay dos o más participantes de conferencia y se detiene cuando hay menos de dos participantes. Una vez finalizada la grabación, todos los participantes reciben el mismo archivo de la grabación de la conferencia completa.

13.7.5 Conferencia abierta

Las conferencias abiertas son para un número determinado de participantes. Pueden acceder todos los participantes que tengan los datos de acceso.

El controlador de conferencia guarda las conferencias abiertas con un nombre propio. La conferencia se mantiene hasta que es eliminada.

Opciones de configuración de las conferencias abiertas

El usuario que ha iniciado la conferencia puede establecer:

- El número de participantes de conferencia (máx. 16).
- Si los participantes de conferencia se deben autenticar al incorporarse a ella mediante la introducción de un ID de conferencia y una contraseña a través del teclado del teléfono.

  Nota: Las extensiones Mobility Entry deben introducir el código para marcación posterior MF antes de proceder a la autenticación.

  La contraseña estándar para las conferencias es 123456. El controlador de conferencia puede modificar este ajuste para cada uno de los participantes de forma individual.
- Qué ID de conferencia común es válido para todos los participantes de conferencia.

- El idioma de los anuncios grabados al comienzo de la conferencia.

Inicio de conferencia

Los participantes de conferencia deben acceder por sí mismos. El sistema anuncia a todos los participantes internos que se incorporan a la conferencia mediante un anuncio grabado: "… participa en la conferencia".

Acceso telefónico

Los participantes de conferencia pueden acceder a ella en cualquier momento mediante un número de acceso telefónico. En el acceso telefónico mediante un ITSP, este debe admitir RFC 2833 (caracteres MF).

Grabación de la conferencia

El controlador de la conferencia puede grabar la conferencia de forma automática o manual para sí mismo y para todos los participantes internos conectados, siempre que la grabación de llamadas esté activa en el sistema. Los participantes del nodo propio recibirán la grabación en su buzón de voz y los participantes de otros nodos por correo electrónico. La duración de la grabación solo está limitada por la capacidad de memoria disponible del sistema.

13.8 Web Collaboration

Los clientes de PC de UC myPortal for Desktop (Windows) y myPortal for Outlook permiten la integración del producto Web Collaboration durante conferencias y llamadas telefónicas, para la colaboración simultánea y multimedia. Este producto permite acceder rápidamente a funciones como publicación de aplicaciones y de uso de escritorio, publicación de archivos, navegación simultánea, whiteboarding, push de URL, chat de IM o chat de vídeo con varios participantes.

Un usuario puede iniciar Web Collaboration durante una llamada mediante la ventana emergente del cliente de PC de UC; también pueden iniciarla los moderadores desde una conferencia activa. Al hacerlo se abre la sesión de Web Collaboration. Los participantes de la conferencia no necesitan hacer una instalación local de Web Collaboration. Si en el cliente de PC de UC hay un programa de correo electrónico, se puede enviar a los interlocutores un correo electrónico con un enlace para el cliente de Web Collaboration. Encontrará información sobre Web Collaboration en la documentación del producto de Web Collaboration.

Al crear o modificar una conferencia, el controlador de la conferencia puede programar una sesión de Web Collaboration. Al borrar o finalizar una conferencia, la sesión de Web Collaboration correspondiente se borra automáticamente.

Nota: Para que los clientes de PC de UC puedan iniciar automáticamente Web Collaboration, si estos acceden a Internet mediante un servidor proxy, la autenticación proxy debe estar desactivada.

Tipos compatibles de conexiones

La integración de Web Collaboration admite llamadas telefónicas, conferencias con control telefónico y los siguientes tipos de conferencias controladas por aplicación:

- Conferencia Ad-hoc
- Conferencia programada
- Conferencia permanente

Integración de Web Collaboration

Para la integración de Web Collaboration, el sistema de comunicación debe conocer la dirección del servidor de Web Collaboration. El fabricante ofrece el servidor de Web Collaboration en Internet como servicio (Pubic Server). Como alternativa, también puede ser un servidor de la red de clientes o de un colateral (Custom Server). Si el servidor se encuentra en la red de clientes, el sistema de comunicación suele acceder a él mediante http o mediante el puerto TCP 5004. Con la solución alojada en Internet (Public Server) se utiliza una conexión segura https, ya que mediante esta conexión se transmiten el número de licencia y la contraseña. De forma predeterminada se utiliza el puerto TCP 5100.

Nota: Para utilizar Web Collaboration, el sistema de comunicación requiere una conexión a Internet (router estándar y servidor DNS). No se admiten las conexiones mediante proxy.

Los participantes de conferencia internos con clientes de PC de UC se conectan automáticamente con la sesión de Web Collaboration correspondiente al inicio de la conferencia. Para ello, FastViewer se descarga y se abre automáticamente en segundo plano, lo que puede durar algunos segundos. Los participantes externos de la conferencia que tengan una dirección de correo electrónico conocida recibirán por correo electrónico un enlace para la sesión de Web Collaboration.

Nota: Una vez finalizada la sesión de Web Collaboration, si los usuarios utilizan MAC OS tienen que cerrar manualmente el cuadro de diálogo de aviso por la sesión finalizada.

En una conferencia programada, la conexión con al sesión de Web Collaboration ya se puede realizar 5 minutos antes del comienzo programado de la conferencia.

Instant Messaging y Web Collaboration

Las funciones de Instant Messaging (mensajería instantánea) del sistema y de Web Collaboration (colaboración web) son independientes entre sí: los mensajes instantáneos de un cliente de PC de UC no aparecen en una sesión de Web Collaboration del mismo participante, y a la inversa.

13.8.1 Cómo configurar la conexión con el servidor de Web Collaboration (Custom Server)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Hay disponible un acceso a Internet.

Para una conexión protegida con el servidor de Web Collaboration (Custom Server) se requiere un número de licencia y una contraseña.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **Web Services**.
3) En el grupo de menús, desplácese a **Web Services** > **Web Collaboration**.
4) Active el campo de opción **Custom Server**.
5) Si desea establecer una conexión protegida con el servidor de Web Collaboration (Custom Server), siga este procedimiento:
   a) En el campo **URL/Dirección IP:** introduzca la dirección IP del servidor de Web Collaboration (Custom Server) siguiendo este patrón:

      `https://<URL Web Collaboration Server>:5100/xmlrpcsecure`

      o

      `https://<Dirección IP Web Collaboration Server>:5100/xmlrpcsecure`
   b) En el campo **Número de licencia**, introduzca el número de licencia para la conexión protegida con el servidor de Web Collaboration (Custom Server).
   c) En el campo **Contraseña**, introduzca la contraseña para la conexión protegida con el servidor de Web Collaboration (Custom Server).
6) Si desea establecer una conexión no protegida con el servidor de Web Collaboration (Custom Server), siga este procedimiento:
   a) En el campo **URL/Dirección IP:** introduzca la dirección IP del servidor de Web Collaboration (Custom Server) siguiendo este patrón:

      `http://<URL Web Collaboration Server>:5004/OscInterface`

      o

      `http://<Dirección IP Web Collaboration Server>:5004/OscInterface`
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

13.8.2 Cómo configurar la conexión con el servidor de Web Collaboration (Public Server)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Hay disponible un acceso a Internet.

Para una conexión protegida con el servidor de Web Collaboration (Public Server) se requiere un número de licencia y una contraseña.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Aplicaciones** > **Web Services**.
3) En el grupo de menús, desplácese a **Web Services** > **Web Collaboration**.
4) Active el campo de opción **Public Server**.
5) En el campo **Número de licencia** introduzca el número de licencia para la conexión con el servidor de Web Collaboration (Public Server).
6) En el campo **Contraseña** introduzca la contraseña para la conexión protegida con el servidor de Web Collaboration (Public Server).

Nota: Si desea probar Web Collaboration durante 5 minutos, puede activar el campo de opción **Public Server (Demo Mode/Evaluation Mode)**. Para ello no requiere número de licencia ni contraseña.

---

7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

13.8.3 Cómo desactivar la conexión con el servidor de Web Collaboration

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **Web Services**.
3) En el grupo de menús, desplácese a **Web Services** > **Web Collaboration**.
4) Active el campo de opción **Ningún servidor de Web Collaboration**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**. La opción para iniciar una sesión de Web Collaboration está desactivada en los clientes de Unified Communications.

13.9 Mensajería instantánea

Mensajería instantánea ("Instant Messaging") es la comunicación mediante mensajes instantáneos (Chat).

13.9.1 Mensajería instantánea

Los mensajes instantáneos permiten conversar (chat) con otros interlocutores. El sistema admite mensajería instantánea con usuarios de UC Smart, interlocutores externos y chats multiusuario (o una combinación de ambos).

Los mensajes instantáneos se admiten con los siguientes clientes:

- myPortal for Desktop
- myPortal for Outlook
- myAgent
- myAttendant

En calidad de administrador puede activar o desactivar los mensajes instantáneos a nivel de sistema. Los mensajes instantáneos enviados y recibidos se muestran a ambos interlocutores en forma de diálogo. Al seleccionar un destinatario, el cliente indica si en ese momento el interlocutor está conectado. Si un interlocutor está desconectado, en función del tipo de destinatario seleccionado, sucede lo siguiente con el mensaje instantáneo:

Destinatarios	Comportamiento
Extensiones individuales	El mensaje instantáneo aparece en el siguiente inicio de sesión.
Grupo en Favoritos	El mensaje instantáneo no se muestra nunca en las extensiones que estén desconectadas.

Mensajes instantáneos externos

En calidad de usuario puede conversar (chat) con *un* interlocutor de comunicación externo (por ejemplo, con usuarios de Google Talk).

Chat entre varios usuarios

Chat entre varios usuarios es el intercambio de mensajes instantáneos con varios interlocutores de comunicación. El sistema admite como máximo un interlocutor externo.

Mensajería instantánea y Web Collaboration

Las funciones de mensajería instantánea del sistema y de Web Collaboration son independientes entre sí: los mensajes instantáneos de un cliente de UC no aparecen en una sesión de Web Collaboration del mismo participante: y a la inversa.

13.9.1.1 Cómo activar o desactivar los mensajes instantáneos

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor**.
4) Clic **Ajustes generales**.

5) Seleccione una de las opciones siguientes en la sección **Mensaje instantáneo**:
   - Si desea activar los mensajes instantáneos a nivel de sistema, desactive la casilla de verificación **Desactivar mensajería instantánea**.
   - Si desea desactivar los mensajes instantáneos a nivel del sistema, seleccione la casilla de verificación **Desactivar mensajería instantánea**.

   Nota: La desactivación de los mensajes instantáneos no se aplica inmediatamente en la ventana de mensajes instantáneos activa.

6) Haga clic en **Guardar**.

13.10 AutoAttendant

AutoAttendant ofrece a los llamantes, en función del estado de presencia de la extensión llamada, distintas opciones de selección para la transferencia de llamadas de voz a números de teléfono preestablecidos o al buzón de voz del usuario llamado. Los llamantes hacen la selección introduciendo determinados dígitos por teléfono.

13.10.1 AutoAttendant personal

El AutoAttendant en el AutoAttendant que pueden configurar los usuarios.

AutoAttendant personal

En calidad de usuario, dispone de las siguientes opciones para su número de teléfono con myPortal for Desktop o myPortal for Outlook:

- Grabar o importar anuncios grabados para el AutoAttendant personal
- Configurar perfiles para el AutoAttendant personal

Las llamadas se gestionan, en primer lugar, en el AutoAttendant central.

13.11 Mensajes de voz y de fax

Los servicios de mensajería de voz y fax integrados en el sistema permiten a los usuarios recibir y administrar mensajes de voz y fax a través de myPortal for Desktop y myPortal for Outlook. Fax Printer permite a las extensiones enviar mensajes de fax.

13.11.1 Buzón de voz

El buzón de voz registra mensajes de voz y las comunicaciones grabadas. Los usuarios pueden acceder a él por teléfono y con los clientes de UC Smart.

Nota: La contraseña predeterminada del buzón de voz solo se puede cambiar mediante un número de teléfono interno.

Solo se graban los mensajes de voz que duren más de dos segundos.

Administración de mensajes de voz

En calidad de usuario, puede escuchar sus mensajes de voz:

- a través del PC con myPortal for Desktop o myPortal for Outlook
- a través de su teléfono si su estado de presencia es **Oficina** o **CallMe**
- a través de cualquier teléfono externo

El puesto de operadora puede acceder a los mensajes de voz de los usuarios que así lo permitan a través de myAttendant.

El usuario administra los mensajes de voz entrantes con las carpetas, por ejemplo, Bandeja de entrada, Reproducido, Guardado o Eliminado.

Los mensajes de voz también se pueden rebobinar, detener y reenviar a otro usuario. El usuario también puede guardar los mensajes de voz en formato .wav y reenviarlos a cualquier dirección de correo electrónico.

El usuario también puede administrar a través del buzón de voz las llamadas grabadas. Las llamadas grabadas se identifican en el buzón de voz con un símbolo adecuado.

Nota: Puede encontrar información sobre el menú telefónico en el documento UC Suite Telefon User Interface (TUI), Instrucciones breves.

Cómo devolver llamada al remitente de un mensaje de voz

Al escuchar un mensaje de voz, el usuario puede devolver la llamada directamente a la persona que haya dejado el mensaje.

En calidad de administrador, puede configurar en el sistema si se pueden ejecutar devoluciones de llamada desde el buzón de voz

- desde cualquier número de teléfono
- solo desde números de teléfono propios de la extensión que estén configurados en la sección de Mis detalles personales de los clientes myPortal for Desktop, myPortal for Outlook, myAttendant o myAgent (**Extensión**, **Número de móvil**, **Número de teléfono externo 1**, **Número de teléfono externo 2**, **Número de teléfono privado** y **Número del asistente**).

Tiempo de retención

En calidad de administrador, puede configurar el tiempo de retención de los mensajes de voz.

Definición de prioridades en los mensajes de voz

Los llamantes pueden identificar los mensajes de voz como normales, urgentes o privados.

En myPortal for Desktop y myPortal for Outlook, las prioridades de los mensajes de voz existentes se representan mediante distintos colores.

Si el usuario escucha sus mensajes de voz a través del teléfono, se le informará en primer lugar del número de mensajes urgentes, privados y normales. En primer lugar se reproducen los mensaje urgentes.

Si los mensajes de voz se transfieren en forma de correo electrónico y dichos mensajes de voz están identificados como urgentes, el correo electrónico también se identificará con la prioridad más alta.

Funciones del buzón de voz

El administrador puede establecer el ámbito de funciones del buzón de voz. Puede elegir entre:

- **Completo**

  Todas las funciones del buzón de voz (valor estándar)
- **Menú abreviado**
- Después del anuncio grabado personalizado o relativo al estado se ofrece la conexión con la recepción.
- **Sin menú**
- Después del anuncio de bienvenida, el llamante se transfiere directamente a la grabación de mensajes.

Visualización de mensajes nuevos en el teléfono

Los mensajes nuevos se indican en el teléfono. En cuanto se reproduzca el mensaje de voz, desaparecerán las indicaciones.

El tipo de señalización de los mensajes nuevos depende del terminal:

- En todos los teléfonos se realiza una señalización acústica a través de un tono de marcado especial.
- En los teléfonos del sistema sin display se ilumina, además, la tecla de buzón (si está configurada).
- En los teléfonos del sistema con display, se ilumina la tecla de buzón (si está configurada) y en el display aparece un mensaje.

Servicio de notificación

myPortal for Desktop o myPortal for Outlook permiten establecer al usuario si desea transferir la información sobre la recepción de un nuevo mensaje de voz y el destino de la transferencia.

El usuario también puede decidir si desea transferir el mensaje en forma de correo electrónico. Además, puede decidir si desea que se le notifique la recepción de un nuevo mensaje de voz a través de una llamada de teléfono o de un SMS.

Idioma del buzón de voz

En calidad de administrador, puede seleccionar el idioma estándar del buzón de voz para el menú y para los anuncios grabados del sistema.

Dependencias

Tema	Dependencia
Reproducir un mensaje por el teléfono	El usuario solo puede reproducir mensajes de voz a través del teléfono con los estados de presencia **Oficina** o **CallMe**. En todas las demás configuraciones, los mensajes solo se pueden reproducir a través del PC.

13.11.1.1 Cómo configurar el número de teléfono del buzón de voz

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Buzón de voz**.
4) Indique el **Número de buzón de voz**.
5) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

13.11.1.2 Cómo configurar la transferencia automática diferida al buzón de voz

Con el asistente **Transferencia automática diferida** puede configurar la transferencia automática diferida al buzón de voz de cualquier usuario.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Transferencia automática diferida**. Se abre la ventana **Configuración de la función "Transferencia automática diferida de llamadas"**.
4) En la sección **Seleccionar ext. / grupo**, seleccione la extensión deseada.
5) Arrastre el **Buzón de voz** con el ratón y suéltelo en la sección **Modificar transferencia autom. diferida**.
6) Si es necesario, modifique el tiempo que debe transcurrir hasta la transferencia automática diferida (valor estándar: 15 segundos).
7) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

13.11.1.3 Cómo configurar parámetros del buzón de voz

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor**.
4) Haga clic en la pestaña **Buzón de voz**.

5) En la lista desplegable **Idioma del buzón de voz**, seleccione el idioma para el control de menús y los anuncios grabados predefinidos del buzón de voz.
6) En el campo **Orden de reproducción de mensajes de voz**, determine en qué orden se han de reproducir los mensajes.
7) En el campo **Tiempo de grabación de mensaje de voz**, introduzca la duración en segundos.
8) En el campo **Modo buzón de voz**, establezca el ámbito de su buzón de voz.
9) Si desea que las devoluciones de llamada desde el buzón de voz solo se hagan a los números de teléfono registrados en los clientes de Unified Communications en **Datos personales**, active la casilla de verificación **Autorizar devolución de llamada desde buzón de voz solo a números conocidos**.
10) Si desea desactivar el último anuncio que se reproduce desde el sistema, seleccione la casilla de verificación **Omitir la solicitud "deje su mensaje al oír el tono..."**. El anuncio del sistema no se oirá aunque se utilice un anuncio de grabación profesional.
11) Haga clic en **Guardar**.

13.11.1.4 Cómo configurar periodos de retención para los mensajes de voz

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor**.
4) Haga clic en **Mantenimiento**.
5) En los campos de **Mensaje**, introduzca el tiempo de conservación en días.
6) Haga clic en **Guardar**.

13.11.1.5 Cómo activar o desactivar la solicitud de contraseña del buzón de voz

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Directorio de usuario**.
4) Haga clic en la entrada pertinente, y luego en **Editar** > **Sensibilidad**.
5) Haga clic en **Seguridad y acceso**.

6) Elija una de estas opciones:
   - Si desea activar la solicitud de contraseña en caso de llamada a su buzón de voz, desactive la casilla de verificación **Saltar contraseña en caso de llamada del buzón de voz.**.
   - Si desea desactivar la solicitud de contraseña en caso de llamada a su buzón de voz, active la casilla de verificación **Saltar contraseña en caso de llamada del buzón de voz.**.
7) Haga clic en **Guardar**.

13.11.1.6 Cómo configurar la información para mensajes de voz recibidos

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema**.
4) En el grupo de menús, haga clic en **Display**.
5) En la sección **Interruptor**, active la casilla de verificación **Indicac. estado display en mens. inf**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

13.11.1.7 Cómo configurar la tecla de buzón para consultar mensajes de voz

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Terminales/ Extensiones**.
3) Haga clic en **Editar** para iniciar el asistente **Programación de teclas**.
4) Seleccione la extensión correspondiente.
5) En la primera columna, seleccione la tecla correspondiente.
6) En la columna **Func. de teclas** seleccione la función **Buzón**.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

13.11.2 Anuncios grabados del buzón de voz

Los anuncios grabados del buzón de voz ofrecen información a los llamantes, por ejemplo, acerca del estado de presencia del usuario.

Los anuncios grabados estándar están disponibles en todos los idiomas. En calidad de usuario puede grabar o importar anuncios grabados personalizados para el buzón de voz. El anuncio grabado estándar correspondiente es sobrescrito con el anuncio grabado personal. En calidad de administrador puede modificar los anuncios grabados estándar. Para ello, se realiza la importación de anuncios grabados. Los anuncios grabados personales de los usuarios se sobrescriben. Al importar anuncios grabados, el sistema realiza una limitación de nivel y una normalización automáticas para cumplir los requisitos de la norma "USA / TIA 968 Signal Power Limitations".

Nota: Antes de utilizar anuncios grabados o música de otra fuente asegúrese de que el material no está protegido por derechos de copyright.

Anuncios grabados del buzón de voz en el idioma del sistema

El idioma del sistema del buzón de voz se configura en la inicialización del país. Adicionalmente, el usuario puede configurar individualmente el idioma de su buzón de voz. De esta forma, los llamantes oirán los anuncios grabados relativos al usuario en el idioma configurado por él. Los anuncios grabados relativos al sistema se escucharán en el idioma del sistema.

Anuncios grabados en función del estado de presencia y del perfil

Los anuncios grabados del buzón de voz cambian automáticamente en función del estado de presencia establecido. Por ejemplo, si el estado de presencia es **Reunión**, el anuncio grabado podría ser: Este usuario está en una reunión hasta las 15:00 horas de hoy. Si se alcanza el final programado de la reunión, pero el usuario no ha restablecido su estado de presencia a Oficina, el anuncio del buzón de voz se ajusta automáticamente o se restablece automáticamente el estado de presencia a Oficina (el usuario puede configurar la acción deseada).

La siguiente tabla indica qué saludo escucharán los llamantes en función del estado de presencia definido y del perfil configurado. El menú de llamante se refiere al AutoAttendant central. El perfil se refiere aquí al AutoAttendant personal de la extensión. El usuario debe grabar el saludo estándar, el nombre y el saludo personalizado de sus perfiles. En función de la configuración, el menú de llamante puede tener distinta extensión e incluso no estar disponible.

	Ocupado No contesta No molestar	Reunión Sick Pausa Fuera de oficina ...
Buzón de voz con presencia	Saludo estándar + Menú de llamante	Nombre + Presencia + Menú de llamante
Buzón de voz en caso de presencia bloqueada	Saludo estándar + Menú de llamante (en caso de activado)	

	Ocupado No contesta No molestar	Reunión Sick Pausa Fuera de oficina ...
Perfiles con anuncio dinámico	Saludo personalizado de perfil	Nombre + Presencia + Saludo personalizado de perfil
Perfiles si se ignoran los anuncios grabados dinámicos	Saludo personalizado de perfil	

Si el usuario ha configurado que su estado de presencia no se transmita a llamantes externos, estos recibirán el saludo "Ocupado" con todos los estados de presencia excepto "Oficina", aunque el usuario llamado no esté realmente ocupado. En este caso, el usuario debe configurar un anuncio grabado para el saludo "Ocupado", para decir que no puede aceptar la llamada.

13.11.2.1 Cómo importar anuncios grabados para el buzón de voz

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Los archivos de sonido a reproducir tienen formato de archivo PCM y estas propiedades: 8 kHz, 16 bit, mono. 8 kHz, 16 bits, mono. El nombre de archivo de sonido puede tener, como máximo, 30 caracteres.

Nota: Previamente, puede crear archivos de sonido adecuados con el asistente de audio y mezclar dos fuentes (por ejemplo, música de fondo y un anuncio grabado).

Consejo: Antes de usar este material, asegúrese de que no está protegido por copyright.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en Editar para iniciar el asistente Carga de archivo.
4) En la pestaña Administrador de archivos de audio, en Destino de carga seleccione la entrada Saludo de buzón de voz.

5) Si desea reproducir un archivo de sonido, siga este procedimiento:
   a) Seleccione el botón de radio **Uploader** y haga clic en **Choose File** para seleccionar un archivo de audio apropiado.
   b) En el área Detalles de archivo de sonido puede ver las propiedades del archivo de sonido (por ejemplo, el nombre de archivo, el tamaño de archivo, tasa de bits, etc.).
   c) Haga clic en Carga.
6) Si desea grabar un saludo con un teléfono, siga este procedimiento:
   a) Seleccione el botón de radio **Grabador** y en el campo **Extensión** , seleccione el teléfono con el que se va a grabar el anuncio.
   b) En el campo **Nombre de archivo** introduzca el nombre del archivo de la grabación.
   c) Haga clic en Realizar llamada. El teléfono seleccionado suena.
   d) Descuelgue el auricular y haga clic en Grabar.
   e) Diga el saludo por el micrófono del teléfono y para terminar haga clic en Salir.
   f) Con Reproducir puede escuchar de nuevo la grabación.

13.11.2.2 Cómo modificar el idioma de los anuncios grabados del buzón de voz

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor**.
4) Haga clic en **Buzón de voz**.
5) En la lista desplegable **Idioma de buzón de voz**, seleccione el idioma.
6) Haga clic en **Guardar**.

13.11.3 Buzón de fax

El buzón de fax permite a los usuarios recibir y administrar mensajes de fax sin un dispositivo de fax mediante myPortal for Desktop o myPortal for Outlook.

En calidad de administrador, puede configurar un buzón de fax para las extensiones con licencia. Además, puede conectar dispositivos o servidores de fax a través de la interfaz a/b o RDSI.

A través de myPortal for Desktop o myPortal for Outlook, puede acceder a sus mensajes de fax en calidad de usuario. myAttendant puede acceder a los mensajes de fax de las extensiones que lo hayan autorizado.

Administración de mensajes de fax

El usuario puede administrar los mensajes de fax recibidos arrastrándolos a las distintas carpetas, por ejemplo, Guardado o Eliminado. También se pueden reenviar mensajes de fax a otros usuarios. Los usuarios pueden, además,

guardar mensajes de fax en formato PDF o TIFF, y reenviarlos a cualquier cuenta de correo electrónico.

El administrador puede configurar para todo el sistema si los mensajes de fax se guardarán en formato de archivo TIFF (estándar) o PDF.

Nota: Para convertir un archivo TIFF a PDF, el tamaño de la página debe ser A4.

Tiempo de retención para mensajes de fax

El sistema borra automáticamente los mensajes de fax que hayan superado el tiempo de retención:

Mensaje de fax	Tiempo de retención (Días)
Nuevo	120
Leído	365
Enviado	365
Eliminado	60

13.11.3.1 Cómo añadir un buzón de fax para extensiones

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Terminales/ Extensiones**.
3) Haga clic en **Editar** para iniciar el asistente **Terminales IP**.
4) Haga clic en el campo **N.º llam fax** de la extensión e introduzca el número de fax con el que la extensión podrá recibir mensajes de fax (hay que borrar el guión preestablecido).
5) Si desea configurar un número de marcación directa para el buzón de faz, haga clic en el campo **Marcación directa para fax** e introduzca el número de marcación directa para el fax (hay que borrar el guión preestablecido).
6) Haga clic en **OK & Continuar**. Si es necesario, utilice la opción **Imprimir** para imprimir una lista de extensiones con los números de fax configurados.
7) Haga clic en **OK & Continuar** y, a continuación, en **Salir**, para cerrar el asistente.

13.11.3.2 Cómo configurar el tipo de archivo para los mensajes de fax memorizados (UC Suite)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor**.
4) Haga clic en **Ajustes generales**.
5) Si desea que los mensajes de fax se guarden en formato PDF, en el área **Formato de fax** active la casilla de verificación **Usar PDF como formato de fax**.
6) Si desea que los mensajes de fax se guarden como archivos TIFF, en el área **Formato de fax** desactive la casilla de verificación **Usar PDF como formato de fax**.
7) Haga clic en **Guardar**.

13.11.4 Envío de mensajes de fax con Fax Printer

Fax Printer (Impresora de fax) es una aplicación para el envío de mensajes de fax desde aplicaciones Windows (por ejemplo, Microsoft Word) con portadas personalizadas o centrales.

Fax Printer incluye los siguientes componentes:

- Fax Printer Cover Editor
- Fax Printer Driver

Fax Printer se puede utilizar desde cualquier programa habitual de Windows. Los grupos de fax facilitan la distribución. Los mensajes de fax se envían como correos electrónicos o directamente al escritorio. Una ventana emergente ofrece información al usuario sobre el correcto estado del envío.

Líneas enc.

En calidad de administrador puede configurar distintos encabezados para los usuarios de Fax Printer. Puede definir un encabezado como estándar. Los encabezados pueden incluir estos elementos:

Detalles	Marc. pos.
Fecha/Hora	`{{date_time}}`
Nombre compañía	`{{company_name}}`
Nom. us.	`{{user_name}}`
Tel. compañía	`{{company_number}}`
Núm. pág.	`{{page_number}}`
N.º págs.	`{{page_count}}`

Los encabezados de mensajes de fax enviados con Fax Printer no pueden incluir caracteres especiales ni diéresis. Solo pueden incluir los caracteres del juego ANSI. Dado que el encabezado puede incluir el nombre del remitente, estos nombres no pueden incluir caracteres especiales ni diéresis.

13.11.4.1 Cómo agregar una portada de fax central

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Hay disponible una portada de fax con el formato de archivo .ocp.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Carga de archivo**.
4) Haga clic en la pestaña **Carga de portada de fax central**.
5) Haga clic en **Seleccionar archivo**.
6) Seleccione un archivo .ocp.
7) Haga clic en **Abrir**.
8) En **Nombre**, introduzca un nombre para la página de portada de fax.
9) Introduzca una **Descripción** para la página de portada de fax.
10) Haga clic en **Cargar**.
11) Una vez finalizada la carga, haga clic en **Aceptar**.
12) Si desea definir esta portada de fax como predeterminada, haga clic en ella, en la lista de portadas de fax, y luego haga clic en **Establecer como predeterminado**.
13) Haga clic en **Guardar**.

13.11.4.2 Cómo editar una portada de fax central

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Carga de archivo**.
4) Haga clic en la pestaña **Carga de portada de fax central**.
5) En la lista de portadas de fax, haga clic en la portada correspondiente.
6) Clic en **Edit.**.
7) En **Nombre**, introduzca un nombre para la página de portada de fax.
8) Introduzca una **Descripción** para la página de portada de fax.
9) Haga clic en **Guardar**.

13.11.4.3 Cómo añadir encabezados para Fax Printer

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Encabezados de fax**.
4) Haga clic **Agregar**.
5) Introduzca el **Nombre de la plantilla** del encabezado de fax.
6) Para añadir detalles al encabezado, haga clic en el orden deseado en los botones correspondientes **Fecha/Hora**, **Nombre de la compañía**, **Nombre de usuario**, **Teléfono de empresa**, **Número de página** y **Recuento de páginas**. Por cada uno de estos detalles, aparecerá un marcador de posición en el campo **Texto**.
7) Para eliminar un detalle del encabezado, en el campo **Texto** seleccione el marcador de posición correspondiente, por ejemplo `{{page_count}}` (**Número de páginas**) y pulse la tecla `Supr`.
8) Si es necesario, en el campo **Texto** agregue texto adicional. Por ejemplo, puede añadir el texto "de" entre los marcadores de posición `{{page_number}}` (**Número de página**) y `{{page_count}}` (**Número de páginas**).
9) Haga clic en **Guardar**.

13.11.4.4 Cómo cambiar encabezados para Fax Printer

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **UC Suite**.
3) Clic **Encabezados fax**.
4) En la lista de encabezados de fax, haga clic en el encabezado deseado.
5) Clic en **Edit.**.
6) Introduzca el **Nombre de la plantilla** del encabezado de fax.
7) Para añadir detalles al encabezado, haga clic en el orden deseado en los botones correspondientes **Fecha/Hora**, **Nombre de la compañía**, **Nombre de usuario**, **Teléfono de empresa**, **Número de página** y **Recuento de páginas**. Por cada uno de estos detalles, aparecerá un marcador de posición en el campo **Texto**.
8) Para eliminar un detalle del encabezado, en el campo **Texto** seleccione el marcador de posición correspondiente, por ejemplo `{{page_count}}` (**Número de páginas**) y pulse la tecla `Supr`.
9) Si es necesario, en el campo **Texto** agregue texto adicional. Por ejemplo, puede añadir el texto "de" entre los marcadores de posición `{{page_number}}` (**Número de página**) y `{{page_count}}` (**Número de páginas**).
10) Haga clic en **Guardar**.

13.11.4.5 Cómo borrar un encabezado para Fax Printer

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Encabezados de fax**.
4) En la lista de encabezados de fax, haga clic en el encabezado deseado.
5) Haga clic en **Eliminar**.

13.11.5 Servicio de notificación de nuevos mensajes (UC Suite)

En calidad de usuario, el sistema puede informarle de la llegada de nuevos mensajes por correo electrónico, por teléfono o por SMS.

El servicio de notificación funciona de este modo:

Notificación	de mensaje de voz	de mensaje de fax	Requisito
Correo electrónico	Recibirá un correo electrónico con un mensaje en forma de archivo WAV anexo, con la fecha y hora de recepción, duración del mensaje, número de teléfono disponible y nombre del remitente. Si el tamaño del archivo WAV supera 10 MB (promedio 1 MB/min), no se incorpora como anexo al correo electrónico. Los mensajes de voz con prioridad "Urgente" se entregan en forma de correo electrónico con nivel de importancia "Alto". En Outlook, los mensajes de correo electrónico con un mensaje de voz tienen un símbolo propio. Si utiliza un buzón IMAP que solo muestre el encabezado del correo electrónico, aparecerá el símbolo habitual para los mensajes de correo electrónico.	Recibirá un correo electrónico con el mensaje en forma de archivo PDF o TIFF anexo, con la fecha y hora de recepción, número de páginas, número de teléfono disponible y nombre del remitente. Si el tamaño del archivo PDF o TIFF supera 10 MB, no se incorpora como anexo al correo electrónico. En Outlook, los mensajes de correo electrónico con un mensaje de fax tienen un símbolo propio. Si utiliza un buzón IMAP que solo muestre el encabezado del correo electrónico, aparecerá el símbolo habitual para los mensajes de correo electrónico.	El envío de correo electrónico está configurado en el sistema. Como remitente se utiliza la dirección correspondiente.
SMS	Se le enviará un SMS al número de teléfono que haya definido en cuanto se reciba el mensaje		Plantillas SMS está configurado

Notificación	de mensaje de voz	de mensaje de fax	Requisito
telefónico	El buzón de voz le llama al número de teléfono configurado y reproduce el mensaje.	-	

Cada uno de estos tipos de notificación se pueden activar o desactivar de forma independiente para cada estado de presencia. Puede restringir la notificación telefónica al horario laboral configurado por el administrador. Puede establecer el número y los intervalos de reintentos de notificación telefónica.

13.11.6 Envío de correo electrónico

El envío de correos electrónicos permite notificar a los usuarios en caso de recepción de nuevos mensajes de voz y fax. Los administradores son notificados de nuevos mensajes de sistema.

13.11.6.1 Cómo configurar el envío de correo electrónico

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Hay configurada cuenta correo con contraseña en proveedor de correo y conoce los datos de acceso.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Centro de servicios** > **Transferencia de correos electrónicos**.
3) Indique **servidor band. salida (SMTP)** del servidor correo para envío correo (p. ej., `smtp.web.es`). Si es necesario, consulte servidor band. salida proveedor correo.

   Nota: En algunos casos, el envío de correo electrónico no se realiza porque no se puede resolver el nombre del servidor de bandeja de salida. Para resolver este problema no introduzca el nombre sino la dirección IP del servidor.

4) Si es necesario establecer una conexión segura, active la casilla de verificación. Si es necesario, consulte a su proveedor de correo electrónico si es necesario activar esta opción.
5) Indique el **Nombre de usuario** de la cuenta de correo electrónico.
6) En **Contraseña** y **Repetir clave**, introduzca la contraseña de la cuenta de correo.
7) Indique la **Dirección de correo electrónico**, por ejemplo, `pepe.ejemplo@web.es`.

8) Si desea comprobar inmediatamente el envío de correo electrónico, siga este procedimiento:
   a) Haga clic en **Prueba de conexión**.
   b) En **Enviar a correo**, indique dir. correo de buzón al que tenga acceso.
   c) Indique el **Asunto** del correo electrónico.
   d) Clic **Enviar correo prueba**.
   e) Compruebe si ha recibido el correo electrónico.
   f) Si el correo electrónico no ha podido entregarse, haga clic en **Volver** y corrija sus ajustes de correo electrónico (empezando por el paso 3).
9) Introduzca **Dir correo 1** para recibir notific. cuando se haya utilizado tolerancia ALI. También puede introducir otra dirección.
10) Haga clic en**OK & Continuar** y, a continuación, en **Salir**.

Ejemplo

Nota: Si realiza cambios de configuración en Transferencia de correos electrónicos en un sistema OpenScape Business X con Booster Server, deberá reiniciar Booster Server para que se apliquen los cambios.

13.11.7 Plantillas SMS

Las plantillas SMS permiten notificar a los usuarios en el caso de recepción de nuevos mensajes de voz a través de un SMS.

Para recibir las notificaciones por SMS se debe activar una dirección de correo electrónico móvil personal del proveedor correspondiente. Para hacerlo, el usuario deberá enviar un SMS de activación a un número de marcación abreviada. A continuación, recibirá por SMS su dirección personal de correo electrónico, compuesta, normalmente, por el número de teléfono y el nombre de gateway. De esta forma, por ejemplo, un cliente de T-Mobile con el número de teléfono 0171/1234 567 tendría la dirección de correo electrónico móvil: 01711234567@t-mobile-sms.de. Lo mismo se aplica, de forma análoga, a otras redes.

Una plantilla SMS se compone de las secciones Detalles de plantilla y Detalles SMS. El administrador debe introducir el nombre de la plantilla en la sección Detalles de plantilla que, normalmente, coincide con el nombre del proveedor del servicio email a SMS.

Los datos introducidos en la sección Detalles SMS dependen del proveedor. En Destinatario, el administrador debe introducir la dirección de correo electrónico a la que será enviado el SMS. Las entradas de la línea de asunto se pueden elegir libremente o bien, el administrador deberá introducir unos valores determinados, por ejemplo, el número de cliente.

Nota: Cada proveedor exige una plantilla específica. Para obtener los datos necesarios, póngase en contacto con su proveedor de telefonía móvil.

Marcador de posición

En los campos **Destinatarios**, **Asunto** o **Texto**, las plantillas SMS pueden incluir los siguientes marcadores de posición:

Detalles	Marcador de posición
El número de móvil al que realizar el envío	`{\MobileNumber}}`
Nombre o número de teléfono del remitente	`{{Sender}}`
Fecha y hora de recepción del mensaje	`{{DateTime}}`
El número del llamante	`{{CallingNumber}}`
Prioridad del mensaje	`{{Priority}}`

Información específica de sistema

La longitud del mensaje se reduce a los primeros 160 caracteres.

13.11.7.1 Cómo agregar plantillas SMS

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Plantillas**.
4) Haga clic **Agregar**.
5) Introduzca el nombre de la plantilla en **Nombre plantilla**.

   Nota: El nombre de la plantilla no debe tener espacios.

6) Introduzca el nombre del autor en **Nombre autor**.
7) Si desea insertar un marcador de posición, siga estos pasos:
   a) Haga clic en el campo en el que desea insertar el marcador de posición: **Destinatarios**, **Asunto** o **Texto**.
   b) En la lista desplegable **Campos VSL**, seleccione el marcador de posición deseado.
   c) Haga clic en **Insertar**.
   d) Si desea añadir más marcadores, repita el paso 7 a-c, según corresponda.
8) Introduzca el **Destinatario**.
9) Introduzca el **Asunto**.
10) Introduzca el **Texto**.
11) Haga clic en **Crear**.

13.11.7.2 Cómo editar plantillas SMS

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Plantillas**.
4) Seleccione la plantilla de SMS deseada en la tabla **Proveedor de SMS**.
5) Clic en **Edit.**.
6) Introduzca el nombre de la plantilla en **Nombre plantilla**.

   Nota: El nombre de la plantilla no debe tener espacios.

7) Introduzca el nombre del autor en **Nombre autor**.
8) Si desea insertar un marcador de posición, siga estos pasos:
   a) Haga clic en el campo en el que desea insertar el marcador de posición: **Destinatarios**, **Asunto** o **Texto**.
   b) En la lista desplegable **Campos VSL**, seleccione el marcador de posición deseado.
   c) Haga clic en **Insertar**.
   d) Si desea añadir más marcadores, repita el paso 8 a-c, según corresponda.
9) Introduzca el **Destinatario**.
10) Introduzca el **Asunto**.
11) Introduzca el **Texto**.
12) Haga clic en **Crear**.

13.11.7.3 Cómo eliminar plantillas SMS

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Plantillas**.
4) Seleccione la plantilla de SMS deseada en la tabla **Proveedor de SMS**.
5) Haga clic en **Eliminar**.
6) Haga clic en **Aceptar**.

13.11.8 Fax over IP (T.38 / G.711 Fax)

Fax over IP permite la transmisión de mensajes de fax según el estándar G2 y G3 a través de Internet mediante el protocolo de red IFP (Internet Facsimile Protocol).

Por norma general, la UC Suite puede procesar hasta 8 conexiones de fax simultáneas. OpenScape Business X3/X5/X8 como gateway RDSI puede procesar de 3 a 12 faxes simultáneos en función del módulo DSP. Los dos parámetros determinan el número de conexiones de fax T.38 o G.711 simultáneas.

Nota: Si es posible, se recomienda utilizar fax T.38.

El sistema ofrece compatibilidad para T.38 o G.711 en las siguientes situaciones:

- Una extensión recibe mensajes de fax a través de un proveedor de servicios de telefonía por Internet (ITSP) en su buzón de fax y realiza los envíos externos con Fax Printer a través del ITSP.
- Una extensión recibe mensajes de fax a través de Mediatrix 4102S (SIP) en su buzón de fax y realiza los envíos con Fax Printer a través de Mediatrix 4102S (SIP).
- Una extensión recibe mensajes de fax a través de un proveedor de servicios de telefonía por Internet (ITSP) en un dispositivo de fax conectado directamente a una interfaz RDSI o analógica. Realiza los envíos externos con ese dispositivo de fax a través del ITSP.
- Una extensión recibe mensajes de fax a través de un ITSP en un dispositivo de fax conectado a Mediatrix 4102S y realiza los envíos externos desde ese dispositivo de fax a través de Mediatrix 4102S e ITSP.
- Una extensión recibe mensajes de fax a través de RDSI en un dispositivo de fax conectado a Mediatrix 4102S y realiza los envíos externos desde ese dispositivo de fax a través de Mediatrix 4102S y RDSI.
- Una extensión envía mensajes de fax desde un dispositivo de fax conectado a Mediatrix 4102S y lo hace a otro dispositivo de fax que también está conectado a Mediatrix 4102S.
- Mensaje de fax interno desde un dispositivo de fax conectado a una interfaz RDSI y destinado a un dispositivo de fax conectado a Mediatrix 4102S, y a la inversa.
- Mensaje de fax interno desde un dispositivo de fax conectado a una interfaz RDSI y destinado a un buzón de fax, y a la inversa.

Nota: Para el buzón de voz, hay que activar T.38 en el sistema. En el envío de fax desde el sistema de comunicación a través de un ITSP, éste debe ser compatible con T.38. Si el ITSP no puede conmutar a T.38, el fax se tratará como G.711.

13.11.8.1 Cómo activar o desactivar Fax over IP (Fax T.38)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Gateway de voz**.
3) En el grupo de menús, haga clic en **Gateway voz**.
4) En el grupo de menús, haga clic en **Parámetros codec**.
5) En la sección **Fax T.38** seleccione una de estas opciones:
   - Si desea activar Fax over IP (Fax T.38), active la casilla de verificación **Fax T.38**.
   - Si desea desactivar Fax over IP (Fax T.38), desactive la casilla de verificación **Fax T.38**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

13.12 Descripción general de la integración de Microsoft Office 365

Puede trabajar de forma conjunta fácilmente con acceso desde cualquier lugar al correo electrónico, conferencias web, documentos y calendarios. Incluye seguridad de clase empresarial y está respaldado por Microsoft. Ya sea una pequeña empresa o una empresa multinacional, Office 365 ofrece planes diseñados para adaptarse a las necesidades exclusivas de su empresa. Para obtener más información, o una cuenta de 30 días, visite

OpenScape Business con Microsoft Office 365

Cuando un usuario configura una cita en su calendario de Microsoft Outlook, el sistema OpenScape Business comprueba automáticamente las palabras clave en los temas de las citas del calendario como: "reunión", "enfermo", "descanso," fuera de la oficina". Si encuentra dicha palabra clave, el sistema configura la presencia del usuario automáticamente cuando se alcanza la hora de la cita, incluso si la sesión de Microsoft Outlook de este usuario ya no está activa.

El usuario configura las citas con estas palabras clave y OpenScape Business configura la presencia telefónica del usuario automáticamente y reenvía las llamadas al buzón de voz o, por ejemplo, al teléfono móvil, según la configuración. El usuario también puede configurar en un estado de cliente general, si la presencia debe volver al estado En la oficina cuando finaliza la hora de la cita.

Esto también funciona incluso si el usuario no usa el cliente de Outlook local y programará una cita con las palabras clave mencionadas anteriormente directamente desde la página web de Outlook en la nube.

Reenvío de correo electrónico:

OpenScape Business puede enviar correos electrónicos a Microsoft Office 365 incluido el servidor Microsoft Exchange,

lo que permite a los usuarios recibir correos electrónicos para nuevos mensajes de voz, faxes o conferencias telefónicas con la capacidad de realizar automáticamente sesiones de colaboración web desde OpenScape Business.

OpenScape Business genera correos electrónicos para dichas acciones y mantiene a los usuarios actualizados también por correo electrónico, si dicha nueva notificación llega al cuadro de mensajes de OpenScape Business.

13.12.1 Cómo conectar el sistema OpenScape Business a Microsoft Office 365 mediante autenticación básica

Puede conectar el sistema OpenScape Business a Microsoft Office 365 en la nube mediante autenticación básica para utilizar la integración del calendario OpenScape Business Exchange y el reenvío de correo electrónico del Microsoft Exchange Server integrado en Microsoft Office 365.

Requisitos previos

- Microsoft Office 365: Office 365 Enterprise E3 con el conocido conjunto de aplicaciones "Microsoft Office Professional Plus" instaladas localmente y el uso de las aplicaciones de Office Web.
- Los usuarios están disponibles en Microsoft Office 365 y conectados con el Microsoft Outlook local con el correo electrónico asignado; al que se accede en Microsoft Exchange de Microsoft Office 365.
- Se instalan todas las actualizaciones y paquetes de servicio de Microsoft disponibles.
- Consulte las licencias de Microsoft Enterprise adecuadas que se necesitan.
- Consulte la nota de la versión de OpenScape Business para conocer las versiones publicadas de Microsoft Office.
- Microsoft Office y las aplicaciones de Office Web deben instalarse localmente.

Avisos importantes:

- Cambie el valor del dominio de Microsoft Office 365 (ejemplo: test.onmicrosoft.com) para que coincida con la configuración de su entorno.
- El usuario "oso" se utiliza en este ejemplo como cuenta de servicio con el privilegio de función para "ApplicationImpersonation" que se utiliza para dar acceso a OpenScape Business a la base de datos de buzones de correo del servidor Microsoft Exchange. Este usuario debe añadirse al directorio de usuarios de Microsoft Office 365 como se muestra más adelante. Asimismo, requiere una dirección de correo electrónico configurada.
- La conocida "búsqueda de contactos de carpetas públicas de Microsoft Exchange" de Openscape Business Client está disponible, porque Microsoft Office 365 ofrece esta funcionalidad.

Paso a paso

1) Regístrese en **Microsoft Office 365 Enterprise E3** en la página web oficial de Microsoft.

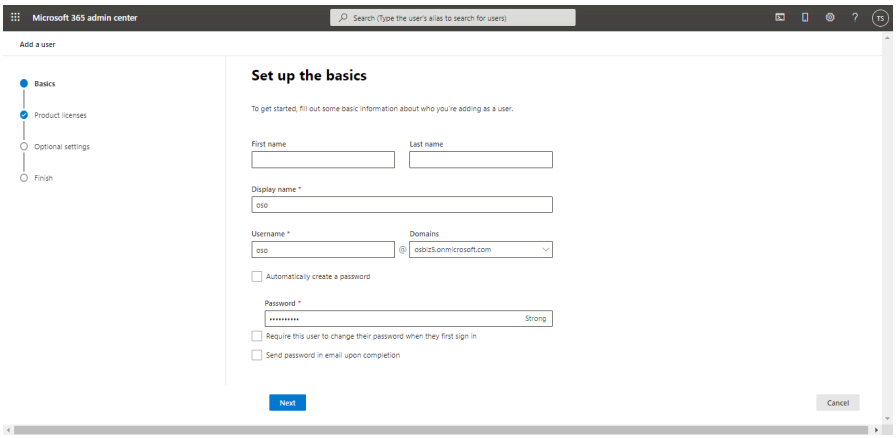
   a) Asigne derechos de administrador global al usuario "oso".

2) Inicie sesión en Centro de administración de Microsoft 365 y navegue a **Usuarios > Usuarios activos** agregue el usuario "oso" y pruebe los

usuarios "usuario1-usuario3" y asigne direcciones de correo electrónico válidas.

Siga el asistente de configuración para configurar los usuarios.

Añada derechos de administrador global al usuario "oso".



3) Cierre sesión en el centro de administrador de Microsoft 365 e inicie sesión con el nuevo usuario creado "oso" para cambiar la contraseña temporal.

Compruebe que el usuario "oso" tenga acceso a la página del administrador: **Salud> Salud del servicio**. Después de que se complete la verificación del estado del servicio sin problemas importantes, cierre la sesión y vuelva a iniciar sesión con el administrador de Microsoft 365.

Asegúrese de que los usuarios estén disponibles en el directorio de usuarios de Microsoft Office 365 y que ya hayan iniciado sesión en su perfil una vez para cambiar las contraseñas temporales y puedan iniciar sesión en su buzón de correo de Microsoft Office 365 con el Microsoft Outlook instalado localmente. Esta instalación local de Microsoft Office 365 debe estar conectada al portal de Microsoft Office 365 e instálela y actualícela con todas las actualizaciones de Microsoft disponibles.

4) Descargue Microsoft Office desde el portal de Microsoft Office 365, si aún no lo ha hecho. Instálelo y actualícelo con las últimas actualizaciones de Microsoft disponibles.

5) Configure el usuario "oso" como usuario privilegiado para poder acceder a los calendarios de usuarios para la **Integración de calendarios de Exchange**.

a) En un ordenador con Microsoft Windows 10, abra PowerShell en modo ampliado:

- Abra el menú de inicio y escriba "Power". El comando de "Windows PowerShell" está marcado.
- Mantenga presionadas las teclas Shift + Ctrl y use la tecla Enter para iniciar PowerShell.
- Pulse Sí en el mensaje entrante de UAC para iniciar PowerShell.

b) Compruebe si la política de ejecución local permite el uso de secuencias de comandos en el ordenador: `Get-ExecutionPolicy`

c) Si el resultado no es "RemoteSigned", ejecute el comando: `Set-ExecutionPolicy RemoteSigned`. Si da error, verifique que los

privilegios en este ordenador le permitan cambiarlo y que haya iniciado PowerShell en modo ampliado.

d) Ejecute las líneas de comando para iniciar sesión en el servidor Microsoft Exchange en línea e inicie sesión con su cuenta de administrador principal de Microsoft Office 365:

```
$LiveCred=Get-Credential Import-PSSession $Session -
AllowClobber
```

```
$Session = New-PSSession -ConfigurationName
Microsoft.Exchange -ConnextionUri https://
ps.outlook.com/powershell/-Credential $LiveCred -
Authentication Basic -AllowRedirection
```

```
Import-PSSession $Session -AllowClobber
```

e) Configure Microsoft Office 365: `Enable-OrganizationCustomization`

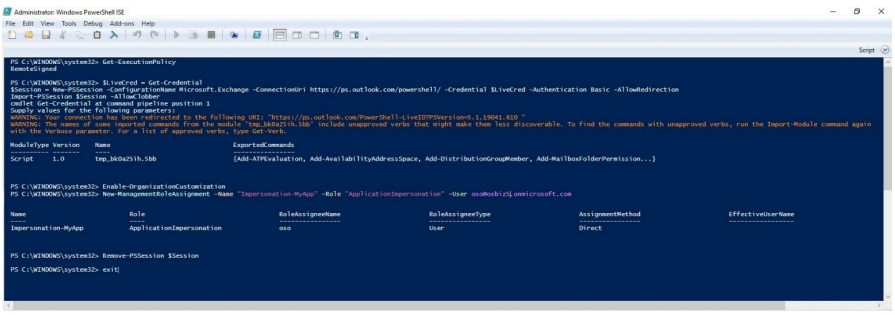
f) Cambie el valor de usuario privilegiado para que coincida con la configuración de su entorno: `New-ManagementRoleAssignment -Name "Impersonatipon-MyApp" -Role "ApplicationImpersonation" -User oso@osbiz5.onmicrosoft.com`

g) Verifique el valor establecido: `Get-ManagementRoleAssignment "Impersonatipon-MyApp"`

h) Salir de la sesión real: `Remove-PSSession $Session exit`

PowerShell se cierra después del comando Salir. Si PowerShell se cierra antes de introducir `Remove-PSSession $Session`, es posible que se bloquee un nuevo acceso durante 15 minutos.

Nota: Asegúrese de que los comandos funcionen y no se muestren mensajes de error rojos durante la ejecución.



Nota: Para obtener más detalles sobre el uso de PowerShell, consulte la ayuda de Microsoft Office 365.

---

6) Inicie sesión en el portal de Microsoft Office 365: www.office.com e inicie sesión con el usuario "oso" para obtener la información y seleccione **Outlook** del árbol de la izquierda. Luego navegue hacia **Configuración> Ver todas las configuraciones de Outlook> Correo> Sincronizar correo electrónico**.

Anote el nombre del servidor y el puerto de la configuración SMTP. Por ejemplo, smtp.office365.com y 587. Necesitará esta información para los siguientes pasos.

7) Navegue a **WBM > Configuración > UC Suite > Configuración de proveedores externos > Integración de calendario de Exchange** y aplique la siguiente configuración para conectarse con el servidor de Microsoft Office 365:

   a) Haga clic en la casilla de verificación **Activar integración del calendario de Exchange**.
   b) En la lista desplegable **Método de autenticación**, seleccione **Básico**.
   c) Introduzca la **URL del servidor**. Por ejemplo: https://outlook.office365.com/ews/exchange.asmx
   d) Introduzca el **Nombre de usuario** del usuario privilegiado configurado en el directorio de Microsoft Office 365.
   e) Introduzca la **Contraseña** del usuario privilegiado configurado en el directorio de Microsoft Office 365.
   f) Haga clic en **Guardar**.

   Estos cambios otorgarán acceso de OpenScape Business al servidor Microsoft Exchange dentro de Microsoft Office 365 para la integración de calendarios de Exchange.

   Nota: El campo **Proveedor de contactos> Exchange** debe llenarse con la dirección de Exchange en línea: https://outlook.office365.com/ews/exchange.asmx y la dirección de correo electrónico del administrador global (oso@osbiz5.onmicrosoft.com en este ejemplo), para poder para buscar contactos en carpetas públicas.

   ---

8) Navegue hacia **Centro de servicios> Transferencia de correos electrónicos** para activar el acceso al correo desde OpenScape Business a Microsoft Office 365

   a) Introduzca la dirección del servidor de Microsoft Office 365 en el campo **Servidor de correo saliente (SMTP)**, el **Puerto del servidor de correo saliente** y active **Este servidor requiere una conexión encriptada (TLS/SSL)** en el área **información de servidor**.
   b) En la lista desplegable **Método de autenticación**, seleccione **Básico**.
   c) Indique el **Nombre de usuario/Contraseña** y pulse **Confirmar contraseña** del usuario privilegiado en Microsoft Office 365 en el área **Información de inicio de sesión**.
   d) Introduzca la **Dirección de correo electrónico** del usuario privilegiado en Microsoft Office 365 en el área **Información de usuario (remitente)**.
   e) Ingrese la dirección de correo electrónico **1** y **Dirección de correo electrónico 2** en el área de destinatarios de notificación de cambio de ALI.
   f) Haga clic en **Aceptar & Siguiente**.
   g) Haga clic en **Probar transferencia** para comprobar que la función funciona.

9) Instale la configuración del cliente de OpenScape Business:

   Desde febrero de 2020, la autenticación OAuth está disponible para conexiones POP3, IMAP4 y SMTP AUTH para Exchange Online. Por lo tanto, es necesario habilitar el envío SMTP de cliente autenticado (SMTP AUTH) en Exchange en línea. Siga las instrucciones en: https://

docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission

Asimismo, es necesario suplantar a los usuarios. Inicie sesión con admin@osbiz5.onmicrosoft.com en Office 365 y navegue hacia la página del administrador en el árbol de la izquierda. Se abrirá una nueva pestaña de ventana. En la nueva ventana, en "Centros de administrador", navegue hacia "Exchange". La pestaña de la nueva ventana se abre de nuevo y en "Roles" en el árbol de la izquierda otra vez, vaya a la pestaña "Roles del administrador" y haga clic en "Añadir grupo de roles". Póngale un nombre y presione siguiente. Haga clic en la viñeta "Suplantación de la aplicación" y luego en "siguiente". Por último, añada los usuarios al grupo y finalice.

Asegúrese de que el paquete de Microsoft Office esté instalado en el ordenador del usuario y conectado a Microsoft Office 365 y, si aún no lo ha hecho, instale CommunicationsClients con al menos la opción myPortal for Outlook.

a) Abra la siguiente ruta en el Explorador de Windows: \\198.6.127.12\applications\install-common\CommunicationsClients.exe

   Sintaxis: \\<Openscape Business ip-address>\applications\install-common\CommunicationsClients.exe

b) Inicie sesión con las credenciales de WBM y siga el asistente de configuración para instalar al menos la opción myPortal for Outlook.

10) Abra Microsoft Outlook e inicie sesión con las credenciales del usuario en el sistema OpenScape Business con los clientes de OpenScape Business. Para obtener más detalles, consulte la guía del usuario de myPortal for Outlook.

Nota: Además, puede utilizar la opción **Instalación silenciosa** para instalar CommunicationsClients desatendido en los ordenadores de los usuarios. Para obtener más información, consulte Instalación/desinstalación silenciosa para clientes de PC de la UC Suite en la página 554.

---

11) Navegue hacia **WBM> Configuración> UC Suite> Directorio de usuario** para añadir la dirección de correo electrónico del usuario.

OpenScapeBusiness enviará automáticamente un correo de "Bienvenida" a todas las nuevas direcciones de correo introducidas con esta configuración.

Nota: También puede realizar este paso en **WBM> Configuración> UC Suite> Directorio de usuario**.

Nota: Se necesita una dirección de correo válida configurada para usar Integración en el calendario de Exchange y también para la notificación por correo opcional cuando el usuario recibe un mensaje de OpenScape Business.

Repita este paso para todos los usuarios.

12) Navegue hacia **WBM> Configuración> UC Suite> Perfiles** para configurar la función **Integración de calendarios de Exchange**.
    a) Seleccione el usuario al que le desea activar la función, haga clic en **Editar** y luego haga clic en **Mis preferencias> conectividad de Outlook**.
    b) Seleccione la opción **Integración de calendarios de Exchange** en **Integración en el calendario**
    c) Haga clic en la casilla de verificación **Generar automáticamente citas de calendario a partir de mis cambios de presencia**
    d) Seleccione **PST Exchange** desde la lista desplegable.

    Repita este paso para todos los usuarios.
13) Navegue hacia **WBM> Configuración> UC Suite> Perfiles**. Seleccione el usuario que desea configurar y haga clic en **Notificación de buzón de voz**, para configurar si las notificaciones de correo de voz se enviarán en estados de presencia específicos, cuando se guarde un nuevo mensaje de voz en el buzón del usuario.

    Repita este paso para todos los usuarios. Este paso es opcional.
14) Navegue hacia **WBM> Configuración> UC Suite> Perfiles**. Seleccione el usuario que desea configurar y haga clic en **Notificación de fax**, para configurar si las notificaciones de fax se enviarán en estados de presencia específicos, cuando se guarde un nuevo fax en el buzón del usuario

    Repita este paso para todos los usuarios. Este paso es opcional.

13.12.2 Cómo conectar el sistema OpenScape Business a Microsoft Office 365 con el método de autenticación moderna

Puede conectar su sistema OpenScape Business a Microsoft Exchange Online/Office 365 con la autenticación moderna (autorización basada en token de Microsoft OAuth 2.0) para utilizar las funciones de reenvío de correo electrónico, integración del calendario de Exchange, integración del directorio de Exchange y colas de correo electrónico.

Puede encontrar instrucciones detalladas sobre cómo configurar la conexión en la wiki de Unify Experts, en `https://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Office_365`.

13.12.3 Cómo comprobar que las funciones de integración de Microsoft Office 365 están configuradas

Dirección de correo electrónico:

Puede comprobar la función de correo electrónico con el botón **Probar transferencia** desde el área **Centro de servicios> Transferencia de correos electrónicos** en WBM. Introduzca una dirección de correo válida como destinatario y verifique la recepción del correo de prueba en la bandeja de entrada de esta cuenta de correo.

Integración de calendarios de Exchange:

Cuando los usuarios configuran citas en su calendario de Microsoft Outlook, el sistema OpenScape Business comprueba automáticamente las palabras clave en los temas de las citas del calendario como: "Reunión", "Enfermo", "Descanso", "Fuera de la oficina", "Vacaciones", "Almuerzo" o "En casa". Si se encuentra dicha palabra clave, el sistema establece el estado de presencia del usuario automáticamente cuando se alcanza la hora de la cita, incluso si la sesión de Microsoft Outlook de dicho usuario ya no esté activa. El usuario simplemente configura las citas con estas palabras clave y OpenScape Business establecerá la presencia del teléfono automáticamente y reenviará las llamadas al buzón de voz o, por ejemplo, al teléfono móvil, según la presencia establecida y el destino de transferencia deseado por el usuario. El usuario también puede configurar en una configuración de cliente general, si la presencia debe cambiarse de nuevo a "En la oficina" cuando finaliza la hora de la cita, lo que también funcionará, incluso si el usuario no utiliza el cliente de Outlook local y configura la cita con las palabras clave del tema mencionadas anteriormente directamente en la página web de Outlook en Outlook Web Access (OWA).

El usuario que utiliza Exchange o la integración del calendario de Outlook local debe tener una dirección de correo electrónico válida en la configuración de su cliente de UC Suite, así como la configuración de Outlook del cliente de UC Suite establecida en el manual anterior. Es obligatorio que la combinación entre los usuarios de UC Suite y los de Exchange se realice mediante la dirección de correo introducida.

La configuración de idioma del buzón de voz de los usuarios de UC Suite se utiliza para combinar palabras clave como: "Reunión", "Enfermo", "Descanso", "Fuera de la oficina", "Vacaciones", "Almuerzo" o "En casa" según la configuración de idioma del usuario, por ejemplo, si se selecciona el idioma alemán en el buzón de voz, las palabras clave en alemán aparecerán en la línea de asunto de las citas como "Besprechung", "Krank", "Pause", "AuEer Haus", "Urlaub", "Mittag" o "Zu Hause" únicamente.

Si no se utiliza la opción "Vuelta autom. a la oficina", la presencia del usuario se mantendrá en el estado establecido después de que finalice la hora de la cita y la hora de regreso que se muestra a otros usuarios o personas que llaman aumentará cada 15 minutos. Si se usa la opción "Vuelta autom. a la oficina" y la hora de la cita finaliza, la presencia del usuario vuelve a establecerse automáticamente como "En la oficina".

Las citas programadas en el futuro con menos de 3 minutos se ignoran, porque el sistema espera que el usuario esté creando una nueva cita allí, todo puede cambiar en esos 3 minutos. El sistema de comunicación comprueba las citas en los calendarios de los usuarios cada 30 segundos. Por este motivo y por posibles retrasos entre el sistema de comunicación y el servidor Exchange, intente utilizar citas de prueba con más de 3,5 minutos. En las pruebas, las citas programadas en el futuro con más de 5 minutos funcionan perfectamente para evitar los pequeños retrasos entre el sistema de comunicación y el servidor Exchange y el retraso de lectura de 30 segundos de las solicitudes de lectura del calendario.

Los valores de las nuevas citas se leen completamente en el minuto en que se establece la hora de inicio de la cita en las consultas de 30 segundos antes mencionadas. Así que, en caso de que se alcance la hora de inicio, tenga en cuenta que la consulta de 30 segundos debe realizarse dentro de este minuto y luego se configura la presencia. La consulta también establece la hora de regreso de los usuarios de acuerdo con la hora de finalización de la cita.

Si desea probar la funcionalidad cuando myPortal for Outlook o myPortal for Desktop estén cerrados para el usuario, solo tendrá que usar la página web de Outlook en Outlook Web Access (OWA). Inicie sesión con las credenciales de los usuarios y añada la cita con la palabra clave al calendario. Verifique en el cliente de otro usuario UC Suite que la presencia cambia cuando se alcanza la hora de la cita.

14 Funciones del teléfono

El sistema de comunicación ofrece numerosas prestaciones de telefonía. El listado es muy amplio. Podría comenzar, por ejemplo, con las funciones de Retener, Alternar y Consulta, pasando por distintas señalizaciones de llamada y para terminar, por ejemplo, con Transferencia automática diferida y Desvío de llamadas.

14.1 Llamar

El sistema de comunicación ofrece distintas opciones para realizar llamadas, entre otras, la llamada directa o la marcación abreviada.

14.1.1 Marcación de dígitos

Con la marcación de dígitos, la marcación de cada cifra se emite directamente después de la entrada.

La conexión comienza a establecerse inmediatamente al introducir el primer dígito. De esta forma, la extensión no puede editar la marcación.

14.1.2 Marcación en bloque

En la marcación en bloque, la conexión se establece si se indica el número de teléfono completo. El número de teléfono se transmite en un único bloque.

El envío de la marcación se puede iniciar con el código de fin de marcación #.

La marcación en bloque es de uso obligatorio para:

- Conexión de línea urbana ITSP
- Conexión múltiple primaria RDSI en EE. UU.

Si en un tiempo de 5 segundos no se introducen más cifras, la última cifra introducida se interpretará como la última cifra del bloque de número de teléfono.

14.1.3 Marc. tecl. num.

En distintos países los servicios de conexiones digitales de línea urbana se controlan a través de la marcación por teclado numérico (Keypad) y no por funciones. Para activar estos servicios en el PSTN, se puede utilizar la denominada interfaz Stimulus.

La prestación se tiene que configurar en Manager E.

En la extensión, el intercambio de mensajes se confirma mediante indicaciones en pantalla. De igual forma, la marcación con teclado numérico solo se puede hacer con teléfonos con display (optiPoint, OpenStage), teléfonos móviles (Cordless) con guía de menús optiPoint y teléfonos IP con interfaz Stimulus. Los teléfonos RDSI no son compatibles. El proveedor de red correspondiente

determina qué servicios se pueden utilizar a través de la marcación con teclado numérico.

Las extensiones autorizadas puede activar la marcación con teclado numérico mediante el menú de servicios o con el código *503. Solo se puede hacer desde el estado de reposo. A continuación hay que marcar una línea urbana RDSI para ejecutar la prestación.

En función de los mensajes enviados desde la línea urbana (p. ej., con Connect) la marcación con teclado numérico puede generar entradas en el registro de datos de llamada. Se registra el número de teléfono de la extensión llamante, la línea utilizada y el tiempo de uso de la prestación.

Nota: Las acciones ejecutadas con la marcación con teclado numérico no son controladas por el sistema. Así pues, el sistema no puede impedir forma de uso abusivas (como abuso de tarifas o bloqueo de línea urbana).

Hay que informar al cliente de que será responsable de los daños que pudiera originar un mal uso de esta prestación.

14.1.4 Identificación de fin de marcación

El fin de marcación se reconoce automáticamente tras 5 segundos o bien es el usuario quien lo señala manualmente mediante el código de fin de marcación "#".

14.1.5 Editar marcación

Con la función Editar marcación, el usuario puede modificar los dígitos indicados del número de teléfono. Esta función es habitual en los teléfonos móviles. Un número de llamada se puede corregir solo durante la entrada.

Después de introducir una secuencia de dígitos, el usuario puede editarla de derecha a izquierda pulsando una tecla. Cada vez que pulsa la tecla se borra un dígito. Una vez introducida la secuencia correcta de dígitos se puede proceder a transmitir la marcación pulsando la tecla de confirmación o descolgando el microteléfono.

No se puede editar un número de teléfono guardado, por ejemplo, para Rellamada.

Consejo: Todos los usuarios pueden activar individualmente la función Editar marcación.

Interdependencias

Tema	Interdependencia
Aviso llam. en espera	Durante la edición se puede recibir un aviso de llamada en espera porque el teléfono se encuentra en estado de recepción de marcación y, por tanto, ocupado para el tráfico entrante.

Tema	Interdependencia
Consulta	Después de una llamada de consulta, el teléfono se encuentra en estado de recepción de marcación. Entonces se pueden editar dígitos de número de teléfono.

14.1.5.1 Cómo activar o desactivar Editar marcación

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el grupo de menús, haga doble clic en **Extensiones**.
4) En el grupo de menús, haga clic en la extensión (Índice - Número de teléfono - Nombre).
5) Haga clic en la pestaña **Editar flags exten.**
6) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Editar marcación**.
   - Si desea desactivar la función, desactive la casilla de verificación **Editar marcación**.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.1.6 Remarcar botón

Cada vez que se establece una llamada externa se guarda el número de teléfono marcado. Si el destino estuviera ocupado o no se lograra establecer comunicación con él, el usuario puede usar la Rellamada para volver a marcar el mismo número.

En la memoria de rellamada también se escriben números de marcación directa.

Sin embargo, la marcación de números de teléfono internos no afecta la memoria de rellamada.

Las posibles cifras de marcación posterior (también denominadas señales por multifrecuencia) no se consideran información de marcación y, por tanto, no se guardan (p. ej. dígitos enviados a un buzón de voz conectado).

La función de rellamada solo se puede activar a través de la tecla, y no a través de un código de acceso.

Al pulsar la tecla de rellamada pueden demandarse selectivamente estos números de teléfono y utilizarse de nuevo para establecer una comunicación. Si se pulsa la tecla una vez, se marca el último número de teléfono marcado. Si se pulsa la tecla dos veces, se marca el penúltimo número de teléfono marcado. Si se pulsa la tecla tres veces, se marca el último número de teléfono marcado.

Después de pulsar la tecla de rellamada, se marca automáticamente el número de teléfono guardado tras 2 segundos. Si necesitara más tiempo para leer los números de teléfono mostrados, seleccione "hojear" con la tecla de confirmación. Cada vez que se pulsa la tecla "Continuar" se muestra el siguiente número de teléfono guardado. El número de teléfono solo se marca al seleccionar el comando "Llamar". De esta forma tendrá más tiempo para comprobar que ha elegido el número de teléfono correcto.

Si se hace una llamada mediante LCR, solo se memoriza el número marcado por la extensión.

Los códigos de proyecto también se depositan en la memoria de rellamada. Para ello se ajustará el flag correspondiente para todo el sistema.

14.1.6.1 Cómo activar o desactivar la repetición de llamada automática

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema**.
4) Haga clic en **Flags del sistema**.
5) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Repetición de llamada automática**.
   - Si desea desactivar la función, desactive la casilla de verificación **Repetición de llamada automática**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.1.7 Marcación abreviada central

Los números de teléfono externos frecuentes se pueden guardar en el sistema de comunicación. Cada número está representado por un número de marcación abreviada que se utiliza en lugar del número de teléfono completo.

Los números de marcación abreviada son números de 4 cifras.

Por defecto, todas las extensiones se encuentran en un grupo al que están asignados todos los números de marcación abreviada. De esta forma, todas las extensiones pueden utilizar todos los destinos de marcación abreviada.

La marcación abreviada central (KWZ) ignora las reglas de acceso a la red urbana. Tenga en cuenta que marcar un destino de marcación abreviada encontrado durante una búsqueda en la agenda interna no anulará las reglas de restricción de llamadas.

El administrador configura y ordena en grupos los números de marcación abreviada central. Cada usuario puede estar asignado a uno de estos grupos. Un usuario únicamente puede utilizar los números de marcación abreviada del grupo que tenga asignado. Se puede asignar a un grupo un área de destinos de marcación abreviada.

Las entradas de los destinos de marcación abreviada se pueden buscar por nombre y apellidos si hay configurado un nombre con formato <Apellidos>, <Nombre> o <Nombre>, <Apellidos>.

Los números de marcación abreviada marcados se anotan en la memoria de rellamada.

Para programar una "Pausa interdigital" y una conmutación MF para la marcación posterior de señales por multifrecuencia (MF) se utiliza la "tecla P" de rellamada o bien la "tecla #".

La tecla de rellamada del cliente debe definirse como: <número_marcación><dígito_dtmf><dígito_pausa><código_acceso> p. ej.: 008007728477#P2210344

Conversión de números de llamada en nombres

Se puede asignar un nombre a cada destino de marcación abreviada. Si está establecida la indicación del número llamante (CLIP), en cuanto llama un número de teléfono guardado, el sistema establece automáticamente el nombre y es éste, y no el número de teléfono, el que aparece en el display.

Marcación posterior

La marcación posterior no se permite para la emisión de la marcación por bloques, por ejemplo una configuración de ITSP. Se permite en una emisión de la marcación por pasos.

Nota: El campo de emisión de marcación se cambia en Gestión basada en Web (WBM) con **Modo Experto > Líneas/ Interconexión > Ruta**

Es posible realizar una marcación posterior:

- Marcación posterior manual

  Después de marcar el código de acceso e indicar el número de índice (número de marcación abreviada), el usuario puede marcar otras cifras. Estas se agregan al número de teléfono almacenado bajo el índice en cuestión y se marcan a continuación.
- Marcación posterior automática

  Al configurar un destino de marcación abreviada, el número indicado se puede dividir en 2 partes. Se utiliza "-" como separador. La primera parte siempre se emite. Comienza entonces el temporizador. Si el usuario no marca más dígitos antes de que expire el temporizador, se marcará automáticamente la segunda parte del número introducido. De otra forma, se transmiten los dígitos marcados manualmente.

  Por ejemplo: SSD = 7007–0

  Si el usuario no marca ningún número de marcación directa tras solicitar el destino de marcación abreviada (marcación posterior manual) y antes de que expire el temporizador, se marcará automáticamente el 0 (marcación posterior automática).

Importar números de marcación abreviada

Puede importar números de marcación abreviada de un archivo XML en formato UTF-8. Los números de marcación abreviada ya existentes se borran antes de la importación.

Puede consultar una plantilla XML con la correspondiente explicación en la Gestión basada en Web (WBM), en **Centro de servicios** > **Documentos** > **Plantillas CSV**. En estas plantillas puede registrar sus destinos de marcación abreviada, por ejemplo con Microsoft Excel.

Nota: Ya no se recomienda importar listas de marcación abreviada desde archivos CSV y solo se admite en casos especiales.

Exportar números de marcación abreviada

En calidad de administrador con el perfil **Experto**, puede exportar números de marcación abreviada a un archivo XML en formato UTF-8 mediante el **modo Experto**. Siempre se exportan todos los registros de datos.

14.1.7.1 Cómo añadir un destino de marcación abreviada

El asistente **Listín telefónico/Marcación abreviada** permite agregar destinos de marcación abreviada para la marcación abreviada central.

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Listín / Marcación abreviada**.
4) En una línea de tabla libre, introduzca el número de **Marcación abreviada**, el **Número de llamada** y el **Nombre** del destino de marcación abreviada.
5) Si desea añadir más destinos de marcación abreviada, haga clic en **Guardar datos** y repita el paso anterior.
6) Haga clic en **OK & Continuar**.
7) Haga clic en **Salir**.

14.1.7.2 Importar destinos de marcación abreviada de un archivo XML

El asistente **Listín telefónico/Marcación abreviada** permite importar números de marcación abreviada y números de teléfono desde un archivo XML.
Los números de marcación abreviada ya existentes se borran antes de la importación.

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

Hay disponible un archivo XML en formato UTF-8 con números de marcación abreviada. Puede encontrar una plantilla XML para importar números de marcación abreviada en **Centro de servicios** > **Documentos** > **Plantillas CSV.**

Nota: Ya no se recomienda importar listas de marcación abreviada desde archivos CSV y solo se admite en casos especiales.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Listín/Marcación abreviada**. Se abre la ventana **Editar registro del listín central**.
4) Haga clic en **Importar/Exportar datos CSV/XML**.
5) En el área **Importar archivo CSV/XML a través de HTTP**, haga clic en **Examinar** para seleccionar el archivo deseado.
6) Haga clic en **OK**. Los números de marcación abreviada existentes se borran y los números de marcación abreviada registrados en el archivo XML se importan en el sistema.
7) Haga clic en **Finalizar**.

14.1.7.3 Cómo exportar destinos de marcación abreviada a un archivo XML

Puede exportar números de marcación abreviada a un archivo XML. Siempre se exportan todos los datos.

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Listín / Marcación abreviada**. Se abre la ventana **Editar registro del listín central**.
4) Haga clic en **Importar/Exportar datos CSV/XML**.
5) En el área **Exportar un archivo xml a través de HTTP** haga clic en **Descarga**. La lista de los números de marcación abreviada se prepara la descarga.
6) Seleccione un lugar de almacenamiento para el archivo y haga clic en **Guardar**.

14.1.7.4 Cómo editar destinos de marcación abreviada

El asistente **Listín telefónico/Marcación abreviada** permite editar destinos de marcación abreviada.

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Listín / Marcación abreviada**.
4) Para buscar una entrada, introduzca un término de búsqueda en los campos de búsqueda **Marc. abr.**, **Número de teléfono** o **Nombre** y, a continuación, pulse la tecla Intro. Se muestran todos los resultados que contienen el término de búsqueda. Si por ejemplo se escribe `521` como número de teléfono, aparecerían los resultados `+495213535` y `+498967521`. O por ejemplo, si se escribe `co` como nombre aparecerían los resultados `Collins`, `Mcoin` y `Branco`.

   Nota: Si no hay nada en ningún campo de búsqueda y se pulsa la tecla Intro, aparecen todas las entradas.

5) En la entrada de tabla deseada, modifique los valores de los campos **Marc. abr.**, **Número de llamada** o **Nombre**.
6) Si desea editar más destinos de marcación abreviada, haga clic en **Guardar datos** y repita el paso anterior.
7) Haga clic en **OK & Continuar**.
8) Haga clic en **Salir**.

14.1.8 Marcación abreviada individual (KWI)

Marcación abreviada individual permite a cada extensión almacenar 10 números de teléfono externos, además de los números de marcación abreviada central, como números de marcación abreviada individuales.

En los teléfonos sin display, después de introducir el número de teléfono el usuario debe esperar a oír un tono de confirmación.

En el pool de marcación abreviada individual se pueden programar números externos. El acceso depende de los niveles de acceso del usuario. Antes de introducir el número de teléfono, el usuario debe introducir el código de acceso a línea urbana (por ejemplo, 0).

Para programar una "Pausa interdigital" o una conmutación MF se utiliza la tecla de rellamada o bien la tecla de almohadilla (#).

14.1.9 Llamada directa

Se pueden configurar como teclas de llamada directa las teclas de función de un teléfono o aparato auxiliar. Para hacerlo, se programan las teclas con el número de teléfono de una extensión interna o de un grupo. Pulsando una de estas teclas se llama inmediatamente al destino programado (llamada directa). El estado actual de la extensión o del grupo se indica por el LED asociado a la tecla de llamada directa.

También se puede utilizar una tecla de llamada directa (también denominada tecla DSS o "Direct Station Selection") para transferir una llamada rápidamente a la extensión o grupo programados para tal fin. Al pulsar una tecla de llamada directa durante una llamada con un interlocutor externo, la comunicación actual se pasa a estado de consulta. El usuario que transfiere la llamada puede transferirla al destino de transferencia colgando el microteléfono (Transferencia ciega). También se puede esperar hasta que el destino de transferencia conteste para transferir la llamada (Transferencia de consulta). Si el destino de la transferencia no acepta la llamada, se activa una llamada recordatoria.

Estados del LED perteneciente a una tecla de llamada directa

El LED perteneciente a una tecla de llamada directa muestra el estado actual de la extensión programada:

- Apagado: el usuario pertinente no está realizando una llamada.
- Encendido: el usuario pertinente está realizando una llamada o ha activado el estado No molestar.
- Parpadea rápido: el usuario pertinente está realizando una llamada. La llamada se puede aceptar pulsando la tecla de llamada directa.
- Parpadea despacio: la extensión ha recibido una llamada y aún no la ha aceptado. La llamada se puede atender pulsando la tecla de llamada directa.

Interdependencias

Tema	Interdependencia
Teléfonos RDSI, Teléfonos SIP	En los teléfonos RDSI y SIP no se pueden programar teclas de llamada directa.

Conceptos relacionados

Configuración de equipo / Grupo Team en la página 720
Jefe/Secretaria / Grupo Top en la página 724

14.1.10 Mensaje directo / Contestación directa

El mensaje directo permite establecer una conexión interna sin que el usuario llamado tenga que descolgar el microteléfono. El altavoz del usuario llamado se activa automáticamente.

En los teléfonos con equipo manos libres (micrófono) el usuario llamado puede responder directamente activando el micrófono. Al descolgar el microteléfono se pasa a una llamada bipartita normal.

La prestación Mensaje directo se puede utilizar a través de una tecla de función programada para ello o a través de la opción de menú o código correspondientes. A continuación se deberá marcar el número de teléfono de la extensión de destino. También se puede programar una tecla de función con un número de teléfono de extensión. Después de pulsar una de estas teclas de función, se establece conexión inmediatamente con el destino programado.

El mensaje directo también permite hacer anuncios a todas las extensiones internas de un grupo.

La prestación Contestación directa se puede activar a través de la opción de menú ofrecida en el display o a través de una tecla de función programada para ello.

Se puede impedir el mensaje directo de una extensión activando el bloqueo de mensaje directo. En este caso, el mensaje directo se señaliza como una llamada normal.

Interdependencias

Tema	Interdependencia
No molestar, Romper No molestar	En las extensiones con el estado No molestar activado no se pueden enviar mensajes directos. Si el usuario que desea utilizar la prestación "Mensaje directo" está autorizado a romper el estado No molestar, escucha, durante cinco segundos, el tono de ocupado. A continuación, se llama a la extensión de destino, no se accede a ella directamente.
Alternar, Consulta, Transferencia	Las prestaciones citadas no se pueden utilizar directamente en una conexión Mensaje directo/ Contestación directa.
Teléfonos RDSI, Teléfonos SIP	Las prestaciones "Mensaje directo" y "Contestación directa" no se pueden utilizar con teléfonos RDSI o SIP.

14.1.10.1 Cómo activar o desactivar el bloqueo de mensaje directo para extensiones

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el grupo de menús, bajo **Extensiones** > **Extensión** > **…**, navegue hasta la extensión deseada (Índice - N.º de llamada - Nombre).
4) Haga clic en la pestaña **Editar flags exten.**
5) Elija una de estas opciones:
   - Si desea activar el bloqueo de mensaje directo para las extensiones, desactive la casilla de verificación **Bloqueo mens. directo desact**.
   - Si desea desactivar el bloque de mensaje directo para las extensiones, active la casilla de verificación **Bloqueo mens. directo desact.**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.1.11 Marcación asoc.

La marcación asociada permite a las extensiones autorizadas marcar un número de teléfono en representación de cualquier otra extensión. El efecto es el mismo que si fuera el otro usuario el que estuviera marcando el número de teléfono.

Se puede acceder a través de un código e indicando el usuario en nombre del que se quiere ejecutar la marcación. Los siguientes de dígitos se interpretan como si fuera el usuario previamente indicado el que los estuviera marcando.

14.1.12 Reserva de línea

Un usuario puede reservar una línea urbana si no hay disponible una línea urbana libre. En cuanto una línea urbana pasa a estar libre, se pone a disposición mediante una llamada recordatoria.

Si la extensión está ocupada en el momento de la llamada recordatoria, recibirá un aviso de llamada en espera. Si no se responde al aviso de llamada en espera, se elimina la reserva y se ofrece la línea al siguiente usuario de la lista de espera. Si el usuario ha activado el estado de no molestar antes de recibir la llamada recordatoria desde una línea urbana puesta en la lista de espera, se suprime la reserva de línea y se ofrece la línea urbana al siguiente usuario de la lista de espera.

Si varias extensiones activan la reserva de una línea urbana, la asignación de esta línea se lleva a cabo siguiendo el orden de la reserva.

Solo se acepta una solicitud de reserva o de lista de espera por teléfono. Si el usuario intenta realizar una segunda reserva, la primera será sobrescrita por ésta.

No se puede activar la prestación Reserva de línea si el intento de llamada se produjo a través de LCR (Ruta más económica).

La prestación Reserva de línea ignora cualquier Transferencia automática diferida de llamadas existente. Si en un plazo de 20 segundos no se responde a la llamada, se elimina la reserva de línea.

Una línea urbana en llamada recordatoria no se puede capturar – ni por "telecaptura selectiva" ni por "telecaptura de grupo".

La reserva de líneas puede activarse de estas formas:

- Las reservas manuales solo funcionan con teléfonos con display.
- Reservas automáticas (en todos los demás teléfonos)

  Si este flag está activado y no se asigna ninguna línea libre a un usuario con los procedimientos habituales de ocupación de líneas, se señaliza un tono de ocupado del lado del usuario. Tras 5 segundos suena un tono de confirmación positivo y la línea se reserva, siempre que el usuario disponga del acceso a la red urbana necesario.

Nota: Con teléfonos S_0, no se pueden reservar líneas.

14.1.12.1 Cómo activar o desactivar la reserva de línea

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema**.
4) Haga clic en **Flags del sistema**.
5) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Reserva de línea automática**.
   - Si desea desactivar la función, desactive la casilla de verificación **Reserva de línea automática**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.1.13 Línea privada

Una línea privada es una línea urbana que únicamente está disponible para una extensión.

14.2 Señalización de llamadas, Indicación del número de teléfono

El sistema de comunicación ofrece distintas opciones de señalización de llamada y de indicación del número de teléfono como, por ejemplo, CLIP, CLIR, COLP y COLR.

14.2.1 Señalización de llamadas diferencial

La señalización de llamadas diferencial permite distinguir entre llamadas internas y externas en el caso de las llamadas entrantes.

Las llamadas entrantes se señalizan de forma óptica y acústica en el teléfono. En el display aparecen estas indicaciones:

- El número del llamante
- En el desvío de llamadas interno: también el número de teléfono marcado en sí

Además, la llamada entrante puede indicarse a través de un LED. Hay distintas señales acústicas para las llamadas internas y externas.

Señalización de llamadas internas

Cada usuario puede tener asignada una de entre ocho posibles señalizaciones de llamada para llamadas internas. Así, la extensión utiliza el tono de llamada modificado para distinguir sus llamadas desde otras extensiones internas. Así, por ejemplo, se puede definir un tono interno especial para el gestor. De esta forma, todos los empleados reconocen, por el tono, que están recibiendo llamadas suyas.

Señalización de llamadas externas

Hay tres tipos de llamadas distintos que se distinguen acústicamente y que se pueden configurar para una llamada externa. De esta forma, por ejemplo, se pueden distinguir acústicamente las llamadas para dos grupos distintos, por ejemplo Ventas y Almacén.

- En Alemania, el administrador configura tres tipos de llamada diferentes para teléfonos analógicos, RDSI y del sistema.
- En otros países, los tipos de llamada de los teléfonos analógicos no tienen diferencias en la señalización.

14.2.2 Transmisión del número de teléfono del llamante (CLIP)

La función Transmisión del número de teléfono del llamante muestra el número de teléfono del llamante en la extensión llamada.

La función Transmisión del número de teléfono del llamante o CLIP (Calling Line Identification Presentation) se refiere a llamadas entrantes y debe admitirla el ofertante de red.

Si el nombre y el número de teléfono del llamante están guardados en la marcación abreviada central (KWZ) del sistema de comunicación, podrá ver el nombre en su pantalla.

Las prestaciones Transmisión del número de teléfono del llamante (CLIP) y Supresión de la indicación del número llamante (CLIR) se excluyen mutuamente. Es decir, si CLIP está activo, se desactiva CLIR, y a la inversa.

CLIP ajustable

CLIP ajustable transmite hacia el exterior un número de teléfono configurado para ello (por ejemplo, el número de teléfono de una línea colectiva) en lugar del número de teléfono del llamante (por ejemplo, un miembro de dicha línea colectiva).

Información específica de sistema

País	activo de forma predeterminada
EE. UU.	LIN (Location Identification Number). Si CLIP se activa para EE. UU., LIN se desactiva automáticamente.
Otros países	CLIP

14.2.2.1 Cómo activar o desactivar CLIP ajustable

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema**.
4) Haga clic en **Flags del sistema**.

5) Elija una de estas opciones:

- Si desea activar CLIP ajustable, active la casilla de verificación **CLIP ajustable**.
- Si desea desactivar CLIP ajustable, desactive la casilla de verificación **CLIP ajustable**.

6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.2.3 Supresión de la indicación del número llamante (CLIR)

La prestación Supresión de la indicación del número llamante suprime la indicación del número de teléfono del llamante en la extensión llamada.

Supresión de la indicación del número de llamada CLIR (Calling Line Identification Restriction) se refiere a las llamadas salientes. PSTN debe admitir la prestación. Supresión de la indicación del número llamante tiene prioridad frente a Transmisión del número de teléfono del llamado.

Las prestaciones Transmisión del número de teléfono del llamante (CLIP) y Supresión de la indicación del número llamante (CLIR) se excluyen mutuamente. Es decir, si CLIP está activo, se desactiva CLIR, y a la inversa.

CLIR y COLR solo se pueden activar y desactivar conjuntamente.

La supresión de la indicación del número llamante no tiene efecto con determinados destinos de llamada (por ejemplo, los números de emergencias de la policía o bomberos).

Supresión de la indicación del número de llamada a nivel de sistema

En calidad de administrador puede activar o desactivar la indicación CLIR a nivel de sistema.

Consejo: El flag "Supresión de la indicación del número de llamada en todo el sistema" no se aplica a los EE. UU.

Supresión de la indicación del número de llamada temporal

En calidad de usuario puede activar o desactivar la supresión de la indicación del número de llamada temporal. Esta supresión temporal solo se puede realizar si la supresión de la indicación del número de llamada está desactivada a nivel de sistema.

Suprimir el número de teléfono de la extensión

En calidad de administrador puede configurar para cada ruta que en lugar del número de teléfono de la extensión solo se transmita el número de teléfono del sistema.

14.2.3.1 Cómo activar o desactivar la supresión del número de teléfono de la extensión

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Ruta**.
4) Seleccione la **Ruta** correspondiente.
5) En **Número de teléfono del sistema saliente**, active la casilla de verificación **Suprimir núm. llam. de extensión**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.2.4 Presentación de identificación de línea conectada (COLP)

La presentación de identificación de línea conectada (COLP) transmite el número de llamada del abonado llamado al emisor de la llamada tan pronto como se conectan ambos.

COLP tiene sentido con el desvío de llamadas, por ejemplo, para que la persona que llama pueda ver el número de teléfono de la persona con la que se comunica realmente en lugar del número de teléfono marcado originalmente.

Las funciones de Presentación de Identificación de Línea Conectada (COLP) y Restricción de Identificación de Línea Conectada (COLR) son mutuamente excluyentes; es decir, tan pronto como se activa COLP, se desactiva COLR, y viceversa.

14.2.4.1 Cómo activar o desactivar Transmisión del número de teléfono del llamado

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Ruta**.
4) Seleccione la **Ruta** correspondiente.
5) Haga clic en la pestaña **Editar parámetros Special**.
6) Active la casilla de verificación **COLP**.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.2.5 Supresión de la indicación del número llamado (COLR)

Supresión de la indicación del número llamado suprime la indicación del número de teléfono de la extensión llamada en el llamante.

Supresión de la indicación del número llamado (COLR, "Connected Line Identification Restriction") se refiere a las llamadas entrantes.

Supresión de la indicación del número llamado (COLR) tiene prioridad sobre la transmisión del número de teléfono de la extensión llamada en el llamante.

Las prestaciones Transmisión del número de teléfono del llamado (COLP) y Supresión de la indicación del número llamado (COLR) se excluyen mutuamente. Es decir, cuando COLP está activo, COLR se desactiva, y a la inversa.

CLIR y COLR solo se pueden activar y desactivar conjuntamente.

14.2.6 CLIP no screening (transmisión de información de número de teléfono específico del cliente)

CLIP no screening en lugar del número de teléfono del llamante transmite un número de teléfono definido por el llamante.

El número de teléfono del sistema saliente no puede coincidir con el número de teléfono del sistema entrante.

Para aplicaciones de cliente especiales se puede activar el flag "Suprimir indicación del número de llamada de extensión". Así se impide que el número de marcación directa del usuario sea enviado con el número de teléfono del sistema saliente.

Ejemplo: No se debe poder acceder directamente a un empleado de servicios al que sí se puede acceder de forma central a través de un número de teléfono general del servicio técnico. Para ocultar el número de marcación directa a su extensión, el número de teléfono general del servicio técnico se registra como Número de teléfono del sistema saliente y se activa el indicador "Suprimir la indicación del número de llamada de extensión". El usuario llamado solo podrá ver el número de teléfono general del servicio técnico como CLIP.

Normalmente se utiliza el mismo número de llamada del sistema para llamadas entrantes y salientes. En tal caso, el registro bajo Número de teléfono del sistema saliente está vacío o es idéntico al Número de teléfono del sistema entrante. De no ser así, se puede

- introducir otro número bajo Número de teléfono del sistema saliente.
- utilizar el parámetro de ruta Tipo nº, saliente para definir si el número de teléfono del sistema saliente registrado incluye el número de extensión sin código de red local, con código de red local (nacional) o adicionalmente el prefijo de país internacional (internacional).

Consejo: La función CLIP no screening debe ser compatible y estar activada por el proveedor de red.

14.2.6.1 Cómo configurar CLIP no screening

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Ruta**.
4) Seleccione la **Ruta** correspondiente.
5) En **Número de teléfono del sistema saliente**, introduzca el **Nº teléfono del sistema** deseado.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.2.7 CLIP para terminales analógicos

CLIP para terminales analógicos transmite el número de teléfono de un terminal analógico de la extensión que realiza la llamada a la extensión llamada y a su indicación y los terminales aptos para ello. Es el denominado CLIP (Calling Line Identification Presentation o Indicación del número llamante en la extensión llamada) analógico.

Se puede configurar la transmisión adicional de la información de nombres CNIP (Calling Name Identification Presentation).

Consejo: CNIP depende del terminal. Tenga en cuenta las indicaciones del fabricante.

14.2.8 Llamada silenciosa / reposo

La prestación Llamada silenciosa / reposo señaliza las llamadas entrantes de forma sonora con un tono breve de advertencia y de forma visual en la pantalla.

Llamada silenciosa / reposo solo está disponible en teléfonos con pantalla y no tiene efecto alguno sobre la señalización de citas.

14.2.9 Conversión de números de teléfono en nombres en la marcación abreviada central

En las llamadas mediante marcación abreviada central (KWZ) y en las llamadas entrantes de destinos de marcación abreviada central, después de la marcación se muestra el nombre del destino de marcación abreviada en lugar del número de marcación abreviada.

14.3 Funciones durante la conexión

El sistema de comunicación ofrece distintas funciones durante la conexión, por ejemplo, retener, desviar o transferir llamadas.

14.3.1 Retener

La función Retener permite a los usuarios poner comunicaciones en espera. Durante ese tiempo, el llamante puede oír la música en espera o un anuncio grabado.

La retención finaliza al recuperar la comunicación en espera.

Estos son los tipos de retención:

- Retención general:

  Cualquier extensión puede recuperar la llamada pulsando una tecla de línea o de conversación.
- Retención exclusiva (solo con función Team o Top y en el Puesto de operadora)

  Solo puede recuperar la comunicación la extensión que inició la retención.

Retener y Llamada recordatoria

Una vez finalizado el temporizador **Tiempo para aparcar + transic. a retención** (valor estándar: 160 s), se produce una llamada recordatoria para las comunicaciones aparcadas.

14.3.2 Aparcamiento

La función Aparcamiento permite a los usuarios pasar una llamada a estado de espera. Durante ese tiempo, el llamante puede oír la música en espera o un anuncio grabado. Las llamadas aparcadas se pueden volver a aceptar desde cualquier teléfono.

En calidad de usuario asigne a las conexiones que va a aparcar una posición de aparcamiento (de 0 a 9) en el sistema de comunicación. Si dicha posición está ocupada, se emitirá un tono de confirmación negativo y la cifra no aparecerá indicada. A continuación, podrá seleccionar otra posición de aparcamiento. Para recuperar una llamada aparcada deberá indicar su posición de aparcamiento.

Las llamadas aparcadas se pueden recuperar mediante un código o con una tecla programada. También se pueden recuperar durante una llamada en curso.

Aparcamiento y Llamada recordatoria

Una vez finalizado el temporizador **Tiempo para aparcar + transic. a retención** (valor estándar: 160 s), se produce una llamada recordatoria para las comunicaciones aparcadas.

Aparcamiento y Desvío de llamadas

Una llamada aparcada no sigue un desvío de llamadas si se ha producido una llamada recordatoria.

Aparcamiento y DISA

Aparcamiento no se puede activar mediante DISA.

Aparcamiento y Conferencia

No se puede aparcar una conferencia.

Aparcamiento e Interconexión

Una llamada aparcada solo se puede volver a aceptar en el mismo nodo. Una llamada entrante a través de una interconexión solo puede aparcarse en el nodo de destino.

Aparcamiento y No molestar

Un usuario que ha activado la función No molestar puede asignar a una llamada una posición de aparcamiento. Si tiene lugar una llamada recordatoria a partir de una comunicación aparcada, y en la Gestión de llamadas no se ha estipulado ningún otro destino, la comunicación se cortará automáticamente tras expirar el temporizador de llamada recordatoria.

Nota: Encontrará instrucciones detalladas sobre cómo aparcar una llamada y sobre cómo recuperar una llamada aparcada en el capítulo pertinente de la guía de usuario del dispositivo en cuestión (guía del usuario de OpenStage X, HiPath/OpenScape 3000/4000).

14.3.3 Consulta

La función Consulta permite a los usuarios realizar una llamada durante una conversación en curso desde el mismo teléfono o aceptar una llamada puesta en espera. La primera llamada se mantiene, entre tanto, en espera.

Las consultas finalizan de esta forma:

- Nueva aceptación de la llamada retenida
- Desconectar

  De esta forma se consigue:

  – Transferir la llamada retenida o
  – Realizar una llamada recordatoria a la extensión retenida por parte del usuario que ha interrumpido la conexión

Consulta mediante tecla de llamada directa

Al pulsar una tecla de llamada directa durante una llamada se inicia una consulta al destino correspondiente.

Conexión de dos interlocutores externos

Durante una llamada se establece una consulta con un destino externo con la consiguiente transferencia de ambos interlocutores. Pueden generarse tasas de llamada.

14.3.4 Alternar

La función Alternar permite cambiar entre dos llamadas. Mientras se mantiene conversación con una de las extensiones, la otra se mantiene en espera.

Los usuarios pueden cambiar de una llamada a otra pulsando la tecla de línea correspondiente.

Alternar y Retener

Los usuarios en espera no pueden activar la comunicación alternativa.

14.3.5 Transferir

La función Transferir permite a las extensiones transferir sus llamadas a otro destino. En cuanto una extensión activa la transferencia, la extensión en espera se mantiene en ese estado.

Estos son los tipos de transferencia:

- Transferencia ciega:

  Puede transferir la llamada sin que conteste el usuario del destino de la transferencia. Si la extensión de destino de la transferencia está ocupada, recibe un aviso de llamada en espera. Si un tercero intenta transferir otra llamada a la extensión ocupada, o si el bloqueo de avisos de llamada en espera está activo, se realiza inmediatamente una llamada recordatoria. Si la extensión del destino no responde a la llamada transferida en el destino dentro de un tiempo determinado (temporizador "Duración de llamada para transf. antes de contestar"), se produce una llamada recordatoria. Transferencia ciega no se puede ejecutar con un agente de otra cola del Multimedia Contact Center.
- Transferencia de consulta:

  Puede hacer que la llamada solo se transfiera si el usuario del destino de la transferencia responde. La llamada se transfiere al colgar el auricular.

Transferir con desvío de llamadas

Sigue un desvío al destino de la transferencia. La pantalla muestra el último destino de la transferencia.

Transferir con No molestar

Si una llamada se transfiere a una extensión con el estado No molestar activo, se realiza inmediatamente una llamada recordatoria en la extensión que inició el desvío, tenga o no el estado No molestar.

Información específica de sistema

Temporizador de "Duración de llamada para transf. Antes de contestar": Valor estándar: 45 segundos

Se pueden transferir hasta 5 llamadas simultáneamente a una extensión ocupada.

Nota: En una transferencia de llamada, no se admite la actualización de la información de pantalla a través de la interfaz ITSP/NATIVE-SIP.

14.3.6 Llamada recordatoria

Con la función Llamada recordatoria, la extensión recibe automáticamente las comunicaciones retenidas o aparcadas durante demasiado tiempo o aquellas llamadas que no han podido ser transferidas.

Las llamadas recordatorias se producen en los siguientes casos:

- Una comunicación aparcada o retenida no se acepta durante un tiempo determinado (temporizador "Tiempo para aparcar + transic. a retención").
- Con la transferencia ciega, en las siguientes situaciones:
  - Si la llamada no se responde antes de un tiempo determinado (temporizador "Duración de llamada para transf. antes de contestar")
  - El destino no existe
  - El destino está ocupado en segundo grado
  - El teléfono digital del destino está dañado
  - No se permite la transferencia

Si la extensión está ocupada durante la llamada recordatoria, se pone en espera. En cuanto la extensión vuelve a estar libre, se señaliza la llamada recordatoria. En la pantalla de la extensión se puede mostrar el número de teléfono del llamante o de la extensión de destino. Si la extensión no responde a la llamada recordatoria antes de que se agote el temporizador "Tiempo de interceptación para llamada recordatoria", se produce una interceptación en el puesto de interceptación, siempre que se haya establecido el flag en caso de llamada recordatoria sin respuesta. Si el puesto de interceptación no responde a la llamada recordatoria antes de que se agote el temporizador "Tiempo para activación de llam. recordatoria en PO", se interrumpe automáticamente la llamada recordatoria.

Llamada recordatoria y Telecaptura de llamadas

Todas las extensiones que formen parte de un mismo grupo de telecaptura que la extensión original pueden aceptar una llamada recordatoria si está establecido el flag del sistema de telecaptura tras llamada recordatoria.

Llamada recordatoria y No molestar

Las llamadas recordatorias ignoran el estado No molestar.

Información específica de sistema

Temporizador Tiempo de interceptación para llamada recordatoria: valor predeterminado 30 s

Temporizador Tiempo para activación de llam. recordatoria en PO: valor predeterminado 60 s

14.3.7 Supervisión de llamadas

La supervisión de llamadas permite a usuarios autorizados escuchar una conversación de cualquier usuario interno. El micrófono del usuario a la escucha se desactiva automáticamente. Los usuarios de la conexión supervisada no reciben ninguna indicación del proceso, por ejemplo una señal sonora o visual.

La función se desactiva en la configuración predeterminada. Debe ser activada solo si las leyes específicas de cada país lo permiten. En casos individuales, siempre deben revisarse las leyes específicas de cada país antes de que se active la función.

Los usuarios autorizados necesitan un teléfono del sistema y la clase de servicio de intercalación.

El usuario que va a ser supervisado debe encontrarse en un estado de comunicación activa. Al iniciar y finalizar la supervisión de llamadas se pueden producir interrupciones en la comunicación de hasta dos segundos. Tan pronto como uno de los interlocutores del enlace vigilado sea retenido, transferido o si se finaliza la comunicación, se cortará la conexión supervisada. La conexión supervisada no podrá recuperarse hasta que la extensión a supervisar retorne a un estado de comunicación activo.

Dependencias

Tema	Dependencia
Teléfonos inalámbricos	La supervisión de llamadas no se puede utilizar con teléfonos inalámbricos porque no son compatibles con la desactivación automática del micrófono.
En conferencia	La supervisión de llamadas restringe el número posible de conferencias. Cantidad máxima posible de conferencias en el sistema = cantidad máxima de usuarios de supervisión de llamadas al mismo tiempo.
Supervisión de llamadas	Solo se puede realizar una intercalación mediante el código *944 + número de teléfono de la extensión (no desde un menú).
Supervisión de llamadas	Para activar el uso de funciones en una extensión, deben estar activados el flag **Supervisión de llamadas** y el flag **Permiso intercal.** act. (La función no se puede utilizar con Supervisión CSTA).

14.3.7.1 Cómo activar o desactivar la supervisión de llamadas para una extensión

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

El permiso de intercalación está activado para la extensión.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el grupo de menús, haga clic en **Extensiones**.
4) En el grupo de menús, en **Extensiones** > **Extensión** > **…** navegue hasta la extensión deseada (Índice - N.º de llamada - Nombre).
5) Haga clic en la pestaña **Editar flags extensiones**.

6) Elija una de estas opciones:

- Si desea adjudicar a un usuario autorización para esta función, active la casilla de verificación (**Supervisión de llamadas**).
- Si desea retirar a un usuario la autorización para esta función, desactive la casilla de verificación (**Supervisión de llamada**).

7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.3.8 Mensaje discreto

La prestación Mensaje discreto permite a una extensión C establecer una conexión fácilmente entre dos aplicaciones A y B y escuchar sin ser notado; la extensión C también puede dar indicaciones a la extensión A sin ser oída por la extensión B. Es habitual en centros de llamada o en instalaciones Jefe/Secretaria.

La prestación se tiene que configurar en Manager E.

Nota: Aunque no hay ninguna conexión entre la extensión B y la extensión C, es posible que el usuario de la extensión B, por realimentación acústica en el teléfono de la extensión A, pueda oír, aunque amortiguado, lo que dice el usuario C.

Como terminales para Mensaje discreto (extensión A) solo se pueden usar teléfonos del sistema con display. La extensión A y C deben encontrarse en el mismo nodo.

Para activar la prestación, la extensión C marca un código estando en reposo/listo. En el teléfono hay una tecla parcialmente asignada (solo está programado el código en la tecla, el número de llamada debe marcarse seguidamente). En el menú de servicio se agrega una opción, el menú de reposo/comunicación se mantiene sin cambios.

La posibilidad de activar la prestación está ligada a una clase de servicio específica de usuario. También existe otra clase de servicio mediante la cual la extensión A puede impedir la comunicación discreta.

La característica se desactiva si la extensión C de activación la inicia o mediante la actividad de otra prestación relacionada con llamadas.

Nota: Si ninguna de las extensiones de la comunicación original es una extensión TDM, en el momento de la activación la red de conmutación no está aún involucrada, y la conmutación no es posible sin que se produzca una breve interrupción de la conexión previa.

Nota: Las funciones de conferencia y de transferencia de llamada no están disponibles en los productos de la UC Suite si Mensaje discreto está activado.

Si está activada la prestación Comunicación discreta y la extensión A o B inician otra prestación que afecta a la conexión, se desactiva sistemáticamente

la prestación Comunicación discreta. Encontrará más detalles acerca del comportamiento con determinadas prestaciones en la siguiente tabla:

Prestación	Extensión A		Extensión B		Extensión C	
	Posible	Acción	Posible	Acción	Posible	Acción
Llamada de consulta, Retención, Aparcar, Retención general	Sí	Finalizar la "Comunicación discreta"	Sí	Finalizar la "Comunicación discreta"	No	Mensaje negativo
Transferir	--	--	--	--	--	--
Conferencia	--	--	--	--	--	--
Aviso llam. en espera	Sí	--	Sí	--	Sí	--
Aceptar 2ª llam.	Sí	Finalizar la "Comunicación discreta"	Sí	Finalizar la "Comunicación discreta"	Sí	Mensaje negativo
Intercalar	No	--	No	--	No	--
Transferencia MF	Sí	--	Sí	--	No	--
Contador de prestaciones	--	--	--	--	--	--
Servicios asociados	--	--	--	--	--	--
DISA / DISI	--	--	--	--	--	--

14.3.9 Grabación de llamadas (grabación de voz)

Esta función se utiliza para registrar datos de una conexión de voz activa entre dos extensiones (una debe ser interna y la otra puede ser externa) o, dicho de otro modo, para grabar llamadas. Se requiere un dispositivo separado para grabar.

La grabación se puede iniciar/detener pulsando una tecla de función o introduciendo un código (teléfonos analógicos). En función de la configuración, la grabación también puede detenerse con el dispositivo de grabación.

El equipo de grabación se puede utilizar desde cualquier teléfono compatible dentro de una interconexión CorNet-NQ. No se admiten las conexiones con CorNet-N y QSIG (ECMA, ISO). Se puede desactivar el tono de grabación durante la grabación.

Se admiten teléfonos TDM y CorNet-IP (HFA) (incluidos los dispositivos sin pantalla), así como OpenScape Personal Edition (HFA) y optiClient Attendant. No se admiten los teléfonos estándar H.323, los teléfonos SIP ni las extensiones EDSS1.

Nota: La grabación de voz activada se indica mediante un LED o un tono de grabación durante la llamada.

La autorización para usar la grabación de voz se puede configurar individualmente para cada extensión.

Dependencias/restricciones

Asunto	Interdependencia/restricción
Llamada de consulta, alternar, transferencia, conferencia	Si se inicia una de estas funciones mientras se graba una llamada, se interrumpe automáticamente la grabación de voz.
Retener	La grabación continua se interrumpe activando "Retener". La grabación no se puede activar cuando hay una extensión en espera.
Intercalar	La grabación de voz no es posible. No puede intercalar una llamada que se está grabando. Del mismo modo, no puede activar la grabación después de intercalar una llamada.
Supervisión de llamadas	La grabación de voz no es posible. No puede supervisar una llamada que se está grabando. Del mismo modo, no puede iniciar la grabación después de activar "Supervisión de llamadas".

Nota: Solo puede grabar llamadas entre dos partes, no conferencias ni llamadas que involucren a una parte retenida.

Nota: Observaciones adicionales:

-) Se puede acceder al dispositivo de grabación en un nodo aleatorio en una interconexión CorNet NQ.

-) Solo se puede asignar la grabación de voz a una cantidad limitada de extensiones en un nodo (actualmente limitada a 50 extensiones).

-) Los recursos de conferencia se asignan durante la grabación.

-) El código de servicio estándar para activar la grabación de llamadas es *493.

14.4 Control de accesibilidad

El sistema ofrece prestaciones de control de accesibilidad como Desvío de llamadas, No molestar y Rechazo de llamadas.

Distintos tipos de desvíos de llamadas utilizan listas de destinos de llamada. Las listas de destinos de llamada establecen cómo se gestionan las llamadas entrantes para las extensiones o los grupos asignados. Los destinos de una

lista de destinos de llamada se procesan consecutivamente. Puede haber entradas diferentes para las llamadas internas y externas (día o noche).

14.4.1 Desvíos de llamadas

La transferencia automática diferida de llamadas transfiere las llamadas que no son aceptadas en un tiempo determinado.

Este tipo de transferencia se denomina "Transferencia automática diferida de llamadas fija" porque solo la puede configurar el administrador.

Por cada transferencia automática diferida de llamadas hay una o varias listas de destinos de llamada que se pueden asignar a las extensiones para los siguientes tipos de llamadas:

- Llamadas externas de día (con Servicio nocturno inactivo)
- Llamadas externas de noche (con Servicio nocturno activo)
- Llamadas internas

Por cada lista de destinos de llamada se pueden introducir hasta 4 destinos de llamada a los que se transferirán las llamadas una vez transcurrido un tiempo configurable.

En el destino de llamada automática diferida se muestran el número de teléfono el nombre del usuario llamado originalmente y el número de teléfono o el nombre del llamante. En calidad de administrador puede desactivar la indicación adicional del número de teléfono o del nombre del llamante.

Transferencia automática de llamadas en caso de ocupado

La transferencia automática de llamadas en caso de ocupado desvía las llamadas entrantes para una extensión ocupada inmediatamente al próximo destino.

Si el destino de llamada también está ocupado, el llamante recibe la señal de ocupado. En caso de llamada interna, la llamada se mantiene en el destino de llamada. Cíclicamente se comprueba el estado de libre de este destino. El administrador establece el ciclo.

Si el destino no está disponible y no hay configurada otra transferencia automática de llamadas, la llamada no se transfiere.

Dependencias

Tema	Dependencia
Terminales analógicos	En estos teléfonos no hay ninguna indicación de que la llamada entrante es una llamada transferida.
Aviso llam. en espera	Si un usuario ha activado el aviso de llamada en espera, se le indica el aviso de llamada en espera aunque tenga configurada la transferencia automática diferida en caso de ocupado.
DND	Los destinos de llamada que tengan activado el bloqueo de avisos de llamada en espera se pasan por alto.

Tema	Dependencia
Desvío de llamadas	Una transferencia automática diferida de llamadas solo se ejecuta si el destino de un desvío de llamadas no responde tras un tiempo definido por el administrador.
Servicio nocturno	Si se utiliza la opción "de día / de noche" para la transferencia automática diferida de un usuario y se activa el servicio nocturno, las llamadas externas se desvían de acuerdo con la configuración establecida para el servicio nocturno. Las llamadas internas mantienen la configuración "de día".
Transferencia automática diferida de llamadas a la línea urbana	Si hay activada una transferencia automática diferida de llamadas a la línea urbana, tiene preferencia frente a otras transferencias automáticas de llamadas.
Línea colectiva/Llamada de grupo	Si se ha registrado un grupo o una línea colectiva como desvío de una transferencia automática diferida de llamadas, se llama a todos los usuarios del grupo antes de evaluar el siguiente destino de la transferencia automática diferida. Las llamadas de grupo y las líneas colectivas pueden verse dentro de la transferencia automática diferida de llamadas como una transferencia automática diferida de llamadas. Una línea colectiva está ocupada si todos los miembros están ocupados o si se han desconectado de la lista colectiva. Un grupo está ocupado si todos los miembros del grupo están ocupados.

14.4.1.1 Cómo configurar una transferencia automática diferida

Con el asistente **Transferencia automática diferida** puede configurar una transferencia automática diferida en caso de llamadas entrantes para las extensiones internas.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Transferencia automática diferida**. Se abre la ventana **Listas de destinos de llamada - Definición**.
4) En primer lugar, defina una lista de destinos de llamada. Para ello, en la lista de destinos de llamada que desee editar, haga clic en el símbolo **Editar**.

5) En las listas desplegables **1. destino** a **4. destino**, seleccione los destinos deseados. Dispone de las siguientes opciones:

- **Ninguna entrada**: el destino se omite
- **Destino externo**: ruta y número de teléfono externo con código de línea urbana
- *** Extensión llamada**: la extensión que recibe la llamada
- **** Definido por el usuario**: destino del desvío de llamadas diferido por la extensión (si está configurado).
- **#9 Búsqueda de sistema**: siguiente extensión disponible (salvo extensiones Jefe)
- **#201 - #260**: Distribución de llamadas (Grupo UCD)
- **#801 - #817**: Equipo de anuncios grabados
- **100, 101, ...**: número de teléfono de un grupo o de una extensión interna (p.ej., buzón de voz)

> **Nota:** Para buscar más rápido un destino de llamada, en los campos **1. - 4. destino** también puede introducir una o varias cifras. Entonces se pasa directamente a la entrada de lista que comience con la secuencia de cifras introducida. También se puede introducir una secuencia de letras.

6) En la lista desplegable **Transferencia autom. diferida comienza después de** seleccione el tiempo en segundos tras el que la llamada se transferirá al siguiente destino.

7) Active la casilla de verificación **Transferencia automática diferida**, si desea que la llamada se transfiera inmediatamente al siguiente destino en caso de ocupado.

8) Si desea que la llamada se señalice en otra extensión interna o, por ejemplo, en un relé (contacto) para un timbre central, en la lista desplegable **Destino de segundo timbre** seleccione el número de teléfono deseado. La opción **Tipo de segundo timbre** permite seleccionar si la llamada se señalizará en la extensión inmediatamente o después de transcurrido todo el tiempo de transferencia automática diferida.

9) Haga clic en **OK & Continuar**. Regresa a la ventana **Configuración básica**.

10) Si desea definir más listas de destinos de llamada, repita los pasos anteriores.

11) Haga clic en **OK & Continuar**.

12) A continuación, asigne las listas de destinos de llamada a las extensiones.

13) Para buscar una extensión, en los campos de búsqueda **N° llam.** o **Nombre** introduzca un término de búsqueda y, a continuación, pulse el botón Intro. Se muestran todos los resultados que contienen el término de búsqueda. Si por ejemplo se escribe `521` como número de teléfono, aparecerían los resultados `+495213535` y `+498967521`. O por ejemplo, si se escribe `co` como nombre aparecerían los resultados `Collins`, `Mcoin` y `Branco`.

> **Nota:** Si no hay nada en ningún campo de búsqueda y se pulsa la tecla Intro, aparecen todas las entradas.

14) En la línea de la extensión deseada, seleccione en las listas desplegables las listas de destinos de llamada para los siguientes casos:

- **Día**: Lista de destinos de llamada para llamadas externas entrantes durante el horario de trabajo (servicio diurno)
- **Noche**: Lista de destinos de llamada para llamadas externas entrantes con el servicio nocturno activado
- **Internas**: Lista de destinos de llamada para llamadas internas entrantes

15) Guarde sus entradas con **Guardar**, antes de pasar a una extensión de otra página.

16) Si desea asignar una lista de destinos de llamada cómodamente a varias extensiones, haga clic en **Copiar**.

a) En **Lista destinos llam.**, seleccione la lista de destinos de llamada a la que desee asignar la extensión.

b) En la ventana **Selección** marque una o varias extensiones y con **Agregar**, añádalas a la ventana **Miembros**.

c) Mediante las casillas de verificación **Día**, **Noche** e **Internas**, seleccione si la lista de destinos de llamada se aplicará a llamadas externas entrantes durante el horario laboral (servicio diurno), cuando esté activado el servicio nocturno o solamente a las llamadas internas.

d) Haga clic en **OK & Continuar**.

17) Haga clic de nuevo en **OK & Continuar**.

18) Aquí puede visualizar todas las extensiones de una lista de destinos de llamada. Para ello, en **Mostrar a todos los miembros con la lista de destinos de llamada** seleccione la lista de destinos de llamada deseada.

19) Haga clic en **OK & Continuar**. La transferencia automática diferida está configurada para una extensión interna.

20) Haga clic en **Salir**.

14.4.2 Transferencia diferida

Con el desvío de llamadas (AUL), los usuarios pueden desviar llamadas entrantes a un destino de su elección.

Si hay disponibles teclas de línea (también denominadas teclas de línea MULAP), el desvío de llamadas también se puede activar de forma individual para una línea determinada (o línea MULAP).

Pueden desviarse estas llamadas:

- Todas las llamadas
- Sólo llamadas externas
- Sólo llamadas internas

Pueden definirse estos destinos para un desvío de llamadas:

- Otro teléfono (interno o externo)
- Puesto de operadora
- Buzón de voz
- Línea colectiva
- grupo UCD (Distribución de llamadas universal UCD)

Con el desvío de llamadas activado se pueden seguir realizando llamadas salientes.

Destino externo

Si el destino del desvío de llamadas es externo, introduzca el código urbano seguido del número de teléfono externo del destino de desvío.

Desvío de llamadas a destinos externos

Si el usuario ha incluido en su lista de destinos de llamada un desvío de llamadas a un destino externo, la transferencia automática diferida finalizará en ese destino. Es posible que los demás destinos registrados en la lista de destinos de llamada no se sigan.

Si se debe realizar una transferencia automática diferida a otros destinos, un técnico de servicio deberá activar el flag del sistema **Transfer. autom. diferida tras desvío a dest. ext.**.

Si se debe realizar un desvío de llamadas a un destino externo también en caso de llamada a través de una línea urbana analógica, un técnico de servicio deberá activar el flag del sistema **Desvío tras HKZ permitido**.

Nota: Cuando una llamada se encamina a través de Smart AA y dicha llamada se transfiere a un usuario A con el desvío de llamadas externas activado (*11) para un usuario B, el usuario B no presentará el CLI de la parte llamante, sino el número de marcación directa del usuario A.

Interdependencias

Tema	Interdependencia
No molestar	No se pueden programar desvíos de llamadas en un teléfono en estado "no molestar".
Cita, Equipo de despertador	Si se alcanza una cita programada, se señaliza en el teléfono desviado sin que influya para nada el desvío configurado.
Grupo UCD como destino de desvío de llamadas	En estos casos no tiene lugar el desvío de llamadas a un grupo UCD: • Si una línea colectiva es llamada y el siguiente es un usuario con un desvío de llamadas a un grupo UCD, la llamada no se desvía. En este caso, se llama directamente al siguiente usuario de la línea colectiva. • Un usuario es miembro de una llamada de grupo con la propiedad "Grupo" y ha activado un desvío de llamadas a un grupo UCD. • Una extensión es miembro de una llamada de grupo en caso de libre. Si el grupo es llamado, no se realiza el desvío de llamadas al grupo UCD. Excepción: el primer usuario registrado ha activado un desvío de llamadas a un grupo UCD. En este caso la llamada se desvía.

14.4.2.1 Cómo activar o desactivar el desvío de llamadas a través de líneas urbanas analógicas

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el árbol de navegación, desplácese hasta **Sistema** > **Flags del sistema**.
4) Elija una de estas opciones:
   - Si desea activar el desvío de llamadas a través de líneas urbanas analógicas, active la casilla de verificación **Desvío tras HKZ permitido**.
   - Si desea desactivar el desvío de llamadas a través de líneas urbanas analógicas, desactive la casilla de verificación **Desvío tras HKZ permitido**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.4.2.2 Cómo activar o desactivar el desvío de llamadas tras desvío de llamadas a un destino externo

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el árbol de navegación, desplácese hasta **Sistema** > **Flags del sistema**.
4) Elija una de estas opciones:
   - Si desea activar el desvío de llamadas tras desvío de llamadas a un destino externo, active la casilla de verificación **Transfer. autom. diferida tras desvío a dest. ext**.
   - Si desea desactivar el desvío de llamadas tras desvío de llamadas a un destino externo, desactive la casilla de verificación **Transfer. autom. diferida tras desvío a dest. ext**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.4.3 Desvío de llamadas diferido

El desvío de llamadas diferido desvía las llamadas no atendidas una vez transcurrido un tiempo determinado. El desvío diferido corresponde a una transferencia automática diferida de llamadas, pero en este caso el usuario puede configurar por sí mismo el desvío.

El usuario puede configurar el desvío diferido en su propio teléfono. También se pueden registrar grupos y destinos externos.

El destino de desvío no se guarda de forma permanente. Se elimina cuando se desactiva la prestación.

En caso de ocupado rigen las reglas de la transferencia automática diferida de llamadas, es decir, se pasa al siguiente destino.

Información específica de sistema

Pueden configurarse tres destinos por cada extensión. Además, hay una identificación especial "definida por el usuario". Con ella, el administrador puede liberar o bloquear la prestación Desvío diferido para un usuario. De forma predeterminada, la prestación está liberada.

Si no se responde a la llamada en el tiempo preestablecido, se busca y llama al destino de desvío guardado por el usuario. Si el usuario no ha registrado ningún destino de desvío individual, se pasa al siguiente destino de la lista de destinos de llamada.

El administrador debe activar el desvío diferido para las distintas extensiones a través de las listas de destinos de llamada.

14.4.4 Transferencia automática diferida en línea urbana (no disponible para EE. UU.)

Todas las extensiones que tengan asignado un MSN (Multiple Subscriber Number en un acceso individual RDSI o conexión ITSP) como número de marcación directa, pueden activar y desactivar la transferencia automática diferida en línea urbana para el MSN. Para hacerlo es necesario que el usuario esté autorizado a realizar transferencias automáticas diferidas externas.

Si un grupo de usuarios tiene asignado un MSN, todos los usuarios del grupo pueden activar o desactivar una transferencia automática diferida en línea urbana para dicho MSN.

La prestación tiene tres versiones distintas:

- Desvío de llamada directo (CFU): El proveedor de red transfiere directamente todas las llamadas de ese MSN, sea cual sea su estado.
- Desvío de llamada en caso de ocupado (CFB): Solo se realiza una transferencia automática diferida, si el MSN marcado está ocupado.
- Desvío de llamada diferido (CFNR): Solo se realiza una transferencia automática diferida si la llamada entrante no se responde pasado un tiempo preestablecido.

Nota: Para todos los escenarios de desvío de llamadas anteriores, solo puede indicarse un destino de transferencia automática diferida por MSN. Se pueden transferir 10 MSN como máximo.

En caso de que ITSP o RDSI estén configurados con marcación directa, este número es 249.

Dependencias

Tema	Dependencia
Servicio nocturno	La transferencia automática diferida en línea urbana, tiene mayor prioridad que el servicio nocturno.

14.4.5 Asignación de llamadas

La Asignación de llamadas permite la transferencia automática diferida de llamadas entrantes de una línea analógica o S_0 a una extensión o grupo, en función del número de teléfono marcado y del estado de activación del servicio nocturno.

Se pueden utilizar distintos destinos para el servicio nocturno y diurno. Las llamadas entrantes no se señalizan en la extensión, sino de acuerdo con las listas de destinos de llamada de la extensión.

14.4.5.1 Cómo configurar la asignación de llamadas

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en **Líneas / Interconexión** > **Líneas**.
4) En el grupo de menús, en **Líneas** > **…** (código de puerto de box), desplácese hasta la línea analógica o S_0 deseada.
5) En la lista desplegable **Día N.º llam.** seleccione el número de teléfono deseado.
6) En la lista desplegable **Noche N.º llam.** seleccione el número de teléfono deseado.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.4.6 Timbre adicional

La prestación Timbre adicional permite a todas las extensiones internas administrar una lista personal de números de teléfono internos a los que también se llamarán cuando se llame a su número de teléfono propio.

Una extensión también puede registrar el número de teléfono propio, por ejemplo si quiere desviar el número de teléfono de forma fija a otra extensión (Jefe-Secretaria).

Para activar o desactivar esta prestación se puede programar una tecla en teléfonos IP, teléfonos TDM de OpenStage y teléfonos optiPoint 500. Para poder hacer variaciones, se pueden programar varias teclas de conmutación de

llamadas en un teléfono. Se pueden activar varias teclas al mismo tiempo, pero nunca puede haber más de cinco teléfonos con señalización de llamadas.

Las extensiones también pueden activar o desactivar esta prestación en el teléfono propio mediante una conexión DISA o en otras extensiones mediante la prestación Servicios asociados.

La indicación en pantalla Transferencia... es una de las tres indicaciones del menú a nivel de sistema del Manager E y ofrece información de estado específica de terminales (no del sistema). Mediante la ventana Desvío puede determinar si el Timbre adicional está activo en un teléfono o si el teléfono forma parte de un grupo de llamadas.

Si la prestación se utiliza con frecuencia, el usuario puede asignarle una tecla libre en su teléfono. El nombre de la tecla es Timbre adicional act. en la programación de teclas. Si la prestación está activa se ilumina el LED.

El flag de extensión “Sin conexión de timbre en caso ocupado" permite controlar a qué extensión receptora de timbre adicional se llamará si el "Maestro" (extensión emisora del timbre adicional) está ocupado. Si varios "Maestros" tienen timbre adicional con la misma extensión, el flag se aplica a todas las conmutaciones de esa extensión.

Si el flag no está establecido, el timbre adicional se realiza siempre que la extensión conmutada esté disponible (comportamiento estándar).

Si el flag está activado, el timbre adicional depende de la accesibilidad del ”master”:

- El "maestro" está libre: se hace el timbre adicional.

  En el "maestro" se puede señalizar aviso de llamada en espera: el timbre adicional se emite al cabo de 5 s.

  En el "maestro" no se puede llamar ni señalizar aviso de llamada en espera: no se realiza ninguna conexión de timbre adicional.

Tema	Interdependencia/restricción
Llamada recordatoria Búsqueda de sistema Devolución de llamada	El Timbre adicional no se ejecuta en caso de Llamada recordatoria inmediata (por ejemplo, error de control), Búsqueda de sistema o Devolución de llamada.
Desvío de llamadas	Si la extensión que ha activado el Timbre adicional ha activado AUL, no se realiza ningún Timbre adicional.
No molestar (DND)	Si la extensión con Timbre adicional ha activado No molestar, no recibe llamadas.
Cita	Después del Timbre adicional no se emite un aviso de cita activo.
Sin conexión de timbre en caso ocupado	Si el flag está activado, no se ejecuta el Timbre adicional si la extensión está ocupada.

14.4.7 Rechazo de llamadas

El usuario puede rechazar llamadas nuevas entrantes internas y externas. Se pueden rechazar las llamadas pulsando la tecla de corte.

La llamada rechazada se desvía de acuerdo a la transferencia automática diferida de llamadas. Si no hay ningún destino de transferencia automática diferida, las llamadas externas se interceptan por el puesto de operadora, siempre que estén configurados los criterios de interceptación adecuados. Si no se puede llamar a ningún destino, el llamante recibe la señal de ocupado.

No pueden rechazarse llamadas/rellamadas transferidas, en cola, retenidas o aparcadas. Si puesto intercep. intercepta una llamada, no puede ser rechazada.

Interdep.

Tema	Interdep.
Llamada de grupo, línea colectiva, MULAP	En estos casos finaliza toda la llamada de grupo y la llamada se rige por la Transferencia automática diferida de llamadas configurada. Si no hay más destinos de llamada, la llamada finaliza.

14.4.8 Reposición de una llamada

Un usuario puede diferir una llamada entrante. El usuario llamado puede establecer una conexión sin aceptar la llamada entrante.

La llamada en espera se señaliza entonces como llamada en espera

Si se señaliza una llamada entrante, el usuario puede pulsar una tecla de línea o de llamada para establecer una comunicación externa. Para hacerlo debe haber programadas dos teclas de llamadas y una tecla de línea. Para ejecutar esta prestación, debe estar libre una de las teclas.

El usuario llamante no observa ningún cambio en la señalización si la señalización de llamada está ajustada a aviso de llamada en espera.

14.4.9 No molestar

No molestar impide la transferencia de llamadas entrantes.

Si la prestación No molestar está activada, al descolgar el microteléfono el usuario puede escuchar un tono de marcar especial. Además, si la prestación está activa, en los teléfonos con display aparece indicado el estado No molestar. En todos los demás teléfonos el LED de la tecla de llamada directa del usuario en estado No molestar parpadea con una breve interrupción.

El puesto de operadora o un usuario autorizado pueden romper el estado No molestar. La llamada también se puede transferir inmediatamente para un usuario con estado No molestar.

Al marcar un teléfono en estado No molestar, el llamante escucha el tono de ocupado.

Interdependencias

Tema	Interdependencia
Puesto de operadora/ Destino nocturno	El puesto de operadora y el puesto de interceptación actual no pueden activar la prestación No molestar.
Desvío de llamadas	La prestación No molestar no se puede activar si el teléfono tiene activado un desvío de llamadas. En un teléfono en estado No molestar no se puede activar ningún desvío de llamadas.
Devolución de llamada	Si se lleva a cabo una devolución de llamada a una extensión en estado “no molestar”, ésta no se ejecuta hasta que no se desactiva “no molestar”. Si la extensión en estado “no molestar” inicia una devolución de llamada, se rompe su estado “no molestar”.
Cita, Equipo de despertador	Si una extensión ha programado un aviso de cita y ha activado “No molestar”, al llegar el momento programado para el aviso de cita se produce una señalización acústica en el terminal.
DISA	DISA puede ser activado por los usuarios para sus propios teléfonos o para otros usuarios (Servicios asociados).

14.5 Optimización de la comunicación

El sistema de comunicación ofrece distintas opciones para gestionar de forma cómoda y efectiva las llamadas, por ejemplo, Devolución de llamada o Aviso de llamada en espera.

14.5.1 Devolución de llamada

De esta forma, se puede activar una devolución de llamada si el usuario llamado no responde o está ocupado. Si la devolución de llamada está activada, activa una llamada en cuanto el usuario llamado vuelve a estar disponible.

Devolución automática de llamada en caso de "Libre" u "Ocupado"

Si no se consigue establecer una llamada porque el usuario llamado está ocupado o no acepta la llamada, el usuario llamante puede activar una devolución de llamada para establecer la comunicación más adelante. Si el usuario llamado estaba ocupado, devolución de llamada controla el final de la comunicación. Cuando el usuario vuelve a estar libre, el usuario llamante recibe una notificación recibiendo una llamada del sistema de comunicación. Si acepta la llamada, vuelve a marcarse el número del usuario que antes estaba ocupado. Si no se puede establecer una comunicación a través de la función de devolución de llamada, la función sigue activa. El intento de devolución se repite en cuanto el usuario deseado finaliza una nueva comunicación.

Un teléfono puede enviar hasta dos peticiones de devolución de llamada y puede ser destino de hasta dos solicitudes. Todas las solicitudes adicionales serán rechazadas.

Las peticiones de devolución de llamada se eliminan cuando

- se establece comunicación, si no es así, la devolución de llamada permanece activa (en caso de devolución de llamada interna),
- si se ha establecido la devolución de llamada sin que se haya establecido la llamada (en caso de devolución de llamada externa),
- el usuario que inició la petición cancela la devolución de llamada,
- el sistema borra diariamente todas las devoluciones de llamada a las 23:57 horas.

Pueden definirse peticiones de devolución de llamadas para usuarios y grupos internos. Si se trata de una conexión de grupo, las peticiones de devolución de llamada se depositan en el primer usuario. Si la devolución de llamada se refiere a un grupo, suenan todos los teléfonos libres.

Devolución de llamada automática en caso de libre en el interfaz de la central pública

Un usuario interno que no consiga establecer comunicación con un usuario externo libre, puede activar una solicitud de devolución de llamada en la central. De esta forma, se supervisa la conexión del usuario llamado. En cuanto el usuario llamado establece una conexión y vuelve a finalizarla, la central intenta establecer una conexión entre ambos usuarios. Esta prestación debe tener compatibilidad en la central pública.

Devolución de llamada en caso de ocupado

Se puede definir una devolución de llamada manual dirigida a extensiones externas y ocupadas. Cuando la extensión está libre, la central intenta establecer una conexión entre ambas extensiones. Esta prestación debe ser compatible y estar activada en la central pública y en el colateral.

14.5.2 Aviso llam. en espera

El aviso de llamada en espera señaliza la entrada de nuevas llamadas cuando una extensión está en comunicación.

La señalización se muestra de forma visual a través de un mensaje en la pantalla. La señalización también puede realizarse de forma acústica a través de un tono de llamada breve. El tono de llamada en espera se escucha cada 5 segundos.

El usuario llamado puede aceptar o ignorar la segunda comunicación. Para aceptar la segunda llamada, el usuario puede finalizar la primera conexión y aceptar la segunda, o bien, seleccionar la función **Noche N.º llam.** que aparece en la pantalla. En tal caso se mantiene la primera llamada.

No puede dejar en espera a un usuario si ya hay un usuario en espera (pueden ponerse en espera un máximo de 4 usuarios) o si ha activado el bloqueo de avisos de llamada en espera. El llamante recibe una señalización de ocupado si no hay configurada ninguna transferencia automática de llamada en caso de ocupado.

Activar el aviso de llamada en espera

Aviso de llamada en espera a través del puesto de operadora

La etiqueta **Bloqueo de avisos de llamada en espera** debe estar establecida para el usuario, para que pueda elegir si activar o suprimir el aviso de llamada en espera a través de menú o código. Si un usuario ha activado el aviso de llamada en espera, las llamadas serán puestas en espera aun cuando haya configurado la transferencia automática de llamada en caso de ocupado.

El ajuste estándar siempre es Aviso llam. en espera diferido. Sin embargo, el puesto de operadora también puede realizar el aviso de llamada de forma inmediata.

Interdependencias

Tema	Interdependencia
Aviso de llamada en espera silencioso	El usuario puede activar o desactivar tono de llamada en espera mediante un código. No desaparece la señalización visual del aviso de llamada en espera en la pantalla del teléfono. Por defecto, el tono de llamada en espera está activado.
Intercalar	Si el bloqueo de avisos de llamada en espera está activado se impiden las intercalaciones en una conexión del usuario.
Llamada de grupo	Si están libres uno o varios miembros de una llamada de grupo, se les ofrece la llamada. Si todos los miembros están ocupados, reciben todos una señalización de llamada en espera, a no ser que todos hayan activado el bloqueo de avisos de llamada en espera.
Mensaje directo	No se pueden enviar mensajes directos a los usuarios ocupados.

14.5.2.1 Cómo activar o desactivar el aviso de llamada en espera

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el grupo de menús, haga doble clic en **Extensiones**.
4) Haga clic, por ejemplo, en **Clientes IP**.
5) Haga clic, por ejemplo, en **Clientes de sistema**.
6) Seleccione la extensión correspondiente.
7) Haga clic en la pestaña **Editar flags exten.**

8) Elija una de estas opciones:
   - Si desea activar el aviso de llamada en espera, desactive la casilla de verificación Bloqueo de aviso de llamada en espera act..
   - Si desea desactivar el aviso de llamada en espera, active la casilla de verificación **Bloqueo de aviso de llamada en espera act.**.
9) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.5.2.2 Cómo activar o desactivar el aviso de llamada en espera inmediato a través del puesto de operadora

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema**.
4) Haga clic en **Interceptación/PO/Hot-line**.
5) En **Otros criterios**, seleccione una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Aviso de llamada en espera inmediato para llamadas de puesto de operadora**.
   - Si desea desactivar la función, desactive la casilla de verificación **Aviso de llamada en espera inmediato para llamadas de puesto de operadora**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Nota:

En los teléfonos de sobremesa CMI DECT - TDM, cuando se llama a una extensión que está ocupada y se permite la llamada en espera, el tono de ocupado está activo durante 5 segundos y, a continuación, se produce la activación, por lo que puede oírse el tono de retorno de llamada.

En los teléfonos de sobremesa IP DECT - SIP, cuando se llama a una extensión que está ocupada y se permite la llamada en espera, la activación es inmediata, por lo que el tono de llamada de retorno puede oírse desde el principio.

14.5.3 Intercalar (Intrusión)

La función Intercalar permite a los usuarios autorizados intercalarse en las comunicaciones de una extensión interna.

La intercalación se realiza mediante códigos o teclas y se comunica a las extensiones implicadas mediante un tono de aviso y una indicación en pantalla.

Esta prestación puede activarse durante la señal de ocupado o durante el tono de aviso de llamada en espera.

Al efectuar la intercalación en una comunicación rige lo siguiente:

- Si el usuario llamado cuelga, recibirá una llamada del usuario que realiza la transferencia.
- Si el usuario que ha activado la intercalación (el que desea transferir la llamada y activa la intercalación) cuelga, la llamada es conmutada a la extensión de destino.
- Si el usuario conectado al usuario llamado cuelga, siguen conectados el usuario llamado y el intercalado.

Todas las extensiones internas y el puesto de interceptación (puesto de operadora) pueden intercalar. Para poder utilizar esta prestación, la extensión interna y el puesto de interceptación deben estar autorizados.

No se puede impedir la intercalación en un determinado teléfono.

Interdependencias

Tema	Interdependencia
Protección de señalización en el canal telefónico	Si el usuario llamado o su interlocutor interno están registrados como terminal de datos (protección de señalización de canal telefónico) o si el usuario llamado está en estado de marcación, no se puede activar la intercalación.
No molestar	Si el usuario llamado ha activado No molestar, solo se puede realizar una intercalación si se encuentra en conversación.
Grupo/Línea colectiva	Si al llamar a un grupo o una línea colectiva están ocupadas todas las extensiones, no es posible la intercalación.
Extensión S_0	La intercalación en una extensión S_0 no es posible.

14.5.3.1 Cómo autorizar a una extensión interna para la intercalación

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.

3) En el grupo de menús, haga doble clic en **Extensiones**.

4) En el grupo de menús, haga clic en la extensión (Índice - Número de teléfono - Nombre).

5) Haga clic en la pestaña **Editar flags exten.**

6) Active la casilla de verificación **Permiso intercal act**.

7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.5.3.2 Cómo autorizar el puesto de interceptación para la intercalación

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema** > **Interceptación/PO/Hot-line**.
4) En el área **Otros criterios**, seleccione la casilla de verificación **Sobrescribir con PO**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.5.4 Mensajes por ausencia

El mensaje por ausencia de una extensión aparece en la pantalla del llamante.

En los mensajes por ausencia (también denominados Texto respuesta) pueden especificarse parámetros variables. Estos parámetros (p. ej. Hora) se introducen durante la activación. Para introducir caracteres adicionales puede utilizar el teclado numérico del terminal. El mensaje por ausencia puede activarse o desactivarse en un teléfono a través de un código o de una tecla de función previamente configurada.

Desvío de llamadas

Con Desvío de llamadas se muestra el texto de ausencia de la extensión llamada y a continuación se desvía la llamada.

14.5.4.1 Cómo modificar el mensaje por ausencia

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema**.
4) Haga clic en **Textos**.
5) En la columna **Textos de respuesta**, haga clic en el campo correspondiente e introduzca su mensaje por ausencia.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.5.5 Mensajes de texto

Los mensajes de texto son textos internos del sistema que puede elegir un usuario y enviarlos a usuarios internos.

Los mensajes de texto (Texto informativo) se pueden enviar a uno o varios destinatarios.

Si se quiere enviar el texto a todos los miembros de un grupo interno o a una línea colectiva interna, debe indicarse como destinatario el número de teléfono del grupo o de la línea colectiva y no a cada uno de los usuarios.

Nota: Solo 100 teléfonos pueden recibir mensajes MWI (Message Waiting Indication), si hay más mensajes, fallarán.

El mensaje se envía a través de la tecla o menú Enviar información.

El envío puede realizarse en estado de reposo, de llamada, de comunicación o de ocupado. En el estado de llamada no se indica el número de llamada del destinatario.

14.5.5.1 Cómo modificar un mensaje de texto

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema**.
4) Haga clic en **Textos**.
5) En la columna **Textos informativos**, haga clic en el campo correspondiente e introduzca el texto.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.5.6 Servicios asociados

Un usuario autorizado puede controlar determinadas funciones en nombre de cualquier otro usuario, por ejemplo, activar o desactivar las funciones de Desvío de llamadas, Candado telefónico o Línea colectiva. El efecto es el mismo que si fuera el propio usuario representado el que activara o desactivara la prestación.

Estas son las prestaciones que se pueden controlar en nombre de otro usuario:

- Desvío de llamadas activado / desactivado
- Candado electrónico act. / des.
- Timbre adicional act. / des.
- Texto de respuesta activado / desactivado
- Línea colectiva y llamada de grupo activado / desactivado
- Servicio nocturno activado / desactivado
- Cita activada / desactivada
- Enviar info / Borrar mensajes informativos enviados
- Modificar clave de candado telefónico
- Agente UCD inicio de sesión / fin de sesión

- Agente UCD disponible / no disponible
- Tiempo administrativo Agente UCD activado / desactivado
- Servicio nocturno Agente UCD activado / desactivado
- Desvío MULAP activado / desactivado
- Restablecer prestaciones activadas

Se utiliza a través de un procedimiento. El usuario debe especificar lo siguiente:

- El código para Servicios asociados
- El número de teléfono del usuario por el que se ejecuta una acción
- El código de la prestación que se quiere controlar

Para que un usuario pueda utilizar los servicios asociados, debe desactivar el candado teléfono del otro usuario si está activado.

14.5.6.1 Cómo activar o desactivar servicios asociados

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el grupo de menús, haga doble clic en **Extensiones**.
4) En el grupo de menús, haga clic en la extensión (Índice - Número de teléfono - Nombre).
5) Haga clic en la pestaña **Editar flags exten.**
6) Elija una de estas opciones:
   - Si desea activar esta función, active la casilla de verificación **Marcación asociada / servicios**.
   - Si desea desactivar esta función, desactive la casilla de verificación **Marcación asociada / servicios**.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.5.7 DISA

DISA (Direct Inward System Access) permite a los usuarios autorizados utilizar las prestaciones del sistema de comunicación de forma externa, por ejemplo desde un teléfono móvil a través de myPortal for Mobile (con Mobile Callback) y Mobility.

DISA también permite a un usuario establecer conexiones salientes, internas y externas. Cada vez que utiliza DISA, el usuario debe introducir la contraseña del candado telefónico. De esta forma se puede acceder a determinadas prestaciones, como para el uso interno.

DISA es compatible con estas prestaciones:

Prestación	por el propio usuario	a través de servicios asociados
Desvío de llamadas activado / desactivado	x	x
No molestar activado / desactivado	x	x
Línea colectiva activado / desactivado	x	x
Mensaje por ausencia activado / desactivado	x	x
Timbre adicional activado / desactivado	x	x
Candado telefónico activado / desactivado	x	x
Restablecer servicios	x	x
Marcación abreviada central	x	–
Enviar mensaje informativo	x	–
Servicio nocturno activado / desactivado	x	–

El administrador establece el número de teléfono con el que los usuarios pueden utilizar DISA. El número de teléfono puede ser diferente para el uso externo e interno. Interno significa a otro nodo interconectado por IP.

La contraseña que debe introducir el usuario se compone del número de teléfono interno y del PIN para el candado telefónico. Después de introducir la contraseña, el usuario debe pulsar la tecla # o esperar hasta que el sistema de comunicación haya identificado su entrada, según cual sea el modo de seguridad que haya establecido el administrador para DISA.

Para hacer más acciones por DISA el usuario tiene que volver a registrarse.

Nota: En OpenScape Business X, cuando se llama a un número DISA, oirá un tono continuo. En OpenScape Business S, cuando se llama a un número DISA, oirá Música en espera.

14.5.7.1 Cómo activar o desactivar la autorización DISA para un usuario

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.

3) En el grupo de menús, haga doble clic en **Extensiones**.

4) En el grupo de menús, haga clic en la extensión (Índice - Número de teléfono - Nombre).
5) Haga clic en la pestaña **Editar flags exten.**
6) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Autorización DISA**.
   - Si desea desactivar la función, desactive la casilla de verificación **Autorización DISA**.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.5.7.2 Cómo configurar el número DISA

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **DISA**.
4) En el campo **Marcación directa** introduzca el número de teléfono que permite utilizar DISA de forma externa.
5) En el campo **Número de teléfono** introduzca el número de teléfono que permite utilizar DISA de forma interna.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.5.7.3 Cómo configurar el modo de seguridad DISA

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **DISA**.
4) En la lista desplegable **Modo de seguridad**, seleccione el modo de seguridad **Diferido** o **Tras entrar #**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.5.8 Flex Call/Pin móvil

Con Flex Call (PIN móvil) otro usuario utiliza provisionalmente un teléfono de sistema para la siguiente comunicación saliente como si fuera el suyo propio.

Flex Call incluye el número de teléfono, el nombre, el acceso a la red urbana y el registro de tarificación del usuario.

Si Flex Call está activo, no se puede acceder al teléfono utilizado a través de su número de teléfono propio. Una vez finalizada la llamada, se vuelve a cancelar este estado.

Para activar Flex Call hay que asignar un candado telefónico individual a la extensión móvil.

Para la activación hay que realizar uno de los siguientes pasos en el teléfono de sistema:

- OpenStage: menú Servicio > PIN y clase de servicio > Flex Call + Número de teléfono móvil + Candado telefónico de la extensión móvil
- Código para FlexCall + Número de teléfono móvil + Candado telefónico de la extensión móvil

14.5.9 Reasignación

Con la función Relocate/Reasignación, las extensiones TDM de OpenStage pueden modificar la asignación entre el puerto de conexión físico y los datos de extensión lógicos (perfil de usuario) por procedimiento.

La Reasignación se puede utilizar si dos usuarios deciden intercambiar sus puestos de trabajo y ambos utilizan el mismo tipo de teléfono. Reasignación permite implementar DeskSharing para usuarios TDM. Las extensiones TDM pueden realizar el cambio de número de teléfono sin ayuda de un administrador.

Solo se pueden intercambiar perfiles de usuario del mismo tipo de teléfono, es decir, con la misma distribución de teclas. Si se intercambian perfiles de usuario entre diferentes tipos de teléfono, las funciones de teclas con programación personalizada del equipo básico son sustituidas por los valores por defecto. Al ejecutar la reasignación tiene lugar una desconexión/reinicio de los teléfonos TDM involucrados. Las prestaciones activadas se gestionan en consecuencia, es decir: se borran las llamadas de devolución de llamada actuales y las informaciones enviadas y se mantienen todas las demás prestaciones.

Para usar la Reasignación hay que habilitar la prestación a nivel de sistema. Para el intercambio de números de teléfono, en el menú de servicio del teléfono que se va a intercambiar seleccione la opción de intercambio de números de teléfono e introduzca el número de teléfono interno de la extensión de destino y el PIN de candado telefónico (este PIN no es necesario si tiene el valor estándar 00000). Después de introducir el número de destino, la prestación queda bloqueada hasta que finaliza el procedimiento para el resto de las extensiones. Al ejecutar el cambio, los dos terminales involucrados se reponen. Si el cambio ha concluido correctamente, se señaliza en los dos teléfonos TDM mediante la indicación del nuevo número de teléfono (indicación de display: Nuevo n.º llam.: XXXXX).

La reasignación no se puede ejecutar en teléfonos del sistema con autorización de programación (para Assistant T). Por norma general por tanto, no se puede realizar en los dos primeros teléfonos del sistema activos.

14.5.9.1 Cómo liberar la reasignación de números de teléfono a nivel de sistema

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Ajustes básicos** > **Sistema**.
3) En el grupo de menús, haga clic en **Flags del sistema**.
4) Active la casilla de verificación **Permitido cambio de terminales**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

14.5.10 Restablecimiento de las prestaciones activadas

En su terminal puede restablecer determinadas prestaciones mediante el uso de códigos.

Solo se puede hacer con estas prestaciones:

- Desvío de llamadas
- Borrar mensajes informativos recibidos
- Texto de respuesta activado / desactivado
- Timbre adicional activado / desactivado
- Línea colectiva activado / desactivado
- Supresión de la indicación del número de llamada activada / desactivada
- Aviso de llamada en espera silencioso activado / desactivado
- No molestar activado / desactivado
- Reposo activado / desactivado
- Cita
- Borrar todas las devoluciones

14.5.11 Procedimientos

El sistema de comunicación permite al usuario guardar códigos, números de teléfono e informaciones de marcación adicionales como procedimientos en una tecla. Si el usuario pulsa la tecla de procedimiento después de la marcación o durante una llamada, el sistema de comunicación envía los dígitos MF correspondientes (MF = procedimiento de marcación multifrecuencia).

Ejemplos de uso:

- Código de Devolución de llamada
- Código de Aviso de llamada en espera
- Código de Intercalar
- Secuencia de cifras para buzón de voz o contestador automático
- Código Flash de línea urbana + Número de destino
- Código para controlar un servicio + Número de destino, por ejemplo enviar / consultar Código de información (Message Waiting) + Número de teléfono + Número de texto
- PRO (código de proyecto) + Código de haz + Número de destino

Los procedimientos que exigen introducir un PIN no se pueden guardar.

Solo el primer nivel de teclas admite las teclas de procedimiento.

En los procedimientos, un usuario puede utilizar las siguientes prestaciones en función de la situación:

Prestación	listo para marcar	ocupado	al teléfono	Llamada saliente	llamada entrante
Telecaptura de llamadas, selectiva	x	–	x	–	–
Desvío de llamadas activado (no en centrales compartidas; no para los MSN de una conexión urbana S_0)	x	–	x	x	–
Desvío de llamadas externo activado / desactivado; Función de conmutación; (no en centrales compartidas);	x	–	x	x	–
Distribución de llamadas, Inicio de sesión / Finalizar sesión; Función de conmutación	x	–	x	x	–
Distribución de llamadas, Destino nocturno activado / desactivado; Función de conmutación	x	–	x	x	–
Desvío de llamadas por configuración de equipo	x	x	x	x	x
Texto de respuesta activado / desactivado; Función de conmutación	x	–	x	x	–
Marcación asoc.	x	x	x	x	x
Servicios asociados	x	–	x	x	–
Mensaje directo	x	–	x	–	–
Liberación de líneas (Emergency Trunk Access)	x	–	x	x	–
Enviar mensajes de información (Message Waiting)	x	–	x	x	–
Marcación de marcación abreviada individual	x	–	x	x	–
Marcación de marcación abreviada central	x	–	x	x	–
Transmisión MF	–	–	x	–	–
Transmisión MF en estado de llamada con una tecla de procedimiento	x	x	x	x	x
Servicio nocturno activado / desactivado; Función de conmutación	x	–	x	x	–
Aparcar / Desaparcar; Función de conmutación	–	x	x	x	–
Código de proyecto	x	–	x	–	–
Código de proyecto PRO en marcación inicial	x	–	x	–	–
Mostrar / borrar solicitudes de devolución de llamada; Función de conmutación	x	–	–	–	–
Timbre adicional activado / desactivado; Función de conmutación	x	–	x	x	–
Selección de idioma	x	x	x	x	x
Telephone Data Service (TDS)	x	–	x	x	–
Abrepuertas mediante adaptador	x	x	x	x	x

Prestación	listo para marcar	ocupado	al teléfono	Llamada saliente	llamada entrante
Cita activada / desactivada; Función de conmutación	x	x	x	x	x
Recuperación de una llamada externa desde una retención general	x	x	x	x	x
Candado telefónico central	x	–	x	–	–

Información específica de sistema

Una tecla de procedimiento puede guardar 32 caracteres como máximo.

14.5.12 Equipo de despertador y citas

Todas las extensiones tienen la posibilidad de programar un aviso de cita. Cuando llega el momento, se emite un aviso. El aviso de cita puede ejecutarse una sola vez (en las 24 horas siguientes) o repetidamente (es decir, diariamente).

La hora de las citas se introduce con cuatro cifras. Las dos primeras se corresponden con la hora y las dos últimas, con el minuto. En los EE. UU., la indicación de tiempo puede tener el formato de 12 horas. En este caso, después de introducir las cuatro cifras se puede seleccionar entre "am" (tecla 2) o "pm" (tecla 7). Si no se introduce ningún valor, se aplica "am".

Los teléfonos analógicos, optiPoint 500 entry o los teléfonos CMI solo se pueden programar citas únicas.

De forma predeterminada, los avisos de cita duran 20 segundos y se repiten hasta cinco veces tras pausas de un minuto. El aviso se borra automáticamente al descolgar el microteléfono o pulsar la tecla de altavoz durante la llamada o después de la quinta repetición (la cantidad se puede configurar). Un aviso de cita programado puede borrarse alternativamente también con un procedimiento. En terminales con display puede además realizarse una consulta.

Si al llegar el momento programado el aviso de cita no puede señalizarse (p. ej. porque la extensión está ocupada), éste se pospone hasta el ciclo siguiente.

Consejo: Se pueden programar recordatorios programados para hasta 50 usuarios, por sistema.

14.6 Descripción general de funciones y códigos

Código de servicio	Descripción
*0	Volver a extensión en espera
*1	Desvío de llamadas
*2	Alternar
*3	Conferencia

Código de servicio	Descripción
*44	Serv. noct. act.
*51	Señal a la red
*52	Mute act.
*53	Marc. DTMF
*55	Aceptar 2ª llam.
*56	Iniciar estacionamiento
*57	Telecaptura de llamadas en grupos de telecaptura
*58	Iniciar devolución de llamada
*59	Telecaptura de llamadas fuera de grupos de telecaptura
*60	Código de cuenta
*61	Abrepuertas
*62	Intercalar
*64	Desvío de llamadas en la central pública (RDSI) act.
*65	Consulta de tasas
*66	Candado telefónico act.
*67	Marcación asociada
*68	Enviar info
*69	Mensaje de aviso act.
*7	Almacenar marc.abr.cent./ind.
*80	Interfono
*90	Acceso para activar los contactos (accionar)
*91	Programación de teclas
*92	Modificar n° marc. abreviada
*93	Cambiar PIN
*940	Prueba de terminales
*95	Administración del sistema
*97	No molestar (DND) act.
	Vigilancia de habitación act.
*81	Timbre adicional act.
#1	Desvío desact.
#44	Serv. noct. desact.
#52	Mute desact.
#56	Recuperar llamada

Código de servicio	Descripción
#58	Consultar / borrar devoluciones de llamada
#64	Desvío de llamadas en la central pública (RDSI) desact.
#66	Candado telefónico desact.
#68	Leer / borrar mensajes informativos (enviados)
#69	Mensaje de aviso desact.
#97	No molestar (DND) desact.
*96	Contestación directa act.
#96	Contestación directa desact.
#90	Acceso para desactivar los contactos (desconectar)
#81	Timbre adicional desact.
#0	Restablecer todos los servicios
#3	Conferencia de 5 part. desact.
#82	Consultar lista de llamantes
*83	Servicios asociados
*84	Identificación llamadas maliciosas
*85	Línea colectiva act.
#85	Llam. grp. desact.
*82	Escribir lista de llamantes
*86	Supresión de indicación n.º de llamada act.
#86	Supresión de indicación n° de llamada desact.
*87	Aviso llam. espera silencioso act.
#87	Aviso llam. espera silencioso desact.
*98	Reposo act.
#98	Reposo desact.
*991	Administración remota del sistema por MF
*992	Liberar administración remota del sistema por MF
*993	Permitir la administración remota RDSI (obsoleto)
*994	Liberar consulta remota de datos del sistema

Código de servicio	Descripción
*89	Liberar abrepuertas mediante código MF
#89	Bloquear abrepuertas a través de código MF
*63	Recuperar llamada externa tras tecla de retención
*41	Asignar números de llamada en MUSAP
*401	Dar de alta agentes UCD
#401	Dar de baja agente UCD
*402	Agente UCD disponible
#402	Agente UCD no disponible
*403	Tiempo administrativo UCD act.
#403	Tiempo administrativo UCD des.
*404	Servicio nocturno UCD act.
#404	Servicio nocturno UCD des.
*405	Consultar estado cola de llamadas UCD
*42	Servicios de datos telefónicos (TDS)
*43	Liberar línea
*45	PSE: Buscar
#45	PSE: Contestar
*46	Equipo de timbre: cita act.
#46	Equipo de timbre: cita des.
*9419	Activar cambio de terminales
#9419	Desactivar cambio de terminales
*942	Disponibilidad para la alta (teléfono móvil)
*943	Candado telefónico central
*944	Supervisión de llamadas
	Drop Last Conference Party en línea urbana (sólo EE.UU.)
*490	Activar liberación para aviso llam. en espera
#490	Desactivar liberación para aviso llam. en espera
*48	Selección de idioma
*508	Flex Call

Código de servicio	Descripción
*502	Transferencia de llamada para MULAP act.
#502	Transferencia de llamada para MULAP act.
*501	AUL para MULAP act.
#501	AUL para MULAP desact.
*509	Congelar seguimiento
*47	DISA interno
*503	Marc. tecl. num.
*54	Listín telefónico interno
*491	terminal de hotel analógico
#943	Candado telefónico central / Reponer candado
*9411	Transferencia de llamadas Cliente en modo de emergencia activado
#9411	Transferencia de llamadas Cliente en modo de emergencia desactivado
*493	Grabación de voz act.
#493	Grabación de voz desact.
*495	Desvío diferido act.
#495	Desvío diferido desact.
*945	Mensaje discreto
*494	E/S datos
*996	Permitir Smart Services mediante HTTPS para administración remota
#996	Deshabilitar Smart Services mediante HTTPS para administración remota
*997	Apagado controlado

15 Trabajar en equipo (Grupos)

El sistema de comunicación ofrece numerosas prestaciones para el trabajo en equipo. Además de grupos de telecaptura, llamadas de grupo y líneas colectivas, también se incluyen grupos con funciones Team y Jefe/secretaria y grupos de buzón de voz y buzón de fax. La prestación "UCD (Uniform Call Distribution)" permite realizar una distribución uniforme de llamadas entrantes en un grupo de extensiones (Grupo UCD)..

Consejo: Al configurar grupos hay que tener en cuenta que los tres primeros grupos están reservados:

El primer grupo se utiliza de forma predeterminada como grupo de búsqueda para el correo de voz externo.

El segundo se utiliza de forma predeterminada como línea colectiva para OpenScape Business Smart VoiceMail.

El tercer grupo se utiliza de forma predeterminada como línea colectiva para el Company AutoAttendant de OpenScape Business Smart VoiceMail.

15.1 Grupo de telecaptura, Llamada de grupo y Línea colectiva

El sistema de comunicación ofrece distintas opciones para agrupar extensiones en grupos. De esta forma, por ejemplo, se puede acceder a varios usuarios y teléfonos a través de un único número de teléfono o las llamadas dirigidas a un usuario se señalizan también en otras extensiones.

En el caso de los grupos de telecaptura, las llamadas dirigidas a un miembro se señalizan en todos los demás miembros del grupo.

Si se trata de una llamada de grupo, se puede acceder a todos los miembros con un único número de teléfono (número de teléfono de grupo). El primer miembro en descolgar será conectado con el llamante.

En una línea colectiva, las llamadas entrantes se señalizan en uno de los miembros. Si este miembro no acepta la llamada, esta se asigna al siguiente miembro. Se puede acceder a todos los miembros de la línea colectiva a través de un único número de teléfono.

15.1.1 Grupo de telecaptura

Una llamada dirigida a un miembro del grupo de telecaptura de llamadas, se señaliza en todos los demás miembros del grupo. Todos los demás miembros del grupo pueden aceptar la llamada a través de una tecla de función programada para ello o a través de la opción de menú o del código correspondientes.

El miembro del grupo de telecaptura llamado en origen recibirá una señal visual y sonora (display). Si está programado, la llamada también se señaliza en el LED de la tecla de función.

Los demás miembros del grupo solo reciben una señalización óptica de la llamada. En el display se muestra el número de teléfono o el nombre del

usuario llamado en origen y el número de teléfono o nombre del llamante. Un administrador con el perfil **Experto** puede desactivar la indicación del número de teléfono o del nombre del llamante a través del **Modo Experto**. Si está programado, la llamada también se señaliza en el LED de la tecla de función.

Si no se acepta la llamada en cuatro ciclos de llamada (4x5 segundos), los demás miembros del grupo reciben también un tono de advertencia (señalización acústica). El tiempo que transcurre entre el inicio de la señalización de llamada y el tono de advertencia no es variable. Un administrador con el perfil **Experto** puede desactivar el tono de advertencia para todos los miembros del grupo a través del **Modo Experto**.

Si un grupo de telecaptura de llamadas recibe varias llamadas, la señalización sigue el orden de entrada de las llamadas.

Para que los miembros de un grupo AUN puedan atender las llamadas recordatorias de otros miembros, un administrador con el perfil **Experto** puede activar la función a través del **Modo Experto**.

Una extensión solo puede ser miembro de un grupo de telecaptura de llamadas.

Las tasas que pudieran derivar de una llamada capturada se asignan al usuario que ha capturado la llamada.

Nota: No se admiten comillas dobles (") para designar una Telecaptura de llamadas en grupos de telecaptura

---

Teléfonos SIP

En un grupo de telecaptura se pueden incluir teléfonos SIP.

Consejo: Además, en los teléfonos SIP se puede programar una tecla de función para los grupos de telecaptura y los mensajes específicos de un grupo de telecaptura se pueden mostrar en el display de los teléfonos SIP. Para utilizar estas funciones, hay que activar la prestación "Grupo de telecaptura" en el teléfono SIP (véanse las Instrucciones de uso del teléfono SIP).

Telecaptura de llamadas fuera de un grupo de telecaptura

Una variante de esta prestación es la "telecaptura de llamadas fuera de un grupo de telecaptura". Esta variante permite capturar llamadas dirigidas a extensiones internas que no pertenecen al mismo grupo de telecaptura de llamadas. Las llamadas se capturan a través de una tecla de función programada para ello o a través de la opción de menú o código de telecaptura de llamadas, introduciendo a continuación el número de teléfono de la extensión llamada.

Dependencias

Tema	Dependencia
Devol. llam.	Los demás miembros del grupo solo reciben señalización de las llamadas recordatorias y de las devoluciones de llamadas si el flag del sistema **Telecaptura de llamadas después de llamada recordatoria** está activado.
No molestar	Los usuarios que tengan activado el estado No molestar, no recibirán ninguna señalización de telecaptura de llamadas.
Teléfonos RDSI	No se pueden incluir teléfonos RDSI en grupos de telecaptura de llamadas.
MULAP	No se pueden incluir números de teléfono MULAP en grupos de telecaptura de llamadas.

Tareas relacionadas

Configurar grupo de telecaptura en la página 707
Cómo añadir o borrar miembros de un grupo de telecaptura en la página 708
Cómo activar o desactivar la indicación del número de teléfono y del nombre del llamante en la página 715
Cómo activar o desactivar tono de advertencia en la página 716
Cómo activar o desactivar la telecaptura de llamadas recordatorias en la página 716

15.1.2 Llamada de grupo

Si varios suscriptores deben estar disponibles a través de un único número de teléfono (número de teléfono de grupo), se puede definir una llamada de grupo. Las llamadas entrantes externas e internas se señalizarán, simultáneamente, en todos los miembros del grupo. La primera extensión en descolgar se conectará con el llamante.

Todos los miembros de una llamada de grupo siguen estando accesibles a través de su propio número de extensión.

El grupo debe asignarse a una de estas propiedades:

- Grupo

  Las llamadas entrantes se señalizan simultáneamente en todos los miembros del grupo disponibles. Los miembros del grupo disponibles son suscriptores que no están ocupados. Si todos los miembros del grupo están ocupados, las nuevas llamadas se señalizan con el tono de llamada en espera. La señalización de llamada continúa para todos los miembros del grupo (tono de aviso para los miembros del grupo ocupados) incluso si el abonado cuelga.

  Si todos los miembros del grupo están ocupados y todos han activado la prestación No molestar, los llamantes recibirán el tono de ocupado. Si hay definido un destino de transferencia automática diferida para el grupo, el llamante no recibe el tono de ocupado sino que se le transfiere directamente al siguiente destino de transferencia automática diferida.

- RNA

  Las llamadas entrantes se señalizan simultáneamente en todos los miembros del grupo. Si un miembro del grupo está ocupado, la llamada se identifica como ocupada para todo el grupo. Los demás llamantes reciben el tono de ocupado.

  Nota: No se puede detectar el estado de presencia de un destino externo que pertenece al grupo.

- Aviso llam. en espera

  Las llamadas entrantes se señalizan simultáneamente en todos los miembros del grupo disponibles. Los miembros del grupo disponibles son suscriptores que no están ocupados. En caso de llamada, los miembros del grupo ocupados recibirán como señal el tono de llamada en espera.

  El requisito para ello es que todos los miembros del grupo hayan desactivado la notificación No molestar.

La transferencia automática diferida de llamadas considera a las llamadas de grupo como extensiones. Esto significa que si una llamada no puede ser aceptada por ningún miembro de una llamada de grupo, se redirigirá a un destino de transferencia automática diferida indicado en la lista de destinos de llamada. Se puede especificar si la transferencia automática diferida de llamadas se realizará en caso de libre (suena el teléfono pero no se atiende la llamada) o en caso de ocupado.

Si ningún miembro de una llamada de grupo atiende una llamada, se muestra como llamada perdida en el diario de los clientes de UC de todos los miembros. Las llamadas aceptadas solo se muestran en el diario del miembro que las haya contestado.

Una misma extensión puede pertenecer a varios grupos al mismo tiempo. Lo siguiente se aplica a los grupos del tipo Llamada de grupo / Línea colectiva, Configuración de equipo / Grupo Team y Jefe/Secretaria / Grupo Top: La suma de todos los suscriptores en estos grupos no debe exceder 32.

En la pantalla de un usuario llamante interno se muestra el nombre del grupo asignado. Después de aceptar una llamada, se indica el nombre del suscriptor que ha aceptado la llamada.

Si un miembro ha definido reglas a través de AutoAttendant (por ejemplo, para la transferencia o desvío de llamadas), estas reglas solo se aplican a las llamadas dirigidas a su número de extensión propio. En las llamadas de grupo se ignoran dichas reglas.

Se pueden configurar hasta 20 suscriptores por llamada de grupo.

Se puede asignar a cada llamada de grupo un nombre de hasta 16 caracteres.

Buzón de voz para llamada de grupo

Al configurar una llamada de grupo se configura también automáticamente un buzón de voz. El número de teléfono de ese buzón de voz de llamada de grupo corresponde siempre al número de la llamada de grupo. Si una llamada de grupo no es aceptada por ningún miembro, la llamada se transfiere al buzón de voz de llamada de grupo. Para ello es necesario que el buzón de voz de llamada de grupo se haya definido como destino de la transferencia de llamadas en caso de no contestarse.

Si un miembro no acepta una llamada entrante dirigida a su número de teléfono de extensión propio, la llamada se transfiere a un destino de transferencia indicado en la lista de destinos de llamada.

Ejemplo de llamada de grupo de tipo Caso de libre con el número de llamada de grupo 404 y los miembros A (número de extensión 200), B (201) y C (202). Para la llamada de grupo se ha configurado una transferencia automática diferida al transcurrir el tiempo de espera, para desviar llamadas al buzón de voz de llamada de grupo. Todos los miembros han definido la prestación Desvío de llamadas: no contesta (CFNA), después de transcurrir el tiempo de espera, para la transferencia a su propio buzón de voz.		
Llamada entrante para el miembro A (200)	Todos los miembros están libres.	El miembro A no acepta la llamada. Se realiza la prestacion Desvío de llamadas: no contesta (CFNA) al buzón de voz del miembro A, después de transcurrir el tiempo de espera.
	El miembro A ha definido el Desvío de llamada directo o CFU, a su propio buzón de voz. Los miembros B y C están libres.	Se realiza una transferencia inmediata al buzón de voz del miembro A.
Llamada entrante para la llamada de grupo (404)	Todos los miembros están libres.	La llamada se señaliza en todos los miembros. Ningún miembro acepta la llamada. Se realiza la prestacion Desvío de llamadas: no contesta (CFNA), hacia el buzón de voz de llamada de grupo.
	El miembro A ha definido el Desvío de llamada directo o CFU, a su propio buzón de voz. Los miembros B y C están libres.	La llamada se señaliza en los miembros B y C. Ningún miembro acepta la llamada. Se realiza la prestacion Desvío de llamadas: no contesta (CFNA), hacia el buzón de voz de llamada de grupo.
	El miembro A ha definido el Desvío de llamada directo a un destino externo. Los miembros B y C están libres.	La llamada se señaliza en los miembros B y C y en el destino externo. Ningún miembro acepta la llamada. Se realiza la prestacion Desvío de llamadas: no contesta (CFNA), hacia el buzón de voz de llamada de grupo.
	El miembro A ha definido reglas para la transferencia automática diferida a través de AutoAttendant. Los miembros B y C están libres.	La llamada se señaliza en todos los miembros. Ningún miembro acepta la llamada. Se realiza la prestacion Desvío de llamadas: no contesta (CFNA), hacia el buzón de voz de llamada de grupo.

Activar/Desactivar una llamada de grupo

Si un suscriptor es miembro de una llamada de grupo puede utilizar códigos para abandonar la llamada de grupo y para volver a unirse a ella.

Si un suscriptor es miembro de varias llamadas de grupo y de varias líneas colectivas, puede utilizar códigos para abandonar todas las llamadas de grupo y todas las líneas colectivas y para volver a unirse a ellas. Para abandonar o para unirse a una determinada llamada de grupo o línea colectiva se pueden utilizar códigos y, a continuación, seleccionar una de las llamadas de grupo o líneas colectivas mostradas.

También se pueden programar teclas de función con función de conmutación para abandonar o unirse a una llamada o línea. Se puede programar una tecla de función válida para una o para todas las llamadas de grupo y líneas colectivas. También se puede hacer una programación variable. Después de pulsar una de estas teclas de función se debe seleccionar una de las llamadas de grupo o líneas colectivas mostradas. Así puede definir a qué llamada de grupo o línea colectiva desea unirse o abandonar.

Tipo de llamada

Para cada llamada grupal, un administrador con el perfil de **Experto** puede definir la señalización acústica de las llamadas externas entrantes a través de la configuración del tipo de timbre. Tiene las siguientes opciones:

- Tono de llamada doble (configuración estándar)
- Tono de llamada triple
- Tono de llamada corto/largo/corto

En los teléfonos analógicos solo se puede aplicar la configuración estándar. Los cambios no tienen ningún efecto.

Teléfonos SIP

En una llamada de grupo se pueden incluir teléfonos SIP.

Nota: En los teléfonos SIP no se pueden programar teclas de función. No se admiten mensajes de visualización específicos de un grupo de búsqueda.

Dependencias

Tema	Dependencia
Desvío de llamadas	Si un miembro de grupo activa un desvío de llamadas para todas las llamadas, todas ellas se señalizan en el teléfono de destino.
No molestar	Si un miembro de grupo activa el estado No molestar, las llamadas entrantes dirigidas a su teléfono no se transfieren. Esto se aplica a todas las llamadas a través del número de llamada de grupo y a las dirigidas a la propia extensión.
Anular	Si todos los miembros de una llamada de grupo están ocupados no se puede realizar ninguna intercalación.

Tema	Dependencia
Teléfonos RDSI	No se pueden incluir teléfonos RDSI en una llamada de grupo.

Conceptos relacionados

Directorio interno en la página 521

Tareas relacionadas

Cómo agregar una llamada de grupo (grupo) en la página 708
Cómo modificar una llamada de grupo (grupo) en la página 709
Cómo borrar una llamada de grupo (grupo) en la página 710
Cómo agregar o borrar miembro a llamada de grupo (grupo) en la página 711
Cómo agregar llamada de grupo (caso de libre o aviso de llamada en espera) en la página 717
Cómo mostrar o modificar llamada de grupo (Caso de libre o Aviso de llamada en espera) en la página 718
Cómo borrar llamada de grupo (caso de libre o aviso de llamada en espera) en la página 718
Cómo agregar o borrar miembro a llamada de grupo (caso de libre o aviso de llamada en espera) en la página 718
Cómo activar o desactivar el bloqueo de avisos de llamada en espera para miembro de grupo en la página 719

15.1.3 Línea colectiva

Los grupos de búsqueda permiten la distribución de llamadas entrantes a suscriptores asociados (miembros). Si un abonado está ocupado o no acepta una llamada entrante, la llamada se reenvía automáticamente al siguiente miembro libre del grupo de búsqueda. Se puede contactar con todos los miembros del grupo de búsqueda en el mismo número de teléfono.

También se puede contactar con cada miembro de un grupo de búsqueda a través de su propio número de estación.

Al grupo de búsqueda se le debe asignar una de las siguientes propiedades.

- Lineal

  Una llamada entrante siempre se señala primero en el primer miembro de un grupo de búsqueda. La señalización adicional se realiza en función de la secuencia en la que se introducen los miembros en la tabla de grupo.
- Cíclico

  Una llamada entrante siempre se señala primero en el miembro que sigue al suscriptor que respondió la última llamada. La señalización adicional se realiza en función de la secuencia en la que se introducen los miembros en la tabla de grupo.

La llamada se reenvía automáticamente al siguiente miembro libre del grupo de búsqueda cuando expira el tiempo de reenvío, siempre que no se responda la llamada o un miembro esté ocupado o la función DND esté activada.

Puede programar un destino de reenvío de llamadas (lista de destinos de llamadas) si ninguno de los miembros del grupo de búsqueda puede responder una llamada.

Una misma extensión puede pertenecer a varios grupos al mismo tiempo. Lo siguiente se aplica a los grupos del tipo Llamada de grupo / Línea colectiva, Configuración de equipo / Grupo Team y Jefe/Secretaria / Grupo Top: La suma de todos los suscriptores en estos grupos no debe exceder 32.

El nombre asignado al grupo de búsqueda se muestra en la pantalla del llamante interno. Después de aceptar una llamada, se indica el nombre del suscriptor que ha aceptado la llamada.

Si un miembro ha definido reglas a través de AutoAttendant (por ejemplo, para la transferencia o desvío de llamadas), estas reglas solo se aplican a las llamadas dirigidas a su número de extensión propio. Las reglas se ignoran para las llamadas de grupo de búsqueda.

Se pueden configurar hasta 20 suscriptores por grupo de búsqueda.

A cada grupo de búsqueda se le puede asignar un nombre que contenga hasta 16 caracteres.

Buzón de voz para grupos de búsqueda

Al configurar un grupo de búsqueda, se crea automáticamente un buzón de correo de voz para él. El número de llamada de este buzón de voz para el grupo de búsqueda siempre coincide con el del grupo de búsqueda. Si ningún miembro acepta una llamada de un grupo de búsqueda, la llamada se reenvía al buzón de correo de voz de ese grupo de búsqueda. Esto requiere que el buzón de correo de voz del grupo de búsqueda se haya definido como destino CFNA (reenvío de llamadas en caso de falta de respuesta) de este grupo de búsqueda.

Si un miembro no acepta una llamada entrante dirigida a su número de teléfono de extensión propio, la llamada se transfiere a un destino de transferencia indicado en la lista de destinos de llamada.

Ejemplo de un grupo de búsqueda lineal con el número de referencia 404 y los miembros A (número de referencia 200), B (201) y C (202). Reenvío de llamadas: No hay respuesta después del tiempo de espera al buzón de correo de voz del grupo de búsqueda que se configuró para el grupo de búsqueda. Todos los miembros han definido la prestación Desvío de llamadas: no contesta (CFNA), después de transcurrir el tiempo de espera, para la transferencia a su propio buzón de voz.		
Llamada entrante para el miembro A (200)	Todos los miembros están libres.	El miembro A no acepta la llamada. Se realiza la prestacion Desvío de llamadas: no contesta (CFNA) al buzón de voz del miembro A, después de transcurrir el tiempo de espera.
	El miembro A ha definido el Desvío de llamada directo o CFU, a su propio buzón de voz. Los miembros B y C están libres.	Se realiza una transferencia inmediata al buzón de voz del miembro A.

Llamada entrante para el grupo de búsqueda (404)	Todos los miembros están libres.	La llamada se señala primero al miembro A, luego al miembro B y luego al miembro C. Ningún miembro acepta la llamada. Reenvío de llamadas: Si no hay respuesta después del tiempo de espera, se produce un error en el buzón de correo de voz del grupo de búsqueda.
	El miembro A ha definido el Desvío de llamada directo o CFU, a su propio buzón de voz. Los miembros B y C están libres.	La llamada se señala primero al miembro B y luego al miembro C. Ningún miembro acepta la llamada. Reenvío de llamadas: Si no hay respuesta después del tiempo de espera, se produce un error en el buzón de correo de voz del grupo de búsqueda.
	El miembro A ha definido el Desvío de llamada directo a un destino externo. Los miembros B y C están libres.	La llamada se señala primero al miembro B y luego al miembro C. Ningún miembro acepta la llamada. Reenvío de llamadas: Si no hay respuesta después del tiempo de espera, se produce un error en el buzón de correo de voz del grupo de búsqueda.
	El miembro A ha definido reglas para la transferencia automática diferida a través de AutoAttendant. Los miembros B y C están libres.	La llamada se señala primero al miembro A, luego al miembro B y luego al miembro C. Ningún miembro acepta la llamada. Reenvío de llamadas: Si no hay respuesta después del tiempo de espera, se produce un error en el buzón de correo de voz del grupo de búsqueda.

Activación/desactivación del grupo de búsqueda

Si un suscriptor es miembro de un grupo de búsqueda, puede usar códigos para abandonar y volver a unirse al grupo de búsqueda.

Si un suscriptor es miembro de varios grupos de búsqueda y de varias llamadas grupales, puede usar códigos para abandonar y volver a unirse a todos los grupos de búsqueda y llamadas grupales. Los suscriptores se agregan o eliminan de un grupo de búsqueda o llamada grupal específico ingresando códigos y luego haciendo una selección entre los grupos de búsqueda y llamadas grupales que se muestran.

También se pueden programar teclas de función con función de conmutación para abandonar o unirse a una llamada o línea. Puede programar aquí una tecla de función que se aplique a un grupo de búsqueda y a una llamada de grupo específicos o a todos ellos. También se puede hacer una programación variable. Después de presionar una tecla de función de este tipo, debe seleccionar uno de los grupos de búsqueda o llamadas grupales que se muestran para definir el grupo de búsqueda o la llamada grupal que desea abandonar/unir.

Tipo de llamada

Para cada grupo de búsqueda, un administrador con el perfil **Experto** puede definir la señalización acústica de las llamadas externas entrantes a través de la configuración del tipo de timbre. Tiene las siguientes opciones:

- Tono de llamada doble (configuración estándar)
- Tono de llamada triple
- Tono de llamada corto/largo/corto

En los teléfonos analógicos solo se puede aplicar la configuración estándar. Los cambios no tienen ningún efecto.

Teléfonos SIP

Los teléfonos SIP se pueden integrar en un grupo de búsqueda.

Consejo: En los teléfonos SIP no se pueden programar teclas de función. No se admiten mensajes de visualización específicos de un grupo de búsqueda.

Dependencias

Tema	Dependencia
Desvío de llamadas	Si un miembro del grupo de búsqueda activa el reenvío de llamadas para todas las llamadas, todas las llamadas se señalizan en el teléfono de destino.
No molestar	Si un miembro del grupo de búsqueda activa la función No molestar, las llamadas entrantes a su teléfono no se transferirán. Esto se aplica a las llamadas al grupo de búsqueda y al número de estación propio del miembro.
Cola	Para los grupos de búsqueda cíclicos y lineales, no es posible configurar una cola de llamadas.
Teléfonos RDSI	No es posible incluir teléfonos ISDN en grupos de búsqueda.

Tareas relacionadas

Cómo agregar una línea colectiva en la página 711
Cómo modificar una línea colectiva en la página 713
Cómo borrar una línea colectiva en la página 714
Cómo agregar o borrar miembro de línea colectiva en la página 714

15.1.4 Configuración de grupos de telecaptura, llamadas de grupo y líneas colectivas mediante asistentes

Distintos asistentes permiten realizar cómodamente la configuración de grupos de telecaptura, llamadas de grupo y líneas colectivas.

El asistente **Telecaptura de llamadas** permite reunir extensiones en un grupo para que puedan realizar una captura de llamadas mutua. Se describe el modo

de proceder para los siguientes casos de aplicación que pueden configurarse a través del asistente:

- Configurar grupo de telecaptura
- Cómo añadir o borrar miembros de un grupo de telecaptura

El asistente **Llamada de grupo / Línea colectiva** permite configurar grupos de llamada del tipo Grupo. Se describe el modo de proceder para los siguientes casos de aplicación que pueden configurarse a través del asistente:

- Cómo agregar una llamada de grupo (grupo)
- Cómo modificar una llamada de grupo (grupo)
- Cómo borrar una llamada de grupo (grupo)
- Cómo agregar o borrar miembro a llamada de grupo (grupo)
- Cómo agregar una línea colectiva
- Cómo modificar una línea colectiva
- Cómo borrar una línea colectiva
- Cómo agregar o borrar miembro de línea colectiva

15.1.4.1 Configurar grupo de telecaptura

El asistente **Telecaptura de llamadas** permite combinar extensiones en un grupo, permitiendo así la captura mutua de llamadas.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Telecaptura de llamadas**. Podrá ver una lista de todos los grupos de telecaptura de llamada posibles.
4) Para configurar un grupo de telecaptura de llamadas, en la línea del grupo deseado haga clic en **Editar**.
5) Si desea agregar Miembros al grupo de telecaptura, active la casilla de verificación **Asignación Grupo <Número>** de los nombres o números de teléfono deseados.
6) Si desea eliminar miembros del grupo de telecaptura, desactive la casilla de verificación **Asignación Grupo <Número>** de los nombres o números de teléfono deseados.
7) Haga clic en **Aceptar**, para aplicar las entradas.
8) En el campo **Nombre**, indique el nombre del grupo de telecaptura configurado.
9) Si desea configurar nuevos grupos de telecaptura, repita los pasos del 4 al 8.
10) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Grupo de telecaptura en la página 697

15.1.4.2 Cómo añadir o borrar miembros de un grupo de telecaptura

El asistente **Telecaptura de llamadas** permite agregar o borrar miembros de grupos de telecaptura.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Telecaptura de llamadas**.
4) En la línea del grupo de telecaptura deseado, haga clic en **Editar**.
5) Elija una de estas opciones:
   - Si desea agregar Miembros al grupo de telecaptura, active la casilla de verificación **Asignación Grupo <Número>** de los nombres o números de teléfono deseados.
   - Si desea eliminar miembros del grupo de telecaptura, desactive la casilla de verificación **Asignación Grupo <Número>** de los nombres o números de teléfono deseados.
6) Haga clic en **Aceptar**, para confirmar las entradas.
7) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Grupo de telecaptura en la página 697

15.1.4.3 Cómo agregar una llamada de grupo (grupo)

El asistente **Llamada de grupo / Línea colectiva** permite configurar grupos de llamada del tipo Grupo.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Llamada de grupo / Línea colectiva**.
4) Haga clic en **Agregar**, para configurar un nuevo grupo.
5) En el campo **N.º de llamada del grupo**, indique el número de teléfono de la nueva llamada de grupo.

6) En el campo **Número de marcación directa** indique el número de marcación directa de la nueva llamada de grupo.

: Si desea utilizar DID 879, 890 o 891, debe hacer la configuración a través de ManagerE y no a través de WBM.

7) En el campo **Nombre del grupo** indique el nombre de la nueva llamada de grupo.
8) En la lista desplegable **Tipo**, seleccione la entrada **Grupo**.
9) Elija una de estas opciones para incluir el número de teléfono de la llamada de grupo en el directorio interno:
   - Si desea que el número de teléfono de la llamada de grupo aparezca en el directorio interno, active la casilla de verificación **Listín tel.**.
   - Si no desea que el número de teléfono de la llamada de grupo aparezca en el directorio interno, desactive la casilla de verificación **Listín tel.**.
10) En la lista desplegable **Número de teléfono de la extensión a la que se va a asignar el grupo**, seleccione el número de teléfono de la extensión deseada.
11) Haga clic en **OK y Continuar**.

Consejo: Si el número de teléfono o el número de marcación directa marcado ya existen, puede consultar el plan de numeración actual para establecer un número de teléfono o número de marcación directa libre.

12) En la línea de la llamada de grupo nueva, haga clic en **Editar** para asignar nuevas extensiones a la llamada de grupo.
13) En la lista desplegable **N.º de llamada**, seleccione el número de teléfono de la extensión a la que desea asignar la llamada de grupo.
14) Haga clic **Agregar**.
15) Si desea asignar otras extensiones a la llamada de grupo, repita los pasos 13 y 14.
16) Haga clic en **Aceptar**, para aplicar las entradas.
17) Si desea configurar una nueva llamada de grupo, repita los pasos del 4 al 16.
18) Haga clic en**OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Llamada de grupo en la página 699

15.1.4.4 Cómo modificar una llamada de grupo (grupo)

El asistente **Llamada de grupo / Línea colectiva** permite editar grupos de llamada del tipo Grupo.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Llamada de grupo / Línea colectiva**.
4) En la línea de la llamada de grupo que desee modificar, haga clic en **Editar**.
5) Modifique los parámetros de grupo deseados.
6) Solo con UC Smart: en caso necesario, asigne un buzón a la llamada de grupo:
   a) Een la lista desplegable **Tipo de buzón UC Smart**, seleccione si la llamada de grupo tendrá un buzón estándar o un buzón de puesto de operadora (AutoAttendant).
   b) Solo con buzón estándar: si los llamantes pueden dejar un mensaje en el buzón de voz, active la casilla de verificación **Grabación**.
   c) En la lista desplegable **Saludo** introduzca un saludo.
   d) Si desea restablecer la contraseña del buzón de voz, active la casilla de verificación **Reponer contraseña**.

   Nota: La casilla de verificación **Reponer contraseña** no debe estar marcada al cambiar la configuración de un buzón de voz. Hace que se restablezca la contraseña del buzón de voz. Al cambiar la configuración, el usuario ya debe modificar la contraseña inicial al acceder por primera vez al buzón de voz.
7) Si desea agregar un miembro a la llamada de grupo, en la lista desplegable **Núm. llam.**, seleccione el número de teléfono de la extensión deseada. A continuación, haga clic en **Agregar**.
8) Si desea borrar un miembro de la llamada de grupo, en la línea del miembro de grupo deseado, haga clic en **Borrar** y, a continuación, en **Aceptar**.
9) Haga clic en **Aceptar**, para confirmar las entradas.
10) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Llamada de grupo en la página 699

15.1.4.5 Cómo borrar una llamada de grupo (grupo)

El asistente **Llamada de grupo / Línea colectiva** permite borrar llamadas de grupo del tipo Grupo.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Llamada de grupo / Línea colectiva**.
4) En la línea de la llamada de grupo que desee borrar, haga clic en **Editar**.
5) Haga clic en **Borrar datos**.
6) Haga clic en **Aceptar**, para confirmar el borrado.
7) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Llamada de grupo en la página 699

15.1.4.6 Cómo agregar o borrar miembro a llamada de grupo (grupo)

El asistente **Llamada de grupo / Línea colectiva** permite agregar o borrar miembros a las llamadas de grupo de tipo Grupo.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Llamada de grupo / Línea colectiva**.
4) En la línea de la llamada de grupo deseada, haga clic en **Editar**.
5) Elija una de estas opciones:
   - Si desea agregar un miembro a la llamada de grupo, en la lista desplegable **Núm. llam.**, seleccione el número de teléfono de la extensión deseada. A continuación, haga clic en **Agregar**.
   - Si desea borrar un miembro de la llamada de grupo, en la línea del miembro de grupo deseado, haga clic en **Borrar** y, a continuación, en **Aceptar**.
6) Haga clic en **Aceptar**, para confirmar las entradas.
7) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Llamada de grupo en la página 699

15.1.4.7 Cómo agregar una línea colectiva

El asistente **Llamada de grupo / Línea colectiva** permite configurar líneas colectivas.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Llamada de grupo / Línea colectiva**.
4) Haga clic en **Agregar** para configurar una nueva línea colectiva.
5) En el campo **N.º de llamada del grupo**, indique el número de teléfono de la nueva línea colectiva.
6) En el campo **Número de marcación directa**, indique el número de marcación directa de la nueva línea colectiva.

   : Si desea utilizar DID 879, 890 o 891, debe hacer la configuración a través de ManagerE y no a través de WBM.

7) En el campo **Nombre del grupo**, indique el nombre de la nueva línea colectiva.
8) En la lista desplegable **Tipo**, seleccione el tipo de la nueva línea colectiva. Tiene las siguientes opciones:
   - Si desea que la señalización de las llamadas se realice siempre en primer lugar en el primer miembro de la línea colectiva, seleccione la entrada **Lín. colectiva lineal**.
   - Si desea que la señalización de las llamadas se realice en primer lugar en aquel miembro de la línea colectiva que esté inmediatamente después de la extensión que atendió la última llamada, seleccione la entrada **Lín. colectiva cíclica**.
9) Elija una de estas opciones para incluir el número de teléfono de la línea colectiva en el directorio interno:
   - Si desea que el número de teléfono de la línea colectiva aparezca en el directorio interno, active la casilla de verificación **Listín tel.**
   - Si no desea que el número de teléfono aparezca en el directorio interno, desactive la casilla de verificación **Listín tel.**
10) En la lista desplegable **Número de teléfono de la extensión a la que se va a asignar el grupo**, seleccione el número de teléfono de la extensión deseada.
11) Haga clic en **OK y Continuar**.

    Consejo: Si el número de teléfono o el número de marcación directa marcado ya existen, puede consultar el plan de numeración actual para establecer un número de teléfono o número de marcación directa libre.

12) En la línea de la línea colectiva nueva, haga clic en **Editar** para asignar nuevas extensiones a la línea colectiva.
13) En la lista desplegable **N.º de llamada**, seleccione el número de teléfono de la extensión a la que se va a asignar la línea colectiva.
14) Haga clic **Agregar**.

15) Si desea asignar más extensiones a la línea colectiva, repita los pasos 13 y 14.
16) Haga clic en **Aceptar**, para aplicar las entradas.
17) Si desea configurar una nueva línea colectiva, repita los pasos del 4 al 16.
18) Haga clic en**OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Línea colectiva en la página 703

15.1.4.8 Cómo modificar una línea colectiva

El asistente **Llamada de grupo / Línea colectiva** permite editar líneas colectivas.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Llamada de grupo / Línea colectiva**.
4) En la línea de la fila colectiva que desee modificar, haga clic en **Editar**.
5) Modifique los parámetros deseados de la línea colectiva.
6) Solo con UC Smart: en caso necesario, asigne un buzón a la línea colectiva:
   a) En la lista desplegable **Tipo de buzón UC Smart**, seleccione si la línea colectiva tendrá un buzón estándar o un buzón de puesto de operadora (AutoAttendant).
   b) Solo con buzón estándar: si los llamantes pueden dejar un mensaje en el buzón de voz, active la casilla de verificación **Grabación**.
   c) En la lista desplegable **Saludo** introduzca un saludo.
   d) Si desea restablecer la contraseña del buzón de voz, active la casilla de verificación **Reponer contraseña**.

   Nota: La casilla de verificación **Reponer contraseña** no debe estar marcada al cambiar la configuración de un buzón de voz. Hace que se restablezca la contraseña del buzón de voz. Al cambiar la configuración, el usuario ya debe modificar la contraseña inicial al acceder por primera vez al buzón de voz.
7) Si desea agregar un miembro a la línea colectiva, en la lista desplegable **Núm. llam.**, seleccione el número de teléfono de la extensión deseada. A continuación, haga clic en **Agregar**.
8) Si desea borrar un miembro de la línea colectiva, en la línea del miembro de grupo deseado, haga clic en **Borrar** y, a continuación, en **Aceptar**.

9) Si desea modificar la posición de un miembro en la línea colectiva, haga clic en **Modificar secuencia**. En el campo **Posición** de cada miembro, indique el número de posición deseado. Haga clic en **OK & Continuar**.
10) Haga clic en **Aceptar**, para confirmar las entradas.
11) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Línea colectiva en la página 703

15.1.4.9 Cómo borrar una línea colectiva

El asistente **Llamada de grupo / Línea colectiva** permite borrar líneas colectivas.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Llamada de grupo / Línea colectiva**.
4) En la línea de la línea colectiva que desee borrar, haga clic en **Editar**.
5) Haga clic en **Borrar datos**.
6) Haga clic en **Aceptar**, para confirmar el borrado.
7) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Línea colectiva en la página 703

15.1.4.10 Cómo agregar o borrar miembro de línea colectiva

El asistente **Llamada de grupo / Línea colectiva** permite agregar o borrar miembros a líneas colectivas.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Llamada de grupo / Línea colectiva**.
4) En la línea de la línea colectiva deseada, haga clic en **Editar**.

5) Elija una de estas opciones:
   - Si desea agregar un miembro a la línea colectiva, en la lista desplegable **Núm. llam.**, seleccione el número de teléfono de la extensión deseada. A continuación, haga clic en **Agregar**.
   - Si desea borrar un miembro de la línea colectiva, en la línea del miembro de grupo deseado, haga clic en **Borrar** y, a continuación, en **Aceptar**.
6) Haga clic en **Aceptar**, para confirmar las entradas.
7) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Línea colectiva en la página 703

15.1.5 Configuración de grupos de telecaptura, llamadas de grupo y líneas colectivas mediante el modo Experto

Además de las opciones de configuración mediante asistentes, los administradores con el perfil **Experto** tienen opciones adicionales para la configuración de grupos de telecaptura, llamadas de grupo y líneas colectivas mediante el **modo Experto**.

Se describe el modo de proceder para los siguientes casos de aplicación que pueden configurarse a través del **Modo Experto**:

- Cómo activar o desactivar la indicación del número de teléfono y del nombre del llamante
- Cómo activar o desactivar tono de advertencia
- Cómo activar o desactivar la telecaptura de llamadas recordatorias
- Cómo agregar llamada de grupo (caso de libre o aviso de llamada en espera)
- Cómo mostrar o modificar llamada de grupo (Caso de libre o Aviso de llamada en espera)
- Cómo borrar llamada de grupo (caso de libre o aviso de llamada en espera)
- Cómo agregar o borrar miembro a llamada de grupo (caso de libre o aviso de llamada en espera)
- Cómo activar o desactivar el bloqueo de avisos de llamada en espera para miembro de grupo

15.1.5.1 Cómo activar o desactivar la indicación del número de teléfono y del nombre del llamante

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema** > **Flags del sistema**.

4) Elija una de estas opciones:
   - Si desea mostrar el número de teléfono y el nombre del llamante, active la casilla de verificación **Número de llamada en grupos de telecaptura / timbre adicional / desvío de llamada en caso de no contesta / caso de libre**.
   - Si no desea mostrar el número de teléfono ni el nombre del llamante, desactive la casilla de verificación **Número de llamada en grupos de telecaptura / timbre adicional / desvío de llamada en caso de no contesta / caso de libre**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Grupo de telecaptura en la página 697

15.1.5.2 Cómo activar o desactivar tono de advertencia

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema** > **Flags del sistema**.
4) Elija una de estas opciones:
   - Si desea activar el tono de advertencia, active la casilla de verificación **Señal de advertencia para grupos de telecaptura**.
   - Si desea desactivar el tono de advertencia, desactive la casilla de verificación **Señal de advertencia para grupos de telecaptura**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Grupo de telecaptura en la página 697

15.1.5.3 Cómo activar o desactivar la telecaptura de llamadas recordatorias

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema** > **Flags del sistema**.

4) Elija una de estas opciones:
   - Si desea permitir la telecaptura de llamadas después de llamadas recordatorias, active la casilla de verificación **Telecaptura de llamadas después de llamada recordatoria**.
   - Si no desea permitir la telecaptura de llamadas después de llamadas recordatorias, desactive la casilla de verificación **Telecaptura de llamadas después de llamada recordatoria**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Grupo de telecaptura en la página 697

15.1.5.4 Cómo agregar llamada de grupo (caso de libre o aviso de llamada en espera)

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el árbol de navegación, haga clic en **Llamadas entrantes** > **Llam. grupo / lín. colectiva**.
4) Haga clic en la pestaña **Añadir grupo**.
5) En el campo **N.º de llamada** indique el número de teléfono de la nueva llamada de grupo.
6) En el campo **Número de marcación directa** indique el número de marcación directa de la nueva llamada de grupo.

   : Si desea utilizar DID 879, 890 o 891, debe hacer la configuración a través de ManagerE y no a través de WBM.
7) En el campo **Nombre** indique el nombre de la nueva llamada de grupo.
8) En la lista desplegable **Tipo** seleccione una de estas opciones:
   - Si desea configurar una llamada de grupo del tipo Caso de libre, seleccione la entrada **Caso de libre**.
   - Si desea configurar una llamada de grupo del tipo Aviso de llamada en espera, seleccione la entrada **Aviso llam. en espera**.
9) En la lista desplegable **N.º de llamada**, seleccione el número de teléfono de la extensión a la que se va a asignar la llamada de grupo.
10) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Llamada de grupo en la página 699

15.1.5.5 Cómo mostrar o modificar llamada de grupo (Caso de libre o Aviso de llamada en espera)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta la llamada de grupo deseada.
4) Haga clic en la pestaña **Editar parámetros grupo**. Podrá ver la configuración actual de los parámetros de grupo.
5) Si es necesario, modifique los parámetros deseados de la llamada de grupo
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Llamada de grupo en la página 699

15.1.5.6 Cómo borrar llamada de grupo (caso de libre o aviso de llamada en espera)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta la llamada de grupo deseada.
4) Haga clic en la pestaña **Borrar grupo**.
5) Haga clic en **Borrar** y a continuación en **Aceptar**.

Conceptos relacionados

Llamada de grupo en la página 699

15.1.5.7 Cómo agregar o borrar miembro a llamada de grupo (caso de libre o aviso de llamada en espera)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.

3) Elija una de estas opciones:

- Si desea agregar un miembro a la llamada de grupo, en el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta la llamada de grupo deseada. Haga clic en la pestaña **Añadir miembro**. En la lista desplegable **N.° de llamada**, seleccione el número de teléfono de la extensión deseada. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
- Si desea borrar un miembro de la llamada de grupo, en el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta el miembro de la llamada de grupo deseado ((Miembro grupo) N.º de llamada Nombre). Haga clic en la pestaña **Borrar miembro**. Haga clic en **Borrar** y a continuación en **Aceptar**.

Conceptos relacionados

Llamada de grupo en la página 699

15.1.5.8 Cómo activar o desactivar el bloqueo de avisos de llamada en espera para miembro de grupo

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el grupo de menús, bajo **Extensiones** > **Extensión** > **…**, navegue hasta la extensión deseada (Índice - N.º de llamada - Nombre).
4) Haga clic en la pestaña **Editar flags exten.**
5) Elija una de estas opciones:

- Si desea activar el bloqueo de avisos de llamada en espera, active la casilla de verificación **Bloqueo de aviso de llamada en espera act.**.
- Si desea desactivar el bloqueo de avisos de llamada en espera, desactive la casilla de verificación **Bloqueo de aviso de llamada en espera act.**.

> **Nota:** Cuando se configura un grupo como grupo de Puesto de operadora, todos sus miembros se definen automáticamente con el marcador "Call waiting rejection on" (Rechazo de llamada en espera activo) en falso. Esto también se aplica a los nuevos miembros que se pudieran incorporal al grupo de Puesto de operadora. El usuario puede definir "Call waiting rejection on" en verdadero para los miembros individuales del grupo de Puesto de operadora para activar el tono de ocupado con ellos, pero este no es el comportamiento predeterminado.

6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados
Llamada de grupo en la página 699

15.2 Configuración de equipo / Grupo Team y Jefe/Secretaria / Grupo Top

Una Configuración de equipo / Grupo Team ofrece cómodas funciones de equipo (Team). Los números de teléfono de todos los miembros de quipo se programan en teclas MULAP (teclas de línea). De esta forma, cada miembro del equipo puede acceder a todas las líneas (por ejemplo, para la telecaptura de llamadas) y puede telefonear al mismo tiempo a través de varias líneas. Un grupo Jefe/Secretaria / Grupo Top ofrece cómodas funciones de Jefe y Secretaria (función Top) para hasta tres jefes y tres secretarias.

Nota: Al crear un MULAP en las opciones Team/Top de WBM/ Manager E, no es posible introducir un número que comience por ** o ***.

15.2.1 Configuración de equipo / Grupo Team

En un teléfono con funciones Team, los números de teléfono propios y de los demás miembros Team se programan en teclas MULAP (Multiple Line Appearance) (teclas de línea). Todos los miembros Team tienen acceso a todas las líneas (por ejemplo, para la telecaptura de llamadas) y pueden también telefonear simultáneamente a través de varias líneas. Además, se programan automáticamente teclas de llamada directa a través de las que los miembros Team pueden llamarse directamente.

Los miembros Team tienen acceso a los números de teléfono de todos los miembros a través de las teclas MULAP.De esta forma, una llamada entrante dirigida a un miembro Team puede ser aceptada por todos los demás miembros pulsando la tecla MULAP parpadeante.También se puede alternar entre varias líneas.Pulsando una tecla MULAP, un miembro Team puede establecer una llamada saliente a través de la correspondiente línea. El usuario llamado verá indicado en su display el número de teléfono perteneciente a dicha línea.

Las llamadas entrantes se señalizan en todos los miembros Team de forma óptica, a través del LED de la tecla MULAP. Además, se puede indicar, para cada uno de los miembros Team, si las llamadas entrantes también deberán ser señalizadas acústicamente.

A través de una tecla de llamada de grupo, todos los miembros Team pueden activar o desactivar la señalización de las llamadas entrantes para cada una de las líneas.

Los administradores con el perfil **avanzado** pueden configurar hasta tres extensiones por configuración de equipo/grupo Team a través del asistente **Configuración de equipo**. Los administradores con el perfil de **Experto** pueden configurar hasta diez extensiones por configuración de equipo/grupo Team a través del **Modo Experto**.

Una extensión puede pertenecer a varios grupos al mismo tiempo. Lo siguiente se aplica a los grupos del tipo Llamada de grupo / Línea colectiva, Configuración de equipo / Grupo Team y Jefe/Secretaria / Grupo Top: La suma de todos los suscriptores en estos grupos no debe exceder 32.

Se puede asignar a cada Configuración de equipo / Grupo Team un nombre de hasta 16 caracteres.

Al configurar una configuración de equipo o un grupo de equipo, las siguientes propiedades se asignan a sus miembros (estas configuraciones pueden ser cambiadas por un administrador con el perfil **Experto** en **modo Experto**.):

- **Maestro**

  Con este parámetro, un miembro se convierte en Maestro de la configuración de equipo/ grupo Team. Si un maestro activa un desvío de llamadas, se aplicará a todos los miembros (teléfonos) de la configuración de equipo/grupo Team.

  Ajuste estándar: Maestro es el primer miembro de la configuración de equipo/grupo Team.
- **Llamada acústica**

  Si este parámetro está activado, se señalizan acústicamente las llamadas entrantes.

  Ajuste estándar: el parámetro está activado.
- **Ocupación automática saliente**

  Si este parámetro está activado, al descolgar el microteléfono se llama automáticamente a través de la línea MULAP de este miembro. Si el parámetro no está activado, el usuario deberá pulsar la tecla MULAP antes de poder marcar.

  Ajuste estándar: el parámetro está activado.
- **Sin aceptación automática de llamadas entrantes**

  Si este parámetro está activado, las llamadas entrantes no se pueden aceptar descolgando el microteléfono. Para aceptar una llamada entrante hay que pulsar la tecla MULAP.

  Ajuste estándar: el parámetro no está activado.
- **Liberación para conferencia automática**

  Si el parámetro está activado, pulsando la tecla MULAP la línea MULAP ocupada se libera para una conferencia. Todos los demás miembros reciben una indicación de la liberación: la tecla MULAP parpadea. Pulsando la tecla MULAP puede unirse a la conferencia.

  Ajuste estándar: el parámetro no está activado.
- **Tecla MULAP configurada**

  Si el parámetro está activado, en el teléfono correspondiente se configura una tecla MULAP. Al pulsar la tecla se realiza una ocupación saliente a través de la línea MULAP del Maestro. En la pantalla del destinatario de la llamada aparece el número de extensión MULAP del maestro.

  Ajuste estándar: el parámetro no está activado.

Utilizar teclas MULAP

Todos los miembros Team tienen asignada una línea propia (línea MULAP). Cada miembro Team configura la línea propia y las líneas de todos los demás miembros como teclas MULAP (teclas de línea). De esta forma, todos los miembros Team pueden utilizar todas las líneas MULAP disponibles.

El LED de una tecla MULAP (tecla de línea) tiene este significado:

- Apagado: la línea pertinente es libre y se puede utilizar.

- Encendido: la línea pertinente está ocupada.
- Parpadea rápido: llamada en la línea pertinente.
- Parpadea despacio: hay una llamada puesta en espera de la línea pertinente.

Utilizar teclas de llamada directa

Cada uno de los miembros Team tiene una tecla de llamada directa para cada uno de los demás miembros. De esta forma todos ellos pueden ponerse directamente en contacto entre sí con tan solo pulsar una tecla.

También se puede utilizar una tecla de llamada directa para transferir una llamada rápidamente al miembro de equipo programado.

El LED de una tecla de llamada directa tiene este significado:

- Apagado: el miembro Team pertinente no está realizando una llamada.
- Encendido: el miembro Team pertinente está realizando una llamada o ha activado el estado No molestar.
- Parpadea rápido: el miembro Team pertinente está realizando una llamada. La llamada se puede atender pulsando la tecla de llamada directa.
- Parpadea despacio: el miembro Team ha recibido una llamada y aún no la ha aceptado. La llamada se puede atender pulsando la tecla de llamada directa.

Tipo de llamada

Para cada configuración de equipo/grupo de equipo, un administrador con el perfil **Experto** puede definir la señalización acústica de las llamadas externas entrantes mediante la configuración del tipo de timbre.Tiene las siguientes opciones:

- Tono de llamada doble (configuración estándar)
- Tono de llamada triple
- Tono de llamada corto/largo/corto

En los teléfonos analógicos solo se puede aplicar la configuración estándar. Los cambios no tienen ningún efecto.

Buzón de fax para Configuración de equipo/grupo Team

En cada configuración de equipo/grupo Team se puede configurar un buzón de fax. A través de este buzón, los miembros pueden recibir mensajes de fax directamente a través de myPortal for Desktop o de myPortal for Outlook.

Si ya hay configurado un buzón de fax para el maestro (el primer miembro) de la configuración de equipo/grupo Team, al establecer la configuración de equipo/grupo Team se aplica dicho buzón. Se eliminan los buzones de fax que hubiera configurados para otros miembros.

Cuando se elimina una configuración de equipo/grupo Team, solo el antiguo maestro (el primer miembro) puede seguir utilizando el buzón de fax.

Pedido de dispositivos miembros de Mulap

Los teléfonos SIP se pueden integrar en un MULAP básico, siempre que se haya definido un dispositivo TDM/HFA como el primer miembro del MULAP básico. Los teléfonos IP se pueden integrar en un MULAP básico, siempre que se haya definido un dispositivo TDM/HFA como el primer miembro del MULAP básico.

Se pueden conectar, por ejemplo, teléfonos móviles Dual-Mode configurados como extensiones Mobility Entry. Los teléfonos móviles de modo dual admiten redes GSM/UMTS y redes WLAN. A través de WLAN se puede registrar un teléfono móvil Dual-Mode como extensión IP (cliente SIP) en el sistema de comunicación.

Los usuarios de movilidad, incluidos los usuarios de movilidad GSM, los clientes de Unify Phone y Microsoft Teams, pueden integrarse en un MULAP básico, siempre que se haya definido un dispositivo TDM/HFA como el primer miembro del MULAP básico.

Nota: La descripción ampliada anterior se aplica a los sistemas OpenScape Business X y OpenScape Business S, pero se limita a Team y Basic Mulap, y no a subcapítulos con declaraciones similares como Ejecutivo/Secretario/Grupo superior.

Consejo: En los teléfonos SIP no se puede hacer una programación de teclas MULAP. Tampoco se pueden activar ni desactivar prestaciones a través de códigos. No se admiten mensajes de visualización específicos del MULAP básico.

Nota: Los teléfonos de gama alta, como CP 400/600/600E/700/700X/710, mantienen sus propias entradas de diario y tienen la capacidad de presentar más información. Pero, con respecto a las configuraciones de grupos, se basan en los datos del sistema, ya que los grupos se configuran en el sistema y no en los teléfonos. Como consecuencia, es posible que la información sobre los grupos no se muestre en las entradas del diario, ya que siguen las limitaciones y la configuración del sistema.

Dependencias

Tema	Dependencia
Desvío de llamadas	Un miembro Team ha activado un desvío de llamadas para todas las llamadas. En este caso, todas las llamadas se desvían a su número de teléfono de extensión propio.
No molestar	Si un miembro Team activa el estado No molestar, no se transfieren las llamadas entrantes. **Nota:** Un equipo completo solo está ocupado si todos los miembros del equipo han activado la función No molestar.
Teléfonos RDSI	No se pueden incluir teléfonos RDSI en configuraciones de equipo/Grupos Team.

Tema	Dependencia
Llam. grupo / lín. colectiva	No se puede incluir un maestro Básico/MULAP Jefe en configuraciones de equipo / Grupo Team.

Conceptos relacionados

Llamada directa en la página 651

Tareas relacionadas

Cómo añadir configuración de equipo / Grupo Team en la página 729
Cómo modificar la configuración de equipo / Grupo Team en la página 730
Cómo borrar configuración de equipo / Grupo Team en la página 731
Cómo agregar o borrar un miembro a configuración de equipo / Grupo Team en la página 735
Cómo modificar miembro de una configuración de equipo / Grupo Team en la página 735
Cómo modificar las propiedades de los miembros de una configuración de equipo / Grupo Team en la página 736
Cómo modificar la ocupación de teclas telefónicas para Configuración de equipo / Grupo Team en la página 736
Cómo agregar un buzón de fax a la configuración de equipo / grupo Team en la página 737

15.2.2 Jefe/Secretaria / Grupo Top

Si se necesitan funciones Jefe y Secretaria (función Top), se pueden configurar grupos Top.

Se pueden configurar funciones Jefe/Secretaria para grupos con hasta tres jefes y hasta tres secretarias.

Consejo: Las designaciones "el Jefe" y "la Secretaria" son válidas también para grupos con más de un jefe y más de una secretaria. En este texto se utiliza "el Jefe" para el femenino y el masculino y "la Secretaria" tanto para secretario como para secretaria.

Todos los miembros Top (cada jefe y cada secretaria) tienen asignada una línea propia, la denominada línea MULAP (Multiple Line Appearance). Cada uno de los miembros TAP puede configurar la línea propia y las líneas MULAP de todos los demás miembros como teclas MULAP (teclas de línea). En caso de llamadas salientes a través de la línea MULAP, en el display del usuario llamado aparece el número de teléfono MULAP. La secretaria puede hacer llamadas a través de su propia línea o a través de la línea MULAP de todos los jefes y de otras secretarias. Así, por ejemplo, si se quiere establecer una conexión para un jefe, se podría utilizar la línea MULAP de dicho jefe.

Además, se programan teclas de llamada directa con las que el jefe puede llamar directamente a la secretaria (y a la inversa).

Las llamadas entrantes se señalizan en todos los miembros Top de forma óptica, a través del LED de la tecla MULAP. Además, se puede indicar, para cada uno de los miembros Top, si las llamadas entrantes también deberán ser

señalizadas acústicamente. La señalización acústica depende aquí de la tecla de conmutación.

A través de una tecla de conmutación se puede conmutar la señalización de las llamadas entrantes. Las llamadas entrantes se señalizan en el Jefe o en la Secretaria. Si el Jefe pulsa la tecla de conmutación, todas sus llamadas entrantes seguirán mostrándose a través de una ventana emergente. Sin embargo, las llamadas solo se pueden atender pulsando una determinada tecla en el teléfono, y no a través de la ventana emergente.

Los teléfonos de secretaria pueden abandonar la configuración Jefe/secretaria (grupo Top) y volverse a unir a ella mediante una tecla de llamada en grupo. En este caso, la conmutación tiene prioridad.

Consejo: Si la secretaria abandona la configuración Jefe/secretaria (grupo Top) con la tecla de llamada de grupo sin activar la conmutación para el jefe, las llamadas entrantes no se señalizarán ni en el Jefe ni en la Secretaria.

Un administrador con el perfil **avanzado** puede configurar hasta dos jefes y dos secretarias por configuración Jefe/secretaria (grupo Top) a través del asistente **Jefe / Secretaria**. Un administrador con el perfil de **experto** puede configurar hasta tres jefes y tres secretarias por configuración Jefe/secretaria (grupo Top) a través del **Modo Experto**.

Se pueden configurar como máximo tres teléfonos por Jefe y dos por Secretaria.

Una extensión puede pertenecer a varios grupos al mismo tiempo. Lo siguiente se aplica a los grupos del tipo Llamada de grupo / Línea colectiva, Configuración de equipo / Grupo Team y Jefe/Secretaria / Grupo Top: La suma de todos los suscriptores en estos grupos no debe exceder 32.

Se puede asignar a cada grupo Top o cada configuración Jefe y Secretaria un nombre de hasta 16 caracteres.

Al configurar una configuración Jefe/secretaria (grupo Top), se asignan a los miembros estas propiedades (los administradores con el perfil de **Experto** pueden hacer cambios en la configuración a través del **Modo Experto**):

- **Maestro**

  Con estos parámetros, un miembro recibe funciones Jefe. Al descolgar el microteléfono se selecciona automáticamente la línea MULAP Jefe. De forma estándar, las llamadas entrantes a través del número de teléfono MULAP Jefe en cuestión solo se señalizan de forma visual.

  Ajuste estándar: Reciben funciones de Jefe todos los jefes de la configuración Jefe/secretaria (grupo Top).
- **Llamada acústica**

  Si este parámetro está activado, se señalizan acústicamente las llamadas entrantes.

  Ajuste estándar: el parámetro está activado para todos los miembros con función Secretaria.
- **Ocupación automática saliente**

  Si este parámetro está activado, al descolgar el microteléfono se llama automáticamente a través de la línea MULAP de este miembro. Si el

parámetro no está activado, el usuario deberá pulsar la tecla MULAP antes de poder marcar.

Ajuste estándar: el parámetro está activado para todos los miembros.

- **Sin aceptación automática de llamadas entrantes**

  Si este parámetro está activado, las llamadas entrantes no se pueden aceptar descolgando el microteléfono. Para aceptar una llamada entrante hay que pulsar la tecla MULAP.

  Ajuste estándar: el parámetro no está activado.
- **Liberación para conferencia automática**

  Si el parámetro está activado, pulsando la tecla MULAP la línea MULAP ocupada se libera para una conferencia. Todos los demás miembros reciben una indicación de la liberación: la tecla MULAP parpadea. Pulsando la tecla MULAP puede unirse a la conferencia.

  Ajuste estándar: el parámetro no está activado.
- **Tecla MULAP configurada**

  Si el parámetro está activado, en el teléfono correspondiente se configura una tecla MULAP. Pulsando la tecla, se realiza una ocupación saliente a través de la línea MULAP Jefe. En la pantalla del destinatario de la llamada aparece el número de teléfono MULAP Jefe.

  Ajuste estándar: el parámetro está activado.

Utilizar teclas MULAP

Todos los miembros Top tienen asignada una línea propia (línea MULAP). Cada miembro Top configura la línea propia y las líneas de todos los demás miembros como teclas MULAP (teclas de línea). De esta forma, todos los miembros Top pueden utilizar todas las líneas MULAP disponibles.

El LED de una tecla MULAP (tecla de línea) tiene este significado:

- Apagado: la línea pertinente es libre y se puede utilizar.
- Encendido: la línea pertinente está ocupada.
- Parpadea rápido: llamada en la línea pertinente.
- Parpadea despacio: una conversación retenida espera a la línea correspondiente o dicha línea fue liberada para una conferencia.

Utilizar teclas de llamada directa

Cada uno de los miembros Top tiene una tecla de llamada directa para cada uno de los demás miembros. De esta forma todos ellos pueden ponerse directamente en contacto entre sí con tan solo pulsar una tecla.

También se puede utilizar una tecla de llamada directa para transferir una llamada rápidamente al miembro de grupo Top programado.

El LED de una tecla de llamada directa tiene este significado:

- Apagado: El miembro Top pertinente no está realizando una llamada.
- Encendido: el miembro Top pertinente está realizando una llamada o ha activado el estado No molestar.
- Parpadea rápido: el miembro Top pertinente está realizando una llamada. La llamada se puede atender pulsando la tecla de llamada directa.
- Parpadea despacio: el miembro Top ha recibido una llamada y aún no la ha aceptado. La llamada se puede atender pulsando la tecla de llamada directa.

Tipo de llamada

En cada una de las configuraciones Jefe/secretaria (grupo Top), los administradores con el perfil de **Experto** pueden definir la señalización acústica de las llamadas externas entrantes a través del ajuste de configuración Tipo de llamada. Tiene las siguientes opciones:

- Tono de llamada doble (configuración estándar)
- Tono de llamada triple
- Tono de llamada corto/largo/corto

En los teléfonos analógicos solo se puede aplicar la configuración estándar. Los cambios no tienen ningún efecto.

Buzones de fax para la configuración Jefe/secretaria (grupo Top)

Se puede configurar un buzón de fax para cada miembro de una configuración Jefe/secretaria o grupo Top. A través de este buzón, los miembros pueden recibir mensajes de fax directamente a través de myPortal for Desktop o myPortal for Outlook.

Si ya hay configurado un buzón de fax para el primer jefe de la configuración Jefe/secretaria (grupo Top), al establecer la configuración Jefe/secretaria (grupo Top) se aplica dicho buzón. Se eliminan los buzones de fax que hubiera configurados para otros miembros.

Cuando se elimina una configuración Jefe/secretaria (grupo Top), solo el antiguo primer jefe puede seguir utilizando el buzón de fax.

Teléfonos SIP

En una configuración Jefe/secretaria (grupo Top) se pueden incluir teléfonos SIP. Para ello es necesario que haya definido un teléfono del sistema (por ejemplo, teléfono IP, HFA o SIP) como primer miembro de la configuración Jefe/secretaria (grupo Top) (Jefe 1).

Se pueden conectar, por ejemplo, teléfonos móviles Dual-Mode configurados como extensiones Mobility Entry. Los teléfonos móviles Dual-Mode son compatibles con redes GSM/UMTS y con redes WLAN. A través de WLAN se puede registrar un teléfono móvil Dual-Mode como extensión IP (cliente SIP) en el sistema de comunicación.

Consejo: En los teléfonos SIP no se puede hacer una programación de teclas MULAP ni de teclas de llamada directa. Tampoco se pueden activar ni desactivar prestaciones a través de códigos. No se admite la muestra de mensajes en display específicos de la configuración Jefe/secretaria / grupo Top

Nota: Los teléfonos de gama alta, como el CP600, mantienen sus propias entradas en el diario y tienen la capacidad de presentar más información. Pero, con respecto a las configuraciones de grupos, se basan en los datos del sistema, ya que los grupos se configuran en el sistema y no en los teléfonos. Como consecuencia, es posible que la información sobre los grupos no se muestre en las entradas del diario, ya que siguen las limitaciones y la configuración del sistema.

Dependencias

Tema	Dependencia
Desvío de llamadas	Un miembro Top ha activado un desvío de llamadas para todas las llamadas. En este caso, todas las llamadas se desvían a su número de teléfono de extensión propio.
No molestar	Si un miembro Top activa el estado No molestar, no se transfieren las llamadas entrantes.
Teléfonos RDSI	No se pueden incluir teléfonos RDSI en configuraciones Jefe/secretaria / Grupos Top.
Llam. grupo / lín. colectiva	No se puede incluir un maestro Básico/MULAP Jefe en configuraciones Jefe/secretaria / Grupos Top.

Conceptos relacionados

Llamada directa en la página 651

Tareas relacionadas

Cómo agregar grupos Jefe/secretaria / Top en la página 732
Cómo modificar grupos Jefe/Secretaria / Top en la página 733
Cómo borrar grupos Jefe/Secretaria /grupo Top en la página 734
Cómo agregar o borrar un miembro a Jefe/secretaria (grupo Top) en la página 737
Cómo modificar miembro de un Jefe/Secretaria (grupo Top) en la página 738
Cómo modificar propiedades de los miembros de Jefe/secretaria (grupo Top) en la página 738
Cómo agregar un buzón de fax a Jefe/secretaria (grupo Top) en la página 739

15.2.3 Configuración de configuraciones de equipo / grupos Team y funciones Jefe/Secretaria / grupos Top mediante asistentes

Distintos asistentes permiten la configuración de configuraciones de equipo (grupos Team) y funciones Jefe/Secretaria (función Top).

El asistente **Configuración de equipo** permite a los administradores ajustar configuraciones de equipo (grupos Team). Se describe el modo de proceder para los siguientes casos de aplicación que pueden configurarse a través del asistente:

- Cómo añadir configuración de equipo / Grupo Team
- Cómo modificar la configuración de equipo / Grupo Team
- Cómo borrar configuración de equipo / Grupo Team

El asistente **Jefe / Secretaria** permite configurar cómodas funciones de Jefe y Secretaria (función Top). Se describe el modo de proceder para los siguientes casos de aplicación que pueden configurarse a través del asistente:

- Cómo agregar grupos Jefe/secretaria / Top
- Cómo modificar grupos Jefe/Secretaria / Top
- Cómo borrar grupos Jefe/Secretaria /grupo Top

Conceptos relacionados

Configuración de myPortal to go y Mobility Entry en la página 980

15.2.3.1 Cómo añadir configuración de equipo / Grupo Team

El asistente **Configuración de equipo** permite a los administradores ajustar configuraciones de equipo (grupos Team).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de equipo**.
4) Haga clic en **Agregar**, para configurar una nueva configuración de equipo.
5) En la lista desplegable **Primera terminal**, seleccione el número de teléfono del primer teléfono de la nueva configuración de equipo.
6) Haga clic en **OK y Continuar**.
7) En el campo **Nombre**, introduzca el nombre de la nueva configuración de equipo, si no aparece ningún nombre o si se requiere una modificación del nombre mostrado.

   Aviso: Si ya se ha asignado un nombre al teléfono, el campo **Nombre** ya tiene preasignado el nombre del primer teléfono de la configuración de equipo.
8) Para modificar el número de teléfono mostrado, en el campo **N.º llam. interno**, indique el número de teléfono interno de la nueva configuración de equipo.

   El campo **Nº llam. interno** ya está predefinido con el número de teléfono interno del primer teléfono de la configuración de equipo.

   : Si desea utilizar DID 879, 890 o 891, debe hacer la configuración a través de ManagerE y no a través de WBM.
9) Para modificar el número de marcación directa mostrado, en el campo **Número de marcación directa**, introduzca el número de marcación directa de la nueva configuración de equipo.

   Aviso: El campo **Número de marcación directa** ya está predefinido con el número de marcación directa del primer teléfono de la configuración de equipo.
10) En la sección **Fax** del campo **N.º llam. interno**, indique el número de teléfono interno del buzón de fax de la nueva configuración de equipo, si no se muestra ningún número o si se requiere una modificación del número de teléfono mostrado.

    El campo **N.º llam. interno** ya está predefinido con el número de teléfono interno del buzón de fax del primer teléfono de la configuración de equipo (si dicho teléfono tiene configurado uno).

11) En la sección **Fax** del campo **Número de marcación directa**, indique el número de marcación directa del buzón de fax de la nueva configuración de equipo, si no se muestra ningún número o si se requiere una modificación del número de marcación directa mostrado.

    El campo **Número de marcación directa** ya está predefinido con el número de marcación directa del buzón de fax del primer teléfono de la configuración de equipo (si dicho teléfono tiene configurado uno).

12) Active el marcador **Team como miembro de grupo**.

    El marcador **Team como miembro de grupo** solo se puede configurar cuando el grupo Team tiene miembros con el mismo tipo de extensión, lo que da como resultado un único grupo MULAP. Cuando se activa este marcador, el grupo MULAP se puede agregar como miembro en Grupos.

13) En la lista desplegable **Segunda terminal**, seleccione el número de teléfono del segundo teléfono de la nueva configuración de equipo.

14) En la lista desplegable **Tercera terminal**, seleccione el número de teléfono del tercer teléfono de la nueva configuración de equipo.

15) Haga clic en **OK y Continuar**.

16) Si desea configurar una nueva configuración de equipo, repita los pasos del 4 al 15.

17) Haga clic en**OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Configuración de equipo / Grupo Team en la página 720

15.2.3.2 Cómo modificar la configuración de equipo / Grupo Team

El asistente **Configuración de equipo** permite a los administradores editar las configuraciones de equipo (grupos Team).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de equipo**.
4) En la línea de la configuración de equipo que desee modificar, haga clic en **Editar**.
5) Modifique los parámetros deseados

6) Solo con UC Smart: en caso necesario, asigne un buzón a la configuración de equipo:
   a) En la lista desplegable **Tipo de buzón UC Smart**, seleccione si la configuración de equipo tendrá un buzón estándar o un buzón de puesto de operadora (AutoAttendant).
   b) Solo con buzón estándar: si los llamantes pueden dejar un mensaje en el buzón de voz, active la casilla de verificación **Grabación**.
   c) En la lista desplegable **Saludo** introduzca un saludo.
   d) Si desea restablecer la contraseña del buzón de voz, active la casilla de verificación **Reponer contraseña**.

> **Nota:** La casilla de verificación **Reponer contraseña** no debe estar marcada al cambiar la configuración de un buzón de voz. Hace que se restablezca la contraseña del buzón de voz. Al cambiar la configuración, el usuario ya debe modificar la contraseña inicial al acceder por primera vez al buzón de voz.

7) Haga clic en **OK & Continuar**.
8) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Configuración de equipo / Grupo Team en la página 720

15.2.3.3 Cómo borrar configuración de equipo / Grupo Team

El asistente **Configuración de equipo** permite a los administradores borrar configuraciones de equipo (grupos Team).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de equipo**.
4) En la línea de la configuración de equipo que desee borrar, haga clic en **Editar**.
5) Haga clic en **Borrar datos**.
6) Haga clic en **Aceptar**, para confirmar el borrado.
7) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

> **Nota:** En aplicaciones que utilizan la interfaz CSTA (UC, OSCC, etc.), si se borra un grupo Team o un miembro de un grupo Team, hay que reiniciar el sistema.

Conceptos relacionados

Configuración de equipo / Grupo Team en la página 720

15.2.3.4 Cómo agregar grupos Jefe/secretaria / Top

Con el asistente **Jefe / Secretaria** puede configurar cómodas funciones de Jefe y Secretaria (función Top).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.

3) Haga clic en **Editar** para iniciar el asistente **Jefe / Secretaria**.

4) Haga clic en **Agregar** para configurar una nueva configuración Jefe/Secretaria (Grupo Top).

5) En el campo **Nombre**, indique el nombre de la nueva configuración Jefe/secretaria.

6) En las listas desplegables correspondientes, seleccione los números de teléfono de la nueva configuración Jefe/secretaria deseados.

7) Haga clic en **OK y Continuar**.

8) En la sección **Fax** del campo **Número de teléfono**, indique el número de teléfono interno del buzón de fax de la nueva configuración Jefe/secretaria, si no se muestra ningún número o si se requiere una modificación del número de teléfono mostrado.

El campo **Número de teléfono** ya está predefinido con el número de teléfono interno del buzón de fax del primer jefe de la configuración Jefe/secretaria (si dicho teléfono tiene configurado un buzón de fax).

9) En la sección **Fax** del campo **Marcación directa**, indique el número de marcación directa del buzón de fax de la nueva configuración Jefe/secretaria, si no se muestra ningún número o si se requiere una modificación del número de marcación directa mostrado.

El campo **Marcación directa** ya está predefinido con el número de marcación directa del buzón de fax del primer jefe de la configuración Jefe/secretaria (si dicho teléfono tiene configurado un buzón de fax).

: Si desea utilizar DID 879, 890 o 891, debe hacer la configuración a través de ManagerE y no a través de WBM.

---

10) Seleccione un valor predeterminado para la ocupación de teclas:

- Para configurar las teclas para las funciones Jefe/secretaria en el primer o segundo aparato auxiliar, active la casilla de verificación **En primera/segunda consola**.
- Para configurar las teclas para las funciones Jefe/secretaria en las primeras teclas de función libres del teléfono, active la casilla de verificación **las primeras teclas libres**.

11) Haga clic en **OK y Continuar**.

12) Si desea configurar una nueva configuración Jefe/secretaria, repita los pasos del 4 al 11.

13) Haga clic en**OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Jefe/Secretaria / Grupo Top en la página 724

15.2.3.5 Cómo modificar grupos Jefe/Secretaria / Top

El asistente **Jefe / Secretaria** permite editar cómodas funciones de Jefe y Secretaria (función Top).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Jefe / Secretaria**.
4) En la línea de la configuración Jefe/Secretaria (grupo Top) que desee modificar, haga clic en **Editar**.
5) Modifique los parámetros deseados
6) Solo con UC Smart: en caso necesario, asigne un buzón al grupo Top:
   a) En la lista desplegable, **Tipo de buzón de voz UC Smart**, seleccione si el grupo Top tendrá un buzón estándar o un buzón de puesto de operadora (AutoAttendant).
   b) Solo con buzón estándar: si los llamantes pueden dejar un mensaje en el buzón de voz, active la casilla de verificación **Grabación**.
   c) En la lista desplegable **Saludo** introduzca un saludo.
   d) Si desea restablecer la contraseña del buzón de voz, active la casilla de verificación **Reponer contraseña**.

   Nota: La casilla de verificación **Reponer contraseña** no debe estar marcada al cambiar la configuración de un buzón de voz. Hace que se restablezca la contraseña del buzón de voz. Al cambiar la configuración, el usuario ya debe modificar la contraseña inicial al acceder por primera vez al buzón de voz.
7) Haga clic en **OK & Continuar**.
8) Modifique la información deseada para el buzón de fax (**Fax**) y la **Asignación de teclas**.
9) Haga clic en **OK & Continuar**.
10) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

Conceptos relacionados

Jefe/Secretaria / Grupo Top en la página 724

15.2.3.6 Cómo borrar grupos Jefe/Secretaria /grupo Top

El asistente **Jefe / Secretaria** permite borrar cómodas funciones de Jefe y Secretaria (función Top).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Jefe / Secretaria**.
4) En la línea de la configuración Jefe/Secretaria (grupo Top) que desee borrar, haga clic en **Editar**.
5) Haga clic en **Borrar datos**.
6) Haga clic en **Aceptar**, para confirmar el borrado.
7) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

Nota: En aplicaciones que utilizan la interfaz CSTA (UC, OSCC, etc.), si se borra un grupo Jefe/Secretaria o Top, o un miembro de un grupo Jefe/Secretaria o Top, hay que reiniciar el sistema.

Conceptos relacionados

Jefe/Secretaria / Grupo Top en la página 724

15.2.4 Configuración de configuraciones de equipo / grupos Team y funciones Jefe/Secretaria / grupos Top mediante el modo Experto

Además de las opciones de configuración mediante asistentes, los administradores con el perfil **Experto** tienen opciones adicionales para la configuración de configuraciones de equipo / funciones de grupos Team y Jefe/secretaria / grupos Top mediante el **modo Experto**.

Se describe el modo de proceder para los siguientes casos de aplicación que pueden configurarse a través del **Modo Experto**:

- Cómo agregar o borrar un miembro a configuración de equipo / Grupo Team
- Cómo modificar miembro de una configuración de equipo / Grupo Team
- Cómo modificar las propiedades de los miembros de una configuración de equipo / Grupo Team
- Cómo modificar la ocupación de teclas telefónicas para Configuración de equipo / Grupo Team
- Cómo agregar un buzón de fax a la configuración de equipo / grupo Team
- Cómo agregar o borrar un miembro a Jefe/secretaria (grupo Top)
- Cómo modificar miembro de un Jefe/Secretaria (grupo Top)
- Cómo modificar propiedades de los miembros de Jefe/secretaria (grupo Top)
- Cómo agregar un buzón de fax a Jefe/secretaria (grupo Top)

15.2.4.1 Cómo agregar o borrar un miembro a configuración de equipo / Grupo Team

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Consejo: El asistente **Configuración de equipo** permite a los administradores con el perfil **avanzado**, puede definir hasta tres miembros (teléfonos) para una configuración de equipo (grupo Team). Para agregar más miembros, los administradores deben disponer del perfil de **experto** y utilizar el **Modo Experto** (véase la siguiente descripción).

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) Elija una de estas opciones:
   - Si desea agregar un miembro al grupo Team (Configuración de equipo), en el grupo de menús **Llamadas entrantes** > **Team/Top** > **…**, desplácese hasta el grupo Team deseado (Configuración de equipo). Haga clic en la pestaña **Añadir miembro Team/Top**. En la lista desplegable **Tipo**, seleccione el tipo de extensión. En la lista desplegable **Núm. llam.**, seleccione el número de teléfono de la extensión deseada. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
   - Si desea borrar un miembro del grupo Team (Configuración de equipo), en el grupo de menús **Llamadas entrantes** > **Team/Top** > **…**, desplácese hasta el miembro del grupo Team deseado (Configuración de equipo) ((Miembro grupo) N.º de llamada Nombre). Haga clic en la pestaña **Borrar miembro Team/Top**. Haga clic en **Borrar** y a continuación en **Aceptar**.

Conceptos relacionados

Configuración de equipo / Grupo Team en la página 720

15.2.4.2 Cómo modificar miembro de una configuración de equipo / Grupo Team

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el árbol de navegación **Llamadas entrantes** > **Team/Top** > **…**, desplácese hasta un miembro del grupo Team (Configuración de equipo) ((Miembro grupo) Número de teléfono Nombre).
4) Haga clic en la pestaña **Editar miembro Team/Top**.
5) Modifique los parámetros deseados
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Configuración de equipo / Grupo Team en la página 720

15.2.4.3 Cómo modificar las propiedades de los miembros de una configuración de equipo / Grupo Team

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el árbol de navegación **Llamadas entrantes** > **Team/Top** > **…**, desplácese hasta un miembro del grupo Team (Configuración de equipo) ((Miembro grupo) Número de teléfono Nombre).
4) Haga clic en la pestaña **Editar parámetros grupos Team/Top**.
5) Modifique las propiedades deseadas
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Configuración de equipo / Grupo Team en la página 720

15.2.4.4 Cómo modificar la ocupación de teclas telefónicas para Configuración de equipo / Grupo Team

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **Team/Top** > **…**, desplácese hasta el grupo Team deseado (Configuración de equipo).
4) Haga clic en la pestaña **Editar grupo Team/Top**.
5) Seleccione un valor predeterminado para la ocupación de teclas:
   - Para configurar las teclas en el primer o segundo aparato auxiliar, active la casilla de verificación **En primera/segunda consola**.
   - Para configurar las teclas en las primeras teclas de función libres del teléfono, active la casilla de verificación **las primeras teclas libres**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Configuración de equipo / Grupo Team en la página 720

15.2.4.5 Cómo agregar un buzón de fax a la configuración de equipo / grupo Team

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **Team/Top** > **…**, desplácese hasta el grupo Team deseado (Configuración de equipo).
4) Haga clic en la pestaña **Agregar buzón de fax**.
5) En el campo **N.º llam. fax** del miembro deseado del grupo Team (Configuración de equipo), introduzca el número de teléfono interno del buzón de fax.
6) En el campo **N.º llam. marc. directa de fax** del miembro deseado del grupo Team (Configuración de equipo), introduzca el número de marcación directa del buzón de fax.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Configuración de equipo / Grupo Team en la página 720

15.2.4.6 Cómo agregar o borrar un miembro a Jefe/secretaria (grupo Top)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Consejo: El asistente **Jefe / Secretaria** permite a los administradores con el perfil **avanzado**, definir hasta dos Jefes y hasta dos Secretarias por cada configuración Jefe/secretaria (grupo Top). Para agregar más miembros, los administradores deben disponer del perfil de **experto** y utilizar el **Modo Experto** (véase la siguiente descripción).

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) Elija una de estas opciones:
   - Si desea agregar un miembro al grupo Top (Configuración Jefe/secretaria), en el grupo de menús **Llamadas entrantes** > **Team/Top** > **…**, desplácese hasta el grupo Top deseado (Configuración Jefe/secretaria). Haga clic en la pestaña **Añadir miembro Team/Top**. En la lista desplegable **Tipo**, seleccione el tipo de extensión. En la lista desplegable **Núm. llam.**, seleccione el número de teléfono de la extensión deseada. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
   - Si desea borrar un miembro del grupo Top (Configuración Jefe/secretaria), en el grupo de menús **Llamadas entrantes** > **Team/Top** > **…**, desplácese hasta el miembro del grupo Top deseado (Configuración

Jefe/Secretaria) ((Miembro grupo) N.º de llamada Nombre). Haga clic en la pestaña **Borrar miembro Team/Top**. Haga clic en **Borrar** y a continuación en **Aceptar**.

Conceptos relacionados

Jefe/Secretaria / Grupo Top en la página 724

15.2.4.7 Cómo modificar miembro de un Jefe/Secretaria (grupo Top)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el árbol de navegación **Llamadas entrantes** > **Team/Top** > **…**, desplácese hasta un miembro del grupo Top (Configuración Jefe/secretaria) ((Miembro grupo) Número de teléfono Nombre).
4) Haga clic en la pestaña **Editar miembro Team/Top**.
5) Modifique los parámetros deseados
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Jefe/Secretaria / Grupo Top en la página 724

15.2.4.8 Cómo modificar propiedades de los miembros de Jefe/secretaria (grupo Top)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el árbol de navegación **Llamadas entrantes** > **Team/Top** > **…**, desplácese hasta un miembro del grupo Top (Configuración Jefe/secretaria) ((Miembro grupo) Número de teléfono Nombre).
4) Haga clic en la pestaña **Editar parámetros grupos Team/Top**.
5) Modifique las propiedades deseadas
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Jefe/Secretaria / Grupo Top en la página 724

15.2.4.9 Cómo agregar un buzón de fax a Jefe/secretaria (grupo Top)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **Team/Top** > **…**, desplácese hasta el grupo Top deseado (Configuración Jefe/Secretaria).
4) Haga clic en la pestaña **Agregar buzón de fax**.
5) En el campo **N.º llam. fax** del miembro deseado del grupo Top (Configuración Jefe/Secretaria), introduzca el número de teléfono del buzón de fax.
6) En el campo **N.º llam. marc. directa de fax** del miembro deseado del grupo Top (Configuración Jefe/secretaria), introduzca el número de marcación directa del buzón de fax.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Jefe/Secretaria / Grupo Top en la página 724

15.3 MULAP básico y MULAP Jefe

Un MULAP básico permite a un usuario que utiliza varios teléfonos (por ejemplo, un teléfono de red fija y un teléfono móvil) estar accesible con un único número de teléfono. Los MULAP Jefe pueden configurarse para utilizar funciones Jefe y Secretaria restringidas.

15.3.1 MULAP básico

Se pueden configurar MULAP básicos si un suscriptor utiliza varios teléfonos diferentes (por ejemplo, un teléfono de red fija y un teléfono móvil) pero desea que lo contacten en un solo número de teléfono (número de teléfono MULAP básico).

Si una persona que llama al número de teléfono MULAP básico, la llamada se señala visualmente en todos los teléfonos que pertenecen al MULAP básico. El abonado también puede configurar si las llamadas entrantes deben señalizarse acústicamente o no para cada miembro individual. El estado del MULAP básico cambia a ocupado y otras personas que llaman escuchan la señal de ocupado cuando se responde una llamada.

El número de teléfono MULAP básico se muestra en la pantalla de la parte llamada para las llamadas salientes a través de la troncal MULAP básica.

Se pueden configurar hasta 20 miembros por MULAP básico.

A cada MULAP básico se le puede asignar un nombre que contenga hasta 16 caracteres.

Cada uno de los teléfonos del suscriptor es miembro del MULAP básico y a cada miembro se le pueden asignar las siguientes propiedades:

- **Maestro**

  Este parámetro cambia a un miembro en un maestro del MULAP básico. Si un maestro activa el reenvío de llamadas, esta función se aplica a todos los miembros (teléfonos) en el MULAP básico. Si el maestro activa una devolución de llamada automática en un MULAP básico, la devolución de llamada se inicia tan pronto como todos los maestros estén libres.

  Un suscriptor no puede ser incluido como maestro MULAP en grupos de búsqueda más de 25 veces.

  Configuración predeterminada: maestro es el primer miembro del MULAP básico.
- **Llamada acústica**

  Si este parámetro está activado, se señalizan acústicamente las llamadas entrantes.

  Configuración predeterminada: el parámetro está activo para todos los maestros.
- **Ocupación automática saliente**

  Si este parámetro está activo, se llama automáticamente al troncal MULAP básico cuando el suscriptor levanta el auricular. Si el parámetro no está activado, el usuario deberá pulsar la tecla MULAP antes de poder marcar.

  Configuración predeterminada: la captura automática de salida se asigna a todos los maestros.
- **Sin aceptación automática de llamadas entrantes**

  Si este parámetro está activado, las llamadas entrantes no se pueden aceptar descolgando el microteléfono. Para aceptar una llamada entrante hay que pulsar la tecla MULAP.

  Ajuste estándar: el parámetro no está activado.
- **Liberación para conferencia automática**

  Si el parámetro está activado, pulsando la tecla MULAP la línea MULAP ocupada se libera para una conferencia. Todos los demás miembros reciben una indicación de la liberación: la tecla MULAP parpadea. Pulsando la tecla MULAP puede unirse a la conferencia.

  Ajuste estándar: el parámetro no está activado.
- **Tecla MULAP configurada**

  Si el parámetro está activado, en el teléfono correspondiente se configura una tecla MULAP. Puede presionar la tecla para configurar una llamada saliente a través de la troncal MULAP básica. El número MULAP básico aparece en la pantalla de la parte llamada.

  Ajuste estándar: el parámetro está activado.

Visualización de número/nombre

Cuando se establece una llamada saliente, se asigna un número de estación (número de estación local o número de grupo MULAP).

Cuando se responde una llamada MULAP entrante, se asigna el número de grupo MULAP.

En el caso de llamadas a un MULAP:

- Antes de contestar la llamada, la pantalla de la parte que llama muestra el nombre MULAP y/o el número MULAP al que se llama.
- Después de contestar la llamada, la pantalla de la parte que llama muestra el nombre de la estación y/o el número MULAP de la parte que responde.
- En el caso de llamadas desde una estación MULAP (tecla MULAP o preferencia), la pantalla de la parte llamada y la que responde siempre muestra el nombre de la estación y/o el número MULAP.
- En general, se aplica lo siguiente a las llamadas salientes: Si una estación realiza una llamada utilizando el número de estación local y la preferencia de salida difiere del número de estación local, la pantalla de la parte llamada siempre muestra el número de estación de la preferencia de salida.

Utilizar teclas MULAP

El LED de una tecla MULAP puede tener diferentes estados con el siguiente significado:

- Apagado: la línea pertinente es libre y se puede utilizar.
- Encendido: la línea pertinente está ocupada.
- Parpadea rápido: llamada en la línea pertinente.
- Parpadeo lento: hay una llamada en espera en el troncal correspondiente o el troncal correspondiente fue liberado para una conferencia.

Tipo de llamada

Para cada MULAP básico, un administrador con el perfil **Experto** puede definir la señalización acústica de las llamadas externas entrantes a través de la configuración del tipo de timbre. Tiene las siguientes opciones:

- Tono de llamada doble (configuración estándar)
- Tono de llamada triple
- Tono de llamada corto/largo/corto

En los teléfonos analógicos solo se puede aplicar la configuración estándar. Los cambios no tienen ningún efecto.

Pedido de dispositivos miembros de Mulap

Los teléfonos SIP se pueden integrar en un MULAP básico, siempre que se haya definido un dispositivo TDM/HFA como el primer miembro del MULAP básico. Los teléfonos IP se pueden integrar en un MULAP básico, siempre que se haya definido un dispositivo TDM/HFA como el primer miembro del MULAP básico.

Se pueden conectar, por ejemplo, teléfonos móviles Dual-Mode configurados como extensiones Mobility Entry. Los teléfonos móviles de modo dual admiten redes GSM/UMTS y redes WLAN. A través de WLAN se puede registrar un teléfono móvil Dual-Mode como extensión IP (cliente SIP) en el sistema de comunicación.

Los usuarios de movilidad, incluidos los usuarios de movilidad GSM, los clientes de Unify Phone y Microsoft Teams, pueden integrarse en un MULAP básico, siempre que se haya definido un dispositivo TDM/HFA como el primer miembro del MULAP básico.

Nota: La descripción ampliada anterior se aplica a los sistemas OpenScape Business X y OpenScape Business S, pero se limita a Team y Basic Mulap, y no a subcapítulos con

declaraciones similares como Ejecutivo/Secretario/Grupo superior.

Consejo: En los teléfonos SIP no se puede hacer una programación de teclas MULAP. Tampoco se pueden activar ni desactivar prestaciones a través de códigos. No se admiten mensajes de visualización específicos del MULAP básico.

Dependencias

Tema	Dependencia
No molestar	Cuando No molestar está activado, las llamadas entrantes ya no se transfieren.
Teléfonos RDSI	No es posible incluir teléfonos ISDN en MULAP básicos.

Tareas relacionadas

Cómo agregar MULAP básico en la página 745
Cómo mostrar o modificar MULAP básico en la página 746
Cómo borrar MULAP básico en la página 746
Cómo agregar o borrar miembro de MULAP básico en la página 746
Cómo modificar miembro de un MULAP básico en la página 747

15.3.2 MULAP Jefe

Los MULAP Jefe pueden configurarse para utilizar funciones Jefe y Secretaria restringidas.

Se puede acceder a todos los miembros de un MULAP Jefe a través del número de teléfono MULAP Jefe y a través de sus propios números de extensión.

Consejo: En este texto se utiliza "el Jefe" para el femenino y el masculino y "la Secretaria" tanto para secretario como para secretaria.

Se pueden configurar hasta 20 miembros por MULAP Jefe.

Se puede asignar a cada MULAP Jefe un nombre de hasta 16 caracteres.

A través de los parámetros descritos a continuación se definen qué miembros de un MULAP Jefe pueden utilizar funciones Jefe y cuáles funciones Secretaria.

Si un llamante marca el número de teléfono MULAP Jefe, la llamada se señaliza de forma visual en todos los teléfonos pertenecientes al MULAP Jefe. En el caso de los miembros con funciones de Secretaria, las llamadas entrantes también se señalizan acústicamente.

En el caso de las llamadas salientes a través de la línea MULAP Jefe, en el display del usuario llamado aparece el número de teléfono MULAP Jefe.

Estas son las propiedades que se pueden asignar a los miembros de un MULAP Jefe:

- **Maestro**

  Con este parámetro se asignan funciones Jefe a un miembro. Al descolgar el microteléfono se llama automáticamente a través de la línea MULAP Jefe. Las llamadas entrantes a través del número de teléfono MULAP Jefe solo se señalizan de forma óptica.

  Una extensión no puede incluirse como maestro MULAP en líneas colectivas más de 25 veces.

  Ajuste estándar: el primer miembro del MULAP Jefe recibe funciones Jefe.
- **Llamada acústica**

  Si este parámetro está activado, se señalizan acústicamente las llamadas entrantes.

  Ajuste estándar: el parámetro está activado para todos los miembros con función Secretaria.
- **Ocupación automática saliente**

  Si este parámetro está activado, al descolgar el microteléfono se llama automáticamente a través de la línea MULAP Jefe. Si el parámetro no está activado, el usuario deberá pulsar la tecla MULAP antes de poder marcar.

  El parámetro no puede ser utilizado por miembros con función Secretaria.

  Ajuste estándar: el parámetro está activado para todos los miembros con función Jefe.
- **Sin aceptación automática de llamadas entrantes**

  Si este parámetro está activado, las llamadas entrantes no se pueden aceptar descolgando el microteléfono. Para aceptar una llamada entrante hay que pulsar la tecla MULAP.

  Ajuste estándar: el parámetro no está activado.
- **Liberación para conferencia automática**

  Si el parámetro está activado, pulsando la tecla MULAP la línea MULAP ocupada se libera para una conferencia. Todos los demás miembros reciben una indicación de la liberación: la tecla MULAP parpadea. Pulsando la tecla MULAP puede unirse a la conferencia.

  Ajuste estándar: el parámetro no está activado.
- **Tecla MULAP configurada**

  Si el parámetro está activado, en el teléfono correspondiente se configura una tecla MULAP. Pulsando la tecla, se realiza una ocupación saliente a través de la línea MULAP Jefe. En la pantalla del destinatario de la llamada aparece el número de teléfono MULAP Jefe.

  Ajuste estándar: el parámetro está activado.

Utilizar teclas MULAP

El LED de una tecla MULAP tiene este significado:

- Apagado: la línea pertinente es libre y se puede utilizar.
- Encendido: la línea pertinente está ocupada.
- Parpadea rápido: llamada en la línea pertinente.

- Parpadea despacio: una conversación retenida espera a la línea correspondiente o dicha línea fue liberada para una conferencia.

Tipo de llamada

En cada uno de los MULAP Jefe, un administrador con perfil **Experto** puede definir la señalización acústica de las llamadas externas entrantes a través del ajuste de configuración de tipo de llamada. Tiene las siguientes opciones:

- Tono de llamada doble (configuración estándar)
- Tono de llamada triple
- Tono de llamada corto/largo/corto

En los teléfonos analógicos solo se puede aplicar la configuración estándar. Los cambios no tienen ningún efecto.

Teléfonos SIP

En un MULAP Jefe se pueden incluir teléfonos SIP. Para ello es necesario que haya definido un teléfono del sistema (por ejemplo, un teléfono HFA o UP0) como primer miembro del MULAP Jefe (Jefe 1).

Se pueden conectar, por ejemplo, teléfonos móviles Dual-Mode configurados como extensiones Mobility Entry. Los teléfonos móviles Dual-Mode son compatibles con redes GSM/UMTS y con redes WLAN. A través de WLAN se puede registrar un teléfono móvil Dual-Mode como extensión IP (cliente SIP) en el sistema de comunicación.

Consejo: En los teléfonos SIP no se puede hacer una programación de teclas MULAP. Tampoco se pueden activar ni desactivar prestaciones a través de códigos. No se admite la muestra de mensajes en display específicos del MULAP Jefe.

Dependencias

Tema	Dependencia
No molestar	Una vez activado el estado No molestar, no se transfieren las llamadas entrantes.
Teléfonos RDSI	No se pueden incluir teléfonos RDSI en un MULAP Jefe.

Tareas relacionadas

Cómo agregar un MULAP Jefe en la página 747
Cómo mostrar o modificar MULAP Jefe en la página 748
Cómo borrar MULAP Jefe en la página 748
Cómo agregar o borrar miembro de MULAP Jefe en la página 749
Cómo modificar miembro de un MULAP Jefe en la página 749

15.3.3 Configuración de MULAP básicos y MULAP Jefe

Los MULAP básicos y los MULAP Jefe solo pueden ser configurados por un administrador con el perfil **Experto** a través del **modo Experto**.

Se describe el modo de proceder para los siguientes casos de aplicación que pueden configurarse a través del **Modo Experto**:

- Cómo agregar MULAP básico
- Cómo mostrar o modificar MULAP básico
- Cómo borrar MULAP básico
- Cómo agregar o borrar miembro de MULAP básico
- Cómo modificar miembro de un MULAP básico
- Cómo agregar MULAP Jefe
- Cómo mostrar o modificar MULAP Jefe
- Cómo borrar MULAP Jefe
- Cómo agregar o borrar miembro de MULAP Jefe
- Cómo modificar miembro de un MULAP Jefe

15.3.3.1 Cómo agregar MULAP básico

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el árbol de navegación, haga clic en **Llamadas entrantes** > **Llam. grupo / lín. colectiva**.
4) Haga clic en la pestaña **Añadir grupo**.
5) En el campo **N.º de llamada** indique el número de llamada del nuevo MULAP básico.
6) En el campo **Número de marcación directa** indique el número de marcación directa del nuevo MULAP básico.

   : Si desea utilizar DID 879, 890 o 891, debe hacer la configuración a través de ManagerE y no a través de WBM.

7) Introduzca el nombre del nuevo MULAP básico en los campos **Nombre** y **Apellidos**.
8) En la lista desplegable **Tipo**, seleccione la entrada **MULAP básico**.
9) En la lista desplegable **N.º de llamada**, seleccione el número de llamada del suscriptor que desea asignar al grupo MULAP básico.
10) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

    Nota: En una aplicación que use una interfaz CSTA (UC, OSCC, etc.), si se borra un grupo MULAP básico o un miembro de un grupo MULAP básico, hay que reiniciar el sistema.

Conceptos relacionados

MULAP básico en la página 739

15.3.3.2 Cómo mostrar o modificar MULAP básico

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta el MULAP básico deseado.
4) Haga clic en la pestaña **Editar parámetros grupo**. Podrá ver la configuración actual de los parámetros de grupo.
5) Si es necesario, modifique los parámetros deseados del MULAP básico.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

MULAP básico en la página 739

15.3.3.3 Cómo borrar MULAP básico

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta el MULAP básico deseado.
4) Haga clic en la pestaña **Borrar grupo**.
5) Haga clic en **Borrar** y a continuación en **Aceptar**.

Nota: En aplicaciones que utilizan la interfaz CSTA (UC, OSCC, etc.), si se borra un grupo MULAP básico o un miembro de un grupo MULAP básico, hay que reiniciar el sistema.

Conceptos relacionados

MULAP básico en la página 739

15.3.3.4 Cómo agregar o borrar miembro de MULAP básico

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) Elija una de estas opciones:
   - Si desea agregar un miembro al MULAP básico, en el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta el MULAP básico deseado. Haga clic en la pestaña **Añadir miembro**. En la lista desplegable **N.° de llamada**, seleccione el número de teléfono de la extensión deseada. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
   - Si desea borrar un miembro del MULAP básico, en el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**. desplácese hasta el miembro del MULAP básico deseado ((Miembro grupo) N.º de llamada Nombre). Haga clic en la pestaña **Borrar miembro**. Haga clic en **Borrar** y a continuación en **Aceptar**.

Conceptos relacionados

MULAP básico en la página 739

15.3.3.5 Cómo modificar miembro de un MULAP básico

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús, bajo **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **...**, navegue hasta el miembro del MULAP básico deseado ((miembro del grupo) número de llamada nombre).
4) Haga clic en la pestaña **Editar miembro**.
5) Modifique los parámetros deseados
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

MULAP básico en la página 739

15.3.3.6 Cómo agregar un MULAP Jefe

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.

3) En el árbol de navegación, haga clic en **Llamadas entrantes** > **Llam. grupo / lín. colectiva**.
4) Haga clic en la pestaña **Añadir grupo**.
5) En el campo **N.º de llamada** indique el número de llamada del nuevo MULAP Jefe.
6) En el campo **Número de marcación directa** indique el número de marcación directa del nuevo MULAP Jefe.

: Si desea utilizar DID 879, 890 o 891, debe hacer la configuración a través de ManagerE y no a través de WBM.

7) Introduzca el nombre del nuevo MULAP Jefe en los campos **Nombre** y **Apellidos**.
8) En la lista desplegable **Tipo**, seleccione la entrada **MULAP Jefe**.
9) En la lista desplegable **N.º de llamada**, seleccione el número de llamada del suscriptor que desea asignar al grupo MULAP Jefe.
10) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

MULAP Jefe en la página 742

15.3.3.7 Cómo mostrar o modificar MULAP Jefe

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta el MULAP Jefe deseado.
4) Haga clic en la pestaña **Editar parámetros grupo**. Podrá ver la configuración actual de los parámetros de grupo.
5) Si es necesario, modifique los parámetros deseados del MULAP Jefe.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

MULAP Jefe en la página 742

15.3.3.8 Cómo borrar MULAP Jefe

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.

3) En el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta el MULAP Jefe deseado.
4) Haga clic en la pestaña **Borrar grupo**.
5) Haga clic en **Borrar** y a continuación en **Aceptar**.

Nota: En aplicaciones que utilizan la interfaz CSTA (UC, OSCC, etc.), si se borra un grupo MULAP Jefe o un miembro de un grupo MULAP Jefe, hay que reiniciar el sistema.

Conceptos relacionados

MULAP Jefe en la página 742

15.3.3.9 Cómo agregar o borrar miembro de MULAP Jefe

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) Elija una de estas opciones:
   - Si desea agregar un miembro a un MULAP Jefe, en el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta el MULAP Jefe deseado. Haga clic en la pestaña **Añadir miembro**. En la lista desplegable **N.° de llamada**, seleccione el número de teléfono de la extensión deseada. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
   - Si desea borrar un miembro del MULAP Jefe, en el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta el miembro del MULAP Jefe deseado ((Miembro grupo) N.º de llamada Nombre). Haga clic en la pestaña **Borrar miembro**. Haga clic en **Borrar** y a continuación en **Aceptar**.

Conceptos relacionados

MULAP Jefe en la página 742

15.3.3.10 Cómo modificar miembro de un MULAP Jefe

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús, bajo **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **...**, navegue hasta el miembro del MULAP básico deseado ((miembro del grupo) número de llamada nombre).

4) Haga clic en la pestaña **Editar miembro**.
5) Modifique los parámetros deseados
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

MULAP Jefe en la página 742

15.3.3.11 Cómo agregar un MULAP básico a un grupo

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Llamadas entrantes**.
3) Haga clic en el MULAP básico deseado en el grupo de menús, bajo **Llamadas entrantes > Llam. grupo / lín. colectiva**.
4) Haga clic en la pestaña **Editar parámetros grupo**. Se mostrará la configuración actual de los parámetros de grupo.
5) Active el marcador **MULAP como miembro de grupo**.
6) Haga clic en el grupo deseado en el grupo de menú bajo **Llamadas entrantes > Llam. grupo / lín. colectiva** para agregar un MULAP básico como miembro del grupo.
7) Haga clic en la pestaña **Añadir miembro** y seleccione el MULAP básico en el menú desplegable del campo **Número de llamada**.
8) Haga clic en **Aplicar** y, a continuación, en **OK**.

Restricciones:

- Todos los miembros del MULAP básico deben configurarse con parámetros M, R, A.
- El número máximo de miembros del grupo es 20, incluidos los miembros del MULAP básico.
- Los miembros del MULAP básico no pueden ser miembros previos del grupo.
- Se permite añadir un MULAP para:
  1) Línea colectiva lineal
  2) Línea colectiva cíclica
  3) Grupo
- No se permite añadir un MULAP para:
  1) Aviso llam. en espera
  2) Caso de libre
- No se puede cambiar un grupo a Aviso llam. en espera o Caso de libre si contiene un MULAP.

15.4 Grupo de buzón de voz y Grupo de buzón de fax

Un grupo de buzón de voz (grupo Contestador automático) permite a un determinado grupo de extensiones acceder a mensajes de voz. A través del número de teléfono del grupo de buzón de voz no se llama a los miembros del grupo, sino que se accede directamente al buzón de voz (contestador automático) del grupo. Un grupo de buzón de fax (grupo de fax) permite a un determinado grupo de extensiones acceder a mensajes de fax. El número de teléfono de un grupo de buzón de fax permite acceder directamente al buzón de fax del grupo.

15.4.1 Grupo de buzón de voz

Un grupo de buzón de voz (grupo Contestador automático) permite a un determinado grupo de extensiones acceder a mensajes de voz. A través del número de teléfono del grupo de buzón de voz no se llama a los miembros del grupo, sino que se accede directamente al buzón de voz (contestador automático) del grupo. Cuando se deposita un mensaje en el buzón de voz del grupo, éste se transfiere a los buzones de voz de todos los miembros.

Todos los miembros reciben el mensaje de voz simultáneamente. Si un miembro del grupo borra un mensaje de voz, también es eliminado de los buzones de voz de todos los demás miembros y del buzón de voz del grupo. No se ven afectados los mensajes de voz personales de todos los miembros.

Se puede acceder a todos los miembros de un grupo de buzón de voz a través de su número de teléfono de extensión propio.

Se pueden configurar hasta 20 miembros por cada grupo de buzón de voz.

Se puede asignar a cada grupo de buzón de voz un nombre de hasta 16 caracteres.

Al menos una extensión de un grupo de buzón de voz requiere una licencia de buzón de voz.

Interdependencias

Tema	Interdependencia
Timbre adicional	No se puede utilizar la prestación *Timbre adicional*.

Tareas relacionadas

Cómo añadir un grupo de buzón de voz en la página 752
Cómo mostrar o modificar un grupo de buzón de voz en la página 753
Cómo borrar un grupo de buzón de voz en la página 753
Cómo agregar o borrar un miembro de un grupo de buzón de voz en la página 754
Cómo modificar miembro de un grupo de buzón de voz en la página 754

15.4.2 Grupo de buzón de fax

Un grupo de buzón de fax (grupo de fax) permite a un determinado grupo de extensiones acceder a mensajes de fax. El número de teléfono de un grupo de

buzón de fax permite acceder directamente al buzón de fax del grupo. Cuando se deposita un mensaje en el buzón de fax del grupo, éste se transfiere a los buzones de fax de todos los miembros.

Todos los miembros reciben el mensaje de fax simultáneamente. Si un miembro del grupo borra un mensaje de fax, también es eliminado de los buzones de fax de todos los demás miembros y del buzón de fax del grupo.

Se puede acceder a todos los miembros de un grupo de buzón de fax a través de su número de teléfono de extensión propio.

Se pueden configurar hasta 20 grupos de buzón de fax.

Se puede asignar a cada grupo de buzón de fax un nombre de hasta 16 caracteres.

Al menos una extensión de un grupo de buzón de fax requiere una licencia de fax.

Tareas relacionadas

Cómo configurar un grupo de buzón de fax en la página 755
Cómo mostrar o modificar un grupo de buzón de fax en la página 756
Cómo agregar o borrar un miembro de un grupo de buzón de fax en la página 756

15.4.3 Configuración de grupos de buzón de voz y grupos de buzón de fax

Los grupos de buzón de voz y los grupos de buzón de fax solo pueden ser configurados por un administrador con el perfil **Experto** a través del **modo Experto**.

Se describe el modo de proceder para los siguientes casos de aplicación que pueden configurarse a través del **Modo Experto**:

- Cómo añadir un grupo de buzón de voz
- Cómo mostrar o modificar un grupo de buzón de voz
- Cómo borrar un grupo de buzón de voz
- Cómo agregar o borrar un miembro de un grupo de buzón de voz
- Cómo modificar miembro de un grupo de buzón de voz
- Cómo configurar un grupo de buzón de fax
- Cómo mostrar o modificar un grupo de buzón de fax
- Cómo borrar un grupo de buzón de fax
- Cómo agregar o borrar un miembro de un grupo de buzón de fax

15.4.3.1 Cómo añadir un grupo de buzón de voz

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.

3) En el árbol de navegación, haga clic en **Llamadas entrantes** > **Llam. grupo / lín. colectiva**.
4) Haga clic en la pestaña **Añadir grupo**.
5) En el campo **N.º de llamada**, introduzca el número de teléfono del nuevo grupo de buzón de voz.
6) En el campo **Número de marcación directa**, introduzca el número de marcación directa del nuevo grupo de buzón de voz.

: Si desea utilizar DID 879, 890 o 891, debe hacer la configuración a través de ManagerE y no a través de WBM.

7) En el campo **Nombre**, introduzca el nombre del nuevo grupo de buzón de voz.
8) En la lista desplegable **Tipo**, seleccione la entrada **Contestador automático**.
9) En la lista desplegable **N.º de llamada**, seleccione el número de teléfono de la extensión a la que se va a asignar el nuevo grupo de buzón de voz.
10) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Grupo de buzón de voz en la página 751

15.4.3.2 Cómo mostrar o modificar un grupo de buzón de voz

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta el grupo Contestador automático deseado.
4) Haga clic en la pestaña **Editar parámetros grupo**. Podrá ver la configuración actual de los parámetros de grupo.
5) Si es necesario, modifique los parámetros deseados del grupo de buzón de voz.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Grupo de buzón de voz en la página 751

15.4.3.3 Cómo borrar un grupo de buzón de voz

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta el grupo Contestador automático deseado.
4) Haga clic en la pestaña **Borrar grupo**.
5) Haga clic en **Borrar** y a continuación en **Aceptar**.

Conceptos relacionados

Grupo de buzón de voz en la página 751

15.4.3.4 Cómo agregar o borrar un miembro de un grupo de buzón de voz

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) Elija una de estas opciones:
   - Si desea agregar un miembro a un grupo de buzón de voz, en el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta el grupo deseado. Haga clic en la pestaña **Añadir miembro**. En la lista desplegable **N.° de llamada**, seleccione el número de teléfono de la extensión deseada. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
   - Si desea borrar un miembro del grupo de buzón de voz, en el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **…**, desplácese hasta el miembro del grupo deseado ((Miembro grupo) N.º de llamada Nombre). Haga clic en la pestaña **Borrar miembro**. Haga clic en **Borrar** y a continuación en **Aceptar**.

Conceptos relacionados

Grupo de buzón de voz en la página 751

15.4.3.5 Cómo modificar miembro de un grupo de buzón de voz

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **Llam. grupo / lín. colectiva** > **...**, desplácese hasta el miembro del grupo de buzón de voz deseado ((miembro del grupo) número de llamada nombre).

4) Haga clic en la pestaña **Editar miembro**.
5) Modifique los parámetros deseados
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Grupo de buzón de voz en la página 751

15.4.3.6 Cómo configurar un grupo de buzón de fax

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensión**
3) En el árbol de navegación, haga clic en **Extensiones** > **Aplicaciones de UC** > **Fax Grupo**. Se muestran los grupos de buzón de fax que ya están configurados.
4) Seleccione la siguiente fila libre y en el campo **N.º de llamada**, introduzca el número de teléfono del nuevo grupo de buzón de fax.
5) En el campo **N.º llam. marc. directa**, introduzca el número de marcación directa del nuevo grupo de buzón de fax.

   : Si desea utilizar DID 879, 890 o 891, debe hacer la configuración a través de ManagerE y no a través de WBM.

6) En el campo **Nombre**, introduzca el nombre del nuevo grupo de buzón de fax.
7) En la lista desplegable **Tipo**, seleccione la entrada **Fax Grupo**.
8) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
9) Cierre la ventana **Grupo de fax**.
10) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
11) Haga clic en **Grupos**.
12) Haga clic en la pestaña **Grupo de fax**.
13) Seleccione el nuevo grupo de buzón de fax y haga clic en **Editar**.
14) Elija una de estas opciones:
    - Si quiere agregar un miembro al grupo de buzón de fax, marque al miembro deseado en la lista **Usuarios**.
    - Si desea agregar varios miembros al grupo de buzón de fax, pulse <Ctrl> y marque a los miembros deseados en la lista **Usuarios**.
15) Haga clic en **Guardar**.

Conceptos relacionados

Grupo de buzón de fax en la página 751

15.4.3.7 Cómo mostrar o modificar un grupo de buzón de fax

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el grupo de menús, haga clic en **Extensiones** > **UC Applications** > **Grupo de fax**.
4) En el grupo de menús, haga clic en el grupo de buzón de fax.
5) Haga clic en la pestaña **Editar parámetros exten.**.
6) Si es necesario, modifique los parámetros deseados del grupo de buzón de fax.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Conceptos relacionados

Grupo de buzón de fax en la página 751

15.4.3.8 Cómo borrar un grupo de buzón de fax

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Grupos**.
4) Haga clic en la pestaña **Grupo de fax**.
5) Seleccione el grupo de buzón de fax deseado y haga clic en **Eliminar**.

15.4.3.9 Cómo agregar o borrar un miembro de un grupo de buzón de fax

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en Grupos.
4) Haga clic en la pestaña **Grupos de fax**.

5) Seleccione el grupo de buzón de fax deseado y haga clic en Editar. Se muestra la lista Usuarios, en la que aparecen indicados los miembros ya existentes.
6) Elija una de estas opciones:
   - Si desea agregar un miembro al grupo de buzón de fax, pulse <CTRL> y marque el nuevo miembro junto con los miembros ya existentes en la lista Usuarios.
   - Si desea borrar un miembro del grupo de buzón de fax, pulse <CTRL> y elimine la marca del miembro deseado en la lista Usuarios.
7) Haga clic en **Guardar**.

Conceptos relacionados

Grupo de buzón de fax en la página 751

15.5 Mensajes directos para grupos

El mensaje directo de grupos permite hacer anuncios a las extensiones internas de un grupo.

15.5.1 Mensaje a grupo

Mensaje a grupo permite enviar mensajes directos de extensiones internas de un grupo. Esta prestación también se designa "Búsqueda interna" (Paging Intern). Los miembros de grupo que estén ocupados o que hayan activado el estado No molestar, no recibirán Búsqueda interna. Los miembros de grupo llamados no tienen opción de contestación directa. Solo se puede contestar descolgando el microteléfono, lo que da paso a una llamada bipartita normal.

El Mensaje a grupo (Búsqueda interna) se puede utilizar a través de una tecla de función programada para ello o a través de la opción de menú **Interfono** o del código correspondiente, marcando a continuación el número de teléfono del grupo. También se puede programar una tecla de función con un número de teléfono de grupo Después de pulsar una de estas teclas de función, se establece conexión inmediatamente con el grupo programado.

Interdependencias

Tema	Interdependencia
No molestar	Los miembros del grupo con el estado No molestar activado no recibe ningún mensaje.
Teléfonos RDSI, Teléfonos SIP	La prestación "Mensaje a grupo (Búsqueda interna)" no se puede utilizar con teléfonos RDSI o SIP.

15.5.2 Transferencia a grupo desde mensaje

Una llamada es estado de consulta se puede transferir a un grupo a través de Transferencia desde mensaje. Para hacerlo se inicia un mensaje al grupo

(Búsqueda interna). En cuanto un usuario del grupo descuelga el auricular o activa el altavoz, y el usuario que transfiere cuelga, se establece una conexión bipartita. Todos los demás miembros de grupo ven interrumpida la conexión.

El Mensaje a grupo (Búsqueda interna) se puede utilizar a través de una tecla de función programada para ello o a través de la opción de menú **Interfono** o del código correspondiente, marcando a continuación el número de teléfono del grupo. También se puede programar una tecla de función con un número de teléfono de grupo Después de pulsar una de estas teclas de función, se establece conexión inmediatamente con el grupo programado.

Interdependencias

Tema	Interdependencia
No molestar	Los miembros del grupo con el estado No molestar activado no recibe ningún mensaje.
Teléfonos RDSI, Teléfonos SIP	La prestación "Transferencia desde mensaje a grupo" no se puede utilizar con teléfonos RDSI o SIP.

15.6 UCD (Uniform Call Distribution)

A través de la prestación "UCD (Uniform Call Distribution)", el sistema de comunicación permite una distribución uniforme de llamadas entrantes en un grupo de extensiones (grupo UCD).

Los grupos UCD, especialmente en el ámbito de las hotlines técnicas (p. ej., una hotline de servicio de atención al cliente), son utilizadas para la gestión de quejas, la investigación de mercado, la aceptación de pedidos o solicitudes (p. ej., centrales de envío, servicio de tickets) o para servicios de emergencia.

Por norma general, la distribución de llamadas se realiza de forma que las llamadas entrantes dirigidas a un grupo UCD son transferidas a aquellas extensiones del grupo (agentes) lleve más tiempo sin atender llamadas. También se pueden establecer otras reglas de distribución.

Si no hay ningún agente libre que pueda aceptar una llamada entrante, la llamada se transfiere automáticamente a una cola de espera (Queue). Las llamadas en espera se distribuyen entre los agentes que pasan a estar libres en función de su prioridad y tiempo de espera.

Las llamadas que se encuentran en estado de espera pueden escuchar la reproducción de anuncios grabados o de música.

Configuración

El asistente **UCD** permite configurar los grupos y extensiones para una distribución de llamadas (UCD) inteligente. Se describe el modo de proceder para los siguientes casos de aplicación que pueden configurarse a través del asistente:

- Cómo configurar distribución de llamadas / Grupos UCD
- Cómo agregar o eliminar agentes UCD
- Cómo modificar anuncios grabados/ música en espera en UCD

Además de las opciones de configuración mediante asistentes, los administradores con el perfil **Experto** tienen opciones adicionales para la configuración mediante el **modo Experto**.

15.6.1 Distribución de llamadas (UCD)/Grupo UCD

Un grupo UCD incluye agentes (extensiones) que pertenecen a un grupo de trabajo y a los que se puede acceder a través de un número de teléfono. Una llamada entrante interna o externa se distribuye automáticamente al agente que lleve más tiempo en Reposo.

Los grupos UCD se pueden configurar a través de Gestión basada en Web (WBM) (**Modo Experto**) de forma tal que las llamadas de un agente sean aceptadas automáticamente por el sistema de comunicación (Automatic Incoming Call Connection AICC).

Si todos los agentes de un grupo UCD están ocupados, las llamadas entrantes se pueden registrar en una cola de espera. Por cada grupo UCD se puede establecer, de forma individualizada, el número máximo de llamadas de la cola de espera. Si se supera el número máximo de llamadas en espera, las demás llamadas se pueden desviar a un destino de desbordamiento (un destino externo, otro grupo UCD, una extensión interna o un grupo).

Si el destino de desbordamiento es otro grupo UCD y todos los agentes del grupo UCD están ocupados, la llamada permanece en la cola de espera del grupo original y, además, se coloca en la cola de espera del otro grupo UCD (destino de desbordamiento).

Los llamantes puestos en espera pueden escuchar la reproducción de anuncios grabados o música.

Se puede asignar a cada grupo UCD un nombre de hasta 16 caracteres.

Interdependencias

Tema	Interdependencia
Desvío de llamadas	En estos casos no tiene lugar el desvío de llamadas a un grupo UCD: • Si una línea colectiva es llamada y el siguiente es un usuario con un desvío de llamadas a un grupo UCD, la llamada no se desvía. En este caso, se llama directamente al siguiente usuario de la línea colectiva. • Un usuario es miembro de una llamada de grupo con la propiedad "Grupo" y ha activado un desvío de llamadas a un grupo UCD. • Una extensión es miembro de una llamada de grupo en caso de libre. Si el grupo es llamado, no se realiza el desvío de llamadas al grupo UCD. Excepción: el primer usuario registrado ha activado un desvío de llamadas a un grupo UCD. En este caso la llamada se desvía.

15.6.1.1 Cómo configurar distribución de llamadas / Grupos UCD

El asistente **UCD** permite configurar una distribución de llamadas inteligente en un grupo de extensiones seleccionadas.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **UCD**. Podrá ver una lista de todos los grupos UCD posibles.
4) Para configurar un grupo UCD, en la fila del grupo UCD deseado haga clic en **Editar**.
5) En el campo **N.° de llamada**, indique el número de teléfono del grupo UCD.
6) En el campo **Número de marcación directa**, indique el número de marcación directa del grupo UCD.

   : Si desea utilizar DID 879, 890 o 891, debe hacer la configuración a través de ManagerE y no a través de WBM.

7) En el campo **Nombre**, indique el nombre del grupo UCD.
8) Haga clic en **OK & Continuar**. Se abre la ventana **Asignación de agentes UCD**.
9) Seleccione las ID de agente UCD deseadas en **Selección** y asigne los agente al grupo UCD. Para hacerlo, haga clic en **Agregar**.
10) Haga clic en **OK & Continuar**. Se abre la ventana **Editar anuncio grabado/desbordamiento**.
11) En la lista desplegable **Anuncio grabado** seleccione el equipo de anuncios grabados del grupo UCD. Puede seleccionar un anuncio grabado (si está configurado) o la música en espera interna (Music on Hold, MoH). Después de seleccionar un equipo de anuncios grabados, se abre el campo **Retraso de anuncio grabado**.
12) En el campo **Retraso de anuncio grabado**, indique el tiempo en segundos en que serán mantenidos en la cola de espera los llamantes.
13) En la lista desplegable **Tiempo de espera entre agentes**, seleccione el tiempo que debe transcurrir para proceder a la transferencia de la llamada al siguiente agente UCD del grupo.

14) En la lista desplegable Destino de desbordamiento, seleccione el **destino de desbordamiento** del grupo UCD. Puede seleccionar un destino externo, otro grupo UCD, una extensión interna o un grupo.

    Si selecciona **Destino externo** como el destino de desbordamiento, aparece el campo **Destino externo** en la lista desplegable **Dirección**.

    a) En el campo **Destino externo**, introduzca el número de teléfono del destino de desbordamiento externo.
    b) Si desea acceder al destino de desbordamiento externo a través de una dirección determinada, seleccione esa dirección en la lista desplegable **Dirección**.

15) Haga clic en **Aceptar**, para aplicar las entradas.
16) Si desea configurar más grupos UCD, repita los pasos del 4 al 15.
17) Haga clic en**OK & Continuar** y, a continuación, en **Salir**.

15.6.2 Agentes UCD

Los usuarios de un grupo UCD (Agentes) forman un grupo de trabajo que, por ejemplo, puede ponerse en uso en las hotlines técnicas o en el procesamiento de pedidos o consultas. Todas las llamadas entrantes se distribuyen uniformemente entre las extensiones disponibles de un grupo UCD.

Los agentes se asignan a los grupos UCD a través de identificaciones (IDs). Una ID solo puede estar asignada a un grupo UCD- Un agente puede tener asignadas varias ID. De esta forma un agente puede trabajar en más de un grupo UCD. Sin embargo, un agente solo puede registrarse y estar activo en un grupo UCD al mismo tiempo.

Para poder utilizar las funciones UCD con eficacia, los agentes deberían disponer de teléfonos con display, teclas de función y casco telefónico.

Inicio de sesión / Finalizar sesión

Un agente puede iniciar sesión en cualquier teléfono del sistema de comunicación (excepto en teléfonos RDSI y SIP) a través de su ID (identificación). Una vez realizado el registro, el agente pasa a estar disponible y tiene asignado de forma permanente el teléfono en cuestión hasta que finalice la sesión. No puede registrarse en otro teléfono. Finalizada la sesión, el agente deja de ser tenido en cuenta para la distribución de llamadas.

Los agentes pueden abrir las funciones UCD Inicio de sesión, Finalizar sesión y Cambio del estado de extensión a través de teclas de función programadas para tal fin, a través de las correspondientes opciones de menú o a través de códigos.

Estado de extensión

Después del registro, el agente se encuentra en estado **Disponible**. Si es necesario, un agente puede configurar otro estado de extensión o bien, este estado se modifica automáticamente en función de la actividad del agente. El estado de extensión aparece indicado en el display del teléfono.

Estas son las posibles indicaciones:

Indicación	Significado
disponible	El agente está disponible y puede aceptar llamadas UCD.
no disponible	El agente se ha dado de baja brevemente de su puesto de trabajo (por ejemplo, para hacer una pausa).
tiempo administrativo	El agente se encuentra en el tiempo administrativo. Dentro del tiempo administrativo no recibe ninguna llamada UCD. Según la configuración puede tratarse de un tiempo administrativo individual (el propio agente determina la extensión del mismo modificando su estado de extensión) o de un tiempo administrativo automático (todos los agentes disponen después de una llamada UCD de un tiempo administrativo automático).
para <nombre de grupo UCD>	El agente recibe una llamada UCD.

Finalizado el tiempo de trabajo, el agente finaliza sesión y deja de estar disponible para las llamadas UCD. Sigue estando accesible a través de su número de teléfono de extensión privado.

Si todos los agentes de un grupo UCD se encuentran en estado **No disponible**, se realiza una Transferencia automática diferida de las llamadas entrantes a un destino de desbordamiento (un destino externo, otro grupo UCD, una extensión interna o un grupo).

Si un agente no acepta una llamada, aunque esté registrado y disponible, el sistema de comunicación cambia automáticamente su estado de extensión a **No disponible**.

Interdependencias

Tema	Interdependencia
Desvío de llamadas	Si un agente activa la prestación "Desvío de llamadas", se da de baja automáticamente y deja de estar disponible para las llamadas UCD.
Teléfonos RDSI, Teléfonos SIP	No se pueden utilizar teléfonos RDSI y SIP.

15.6.2.1 Cómo agregar o eliminar agentes UCD

El asistente **UCD** permite agregar agentes UCD a un grupo UCD o eliminar a los agentes de un grupo UCD.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **UCD**. Podrá ver una lista de todos los grupos UCD posibles.
4) Para agregar o eliminar agentes UCD de un grupo UCD, en la línea del grupo UCD deseado, haga clic en **Editar**.
5) Haga clic en **OK & Continuar** para pasar a la ventana **Asignación de agentes UCD**.
6) Elija una de estas opciones:
   - Si desea agregar agentes UCD, selecciones las ID de agente UCD deseadas en **Selección** y asigne los agentes al grupo UCD. Para hacerlo, haga clic en **Agregar**.
   - Si desea borrar agentes UCD, seleccione el **miembro** deseado y elimínelo del grupo UCD pulsando **Borrar**.
7) Haga clic en **OK & Continuar** para confirmar las entradas.
8) Haga clic en **Aceptar**.
9) Si desea modificar los agentes UCD de otro grupo UCD, repita los pasos del 4 al 8.
10) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

15.6.3 Tratamiento posterior

Esta prestación exceptúa temporalmente a un agente de la distribución de llamadas, dándole así un tiempo para procesar la llamada recién finalizada. Dentro de ese tiempo administrativo no recibe ninguna llamada UCD.

Se distingue entre

- el tiempo administrativo individual

  El propio agente determina la duración del tiempo administrativo modificando su estado de extensión.
- el tiempo administrativo automático

  La prestación "UCD (Uniform Call Distribution o Distribución de llamadas)" está configurada de forma que todos los agentes de todos los los grupos UCD disponen automáticamente de un tiempo administrativo después de una llamada UCD. La definición del tiempo administrativo automático se realiza en ciclos de llamada, esto es, en pasos de 5 segundos.

  Un agente puede ampliar manualmente el tiempo administrativo automático modificando su estado de extensión.

Dentro del tiempo administrativo se puede seguir accediendo al agente a través de su número de extensión privado.

15.6.3.1 Cómo modificar el tiempo administrativo automático

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús, haga clic en **Llamadas entrantes** > **UCD**.
4) Haga clic en la pestaña **Editar parámetros UCD**.
5) En la lista desplegable **Tiempo administrativo (ciclos)**, indique el tiempo a disposición de todos los agentes UCD para el tratamiento posterior. La entrada se realiza en ciclos de llamada, esto es, en intervalos de 5 segundos.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

15.6.4 Asignación de llamadas según prioridad

Se puede asignar una prioridad a las llamadas internas y externas para un grupo UCD. Las llamadas puestas en la cola de espera se distribuyen entre los agentes del grupo UCD en función de la prioridad y del tiempo de espera.

Una llamada en espera con prioridad alta es atendida antes que una llamada que lleve más tiempo en espera pero tenga una prioridad más baja. Una llamada en espera con prioridad baja se desvía antes a un destino de desbordamiento que una llamada en espera con mayor prioridad.

En el caso de las llamadas externas, la prioridad se asigna en función de la línea (por canal B), se trate de líneas IP o TDM.

Ejemplos:

- Sistema de comunicación con conexión múltiplex primaria RDSI (interfaz S_{2M}) y acceso individual RDSI (interfaz S_0)

  Las llamadas entrantes a través de la conexión múltiplex primaria RDSI son llamadas de cliente normales. Todos los canales B de la interfaz S_{2M} reciben una prioridad media. Las llamadas por acceso individual RDSI son llamadas urgentes, por ejemplo, pedidos de piezas de repuesto urgentes. Todos los canales B de la interfaz S_0 reciben una prioridad alta.
- Sistema de comunicación con conexión de centralita a un ITSP (Proveedor de servicios de telefonía Internet) y a un acceso individual RDSI (interfaz S_0)

  Las llamadas entrantes a través del número de teléfono del sistema para la telefonía IP son llamadas de cliente normales. Todos los canales B de la interfaz LAN reciben una prioridad media. Las llamadas por acceso individual RDSI son llamadas urgentes, por ejemplo, pedidos de piezas de repuesto urgentes. Todos los canales B de la interfaz S_0 reciben una prioridad alta.

En el caso de las llamadas internas, la prioridad se configura a nivel de sistema y, de esta forma, se aplica equitativamente a todas las llamadas internas.

Hay disponibles 10 niveles de prioridad (1= alto, 10 = bajo).

Por defecto, hay establecida una prioridad = 10 para las llamadas internas y una prioridad = 1 para las llamadas externas.

15.6.4.1 Cómo modificar la Asignación de llamadas según prioridad

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús, haga clic en **Llamadas entrantes** > **UCD**.
4) Haga clic en la pestaña **Editar parámetros UCD**.
5) En la lista desplegable **Prioridad interna**, seleccione la prioridad que se aplicará a todas las llamadas internas dirigidas a todos los grupos UCD (1 = prioridad más altas, 10 = prioridad más baja).
6) Por cada línea (canal B) de la lista desplegable **Prioridad** , seleccione la prioridad que se aplicará a todas las llamadas externas realizadas a través de esa línea y dirigidas a todos los grupos UCD (1 = prioridad más altas, 10 = prioridad más baja). Se puede configurar una prioridad individual para cada canal B.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

15.6.5 Aceptar automáticamente llamadas UCD

Esta prestación permite a los agentes aceptar llamadas entrantes sin más pasos adicionales (Automatic Incoming Call Connection AICC).

Para poder utilizar la prestación, el teléfono de un agente debe estar equipado con casco telefónico y tecla de corte. El agente es informado de la entrada de una llamada mediante un tono audible en el casco telefónico. La llamada se pasa a continuación de forma automática.

Un agente puede finalizar una llamada en curso pulsando la tecla de corte.

Por defecto, la prestación "AICC" no está activada. La activación es específica para un grupo y se aplica a todos los agentes del grupo UCD, estén equipados o no los teléfonos de agente con cascos telefónicos.

15.6.5.1 Cómo modificar la aceptación automática de llamadas UCD

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **UCD** > **…**, desplácese hasta el grupo UCD deseado.
4) Haga clic en la pestaña **Modificar grupo UCD**.

5) Elija una de estas opciones:
   - Si desea que los agentes UCD del grupo UCD puedan aceptar llamadas entrantes sin pasos adicionales, en la lista desplegable **AICC**, seleccione la entrada **sí**.
   - Si desea que los agentes del grupo UCD no puedan aceptar llamadas sin realizar los pasos anteriores (por ejemplo, descolgar el microteléfono), en la lista desplegable **AICC**, seleccione la entrada **no**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

15.6.6 Cola de espera UCD

Si todos los agentes de un grupo UCD están ocupados, las llamadas entrantes se pueden registrar en una cola de espera. Los llamantes puestos en espera pueden escuchar la reproducción de anuncios grabados o de música.

Si una llamada de la cola en espera no es aceptada durante un determinado tiempo (ciclo de llamada primario) por el agente que lleve más tiempo en estado **Disponible**, se asigna al agente el estado **No disponible**. A continuación, la llamada se transfiere al siguiente agente. Si el agente no responden la llamada dentro de un tiempo determinado (ciclo de llamada secundario), es puesto también en estado **No disponible**. Si todos los agentes están en estado **No disponible**, la llamada se puede trasferir al destino de desbordamiento.

Por cada grupo UCD se puede establecer de forma individual, cuántas llamadas puede haber como máximo en la cola de espera. Si se supera el número máximo de llamadas en espera, las demás llamadas se pueden desviar a un destino de desbordamiento.

Se puede definir como destino de desbordamiento un destino externo, otro grupo UCD, una extensión interna o un grupo. Si el destino de desbordamiento es otro grupo UCD y todos los agentes del grupo UCD están ocupados, la llamada permanece en la cola de espera del grupo original y, además, se coloca en la cola de espera del otro grupo UCD (destino de desbordamiento).

A través de una tecla de función programada para tal fin o a través de la opción de menú o código correspondientes, los agentes pueden consultar el número de llamadas que se encuentran en la cola de espera de su grupo UCD.

Llamadas en una cola

El número máximo de llamadas en la cola de espera es 30 para los grupos UCD del 1 al 59 y 72 para el grupo UCD 60.

El número mínimo de llamadas en la cola de espera es cero. Si Cero está configurado como número mínimo, no hay cola de espera. Si no hay ningún agente disponible, las llamadas se rechazan o se transfieren directamente al destino de desbordamiento.

15.6.6.1 Cómo modificar cola de espera UCD

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **UCD** > **…**, desplácese hasta el grupo UCD deseado.
4) Haga clic en la pestaña **Modificar grupo UCD**.
5) En la lista desplegable **Cicl. llam. prim.** seleccione el número de ciclos de llamada primarios. La entrada se realiza en ciclos de llamada, esto es, en intervalos de 5 segundos. Se configura el tiempo que permanecerá una llamada en la cola de espera si no es aceptada por el agente que lleve más tiempo en estado Disponible. A continuación, la llamada se transfiere al siguiente agente disponible.
6) En la lista desplegable **Cicl. llam. sec.** seleccione el número de ciclos de llamada secundarios. La entrada se realiza en ciclos de llamada, esto es, en intervalos de 5 segundos. Se configura el tiempo que permanecerá una llamada en la cola de espera si no es aceptada por el siguiente agente disponible.
7) Seleccione si debe producirse un Cambio de mensaje:
   - Si desea que los llamantes que se encuentran en la cola de espera oigan un único anuncio grabado, en la lista desplegable **Cambio de mensaje**, seleccione la entrada **una vez**.
   - Si desea que los llamantes que se encuentran en la cola de espera oigan distintos anuncios grabados, en la lista desplegable **Cambio de mensaje**, selecciones la entrada **Cíclico**.
8) En el campo **Retraso de anuncio grabado**, indique el tiempo transcurrido el cual los llamantes de la cola de espera podrán oír un anuncio grabado. La entrada se realiza en segundos.
9) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

15.6.7 Desbordamiento UCD

Las llamadas UCD se pueden transferir a un destino de desbordamiento si no son aceptadas por los agentes de un grupo UCD y si no se ha configurado ninguna cola de espera, si se ha alcanzado el número máximo de llamadas en la cola de espera.

Nota: El concepto "Desbordamiento UCD" solamente define un destino de desbordamiento, la segunda entrada CDL. Por tanto, los anuncios grabados solo se reproducen si la llamada está en el destino del desbordamiento UCD y no cada vez que suene la llamada. Cuando una llamada abandona el destino de desbordamiento UCD, se abre la música en espera predeterminada.

Por cada grupo UCD se puede establecer, de forma individualizada, el número máximo de llamadas de la cola de espera. Si se supera este número, las demás llamadas se pueden transferir a un destino de desbordamiento.

Si no quiere tener ninguna cola de espera, puede definir como Cero el número máximo de llamadas en la cola de espera. De esta forma, las llamadas no aceptadas son transferidas directamente al destino de desbordamiento.

Interdependencias

Tema	Interdependencia
AutoAttendant	No se puede utilizar un AutoAttendant (puesto de operadora automático) como destino de desbordamiento.

15.6.7.1 Cómo modificar el desbordamiento UCD

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.
3) En el grupo de menús **Llamadas entrantes** > **UCD** > **…**, desplácese hasta el grupo UCD deseado.
4) Haga clic en la pestaña **Modificar grupo UCD**.
5) En el campo **Llamadas en espera**, indique el número máximo de llamadas en espera. Las llamadas que superen este número se desvían al destino de desbordamiento.
6) En el campo **Tiempo de desbordamiento**, indique el tiempo deseado. La entrada se realiza en segundos.

   Nota: Este ajuste solo es relevante si hay conectada una aplicación UCD externa. Si la aplicación UCD no acepta una llamada en espera en el tiempo de desbordamiento, el sistema de comunicación procesa la llamada siguiendo las indicaciones de Gestión de llamadas (Call Management).
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

15.6.8 Servicio nocturno UCD

Por cada grupo UCD se puede configurar un servicio nocturno individual. Todos los agentes de un grupo UCD pueden activar y desactivar el servicio nocturno. Después de la activación, todas las llamadas del grupo UCD se desvían al destino nocturno.

Se puede definir como destino del servicio nocturno, por ejemplo, a una extensión interna, a otro grupo, una música en espera o anuncio grabado, el buzón de voz del sistema de comunicación o un destino externo.

Activación / Desactivación

El servicio nocturno UCD se puede activar o desactivar a través de una tecla de función programada, a través de las opciones de menú correspondientes o de códigos. Con la activación, hay que indicar el número de teléfono del destino de servicio nocturno deseado.

Para obtener información sobre el servicio nocturno del sistema de comunicación, véase Serv. nocturno.

Interdependencias

Tema	Interdependencia
Estado de extensión	Activar el servicio nocturno UCD no modifica los estados de extensión activos de los distintos agentes. Los agentes con sesión activa no se ven obligados a finalizar sesión.
Servicio nocturno del sistema de comunicación	El servicio nocturno UCD y el servicio nocturno del sistema de comunicación se pueden activar y desactivar de forma independiente. Ejemplo: un grupo UCD fue registrado como destino de servicio nocturno del sistema de comunicación. Las llamadas que acceden al grupo UCD a través del servicio nocturno del sistema de comunicación permanecen en el grupo UCD, haya o no haya un servicio nocturno UCD.
Llamadas en curso	Las llamadas en curso no se ven afectadas por la activación del servicio nocturno UCD.

15.6.9 Anuncios grabados/ música en espera en UCD

Los llamantes pueden escuchar la reproducción de música en espera (MOH, Music on Hold), si no son transferidos inmediatamente a los agentes de un grupo UCD. La música en espera y los anuncios grabados se pueden asignar de forma individualizada a cada grupo UCD.

Existen estas opciones:

- Música en espera (Music on Hold, MOH)

  Los llamantes en espera pueden escuchar la reproducción de música desde las fuentes integradas del sistema de comunicación. En el sistema de comunicación se pueden cargar archivos de música en espera adicionales desde un PC.

  Para obtener más información, véase Música en espera
- Anuncios grabados

  Los llamantes puestos en espera pueden escuchar la reproducción de anuncios grabados integrados. En el sistema de comunicación se pueden cargar anuncios grabados adicionales desde un PC.

  Para obtener más información, véase Anuncios grabados

Se puede configurar el tiempo hasta el inicio del anuncio grabado (**Retraso de anuncio grabado**). Para suprimir los anuncios grabados se puede establecer el valor más alto (600 segundos). Se da por supuesto que la llamada será aceptada dentro de ese tiempo.

15.6.9.1 Cómo modificar anuncios grabados/ música en espera en UCD

El asistente **UCD** permite configurar anuncios grabados y/o música en espera para grupos UCD.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **UCD**. Podrá ver una lista de todos los grupos UCD posibles.
4) Para modificar los Anuncios grabados o la Música en espera (MOH) de un grupo UCD, en la línea del grupo UCD deseado haga clic en **Editar**.
5) Haga clic en **OK & Continuar** varias veces, hasta que se abra la ventana **Editar anuncio grabado/desbordamiento**.
6) En la lista desplegable **Anuncio grabado** seleccione el equipo de anuncios grabados del grupo UCD. Puede seleccionar un anuncio grabado (si está configurado) o la música en espera interna (Music on Hold, MoH). Después de seleccionar un equipo de anuncios grabados, se abre el campo **Retraso de anuncio grabado**.
7) En el campo **Retraso de anuncio grabado**, indique el tiempo en segundos en que serán mantenidos en la cola de espera los llamantes.
8) Haga clic en **Aceptar**, para aplicar las entradas.
9) Si desea modificar los anuncios grabados o la música en espera (Music On Hold MOH) de otro grupo UCD, repita los pasos 4 a 8.
10) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

15.6.10 Transferencia a grupos UCD

Las llamadas internas y externas se pueden transferir a grupos UCD. Si no se atiende a una llamada en un tiempo determinado, se realiza una llamada recordatoria.

El tiempo para la llamada recordatoria se define a través del parámetro de tiempo **Supervisión de una transferencia antes de contestar a un grupo UCD**. El ajuste estándar es de 300 segundos. Los administradores con el perfil de **experto** pueden modificar este ajuste en el **Modo Experto**.

Interdependencias

Tema	Interdependencia
Anuncios grabados	Las llamadas externas transferidas pueden escuchar la reproducción de anuncios grabados. Esto no es posible en las llamadas internas.
Tiempo para la llamada recordatoria	Para realizar una transferencia a grupos UCD, se aplica un tiempo para la llamada recordatoria distinto al de la transferencia a otras extensiones.

15.6.10.1 Cómo modificar el tiempo para la llamada recordatoria para llamadas transferidas a grupos UCD

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **Parámetros de tiempo**.
4) Indique el tiempo deseado para la llamada recordatoria para el parámetro **Supervisión de una transferencia antes de contestar a un grupo UCD** (ajuste estándar = 300 segundos). Si finalizado este tiempo no se acepta la llamada, se realiza una llamada recordatoria.
   a) En la lista desplegable **Base**, seleccione la base de tiempo deseada.
   b) En el campo **Factor**, indique el valor con el que se debe multiplicar la base de tiempo.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

15.6.11 Liberación de llamadas UCD a través de líneas analógicas

Si las llamadas UCD a través de líneas analógicas no se aceptan en un determinado tiempo, se liberan. De esta forma se impide que las líneas analógicas se mantengan ocupadas.

El tiempo de liberación se define a través del parámetro de tiempo **Supervisión de una llamada UCD en una línea analógica**. El ajuste estándar es de 300 segundos. Los administradores con el perfil de **experto** pueden modificar este ajuste a través del **Modo Experto** (de 0 a 255 minutos).

15.6.11.1 Cómo modificar el tiempo de liberación para llamadas UCD a través de líneas analógicas

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **Parámetros de tiempo**.
4) Indique el tiempo deseado para el parámetro **Supervisión de una llamada UCD en una línea analógica** (se pueden configurar de 0 a 255 minutos, ajuste estándar = 300 segundos). Si transcurrido este tipo no se acepta una llamada, ésta se libera.
   a) En la lista desplegable **Base**, seleccione la base de tiempo deseada.

b) En el campo **Factor**, indique el valor con el que se debe multiplicar la base de tiempo.

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16 Encaminamiento de llamadas

El sistema de comunicación ofrece distintas opciones para asignar llamadas a un destino, tales como Clases de servicio (Control de marcación), Servicio nocturno y diurno, Least Cost Routing y control de llamadas. Sea cual sea la configuración, siempre se pueden realizar llamadas de emergencia.

16.1 Clases de servicio (Control de marcación)

Las clases de servicio (Control de marcación) regulan el acceso de las extensiones a conexiones externas que pueden tener gastos asociados.

Conceptos relacionados

Configuración de las extensiones en la página 458

16.1.1 Grupos de clases de servicio y clases de servicio

Todas las extensiones tienen asignado un grupo de clases de servicio en el que se define la clase de servicio que tiene cada extensión para llamadas entrantes y salientes.

En el grupo de clases de servicio, por cada dirección hay definida una de las siguientes clases de servicio:

- **Internas**

  La extensión solo puede efectuar llamadas internas.
- **Acceso indirecto**

  La extensión solo puede atender llamadas externas, pero no iniciarlas.
- **Lista nos. autorizados** 1-6

  La extensión solo puede marcar los números de teléfono externos definidos en la lista de números autorizados. Si no hay registrado ningún número se aplica el acceso indirecto a la red urbana.
- **Lista nos. prohibidos** 1-6

  El usuario no puede marcar los números de teléfono externos definidos en la lista de números prohibidos. Si no hay registrado ningún número se aplica el acceso directo a la red urbana
- **Acceso directo**

  El usuario puede aceptar y establecer, sin ningún tipo de restricción, comunicaciones externas entrantes y salientes.

Algunos de los 15 grupos de clases de servicio posibles están preasignados con la misma clase de servicio y tienen nombres explicativos (p.ej. el grupo de clases de servicio **Internacional** con la clase de servicio **Acceso directo** o el grupo de clases de servicio **Entrante** con la clase de servicio **Acceso indirecto**. El administrador puede modificar los nombres de todos los grupos de clases de servicio.

Nota: De forma predeterminada, todas las extensiones pertenecen al grupo de clase de servicio 7; este ajuste se

puede modificar. Además, todas las líneas pertenecen al grupo de clase de servicio 7, pero no se puede configurar; en consecuencia, el grupo de clase de servicio 7 no se debe utilizar y debe tener acceso sin restricciones a todos los grupos de línea.

Interdependencias

Tema	Interdependencia
Destinos de marcación abreviada	Los destinos de marcación abreviada central se pueden marcar con independencia del grupo de clases de servicio asignado.
LCR	Los Grupos de clase de servicio (Control de marcación) y la Autorización LCR son cosas diferentes.
Desvío de llamadas	Con el desvío de llamadas se aplica la clase de servicio del llamante.

16.1.1.1 Cómo modificar el nombre de un grupo de clases de servicio

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Día:Grupo de clases de servicio**.

   Nota: En el grupo de menús, también puede hacer clic en **Noche:Grupo de clases de servicio** para obtener el mismo resultado.
4) En el grupo de menús, haga clic en el grupo de clase de servicio deseado.
5) Haga clic en la pestaña **Modificar grupo de clase de servicio**.
6) En el campo **Grupo de clases de servicio** modifique el nombre del grupo de clases de servicio.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.1.1.2 Cómo modificar las clases de servicio de un grupo de clases de servicio

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Día:Grupo de clases de servicio**.
4) En el grupo de menús, haga clic en el grupo de clase de servicio deseado.

5) Haga clic en la pestaña **Modificar grupo de clase de servicio**.
6) Para el servicio diurno, en todas las direcciones utilizadas seleccione la clase de servicio deseada en la lista desplegable.
7) Si es necesario, seleccione la clase de servicio para **Redes** para el servicio diurno.
8) En el grupo de menús, haga clic en **Noche:Grupo de clases de servicio**.
9) En el grupo de menús, haga clic en el grupo de clase de servicio que ha modificado antes.
10) Haga clic en la pestaña **Modificar grupo de clase de servicio**.
11) Ahora, para el servicio nocturno, en todas las direcciones utilizadas seleccione la clase de servicio deseada en la lista desplegable.
12) Si es necesario, seleccione también aquí la clase de servicio para **Redes** para el servicio nocturno.
13) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.1.1.3 Cómo mostrar todos los usuarios de un grupo de clases de servicio

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Día:Grupo de clases de servicio**.

   Nota: En el grupo de menús, también puede hacer clic en **Noche:Grupo de clases de servicio** para obtener el mismo resultado.

4) En el grupo de menús, haga clic en el grupo de clase de servicio deseado.
5) Haga clic en la pestaña **Mostrar miembros del grupo**. Aparecen todos los usuarios que tengan asignado el grupo de clases de servicio seleccionado, con el número de teléfono y el nombre.

16.1.2 Listas de números prohibidos y autorizados

Con las listas de números prohibidos y autorizados se puede definir qué números de teléfono externos pueden marcar los usuarios y cuáles no.

Las **listas de números autorizados** incluyen las secuencias de números que aparecen al comienzo de un número de teléfono y que no están autorizadas. La extensión solo puede marcar los números de teléfono externos definidos en la lista de números autorizados. Asegúrese de que la lista también recoge todos los números de emergencia necesarios.

Las **listas de números prohibidos** incluyen las secuencias de números que aparecen al comienzo de un número de teléfono y que no están autorizadas. El usuario no puede marcar los números de teléfono externos definidos en la lista de números prohibidos. Asegúrese de que en la lista no haya ningún número de emergencia.

La **lista de números de emergencia** es una lista especial de números autorizados. Los usuarios solo pueden marcar los números de emergencia registrados en esta lista. Asegúrese de que la lista incluya todos los números de emergencia necesarios.

En la lista no hace falta registrar los números completos. Para autorizar a una extensión a marcar todos los números 08000 gratuitos, por ejemplo, solo hay que introducir aquí `0800`. Como las listas solo se refieren a llamadas externas salientes, no hace falta indicar el codigo de acceso a linea urbana junto con los números de teléfono registrados. Si se introduce almohadilla (`#`) al comienzo di un número prohibido, se garantiza que se implementará el control de marcación en los teléfonos del sistema cuando se ocupe una línea urbana analógica con procedimiento de marcación MF y se cambie cambiar a MF durante la marcación.

Mediante el **Filtro evaluación**, el administrador puede definir, en una lista de números prohibidos, qué dígitos no deberían compararse con dicha lista. Antes de evaluar la marcación, el sistema de comunicación oculta el rango de números configurado. Al prohibir los caracteres `*` y `#`, los usuarios no pueden eludir el control de marcación introduciendo esos caracteres especiales.

Límites de configuración

Prestación	Cantidad
Lista de números autorizados 1: larga, 100 entradas	1
Listas de números autorizados 2-6: cortas, 10 entradas	5
Lista de números prohibidos 1: larga, 50 entradas	1
Listas de números prohibidos 2-6: cortas, 10 entradas	5
Longitud de caracteres de las entradas de la lista (dígitos 0 - 9 y caracteres * y #)	26

16.1.2.1 Cómo crear una lista de números de emergencia

Con el asistente **Clase de servicio** puede crear una lista con números de emergencia para el grupo de clases de servicio "Números de emergencia".

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

El sistema de comunicación está conectado a una línea urbana.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Clase de servicio**.
4) En el campo de entrada introduzca un número de emergencia y haga clic en **Agregar**. El número de teléfono se incluye en lista de números de emergencia.
5) Si desea registrar más números de teléfono en la lista de números de emergencia, repita el paso anterior.

6) Haga clic varias veces en **OK & Continuar** hasta que concluya la configuración con **Finalizar**.

16.1.2.2 Cómo crear una lista de números autorizados y de números prohibidos

El asistente **Clase de servicio** permite crear una lista de números permitidos y una lista de números autorizados.

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

El sistema de comunicación está conectado a una línea urbana.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Clase de servicio**.
4) Haga clic en **OK y Continuar**.
5) En el campo de entrada, introduzca un número autorizado sin código de acceso a la red urbana y haga clic en **Añadir**. El número de teléfono se añade a la lista de números autorizados.
6) Si desea registrar más números en la lista de números autorizados, repita el paso anterior.
7) Haga clic en **OK y Continuar**.
8) En el campo de entrada, introduzca un número de teléfono prohibido sin código de acceso a la red urbana y haga clic en **Añadir**. El número de teléfono se añade a la lista de números prohibidos.
9) Si desea registrar más números en la lista de números prohibidos, repita el paso anterior.
10) Haga clic varias veces en **OK & Continuar** hasta que concluya la configuración con **Finalizar**.

16.1.2.3 Cómo crear más listas de números autorizados

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Clases de servicio** > **Listas de nos. permitidos**.
4) En el grupo de menús, haga clic en la lista de números autorizados deseada.
5) Haga clic en la pestaña **Añadir n.° de llamada**.
6) Indique el **N.° de llamada** externo sin códigos de ruta.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

8) Si desea añadir más números de teléfono, repita los pasos 6 y 7.
9) Si desea crear más listas de números permitidos, repita los pasos del 4 al 7.
10) En la pestaña **Mostrar lista** puede visualizar todos los números de teléfono de la lista de números permitidos seleccionada.

16.1.2.4 Cómo crear más listas de números prohibidos

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Clases de servicio** > **Listas de nos. prohibidos**.
4) En el grupo de menús, haga clic en la lista de números prohibidos deseada.
5) Haga clic en la pestaña **Añadir n.° de llamada**.
6) Indique el **N.° de llamada** externo sin códigos de ruta.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
8) Si desea añadir más números de teléfono, repita los pasos 6 y 7.
9) Si desea asignar más listas de números prohibidos, repita los pasos del 4 al 7.
10) En la pestaña **Mostrar lista** puede visualizar todos los números de teléfono de la lista de números prohibidos seleccionada.

16.1.2.5 Cómo mostrar todos los números de teléfono de una lista de números prohibidos

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Clases de servicio** > **Listas de nos. prohibidos**.
4) En el grupo de menús, haga clic en la lista de números prohibidos con el número deseado.

16.1.2.6 Cómo mostrar todos los números de teléfono de una lista de números autorizados

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Clases de servicio** > **Listas de nos. permitidos**.
4) En el grupo de menús, haga clic en la lista de números autorizados con el número deseado.

16.1.2.7 Cómo modificar filtro de evaluación para lista de números prohibidos

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Clases de servicio** > **Listas de nos. prohibidos**.
4) En el grupo de menús, haga clic en la lista de números prohibidos con el número deseado.
5) Haga clic en la pestaña **Modificar filtro de evaluación**.
6) En las listas desplegables **a partir de la cifra** y **hasta la cifra**, seleccione un área.

   Se puede configurar un área dentro de un número de teléfono. La posición inicial del área se selecciona con la lista desplegable **a partir de la cifra** y la posición final, con **hasta la cifra**. .

   La preasignación del campo con los caracteres ***** y **#** permite bloquearlos. Es muy útil ya que * y # se pueden utilizar como caracteres "dummy" que no se evalúan en la línea urbana, omitiendo de esta forma el control de marcación. Al introducir * y # en la lista de números prohibidos, estos caracteres no tienen efecto y solo se evalúan las cifras marcadas.
7) En el campo **Carácter**, introduzca el carácter o caracteres a ocultar.
8) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.1.3 Lista negra

Hay una lista negra disponible dentro del sistema OpenScape Business que permite bloquear llamadas entrantes de números de llamantes específicos (CLI) y de llamadas sin número de llamante o presentación restringida del número de llamante.

La lista negra admite hasta 100 números con un máximo de 25 dígitos, ya sea en formato canónico (por ejemplo, +4989) o en formato internacional (por ejemplo, 004989). Los caracteres admitidos son de 0 a 9 dígitos y el carácter '+'. El carácter '+' se refiere al prefijo internacional que está configurado en el sistema. Debe introducirse siempre en la primera posición. Se permiten fragmentos de números desde el principio del número de la persona que llama (CLI). Se realiza una verificación lógica durante la entrada de un número en la lista negra. El número se rechaza si ya se ha ingresado o si está cubierto por un fragmento de número.

La comprobación de los números de llamantes transmitidos se realiza siempre utilizando el formato internacional. Los números de las personas que llaman se convierten al formato internacional de acuerdo con los datos de la ruta, si se transmiten en otros formatos.

La lista negra se aplica a todos las troncales de la Oficina Central que están configurados en el sistema. Es compatible con varios proveedores de telefonía/ oficinas centrales con diferentes códigos de área local/país.

La lista negra crea una entrada de registro de eventos para cada llamada bloqueada.

Dentro de una red de OpenScape Business, la lista negra debe configurarse en cada nodo que esté conectado a la Oficina Central/Proveedores de telefonía, respectivamente, en las puertas de enlace. Las llamadas internas por la red no están restringidas por la lista negra.

El administrador del sistema puede activar/desactivar la lista negra. Además, se puede establecer una marca separada para el bloqueo de llamadas anónimas.

El **registro de servicio** contiene información sobre los números llamados bloqueados. Las entradas de registro que corresponden a números llamados bloqueados contienen el texto de evento **!Llamada en lista negra:**. Para encontrar el número llamado que fue bloqueóado debe verificar los dos últimos dígitos de la entrada del registro. Estos dígitos (en formato hexadecimal) corresponden a la posición en la lista negra que contiene el número bloqueado. Si estos dígitos son ff, entonces la llamada bloqueada es anónima.

Dependencias

Las llamadas con supresión de CLI no están bloqueadas como llamadas anónimas por el sistema en caso de que el indicador **Anulación de supresión de número de llamada** esté configurado dentro del sistema. El número de la persona que llama debe ingresarse explícitamente en la lista negra en este caso. El marcador **Anulación de supresión de número de llamada** está deshabilitado en la configuración predeterminada de fábrica. Solo se puede habilitar usando el Manager E.

La lista negra puede afectar a la función de movilidad del sistema si se ingresan números móviles de usuarios de movilidad en la lista negra. En este caso, la lista negra bloquea la llamada al puerto DISA en el modo Call Through.

16.1.3.1 Cómo crear una lista negra para las llamadas entrantes en el modo Experto

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía> Clases de servicio.**
3) Haga clic en **Clases de servicio> Lista negra** en el árbol de menú.
4) Haga clic en la pestaña **Agregar número de llamada**.
5) Ingrese el **Número de llamada**.
6) Haga clic en **Aplicar**, seguido de **Aceptar**.
7) Si desea añadir más números de teléfono, repita los pasos 5 y 6.
8) Los números de llamada agregados de la Lista negra se muestran en la pestaña **Mostrar lista** en el área **Lista negra** o en **Lista negra** en el árbol del menú.

   El administrador del sistema debe poder bloquear a los llamantes no deseados de forma permanente.

   - Active la casilla de verificación **Bloquear llamadas anónimas** en el área de llamadas anónimas para bloquear una llamada entrante anónima.

     Nota: Las llamadas anónimas se definen como las llamadas para las cuales el número de origen no se mostrará al usuario.

   - Marque la casilla de verificación **Función lista negra activada** en el área de Lista negra para bloquear números de llamada específicos.

     Nota: La función de lista negra se basa únicamente en el número de la parte que llama (originador de la llamada) proporcionado por el proveedor.

16.1.3.2 Cómo editar/eliminar números de llamada en la lista negra

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía> Clases de servicio.**
3) Haga clic en **Clases de servicio> Lista negra** en el árbol de menú.
4) En el árbol de menús, haga clic en el número deseado en la lista negra.

5) El administrador puede modificar o eliminar la entrada seleccionada.

   Para modificar la entrada seleccionada:

   - Haga clic en la pestaña **Editar número de llamada**.
   - Introduzca el número de teléfono deseado en el campo **№ de llamada**.
   - Haga clic en **Aplicar** y, a continuación, en Aceptar.

   Para eliminar la entrada seleccionada:

   - Haga clic en la pestaña **Eliminar número de llamada**.
   - Introduzca el número de teléfono deseado en el campo **№ de llamada**.
   - Haga clic en **Aplicar** y, a continuación, en Aceptar.

6) El administrador del sistema debe poder bloquear a los llamantes no deseados de forma permanente.

   - Active la casilla de verificación **Bloquear llamadas anónimas** en el área de **Llamadas anónimas** para bloquear una llamada entrante anónima

     Nota: Las llamadas anónimas se definen como las llamadas para las cuales el número de origen no se mostrará al usuario.

   - Marque la casilla de verificación **Función lista negra activada** en el área de **Lista negra** para bloquear números de llamada específicos.

     Nota: La función de lista negra se basa únicamente en el número de la parte que llama (originador de la llamada) proporcionado por el proveedor.

16.1.3.3 Cómo mostrar los números de llamada en la lista negra

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía> Clases de servicio.**
3) Haga clic en **Clases de servicio> Lista negra** en el árbol de menú.
4) Los números de llamada se muestran en **Lista negra** en el árbol del menú o en la pestaña **Mostrar lista** en el área **Lista negra**.

16.1.3.4 Cómo crear una lista negra para las llamadas entrantes en la Configuración

Se puede crear una lista negra con el asistente de **Lista negra para llamadas entrantes**.

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar**para iniciar el asistente de **Lista negra para llamadas entrantes**.
4) En el campo de entrada introduzca un número de emergencia y haga clic en **Agregar**. El número de llamada se agrega a la lista negra.
5) Haga clic en OK & Continuar.
6) Si desea ingresar más números en la Lista negra, repita los pasos 4 y 5.
7) Si desea eliminar un número de llamada, haga clic en **Borrar**.
8) Haga clic varias veces en **OK & Continuar** hasta que concluya la configuración con **Finalizar**.

16.1.4 Serv. nocturno

Las llamadas entrantes y salientes se pueden gestionar de distinta forma que durante el día. Las llamadas entrantes se pueden desviar a un destino de servicio nocturno y las extensiones internas pueden tener otras clases de servicio para el teléfono que durante el día. La conmutación a nivel de sistema entre el servicio diurno y nocturno se realiza automáticamente a una hora preestablecida por el administrador.

Servicio nocturno controlado por tiempo

Servicio nocturno variable

Se puede utilizar cualquier teléfono como destino del servicio nocturno, siempre que el grupo de clase de servicio correspondiente permita llamadas entrantes. No se puede registrar como destino del servicio nocturno un teléfono que solo tenga clase de servicio interna. Si el destino de servicio nocturno ha activado un desvío de llamadas, seguirá el desvío.

Durante el servicio nocturno, un grupo de clases de servicio puede tener asignadas otras clases de servicio que durante el día, por ejemplo para evitar el abuso de tarifas.

Además, para el servicio nocturno puede definir otro puesto de interceptación que por el día. El puesto de interceptación puede ser una extensión individual o un grupo.

El sistema de comunicación activa y desactiva el servicio nocturno según un plan horario definido por el administrador.

Consejo: En el servicio nocturno controlado por tiempo, la regulación establecida es válida para TODAS las extensiones del sistema de comunicación. También hay una conmutación automática de clase de servicio diferida que reune a todas las extensiones en grupos (perfiles).

Un usuario autorizado activa y desactiva el servicio nocturno variable de forma manual. Las llamadas se rigen por listas de destinos de llamada configuradas por el administrador.

De forma predeterminada, la primera extensión del sistema de comunicación (el número de teléfono "100") puede activar o desactivar el servicio nocturno. El administrador puede autorizar hasta a 5 extensiones para activar o desactivar el servicio nocturno.

Servicio nocturno UCD

Puede configurar un servicio nocturno individual por cada grupo UCD. Éste puede activarse y desactivarse de forma independiente al servicio nocturno a nivel de sistema. Los agentes del grupo UCD pueden activarlo y desactivarlo. No se ve afectado el estado actual de los distintos agentes ni las comunicaciones existentes. Después de la activación, todas las llamadas para el grupo UCD se desvían al destino de servicio nocturno.

Se puede definir como destino de servicio nocturno otro grupo UCD, una extensión interna o un destino externo.

16.1.4.1 Cómo asignar clases de servicio para el servicio nocturno manual

El asistente **Clases de servicio** permite asignar a las distintas extensiones la autorización de conmutar el sistema de comunicación del servicio nocturno a diurno (y a la inversa) con sus teléfonos. El cambio entre servicio diurno y nocturno se realiza a través del teléfono, mediante un código.

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM). El sistema de comunicación está conectado a una línea urbana.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Clase de servicio**.
4) Haga clic en **OK&Continuar** varias veces hasta que aparezca la ventana **Extensiones autorizadas para servicio nocturno**.
5) Marque la extensión deseada en la lista de **Extensiones** y haga clic en **Agregar**. A continuación, la extensión aparece en la lista de **Extensiones autorizadas**.
6) Haga clic en **OK & Continuar**.
7) En la ventana **Inventario de sistema** puede ver una vista general de todas las clases de servicio asignadas.
8) Haga clic en **Salir**.

16.1.4.2 Cómo borrar clases de servicio para el servicio nocturno manual

El asistente **Clases de servicio** permite borrar la clase de servicio de los usuarios para pasar de servicio diurno a nocturno.

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM). El sistema de comunicación está conectado a una línea urbana.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Clase de servicio**.
4) Haga clic en **OK&Continuar** varias veces hasta que aparezca la ventana **Extensiones autorizadas para servicio nocturno**.
5) Marque la extensión deseada (la extensión cuya clase de servicio desee borrar) en la lista de **Extensiones autorizadas** y haga clic en **Borrar**.
6) Haga clic en **OK & Continuar**.
7) En la ventana **Inventario de sistema** puede ver una vista general de todas las clases de servicio asignadas.
8) Haga clic en **Salir**.

16.1.4.3 Cómo configurar el servicio nocturno controlado por tiempo

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Servicio autom. nocturno** > **Lunes** (Lunes por ejemplo; puede seleccionar cualquier día de la semana).
4) En **Editar zona** seleccione una de las cuatro zonas disponibles para una clase de servicio.
5) Con **Inicio** y **Fin** establezca el tiempo (en horas y minutos) para la clase de servicio.
6) En **Noche N.º llam.** seleccione la extensión autorizada.

   En el campo **Servicio autom. nocturno** se muestra la configuración de la zona correspondiente.
7) Haga clic en **Aplicar** y, a continuación, en **OK**.
   Cuando el servicio nocturno está activo, en la página de inicio del Portal de administración aparece el mensaje **El sistema está funcionando actualmente en modo nocturno**.

16.1.4.4 Cómo configurar un Día especial para el servicio nocturno controlado por tiempo

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Clases de servicio** > **Días especiales**.

4) Mediante **>>** o **<<** seleccione el año para el que quiere establecer un festivo.
5) Mediante **>>** o **<<** seleccione el mes para el que quiere establecer un festivo.
6) En el calendario, haga clic en el día que quiere establecer como festivo.
7) En **Nombre**, indique la designación del festivo.
8) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.1.4.5 Cómo borrar un día especial para el servicio nocturno controlado por tiempo

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Clases de servicio** > **Servicio autom. nocturno** > **Días especiales**.
4) En **Día**, haga clic en el símbolo de papelera que verá a la izquierda del festivo que desea borrar.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.1.5 Conmutación de clase de servicio automática diferida

Con la conmutación de clase de servicio automática diferida, las extensiones se agrupan en los denominados perfiles de extensión en los que se define qué grupo de clase de servicio será válido en cada periodo de la semana. Por cada perfil de extensión se puede configurar un plan horario.

Interdependencias

Diferencias entre la conmutación de clase de servicio automática diferida y el servicio nocturno controlado por tiempo:

- La conmutación automática de clase de servicio diferida solo es válida para el servicio diurno, no para el nocturno.
- Acceso al destino de la llamada mediante la Gestión de llamadas:

  El procesamiento se hace mediante la Gestión de llamadas y no depende de la conmutación de clase de servicio automática diferida. Existen diferentes listas de llamada para día y noche.
- Con el Servicio nocturno controlado por tiempo solo se puede distinguir entre Servicio diurno y nocturno y se aplica a TODAS las extensiones.
- Destinos de interceptación

  El destino de interceptación se determina mediante el Servicio nocturno controlado por tiempo.

- Grupo de clase de servicio:

  Durante la noche, el grupo de clase de servicio está en una relación constante (configurable) con la extensión y la conmutación automática de clase de servicio diferida no influye aquí para nada.

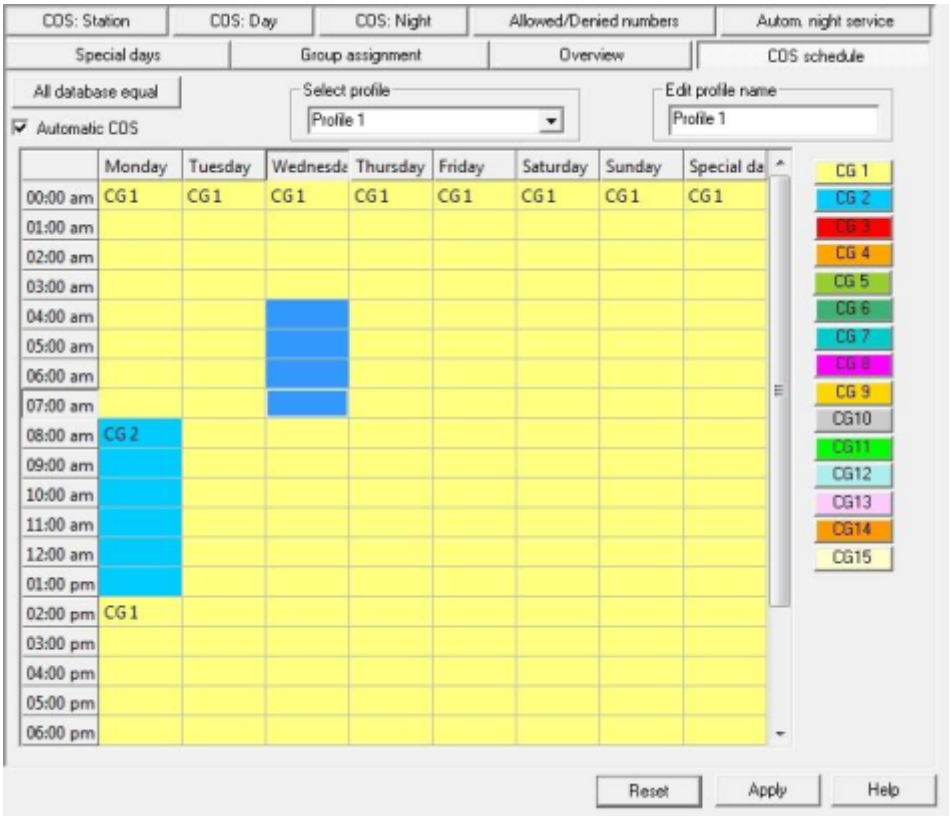
  Durante el día, el grupo de clase de servicio se puede cambiar a determinadas horas o tener una relación fija (configurable) con la extensión.

Tema	Interdependencias
Servicio nocturno	La prestación “Servicio nocturno" tiene prioridad respecto a la prestación de “conmutación automática de clase de servicio diferida". Si está activado el servicio nocturno automático, el grupo de clase de servicio se trata de la forma habitual y se asume el grupo para noche. El plan horario solo tiene efecto durante el día.
Interconexión	La conmutación automática de clase de servicio y el cambio de servicio diurno/nocturno no funcionan de forma general para varios nodos.

16.1.5.1 Plan horario

El plan horario permite controlar las clases de servicio en caso de conmutación automática de clase de servicio por tiempo. Se pueden configurar hasta ocho conmutaciones de clase de servicio al día, todos los días de la semana.

Cada día comienza a las 00:00 horas. La entrada de la hora final de las distintas columnas identifica las zonas horarias. En el siguiente ejemplo, las conmutaciones de clase de servicio de un plan horario se han identificado con CG2, CG4 y CG5.



Una extensión puede tener diferentes grupos de clase de servicio para día y noche.

Si se ha establecido la conmutación automática de clase de servicio durante el día para todo el sistema, una extensión dispondrá del grupo de clase de servicio que se le ha asignado en función del perfil y del plan horario fijados. Por la noche, la extensión tiene el mismo grupo de clase de servicio que tuviera asignado hasta entonces (mediante el Servicio nocturno).

La conmutación automática de clase de servicio diferida está desactivada de forma predeterminada

El sistema de comunicación solo admite una zona horaria (hora mundial). Los grupos remotos de extensiones que trabajan en zonas horarias distintas se ajustan a la zona horaria del sistema de comunicación.

El plan horario solo se puede configurar mediante el Manager E.

16.1.6 VBZ (Relaciones de tráfico)

La prestación VBZ (Relaciones de tráfico) permite establecer qué extensiones del sistema de comunicación pueden establecer conexión con otras extensiones (y cuáles). Esta prestación se utiliza, por ejemplo, para sistemas individuales.

VBZ también permite configurar a qué líneas pueden acceder las distintas extensiones para establecer llamadas entrantes y salientes..

Las funciones VBZ no acceden a aplicaciones y solo son relevantes para la telefonía. La representación del estado de presencia, por ejemplo, no se ve limitada por la restricción de acceso mediante VBZ.

La prestación VBZ se implementa en dos pasos:

- Creación de grupos VBZ
- Configuración de la matriz VBZ

Consejo: La prestación VBZ no se debe utilizar junto con las funciones de UC ya que supondría ciertas restricciones.

16.1.6.1 Grupos VBZ (Grupos de relaciones de tráfico)

Los grupos VBZ (Grupos de relaciones de tráfico) regulan las conexiones autorizadas y prohibidas entre las extensiones y líneas del sistema de comunicación.

Los grupos VBZ permiten agrupar determinadas extensiones y líneas en grupos.

A través de la asignación de grupos VBZ, se asigna un grupo VBZ a las distintas extensiones y líneas del sistema de comunicación. Al codificar la matriz de conexión, se puede acceder al grupo definido con anterioridad y establecer qué extensiones pueden acceder a otras y qué extensiones pueden acceder a determinadas líneas.

Por defecto, todas las extensiones y líneas urbanas están asignados al grupo VBZ 1. De esta forma, todos los usuarios tienen acceso no restringido a otras extensiones y líneas, entrantes y salientes. En la matriz VBZ hay que establecer cuáles grupos VBZ pueden establecer conexiones con qué grupos VBZ.

Se pueden configurar como máximo 64 grupos VBZ.

16.1.6.2 Asignación de números de marcación abreviada (KWZ) a grupos de relaciones de tráfico (VBZ)

Todos los grupos VBZ tienen asignada un área de destinos de marcación abreviada central (destinos KWZ). Si un usuario marca una marcación abreviada, se comprueba el grupo VBZ correspondiente para ver si está autorizado a hacerlo. Si el número de marcación abreviada se encuentra dentro del área de marcación abreviada central del grupo VBZ, se ejecuta la marcación. De lo contrario se emite un mensaje de error.

Si una extensión marca un destino de marcación abreviada, se determina el grupo VBZ correspondiente. De esta forma se determina si la extensión está autorizada a marcar ese destino de marcación abreviada. Si no se hace, la marcación se rechaza con un mensaje de error

Las áreas de destinos de marcación abreviada (KWZ) se pueden solapar en los grupos VBZ.

De forma predeterminada, todos los números de destino de marcación abreviada están asignados al grupo VBZ 1.

Las áreas de números de destino de marcación abreviada (KWZ) se pueden solapar en el grupo VBZ. Se autorizan, por ejemplo:

Grupo VBZ	Área de marcación abreviada (KWZ)
1	0000-7999
2	0050-0150
3	0200-0500

No se permite, sin embargo, especificar varios números de marcación abreviada o varias áreas de marcación abreviada en un grupo VBZ. Debe especificarse una área. No están autorizados, por ejemplo:

Grupo VBZ	Área de marcación abreviada (KWZ)
1	0000, 0005, 0010
2	0050-0100, 0300-0500

16.1.6.3 Cómo asignar extensiones a un grupo de relaciones de tráfico (VBZ)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Clases de servicio** > **Asignación de grupos** > **Asignación de grupos**.
4) Seleccione la entrada con el grupo de relaciones de tráfico deseado para una de las extensiones mostradas en la lista desplegable **Extensión**. Deberá seleccionar la entrada en la lista desplegable **Grupo**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.1.6.4 Cómo asignar una línea a un grupo de relaciones de tráfico (VBZ)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Clases de servicio** > **Asignación de grupos** > **Línea a grupo**.
4) Seleccione la entrada con el grupo de relaciones de tráfico deseado para una de las líneas mostradas en la columna **Líneas**. Deberá seleccionar la entrada en la lista desplegable **Grupo**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.1.6.5 Cómo modificar una matriz VBZ

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Clases de servicio**.
3) En el grupo de menús, haga clic en **Clases de servicio** > **Matriz VBZ**.
4) Modifique las opciones de conexión de esta forma:
   - Si desea bloquear todas las opciones de conexión, haga clic en **Bloquear todo**.
   - Si desea liberar todas las opciones de conexión, haga clic en **Liberar todo**.
   - Si solo desea liberar opciones de conexión internas de grupo, haga clic en **Solo interno al grupo**.
   - Si desea editar de forma selectiva una opción de conexión entre dos grupos VBZ, haga clic en el campo en el punto de intersección de los grupos en la matriz VBZ. Haga clic varias veces en el campo para liberar o bloquear las opciones de conexión en una dirección, en la otra dirección o en ambas direcciones.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.1.7 Candado telefónico central, Conmutación de clase de servicio

El candado telefónico central permite que una extensión autorizada (en su caso, el Administrador) bloquee funciones de telefonía a otras extensiones. Solo siguen disponibles estas prestaciones: llamadas internas, Marcación abreviada central y Conferencia con extensiones internas. La extensión bloqueada puede desactivar el candado telefónico introduciendo su código de candado; también puede desactivarlo la extensión autorizada.

Para definir un bloqueo no se necesita el código de candado telefónico del teléfono en el que la extensión autorizada va a activar o desactivar el candado.

De forma predeterminada, la extensión autorizada es la extensión con el número de teléfono "100" (reconfigurado).

16.1.8 Candado telefónico individual (Candado Sí)

Con la prestación Candado telefónico individual se consigue que desde ese teléfono no se pueda realizar ninguna llamada externa ni modificar los ajustes de usuario.

Esta prestación no impide marcar números de teléfono de emergencia.

Se puede seguir realizando llamadas internas.

También se pueden conectar llamadas entrantes con las extensiones internas.

Si la prestación está activada solo se puede seguir accediendo a aquellas prestaciones que no necesitan marcación externa. La única excepción es la prestación Marcación abreviada central.

Para recordar al usuario que el teléfono está desconectado, se emite un tono de marcación especial. En los teléfonos con display aparece además el mensaje "desbloquear teléfono".

Los usuarios pueden bloquear su teléfono pulsando una tecla o un código después de introducir su candado telefónico personal y volver a desbloquearlo.

Antes de utilizar el candado telefónico por primera vez hay que configurar el código de candado. De forma predeterminada, el código de candado telefónico se establece para todos los teléfonos en 00000 y se puede modificar de forma individual. Sin embargo, para hacerlo el teléfono debe estar bloqueado. El candado telefónico tiene que tener, siempre, 5 caracteres. Solo se permiten los dígitos del 0 al 9. Si el usuario ha obligado el código de candado telefónico, puede restablecer el valor estándar 00000 desde una extensión autorizada (1.ª extensión del sistema con el número de teléfono "100" o el administrador).

16.1.8.1 Cómo restablecer el candado personalizado

El asistente **Versión y nombre de extensión** permite restablecer el candado telefónico personalizado de un teléfono.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Versión y nombre de extensión**. Se abre la ventana **Configuración de nombre y desbloqueo para extensiones y grupos**.
4) Active la casilla de verificación **Reponer candado**.
5) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

16.1.9 Bloqueo de llamadas a cobro revertido por línea urbana (solo para Brasil)

Bloqueo de llamadas a cobro revertido por línea urbana permite activar automáticamente llamadas a cobro revertido entrantes. Esta prestación solo está disponible con el ajuste nacional para Brasil. En todos los demás países este ajuste se omite.

Cada línea urbana analógica se puede configurar individualmente. Bloqueo de llamadas a cobro revertido se puede configurar por cada línea urbana por separado. Si la prestación está habilitada para una línea urbana, 1 s (valor estándar) después de aceptar una llamada se abre el bucle durante 2 s (valor estándar). De esta forma se activan llamadas a cobro revertido en la red y todas las demás llamadas no se modifican.

16.1.10 Bloqueo de llamadas a cobro revertido por extensión (solo Brasil)

Con el bloqueo de llamadas a cobro revertido, por cada extensión se puede configurar un bloqueo de llamadas a cobro revertido personalizado que permite activar automáticamente llamadas a cobro revertido recibidas.
Esto rige también en caso de desvío de llamadas, telecaptura de llamadas, interceptación, etc.

Además se puede generar un bloqueo de llamadas a cobro revertido a nivel del sistema. Esto se aplica si no se marca una extensión individual sino, por ejemplo, una línea colectiva (o también en caso de marcación errónea).

16.2 LCR (Least Cost Routing, Ruta más económica)

Con la función Ruta más económica (Least Cost Routing, LCR) se controla automáticamente la ruta por la que se establecerá una conexión saliente. La ruta puede realizarse a través de la red pública, de distintos proveedores de red (ITSP) o de una red privada. Se busca la ruta de conexión más adecuada para la llamada en función del plan de marcación, de las tablas de ruta y de las reglas de marcación.

Conexiones posibles son llamadas, conexiones de datos analógicas a través de fax y módem y conexiones de datos RDSI.

16.2.1 Funcionalidad LCR

La función LCR permite establecer a través de qué proveedor se realizarán, por ejemplo, una llamada local, una llamada a teléfono móvil o una llamada al extranjero. A través del sistema de comunicación establece el proveedor más económico y realiza todas las llamadas correspondientes a través de la ruta definida.

Si se encuentra un modelo en el plan de marcación que coincida con el número de teléfono marcado, se buscará una ruta adecuada en las tablas de ruta (todas las líneas tienen asignada una ruta). Véase Acceso a línea urbana mediante líneas analógicas y digitales). Se comprueba si la autorización LCR es relevante para esta entrada de tabla de rutas. La autorización LCR y sus diferencias con la Clase de servicio (Control de marcación) se describen en el capítulo Autorización LCR.

Con la funcionalidad LCR se puede controlar qué usuarios del sistema de comunicación pueden utilizar rutas y líneas y cuáles (p. ej., para garantizar que los faxes solo se envíen por líneas urbanas TDM y no por ITSP). También se comprueba si el llamante tiene la clase de servicio necesaria según el control de marcación para ocupar la ruta considerada en ese momento por el LCR. Esta comprobación se puede desactivar para los tronqueos (líneas PABX) mediante la configuración.

Los dígitos marcados se guardan en la memoria intermedia hasta que se evalúan las tablas de rutas con las autorizaciones LCR. Sólo entonces se establece la conexión de acuerdo a las reglas de marcación. Para señalizar la disponibilidad de selección, se puede utilizar un tono de marcación.

Al configurar las reglas de marcación puede introducir información para la extensión que realiza la marcación, por ejemplo, que la conexión se encamina

a través de un determinado proveedor de servicios telefónicos (indicación del proveedor) o que la conexión es cara. Esta información puede aparecer en el display, ser comunicada en forma de tono o indicarse en el display y como tono simultáneamente.

Por regla general:

- Si LCR está activado, se comprueban todas las marcaciones externas. Excepción: al marcar un código de línea o una tecla de línea específicos.
- Si LCR determina que la línea preferida no se puede utilizar, el sistema de comunicación busca una ruta alternativa (posiblemente más cara) en la tabla de rutas.
- Los dígitos se pueden transmitir por separado o en bloque, según el método de acceso y la tabla de rutas.
- Si la tabla de números de marcación directa está vacía, se utiliza en su lugar la tabla de los números de teléfono internos. Se aplican las reglas correspondientes para esa tabla.

Consejo: También en sistemas de comunicación con líneas urbanas analógicas (HKZ) hay que configurar un número de ubicación (Prefijo del país /Código de red local / N.º teléfono del sistema).

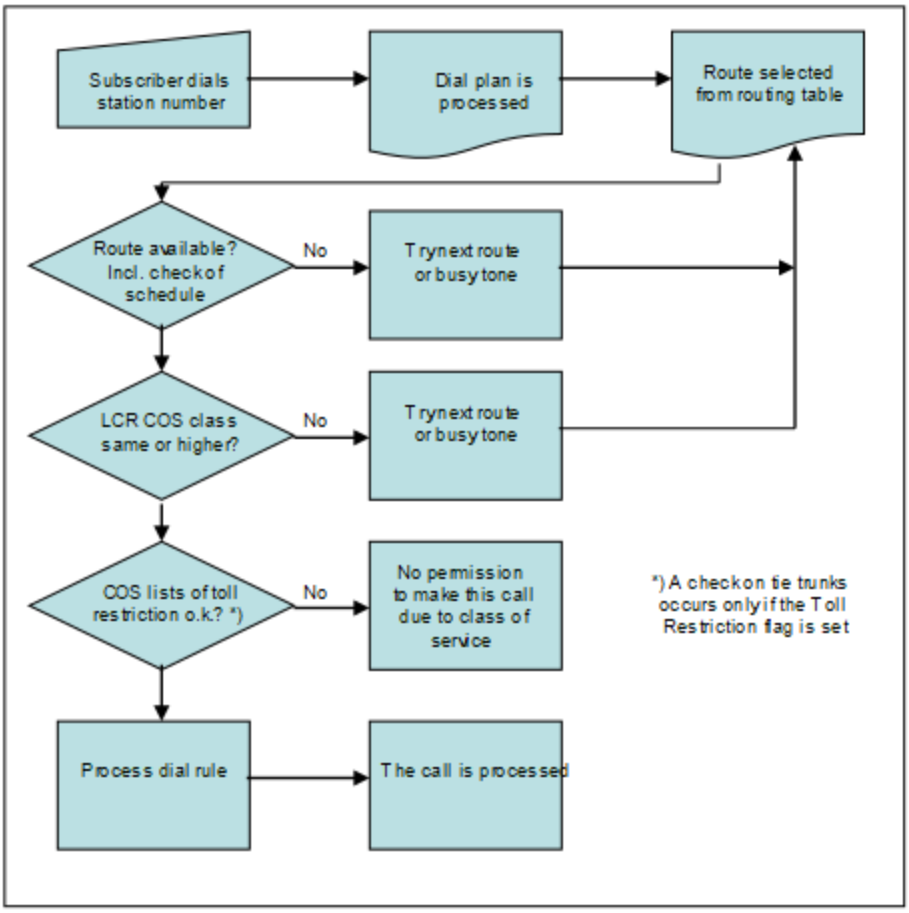
Además, hay que configurar un número de marcación directa o, si la tabla de números de marcación directa está vacía, un número de marcación directa de la línea urbana analógica (HKZ) propio. Solo esto garantiza que se pueda acceder a todos los destinos externos.

Información específica de sistema

El sistema de comunicación evalúa en total 24 caracteres.

El sistema de comunicación puede administrar hasta 1000 planes de marcación y 254 tablas de ruta, cada una con 16 entradas.

Diagrama de flujo de LCR



Emisión de la marcación

En la emisión de la marcación se distingue entre transmisión de la marcación por pasos y transmisión de la marcación en bloque. Con Por pasos, cada dígito se envía y procesa directamente después de la marcación (requisito: evaluación LCR completa, es decir, la entrada del plan de marcación se ha identificado de forma única y se han comprobado las clases de servicio).
Con Marcación en bloque, se forman y envían bloques de dígitos (es decir, la ocupación de línea y la marcación solo se hacen de forma diferida o si hay una identificación de final de marcación explícita).

La emisión de la marcación para las rutas ITSP siempre se debe hacer por bloques. La configuración de la ruta se aplica a toda la tabla de rutas.

Solo para EE. UU.: Carrier Select Override

Carrier Select Override se puede implementar mediante una ocupación de líneas selectiva (código, tecla). En tal caso, se omite por completo el mecanismo de LCR.

Interdependencias

Tema	Interdependencia
Plan horario	Si en un sistema migrado desde HiPath 3000 hay una configuración de LCR con plan horario, las entradas siguen aplicándose y se pueden administrar con el Manager E.
Marcación abreviada central	Para que los destinos de marcación abreviada central funcionen correctamente, en el destino de marcación abreviada hay que indicar el código de acceso LCR seguido del número de destino.
Teclas de destino	Las teclas de destino para destinos externo deben estar programadas con el código de acceso LCR para que funcionen correctamente.
Clase de servicio (Control de marcación)	Las clases de servicio del control de marcación también se aplican en LCR. En las líneas PBX se puede desactivar el control de marcación; la configuración se hace con un flag.
Prime Line	Si la "Ocupación automática de ruta" (Prime Line) con la línea urbana está activada, no se puede implementar LCR. Ambas prestaciones se excluyen entre sí.

16.2.1.1 Cómo liberar LCR

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Consejo:

Determinadas entradas, como el código de red local o el número de extensión, se crean ya en el asistente **Instalación básica**. Solo los técnicos expertos pueden modificar manualmente estas entradas. Si el LCR se configura erróneamente, puede hacer que las conexiones salientes no funcionen o lo hagan con restricciones.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **LCR**.
3) Haga clic en la pestaña **Flags LCR**.
4) Active la casilla de verificación **Liberar LCR**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.2.2 Plan de marcación LCR

Se buscan modelos en el plan de marcación que coincidan con los dígitos marcados (secuencia de marcación). El resultado se utiliza como criterio para elegir la tabla de rutas. Al hacerlo se comprueba si la autorización LCR de la extensión es válida para la entrada de plan de marcación.

El patrón de una secuencia de marcación está asignado a una tabla de rutas en el plan de marcación que define otros parámetros para el establecimiento de conexión.

El plan de marcación se divide en campos independientes para fines de identificación y configuración. La tabla muestra los números 4922000 y 1603656260 al hacer la entrada en el plan de marcación.

Campo 1		Campo 2		Campo 3		Campo 4		Campo 5
0	C	492	–	2000				
0	C	160	–	365	–	62	–	60

Estas son las entradas válidas para los números de teléfono:

0 . . . 9	Dígitos permitidos
–	Separador de campos
C	Tono de marcación simulado (se puede introducir hasta tres veces). Esta entrada también se interpreta como separador de campo
Caracteres globales	
X	Cualquier dígito entre 0 . . 9
N	Cualquier dígito entre 2 . . 9
Z	Siguen, hasta el final de la marcación, uno o varios dígitos

Una secuencia de cifras se puede dividir en 10 campos como máximo.

Separadores de campos sirven para subdividir la secuencia de cifras en campos independientes que pueden ser evaluados por separado. Ejemplo: después del primer dígito de marcación se inserta un separador de campo, de esta forma que un "0" marcado se identifica como campo independiente y simula así un acceso a la red urbana.

La división de los campos, permite repetir o reorganizar estos campos en el plan de marcación. Los campos constituidos en el plan de marcación con los separadores de campo "–" y "C", se pueden activar por separado para repetir, suprimir, intercambiar o agregar dígitos.

Un carácter "#" o "*" en la secuencia de cifras marcada por el usuario, indica el final de la marcación o un cambio en el procedimiento de marcación. Por este motivo, estos caracteres no son entradas válidas en el plan de marcación.

Las entradas con caracteres globales deben ir siempre precedidas por un dígito de marcado inequívoco para evitar conflictos entre distintas entradas de caracteres globales.

Por plan de marcación se puede establecer como obligatoria la indicación del código de proyecto. Para ello se aplica el procedimiento de comprobación de código de proyecto.

Si hay varias entradas de plan de marcación que se correspondan con una determinada cadena, se utiliza la que tenga mayor grado de coincidencia. Ejemplo: Se marca 00894711 y están presentes las entradas de plan de marcación 0CZ y 0C089Z -> se ejecuta 0C089Z. La posición de las entradas en el plan de marcación es irrelevante, no se necesitan entradas "ordenadas".

OpenScape Business puede evaluar una secuencia de marcación de hasta 24 caracteres.

Entradas LCR en la configuración inicial del sistema de comunicación

En la puesta en servicio inicial del sistema de comunicación, se introducen en el plan de marcación una serie de entradas predeterminadas de carácter nacional. Hasta el plan de marcación 34 se preasignan a líneas urbanas RDSI entradas para llamadas de emergencia, información, números de teléfono especiales, ocupación de línea urbana estándar para PSTN y ITSP, UC Suite, anuncios, redes y marcación en formato internacional. Este rango puede verse afectado si se hacen cambios de configuración en otro lugar (p. ej., si se modifica el flag de **Número de ubicación**). Por ello, después de hacer cambios en el número de ubicación hay que comprobar que la ocupación de línea urbana estándar sigue funcionando (es importante para la marcación con números de teléfono públicos).

Consejo: A partir del plan de marcación LCR 36 hay entradas para asignación libre.

16.2.2.1 Cómo editar el plan de marcación

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.
3) Haga clic en **Plan de marcación**.

4) En **Editar plan marcación** aparece un listado de los distintos planes de marcación. Puede editar estos campos:

   - **Nombre**
   - **Cifras marcadas**
   - **Tabla de rutas**
   - **Cód. proyecto**
   - **Control de marcación**

     El flag Control de marcación solo se refiere al tipo de ruta PABX. No es relevante para la ruta Línea urbana, es decir, aquí no se puede desconectar el Control de marcación para las líneas urbanas.
   - **Serv. emerg**

   Nota: Al hacer clic en la flecha azul que aparece junto al campo **Tabla de rutas** se abre directamente la tabla de rutas correspondiente.

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.2.3 Tabla de rutas LCR

En las tablas de rutas de la Ruta más económica (LCR) se busca una ruta adecuada (todas las líneas tienen una ruta asignada). También se comprueba si la clase de servicio (control de marcación) afecta a la ruta. La regla de marcación también depende de la ruta asignada.

La tabla de rutas describe

- la dirección asignada a la ruta en cuestión,
- la regla de marcación,
- la autorización LCR (Clase de servicio, COS) necesaria para una ocupación),
- la opción de advertir de una conexión cara (señal de advertencia).
- el gateway dedicado y
- el ID de nodo de GW.

La tabla se consulta de arriba a abajo, en orden jerárquico. También se comprueba si la ruta está libre o si la extensión tiene la autorización LCR (Clase de servicio, COS) necesaria. Si es así, la marcación se realiza según las reglas de marcación de la tabla de rutas si lo permiten la clase de servicio (Control de marcación) y la asignación VBZ entre extensiones y la línea.#

Si la ruta de enlace principal de la tabla de rutas está ocupada, LCR puede marcar la siguiente ruta configurada en la tabla (probablemente de mayor coste). Se le puede indicar al usuario a través de una señal acústica y/u óptica.

Se pueden crear hasta 254 tablas de rutas con 16 rutas cada una.

Gateway dedicado

Un gateway dedicado es un nodo asociado con definición fija en una interred IP (gateway dedicado -> forzad). Si hay registrado un gateway dedicado con el ID de nodo de GW correspondiente para la ruta de red IP, el encaminamiento se hace a ese gateway de forma forzosa.

En una configuración multigateway se determina un gateway dedicado mediante la configuración de extensión.

16.2.3.1 Cómo editar tablas de rutas

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.
3) Haga clic en **Tabla de rutas**.
4) Aparecerán todas las tablas de rutas:
   - **1-Tabla**
   - **2-Tabla**
   - **Tabla nn**

   Consejo: Las tablas de rutas 1 a 15 son para las entradas predeterminadas o para la configuración mediante asistentes. Al hacer una migración, las entradas existentes se registran automáticamente en estas tablas de rutas.

   Este mecanismo, no obstante, no impide que haya entradas duplicadas. Por ello se recomienda el tratamiento posterior de las tablas de rutas de forma manual.
5) Haga clic en la tabla de rutas deseada. Aparecerá la tabla seleccionada con la pestaña **Editar tabla de rutas**.
6) En **Editar tabla de rutas** aparece un listado de las distintas tablas de rutas. Puede editar estos campos:
   - **Ruta**
   - **Regla de marcación**

     Nota: Para ver y editar las propiedades de una regla de marcación, haga clic en la flecha azul junto a ella.
   - **Clase mín. (Autorización LCR)**
   - **Advertencia**
   - **Gateway dedicado**
   - **ID de nodo de GW**
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.2.4 Autorización LCR

Todas las extensiones tienen asignada una autorización LCR (Clase de servicio, COS). Un usuario solo puede ocupar una ruta si su clase de servicio es igual o superior a la clase de servicio LCR de la tabla de rutas, es decir, un usuario con la clase de servicio 7 no puede ocupar una ruta con clase de

servicio 8. De forma predeterminada, todas las extensiones tienen registrada la autorización LCR máxima (15).

Interdependencias

Tema	Interdependencia
Control de marcación	Las clases de servicio (Control de marcación) tienen prioridad respecto a la autorización LCR. La clase de servicio (Control de marcación) se puede activar y desactivar para líneas cruzadas.
Asignación de grupos VBZ	Solo se hace una marcación si la matriz VBZ lo permite.

16.2.4.1 Cómo asignar y modificar autorizaciones LCR

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.
3) Haga clic en **Classes of Service** (Clases de servicio).
4) En **Editar clase de servicio**, en el campo **Clase de servicio**, asigne una autorización LCR o modifique la clase de servicio existente.

   Esto solo se aplica a la autorización de una extensión para LCR. El campo no tiene ninguna influencia en el acceso a la red urbana.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.2.5 Reglas de marcación LCR

Las reglas de marcación LCR permiten convertir los números de teléfono introducidos en cualquier secuencia de cifras para su procesamiento ulterior. La conversión de dígitos permite acceder a los distintos proveedores de red. La regla de marcación utilizada se determina con la ruta o dirección de la tabla de rutas.

Información específica de sistema

El sistema de comunicación es capaz de administrar hasta 254 reglas de marcación en la tabla de reglas de marcación LCR. El nombre de una regla de marcación puede tener hasta 16 caracteres.

Las reglas se dirigen de forma selectiva a los campos del plan de marcación para las siguientes operaciones:

- Repetición de dígitos
- Supresión de dígitos

- Intercambio de dígitos
- Agregado de dígitos
- Desactivación del procedimiento de marcación
- Identificación de un tono de marcación
- Inserción de pausas de marcación

Regla de marcación

Aquí puede definir hasta un total de 254 reglas de marcación con una longitud máxima de 40 caracteres cada una.

La tabla de reglas de marcación LCR también se denomina tabla de encaminamiento.

Definición de las reglas de marcación (Formato de regla de marcación)

- A:

  Repetir el resto de campos (envío). "A" hace que se envíen todos los campos de dígitos siguientes. El punto de referencia es el último separador de campos presente en el campo de Cifras marcadas del plan de marcación.

  Si se introduce "A" sin referencia explícita, se refiere a todas las cifras detrás del código de acceso, es decir, "A" se corresponde con "E2A"#
- B:

  Se utiliza para la interconexión de varios gateways cuando el número de teléfono llamado desde el exterior es de "tipo" (TON, Type of Number) "desconocido", a fin de poder encaminar a nodos multigateway. Para que este número de teléfono sea único se debe ampliar en formato nacional o internacional según el TON del LCR. Es necesario si los números de marcación directa no son únicos y hay que configurarlos en formato nacional o internacional.
- D (n):

  Marcar secuencia de cifras (entre 1 y 25 cifras). "D" puede aparecer varias veces en la cadena de caracteres y en cualquier posición de la misma.
- E (n):

  Emisión del contenido del campo (1 a 10). "E" puede aparecer varias veces en la cadena de caracteres y en cualquier posición de la misma. "E" puede aparecer en cualquier orden en relación con (n). Un determinado campo puede ser consultado varias veces, también consecutivas. Con la excepción de "E1" (código de acceso), "E" puede aparecer rodeada de cualquier otro parámetro.

  En la marcación por pasos (frente a la marcación en bloque) el último elemento de la regla de marcación no puede ser E(n), sino E(n)A.
- M (n):

  Código de autorización (de 1 a 16). Esta letra no puede aparecer en última posición.
- P (n):

  P (n) puede aparecer varias veces en la cadena y se puede colocar en cualquier posición. P (n) puede estar rodeado de otros parámetros cuales quiera (de 1 a 60 veces la unidad de pausa a nivel del sistema).

- S:

  Conmutación, cambio del método de marcación de MP a MF (con CONNECT, PROGRESS o CALL PROC con PI) "S" solo puede aparecer una vez en la cadena de caracteres y no puede aparecer en última posición. Después de "S" no se puede utilizar el parámetro "C".
- C:

  "C" solo puede aparecer una vez en la cadena de caracteres. Los siguientes caracteres se envían sin pausa de marcación y se utilizan para el acceso de proveedor en "Single Stage", "Two Stage", "DICS" y "PRI".
- U:

  Aplicación del procedimiento de marcación dirección SUB. "U" solo puede aparecer una vez en la cadena de caracteres y no puede aparecer en última posición. Después de "U" no se pueden utilizar los parámetros "S", "P", "M" y "C".
- N (n) (¡solo para EE. UU.!):

  Grupo de red SFG (de 1 a 5) o número de banda (1).
- L (¡solo para EE. UU.!):

  "L" solo puede aparecer al final de la cadena de caracteres. "L" hace que la llamada se gestione como llamada de emergencia.

Ejemplo:

El sistema debería incluir automáticamente un prefijo de proveedor.

La regla de marcación D010xxA significa que el sistema comienza marcando el prefijo de proveedor (010xx), y luego los dígitos marcados por el usuario detrás del código de acceso (A).

16.2.5.1 Cómo editar reglas de marcación

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.

3) Haga clic en **Regla de marcación**. Podrá ver todas las reglas de marcación.

4) En el grupo de menús, haga clic en la regla de marcación deseada.

5) Puede editar los siguientes campos:

- **Nombre de regla**
- **Formato de regla de marcación**
- **Procedimiento de acceso del ofertante de red** (**Desconocido**, **Ofertante de red principal**, **MCL Single Stage**, **MCL Two Stage**, **Red corporativa**, **Servidor de control de marcación**, **Interfaz de línea múltiplex primaria**)
- **Tipo** (**Desconocido**, **Prefijo del país**, **Prefijo de red local**, **Número de teléfono del sistema**)

6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.2.6 Ofertante de red

Puede asignar un proveedor de red a cada ruta. El proveedor de red se selecciona a través de las reglas de marcación para LCR.

Desconocido

Ninguna indicación explícita sobre un ofertante de red.

Ofertante de red principal

En caso de ocupación a través del ofertante de red principal, se realiza la marcación simple a través de marcación en bloque o marcación de dígitos individuales en la red pública.

MCL Single Stage

En MCL Single Stage el ofertante de red deseado se marca con un prefijo y, a continuación, se marca el número de teléfono. En RDSI, la marcación se realiza en el canal D o como marcación normal en líneas urbanas analógicas.

MCL Two Stage

En MCL Two Stage el ofertante de red deseado se marca con un prefijo. Tras una fase de sincronización se envía un código de autorización configurable y, a continuación, el número de teléfono de destino como dígitos MF

En la sincronización por tiempo se ha de programar una pausa de 2 a 12 segundos.

Red corporativa

Hay una red corporativa conectada directamente con el sistema de comunicación. La función LCR determina la ruta correspondiente a partir del número de teléfono marcado por el usuario. A continuación, encamina la llamada a través del haz de líneas de la línea urbana pública o del haz de líneas de la red propia de la empresa.

Servidor de control de marcación

En este tipo LCR el ofertante de red deseado se marca con un prefijo y a través de un DICS (Dial-In Control Server) y se transmite el número de teléfono y un código de autorización configurable en la subdirección. La marcación se realiza en el canal D.

Primary Rate Interface (Interfaz de línea múltiplex primaria) (solo para EE. UU.)

En la interfaz de línea múltiplex primaria, la selección del ofertante de red o del servicio de llamadas se realiza en el mensaje de SETUP a través de los elementos de información Network Specific Facility, Operator System Access y Transit Network Selection.

Interdependencias

Tema	Interdependencia
Recibir/transferir informaciones de llamada	La supresión de la indicación del número de llamada temporal o permanente no puede estar activada.

Tema	Interdependencia
Direccionamiento RDSI/ SUB	La prestación RDSI "SUB" debe solicitarse o activarse en la red pública.

16.2.7 Ocupación selectiva de líneas urbanas

Los usuarios pueden ocupar las líneas urbanas de forma selectiva.

Normalmente hay una asignación de prioridades preasignada para la ocupación de línea urbana mediante Least Cost Routing. Por norma general, el proveedor más económico aparece en primer lugar, el segundo más barato en segundo lugar, etc.

Si un usuario desea establecer una llamada a través de un proveedor que no aparece encaminado en primer lugar (por ejemplo, porque resulta más económico para llamadas a larga distancia), puede seleccionarlo de forma selectiva mediante un código o mediante una tecla de línea.

Del mismo modo, los usuarios pueden utilizar la marcación selectiva por código para marcar un número de teléfono al que solo se puede acceder mediante RDSI (si estuviera preasignado como proveedor, por ejemplo, Vodafone).

De forma predeterminada, hay configurado un código (88) para la asignación selectiva de línea urbana mediante RDSI. El administrador puede configurar o modificar todos los códigos a posteriori.

16.2.7.1 Cómo configurar el código para la asignación selectiva de líneas urbanas RDSI

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.
3) Haga clic en **Plan de marcación**. Aparecen enumerados en forma de lista los distintos planes de marcación.
4) En **Nombre**, introduzca el nombre deseado para el plan de marcación.
5) En **Cifras marcadas**, introduzca el código y la abreviatura de forma exacta (**88CZ**).

   Nota: 88 es el código preasignado de forma predeterminada por el sistema para la ocupación selectiva de una línea urbana RDSI.

   Para información sobre las abreviaturas C y Z, véase Plan de marcación LCR.
6) En **Tabla de rutas**, introduzca un **1**.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.2.7.2 Cómo mostrar los códigos para la ocupación de línea urbana selectiva

El asistente **Línea urbana RDSI / analógico / ITSP** permite mostrar los códigos para la asignación selectiva de línea urbana mediante RDSI.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

El sistema de comunicación está conectado a una línea urbana analógica.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Línea urbana RDSI / analógica / ITSP**.
4) Haga clic varias veces en **OK & Continuar**, hasta llegar a la ventana **Códigos para la ocupación de línea urbana selectiva**.
5) De forma predeterminada, podrá ver los códigos para la asignación selectiva de línea urbana mediante RDSI. En los ITSP configurados se muestran los códigos correspondientes.
6) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

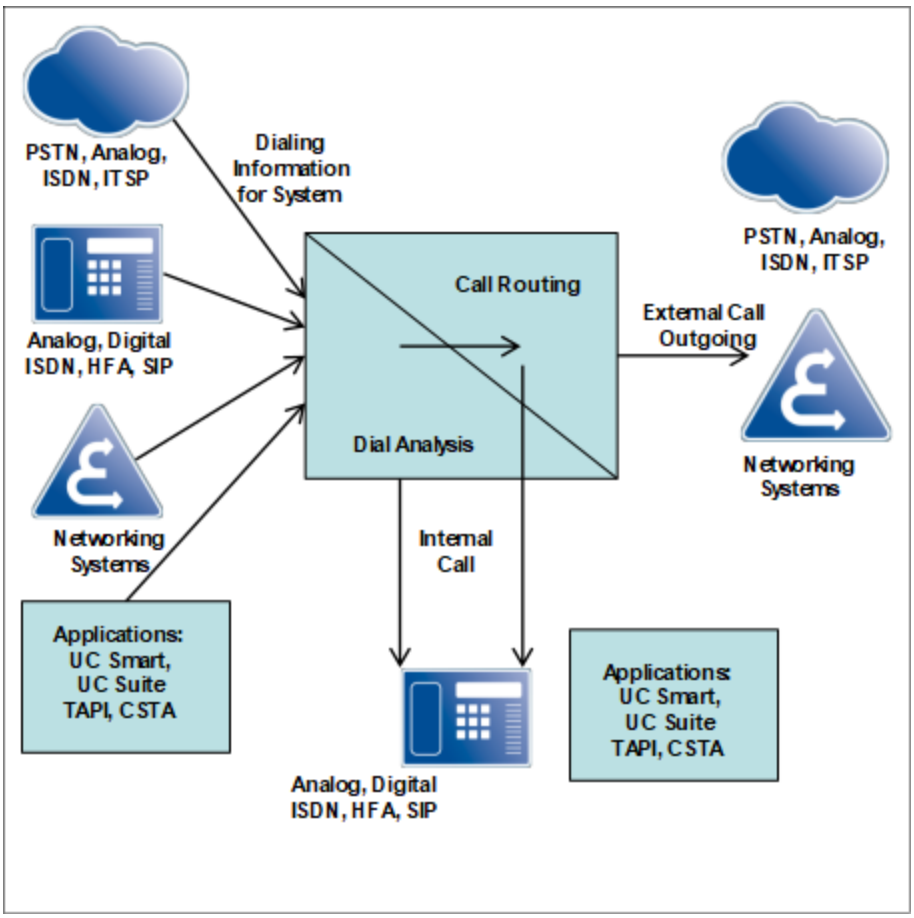
16.3 Evaluación de marcación y encaminamiento de llamadas

Este capítulo aclara la interrelación entre la evaluación de marcación y el encaminamiento de llamadas (Call-Routing). Explica cómo evalúa el sistema de comunicación los números de teléfono que usan las extensiones, las líneas y todo tipo de aplicaciones para acceder a un destino; también explica cómo se hace el encaminamiento una vez finalizada la evaluación de la marcación. Las funciones del sistema relevantes se han descrito ya en gran medida en los capítulos anteriores. La marcación con número de teléfono público en un nodo/ una interconexión se describe detalladamente en esta sección.

La evaluación de marcación

- del sistema de comunicación registra y evalúa todos los números marcados mediante los datos de configuración comprueba las clases de servicio
- comprueba las clases de servicio (por ejemplo, con las clases de servicio para extensiones, flags de extensión, día/nombre, números permitidos y prohibidos, autorizaciones LCR, planes horarios, matrices de conexión, etc.).
- decide si el número marcado se puede marcar internamente o hay que ocupar una línea. Esto es válido para la marcación de números internos, números públicos y números internos de la red.
- normaliza los números de teléfono, es decir, hace posible que el sistema de comunicación marque los números de teléfono. (por ejemplo, el formato canónico "+49nnn" pasa a ser "00049nnn", donde el primer 0 es el código de acceso principal del PBX)
- abrevia, si es necesario, los números de teléfono (se suprimen números iniciales de los números de destino en caso de ocupación de línea urbana

entrante para determinar los destinos de marcación directa en formato abreviado)



16.3.1 Vista general de Call Routing / LCR

En el sistema de comunicación, las llamadas entrantes se someten a distintas comprobaciones y se desvían según los resultados.

Comprobación 1 (¿destino interno?)

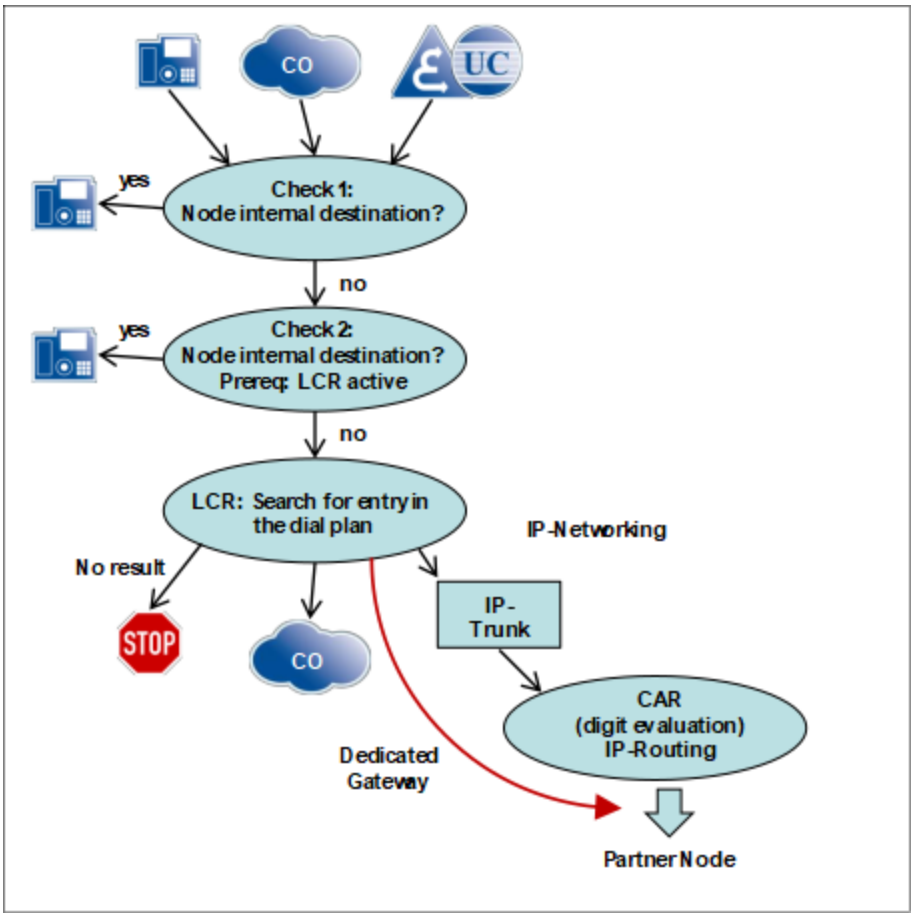
- En primer lugar, los números de teléfono con formato canónico se convierten en números de marcación (en la interfaz de extensión) o se les añade TON=International (interfaz de ITSP).
- En su caso, los números de destino de la línea se acortan con la parte del número de teléfono del número del sistema de la ruta correspondiente.
- Las llamadas internas se evalúan mediante el plan de marcación interno y las llamadas procedentes del exterior con el plan de marcación de los números de marcación directa.

Comprobación 2 (¿destino interno?)

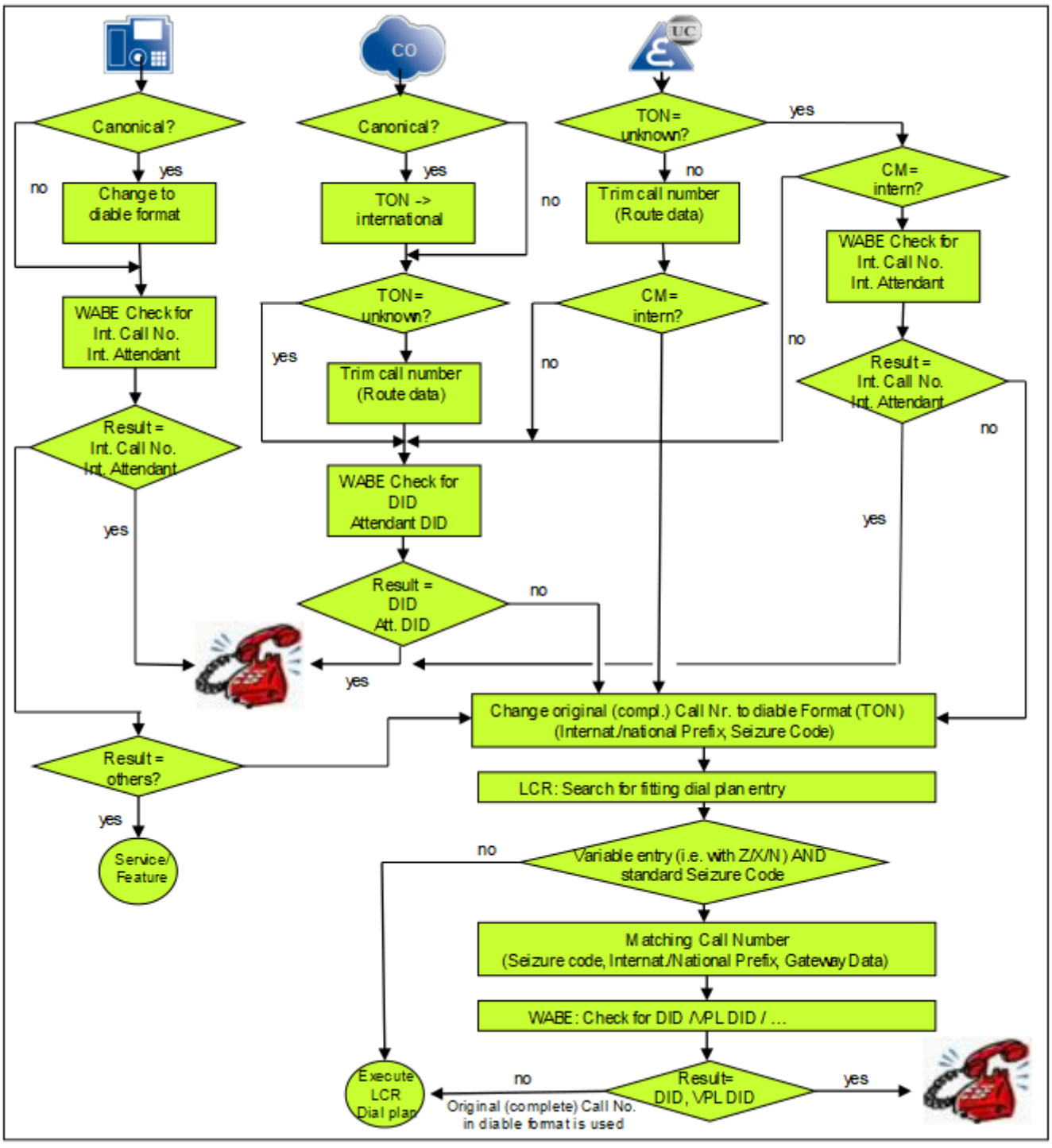
- Las extensiones, las aplicaciones, los clientes u otros sistemas de comunicación marcan números de destino en formato público (por ejemplo, 0 0034nnn)
- Condición: Código de acceso a línea urbana estándar (por ejemplo, "0") configurado

- Los números de destino se abrevian con la parte del número de ubicación (ubicación de gateway) y se evalúan mediante el plan de marcación de los números de marcación directa, se trate de llamadas internas o externas.
- Si no se encuentra ningún destino interno, el número de teléfono de marcación y sin abreviar (!) se procesa en el LCR y la llamada se transfiere a través de una línea.

Dentro de una interconexión IP, el parámetro de tabla de rutas LCR "Gateway dedicado" permite el direccionamiento directo de un nodo para un número de teléfono marcado sin pasar por la evaluación de marcación CAR.



16.3.2 Diagrama de flujo de evaluación de marcación



Explicaciones del diagrama de flujo:

Alemán	Inglés	Explicación
WABE		Evaluación de marcación
CM	CM	Classmark identifica al llamante como llamante externo o interno (de red)

Alemán	Inglés	Explicación
TONO	TONO	Type Of Number (tipo de número de llamada): Unknown, Subscriber (extensión), National o International; se utiliza con los números de destino y en los números de origen.
N.° llam. marc. directa	N.° llam. marc. directa	Número de marcación directa
TNR RNR	Int. Call No.	Número de llamada interno
Int. Attendant	VPL INT	Número de puesto de operadora para llamadas internas
VPL DID	VPL DID	Número de puesto de operadora para llamadas externas
SERVICE	SERVICE	Código de servicio
LCR	LCR	Least Cost Routing

En lo relativo a la evaluación de la marcación, los clientes de UC se comportan como extensiones que se controlan mediante CSTA.

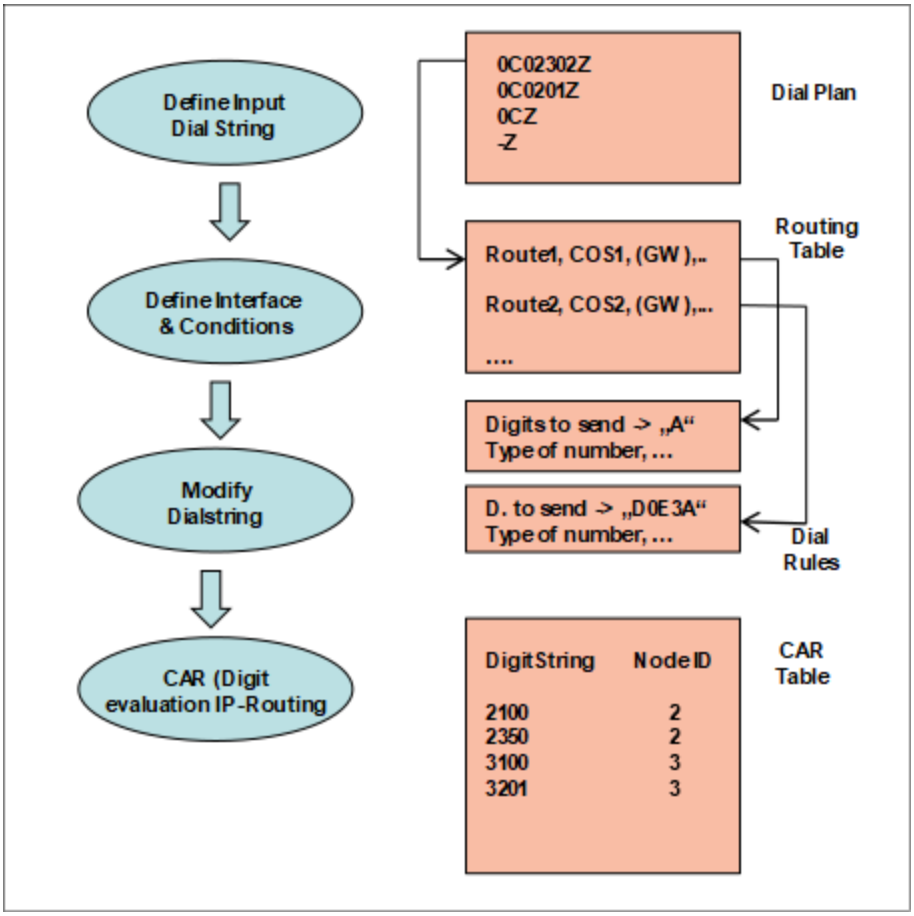
En lo relativo a la evaluación de la marcación, la UC Suite se comporta como un tronqueo SIP-Q.

16.3.3 Call Routing y LCR en la interred

En la Interconexión, el encaminamiento de llamadas (Call Routing) y LCR son muy importantes. Las llamadas se encaminan mediante un plan de marcación y reglas de marcación. Juega un papel clave el gateway dedicado.

Aspectos básicos de LCR

Entradas LCR en la configuración inicial



Si la ocupación de líneas no es correcta, las entradas de la tabla de rutas (Routing table) se procesan consecutivamente en un bucle.

Nota: La regla -z se debe eliminar de la configuración de los sistemas independientes.

En la primera puesta en servicio del sistema de comunicación, se realizan entradas predeterminadas dependientes del país en el plan de marcación LCR. Hasta el plan de marcación 35, se preasignan a líneas urbanas RDSI entradas para llamadas de emergencia, información, números de teléfono especiales, ocupación de línea urbana estándar para PSTN e ITSP, UC Suite, interconexión y para la marcación en formato internacional.

Esta área puede verse afectada por cambios de configuración (p. ej., cambio del flag **Número de ubicación**). Por ello hay que garantizar que la ocupación de línea estándar siga funcionando si se modifica el número de ubicación (importante si se marcan números de teléfono públicos).

Consejo: A partir del plan de marcación LCR 36 hay entradas para asignación libre.

16.3.3.1 Gateway dedicado

El gateway dedicado solo es relevante con la interconexión IP.

¿Por qué es necesario un gateway dedicado?

¿Cómo se pueden configurar de forma permanente destinos a través de la configuración?

Casos de aplicación de un gateway dedicado

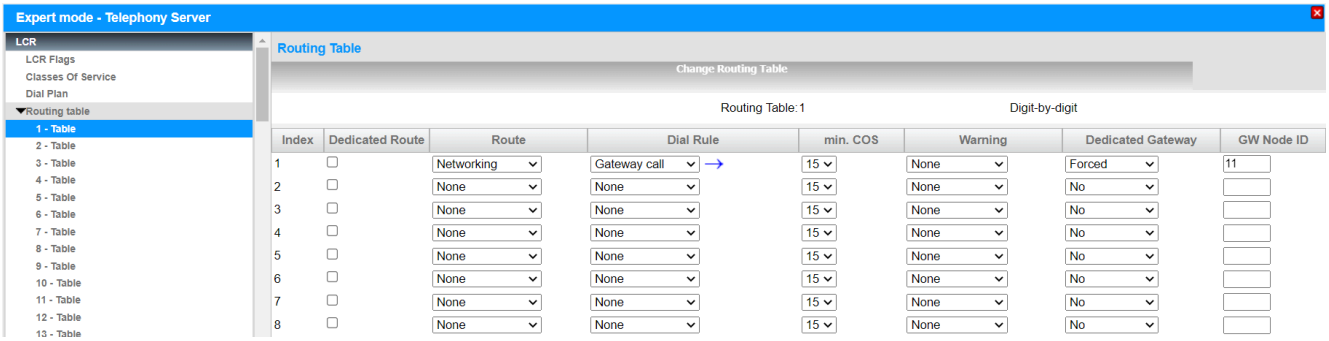
El gateway dedicado en WBM

Se pueden configurar los siguientes valores:

- La tabla CAR de cada sistema de comunicación incluye números de teléfono a nivel de red de todos los demás nodos y se actualiza (sobreescribe) automáticamente y de forma cíclica en las actualizaciones. Por ello las tablas CAR no son adecuadas para usar de forma permanente entradas añadidas de forma manual.
- Solo se registran números de teléfono válidos a nivel de red, es decir, no se admite el encaminamiento individual a nivel de nodo (por ejemplo, "0" para el nodo de gateway correspondiente)
- Con el uso de un direccionamiento directo en el LCR
- El gateway dedicado direcciona directamente el nodo de destino mediante el ID de nodo (dirección IP)
- Si se utiliza el gateway dedicado se omiten las tablas CAR (véase la imagen anterior).

Direccionamiento directo

- de gateways TDM, para ocupar líneas urbanas ("0CZ")
- de gateways TDM, para implementar breakouts mediante códigos independientes
- de nodos internos de la red a los que se va a acceder mediante números de teléfono públicos
- de gateways TDM que tienen asignadas las extensiones de una interconexión multigateway (con un OpenScape Business S) (por ejemplo, la extensión 1 pertenece por definición al gateway 1 y la extensión 2, al gateway 2)
- de gateways y llamadas cuyo origen NO se pueda asociar a un determinado gateway en una configuración multigateway (por ejemplo, el grupo de fax de un Contact Center de UC)



No	Los números de teléfono se evalúan con las tablas CAR (no se requiere ningún **ID de nodo de GW**)
Forzado	Se encamina de forma directa al gateway correspondiente (ID de nodo de GW = N)
Varias ubicaciones (Multi Location)	Solo con configuraciones multigateway: En función de la configuración multigateway de las extensiones OpenScape Business S, el sistema de comunicación identifica la asignación con su gateway y puede encaminar la llamada saliente de forma selectiva al gateway correspondiente. En la configuración **Varias ubicaciones** solo se utiliza el ID de nodo de GW si no se puede identificar ningún gateway mediante la asignación de las extensiones (estándar).

16.3.4 Escenarios: Evaluación de marcación y Call Routing (encaminamiento de llamadas)

Mediante escenarios se describen interdependencias y los parámetros de configuración necesarios para explicar los procesos del sistema de comunicación. Los escenarios representados pueden basarse el uno en el otro, según el caso de aplicación específico.

Sistema individual

Sistema interconectado como sistema secundario (sin línea urbana)

Interred con multigateway

1) La extensión A llama a la extensión B con el número de teléfono interno
2) La extensión A llama a la extensión B mediante un número de teléfono público
3) La extensión A llama a una extensión externa a través de la línea urbana
4) La línea urbana RDSI llama a la extensión A
5) Configuraciones especiales y efectos:

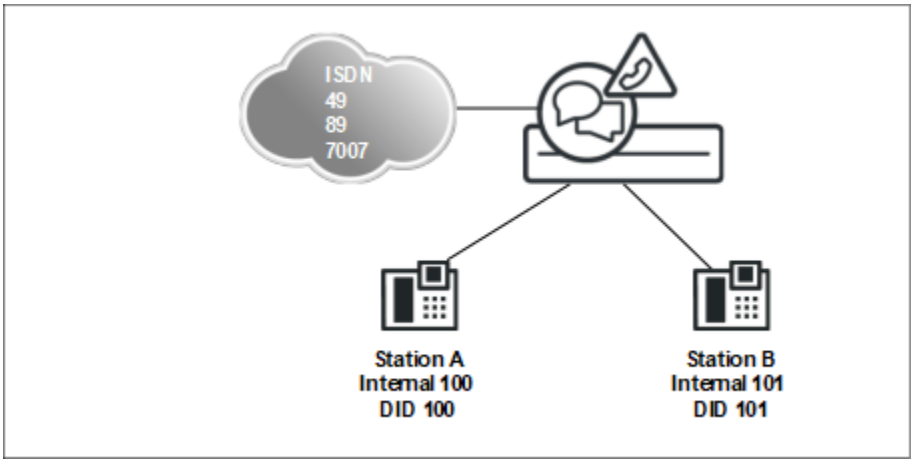
2 rutas urbanas

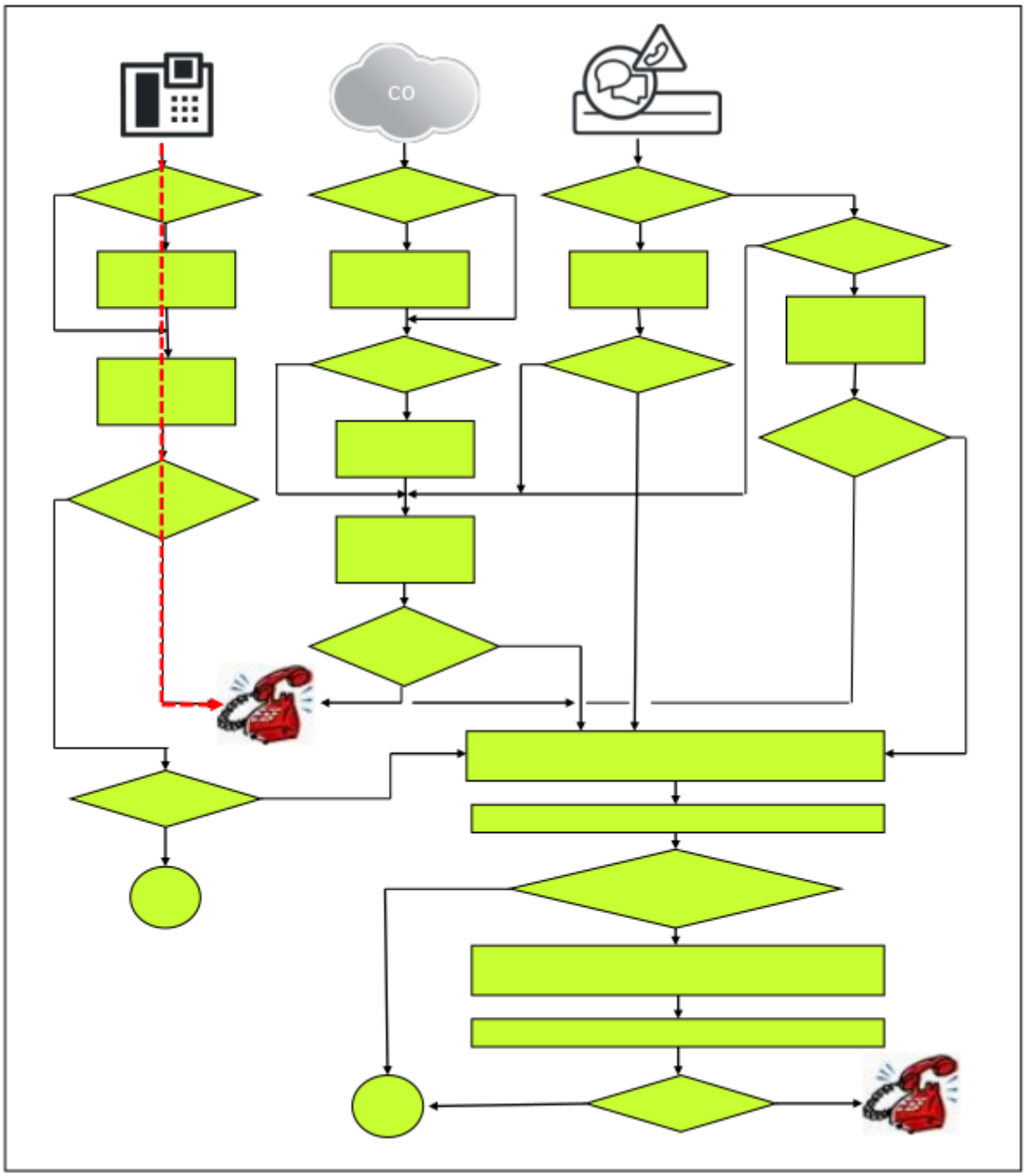
1) La extensión A llama a la extensión C con un número interno
2) La extensión A llama a la extensión C con el número de teléfono público en la interred
3) La línea urbana RDSI llama a la extensión C

1) El gateway 1 de la línea urbana RDSI llama a la extensión D
2) La extensión D llama a una extensión externa mediante la línea urbana

16.3.4.1 La extensión A llama a la extensión B con el número de teléfono interno

Configuración de los dos números de teléfono internos



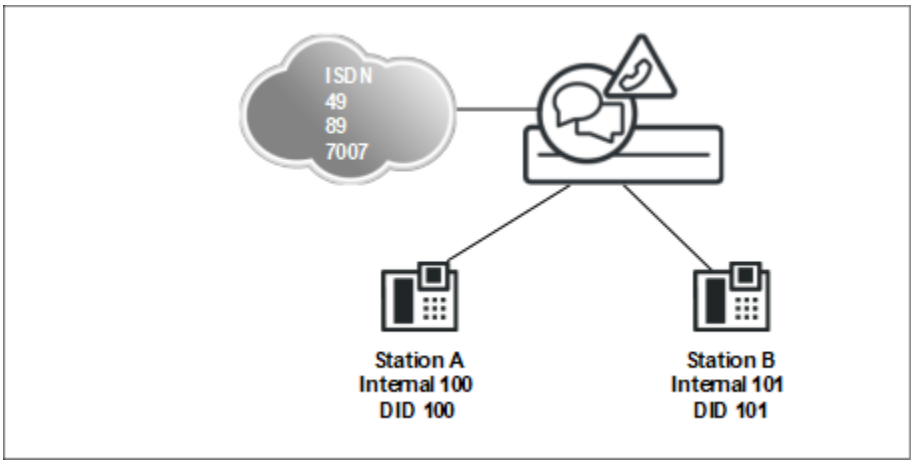


	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

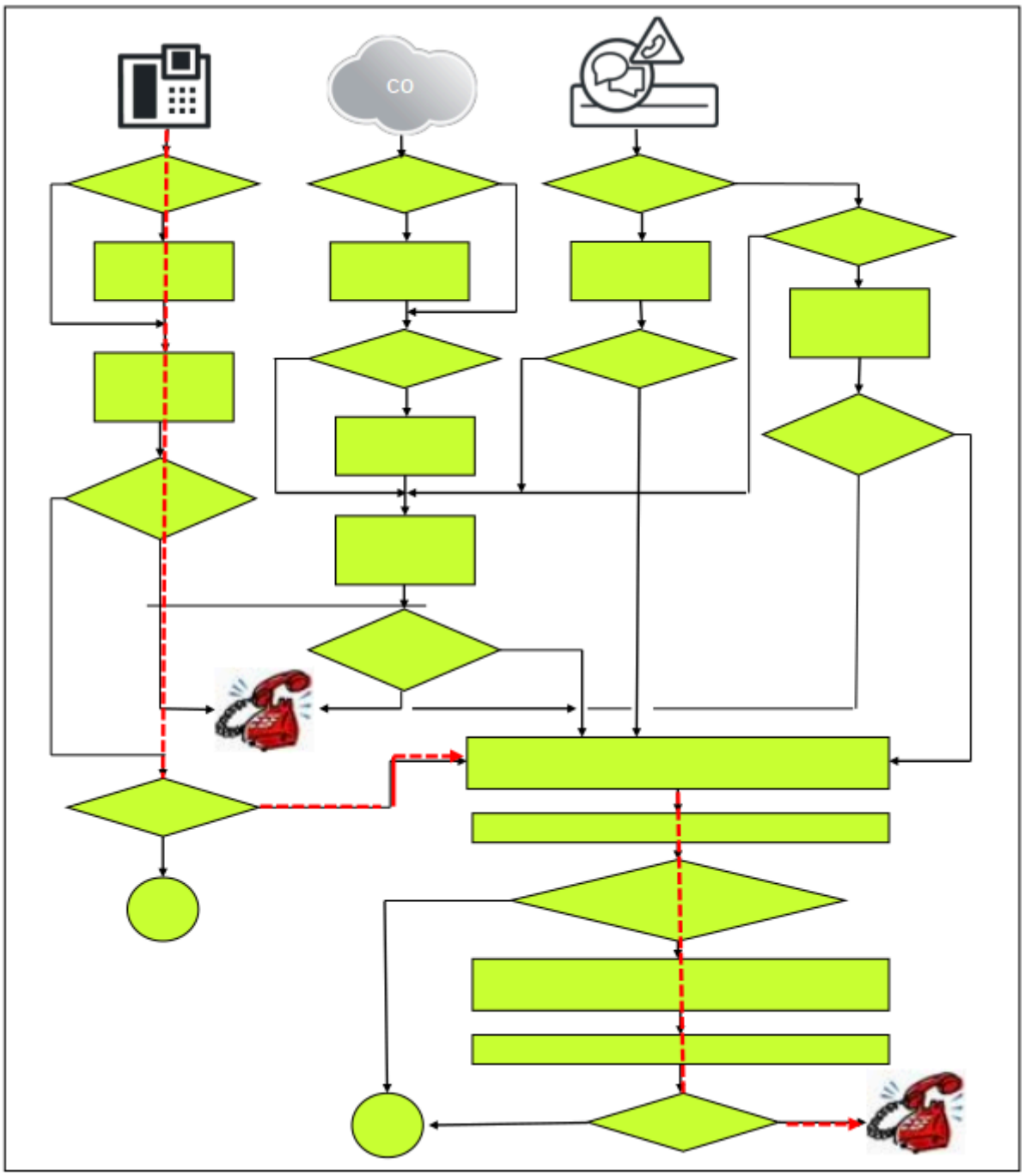
16.3.4.2 La extensión A llama a la extensión B mediante un número de teléfono público

Configuración

Interdependencias del "número de ubicación" (Gateway Location)

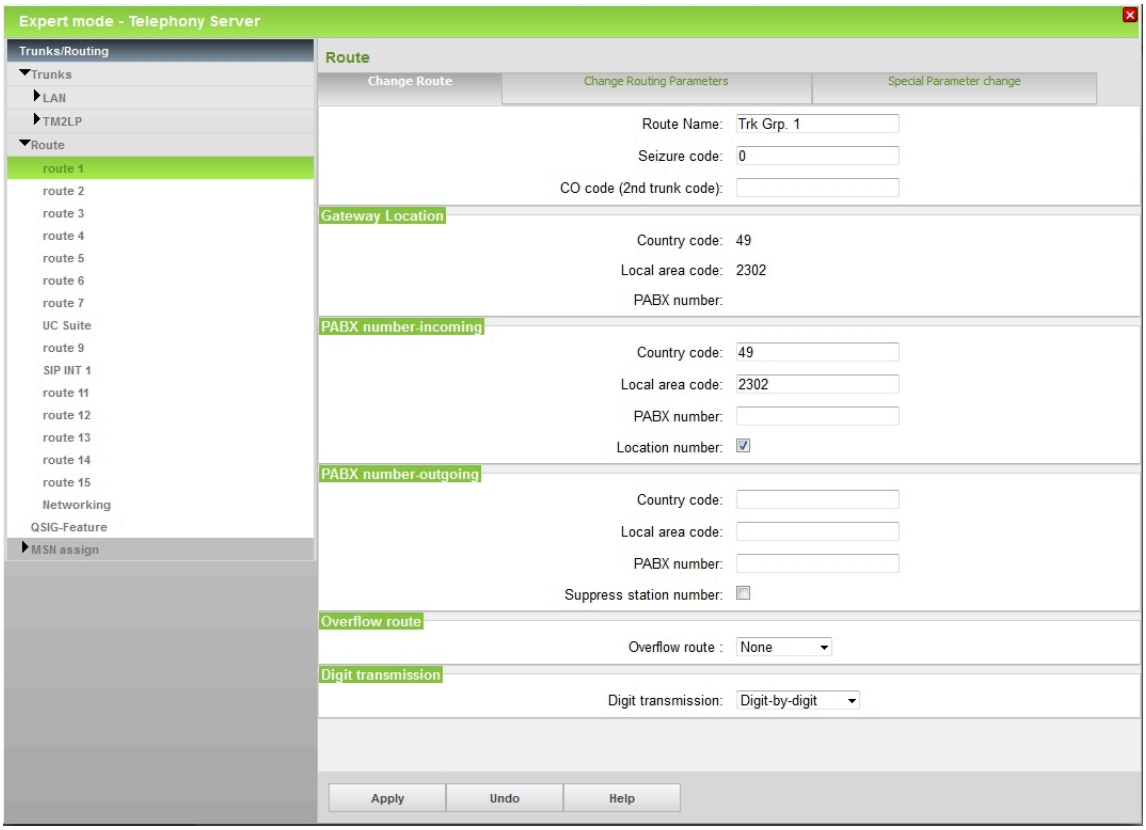


La llamada se entrega de forma interna en el sistema, ya que el número de destino es una extensión de marcación directa del sistema.



	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

Después de descomponer el número de destino con el valor de Gateway Location, el número de teléfono obtenido se usa para buscar un destino en el plan de numeración de marcación directa (DID).

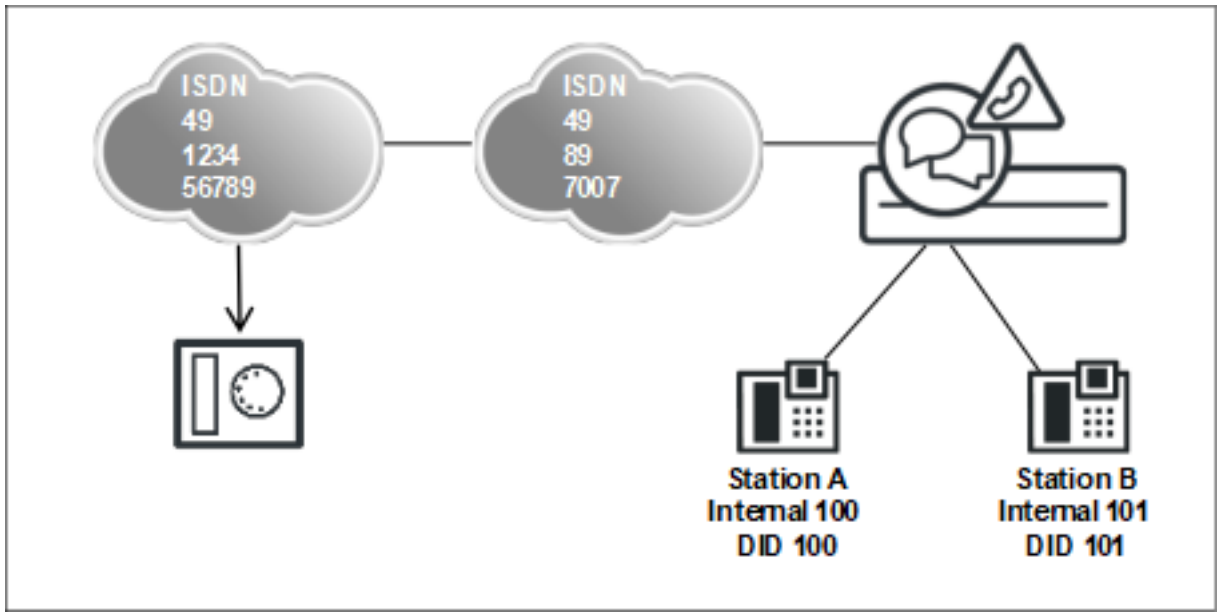


Durante la marcación el número de ubicación (Gateway Location) se evalúa mediante el número de teléfono público. Si el número de teléfono marcado coincide con este número en las instalaciones relevantes se evalúa la tabla de marcación directa y, si hay coincidencia, se llama al destino interno correspondiente (no se ocupa ninguna línea). Al activar el flag Número de ubicación, se aplican inmediatamente los datos de ruta correspondientes (número PABX entrante) para los datos de ubicación y no es necesario cambiarlos en los escenarios estándar.

Por ello en las tablas de marcación directa solo se pueden introducir números de teléfono válidos asignados al sistema, ya que de lo contrario pueden darse enmascaramientos con los números de teléfono de la red pública. Por ejemplo, en algunos casos se podría llamar a un número interno identificado por un DID no válido aunque se pretendiera hacer una llamada a través de una línea a un destino externo.

Los cambios del flag "Número de ubicación" pueden influir en las entradas LCR estándar predefinidas. Hay que comprobar que la ocupación de línea urbana estándar siga funcionando al modificar el número de ubicación. Es importante al marcar con números de teléfono públicos.

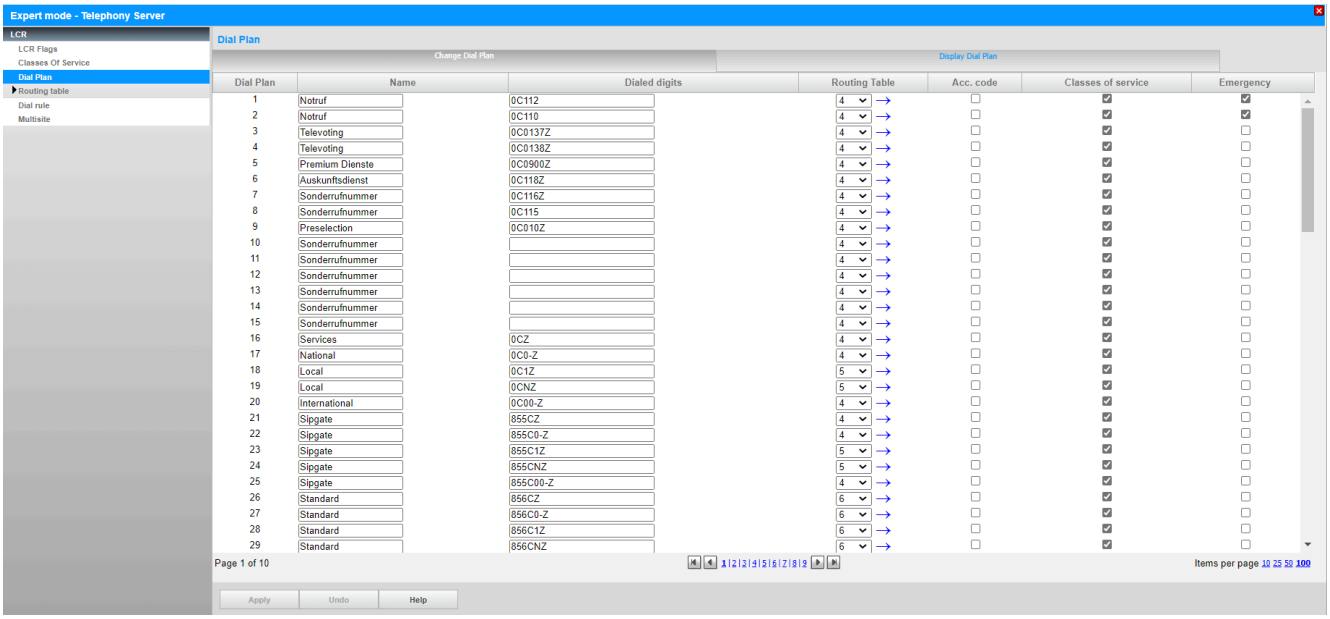
16.3.4.3 La extensión A llama a una extensión externa a través de la línea urbana



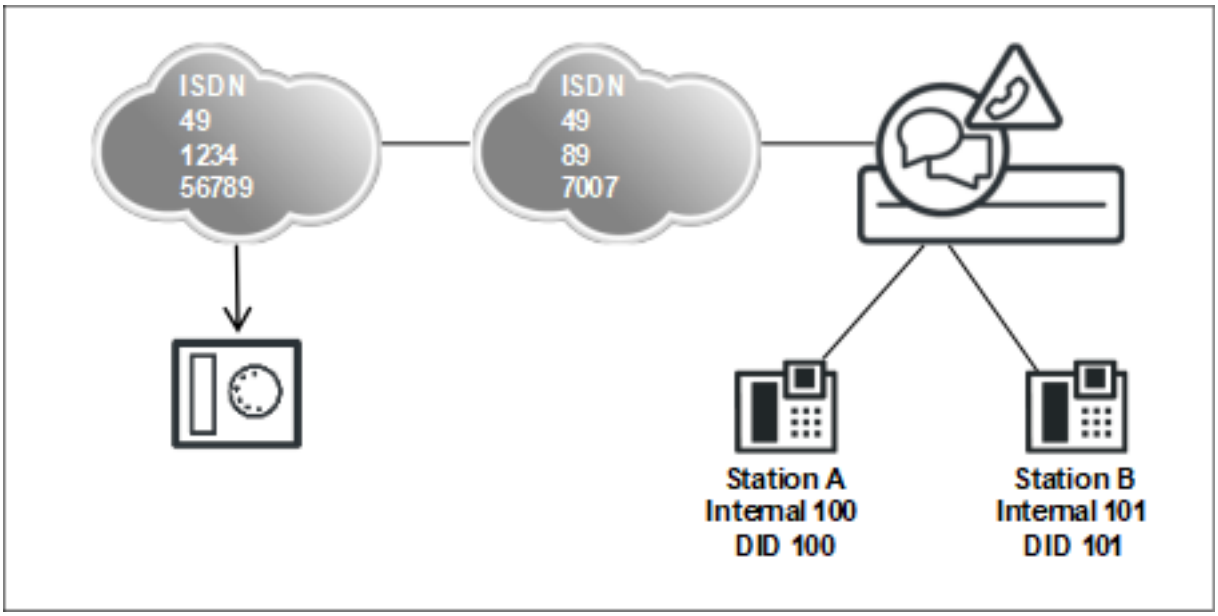
La llamada se encamina por LCR, ya que el destino no está en el sistema de comunicación propio.

Además de los datos del escenario anterior ("La extensión A llama a la extensión B a través del número de teléfono público"), en el LCR debe haber disponible una entrada de plan de marcación adecuada para ocupar la línea urbana (por ejemplo, "0CZ").

La tabla de rutas LCR y el plan de marcación deben estar configurados adecuadamente.

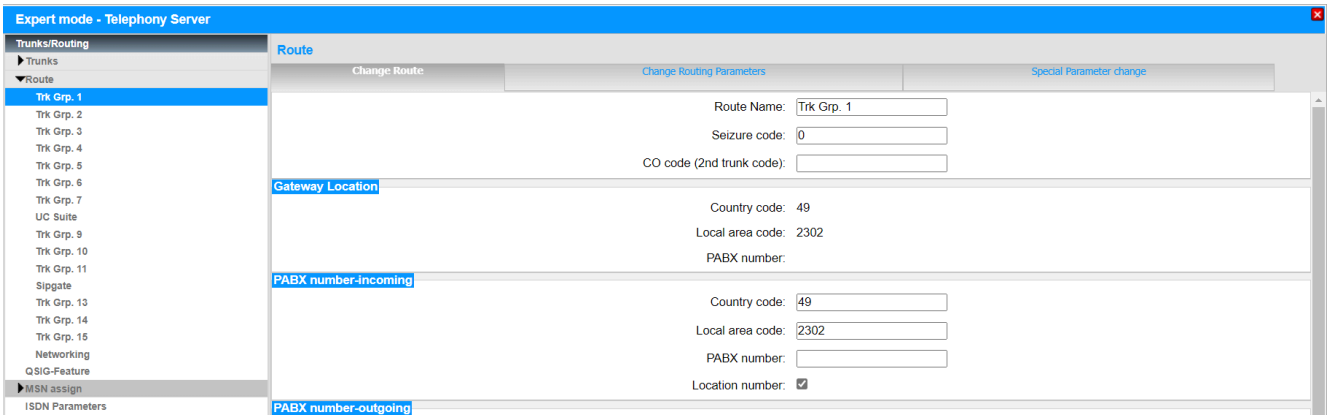


16.3.4.4 La línea urbana RDSI llama a la extensión A



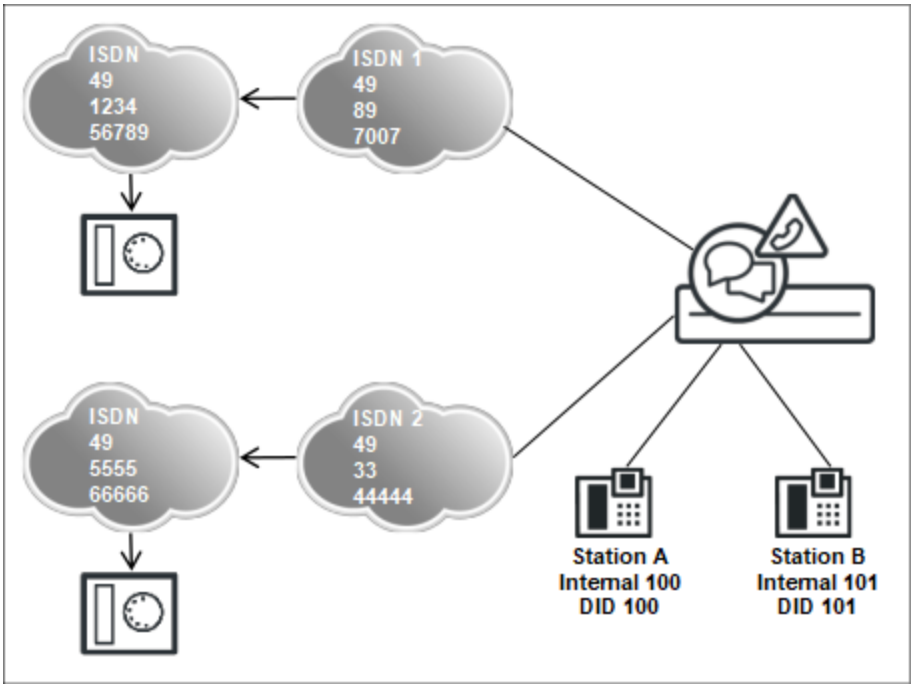
Si se recibe una llamada a través del tronqueo RDSI, la ruta se descompone del número de destino con los datos de configuración del número de teléfono del sistema entrante (PABX number incoming). Con el resto del número de destino (número de marcación directa) se busca un destino en el plan de marcación directa.

Los parámetros de la ubicación de gateway o del flag **Número emplazamiento** no son determinantes en este escenario.

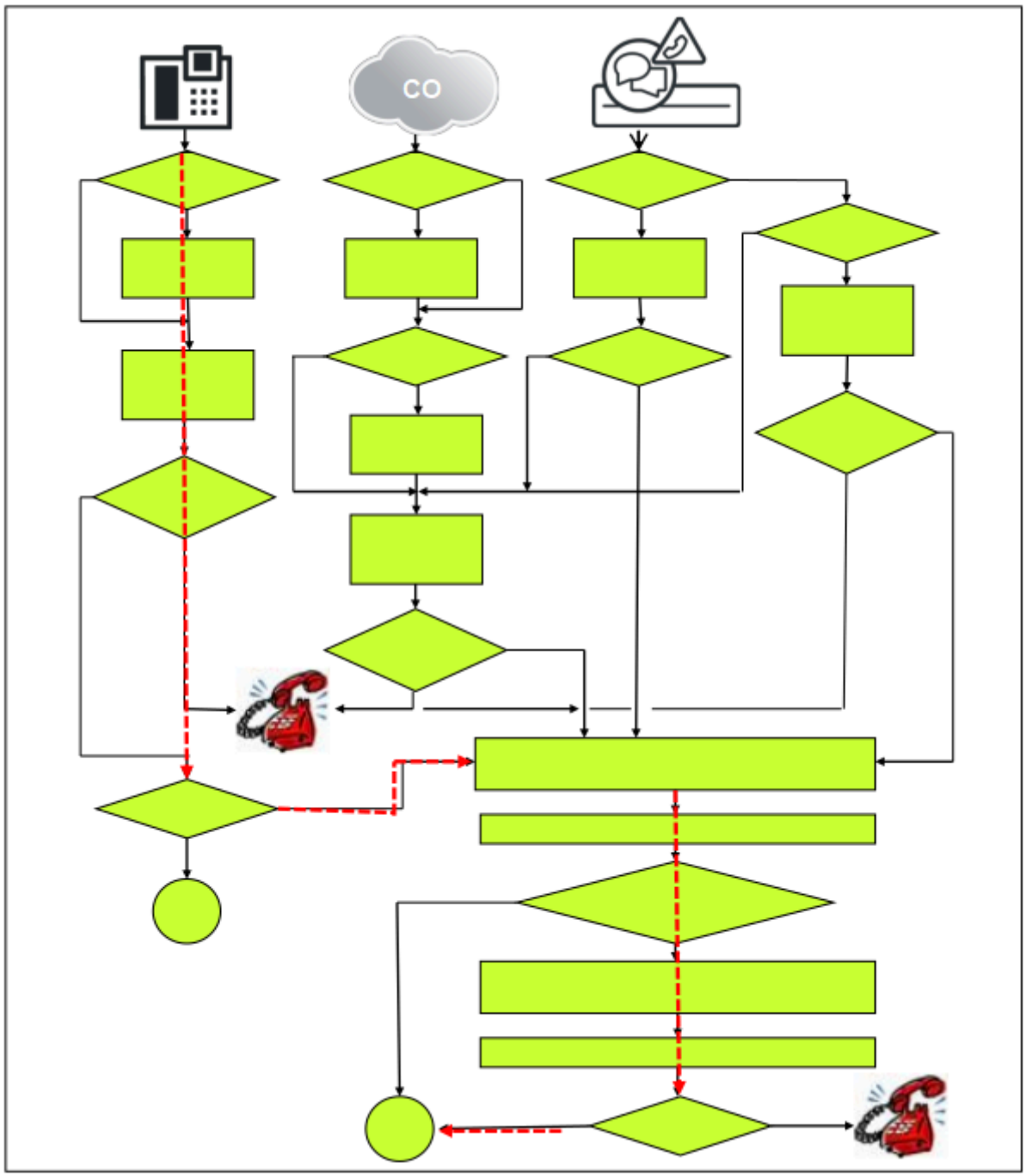


16.3.4.5 Configuraciones especiales

Configuraciones especiales y sus efectos: 2 rutas de línea urbana



La extensión A llama a la una extensión externa con la conexión de línea urbana 1 o 2



Ejemplo:

- Un cliente quiere utilizar una conexión estándar RDSI 1. Esta se configura como número de ubicación.
- Además, se utiliza una segunda conexión RDSI 2 para aplicaciones especiales.

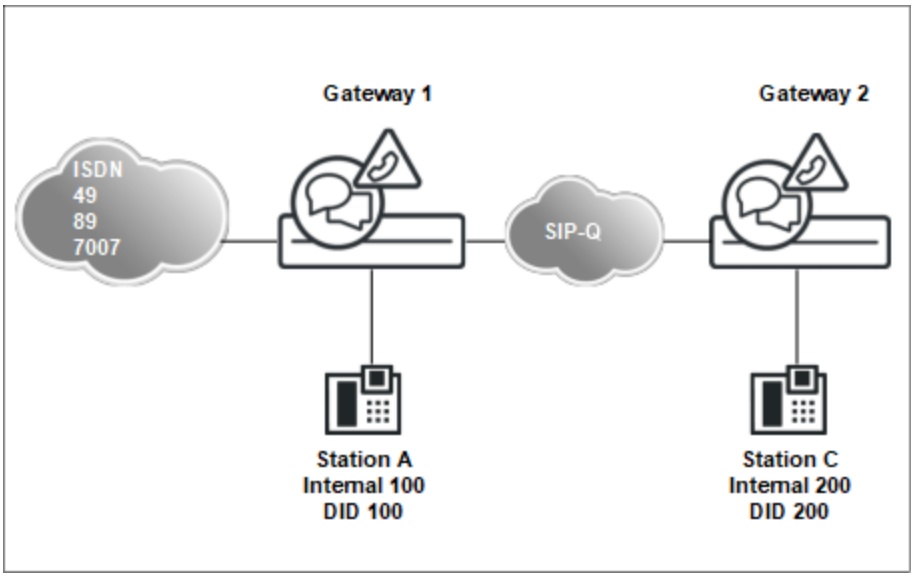
Observaciones o restricciones:

- Solo se admite UNA ruta de línea urbana (RDSI 1 = Ubicación del sistema) al completo, es decir, no se puede hacer una configuración multicliente (central compartida) con conexiones de línea urbana equivalentes.
- La conexión de línea urbana adicional RDSI 2 se puede utilizar para Basic Call (entrante/saliente).

- Es posible que en escenarios de conmutación complejos no se pueda garantizar siempre una representación correcta de los números de teléfono.
- Al integrar aplicaciones solo se admite el número de teléfono de ubicación, como sucede al marcar destinos internos con número de teléfono público.
- La configuración respecto a la configuración de rutas y al LCR puede derivarse de los ejemplos anteriores.

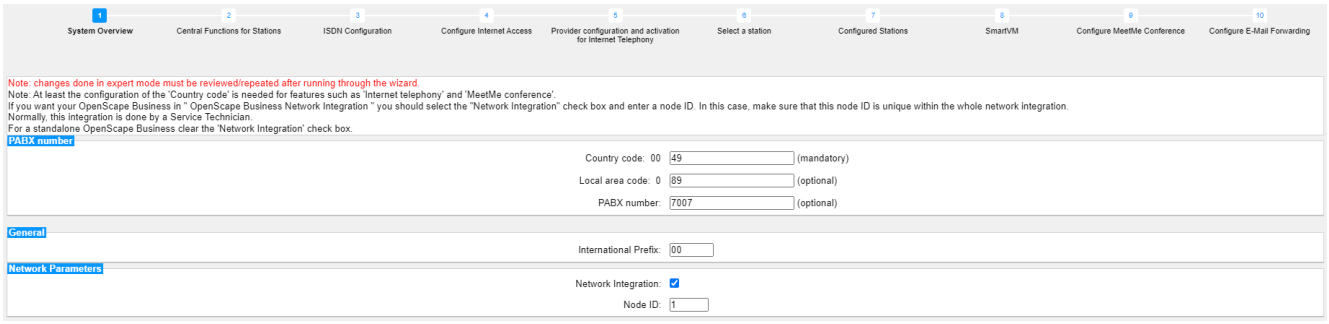
16.3.4.6 La extensión A llama a la extensión C con un número interno

Sistema de comunicación interconectado como sistema secundario (sin línea urbana)



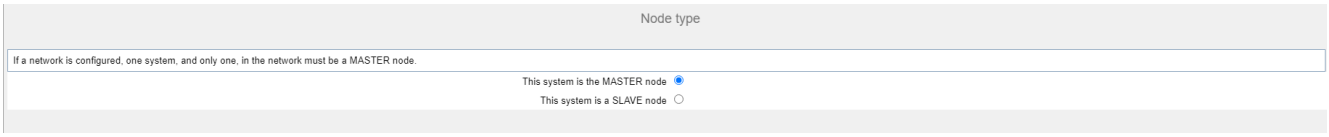
Requisitos de los sistemas independientes antes de la interconexión:

- Los dos sistemas de comunicación tienen direcciones IP únicas y están integrados en la red IP del cliente.
- Los dos sistemas de comunicación se pueden administrar mediante Gestión basada en Web (WBM) en la red de clientes.
- En la instalación básica hay que asignar un ID de nodo exclusivo para la interconexión por cada sistema de comunicación (p. ej. Sistema 1 = ID de nodo 1 y Sistema 2 = ID de nodo 2).
- Definir la numeración en la instalación básica de los sistemas 1 y 2: La numeración de los sistemas autónomos debe tener en cuenta la numeración cerrada de la red futura.
- Este ejemplo supone el uso de una numeración cerrada (¡obligatorio si se usa la UC Suite), confirmación mediante el asistente Redes. Con una numeración abierta (posible con UC Smart) no se utiliza el asistente Redes. Con integración de OpenScape Voice y OpenScape 4000, tampoco.



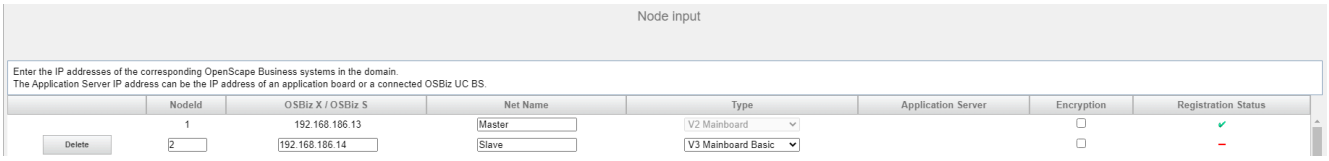
Inicie el asistente Redes en el Sistema 1. Este sistema (este nodo) está declarado como maestro. El maestro tiene diferentes funciones centrales en la interred (p. ej., administración, administración de licencias en el registro central de licencias, CSP a nivel de red).

Si en la interred hay un OpenScape Business S, se recomienda hacerlo maestro (ancho de banda, rendimiento).



Las direcciones IP se registran por nodo para que los sistemas se puedan encontrar después de la administración de forma independiente. En **Tipo** se introducen los sistemas OpenScape Business.

También hay que ejecutar este cuadro de diálogo para el nodo 2 (esclavo).



Una vez terminada correctamente la configuración, los dos sistemas (nodos) sincronizan sus números de teléfono y registran los números de teléfono del otro nodo en la tabla CAR.

Con la creación de las tablas CAR se puede implementar telefonía con números internos a nivel de red. También se inicia la UC Suite a nivel de red. En los demás escenarios se detallan otros pasos para la puesta en servicio íntegra de la red.

Las entradas CAR se controlan mediante **Modo Experto** > **Gateway voz** > **Redes** > **Encaminamiento**.

Puede ver una visión general de la sincronización automática de la interred en la Gestión basada en Web (WBM) (estado de sincronización).

Ahora se pueden administrar más nodos de red con acceso directo en la opción de menú **Redes**, en la barra de navegación.

16.3.4.7 La extensión A llama a la extensión C con el número de teléfono público en la interred

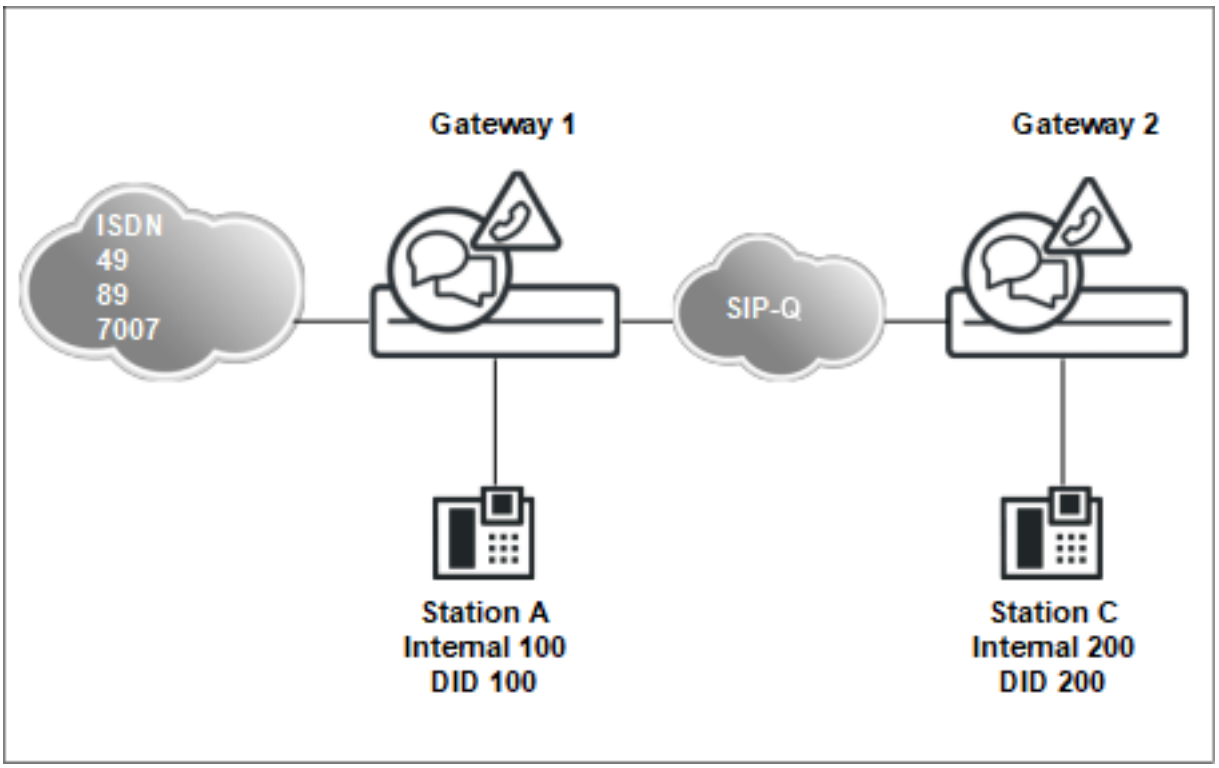
Sistema de comunicación interconectado como sistema secundario

Configuración del nodo 1, configuración en LCR mediante gateway dedicado

Configuración del nodo 2, configuración de la ruta "Redes"

Configuración del nodo 2, configuración del número de ubicación en la "ruta urbana dummy"

Configuración del nodo, configuración en LCR mediante gateway dedicado



Peculiaridades de este escenario:

- El sistema 1 determina que el número de destino no pertenece al sistema propio. De esta forma, la búsqueda subsiguiente se realiza en el LCR.
  El gateway dedicado en el LCR del sistema 1 debe utilizarse para el direccionamiento directo del ID de nodo del sistema 2. El número de destino no es un número interno de la red (de lo contrario estaría en la tabla CAR), sino un número de teléfono público, que la extensión puede marcar en tres longitudes diferentes:

  Largo = 00049897007nnn

  Medio = 00897007nnn

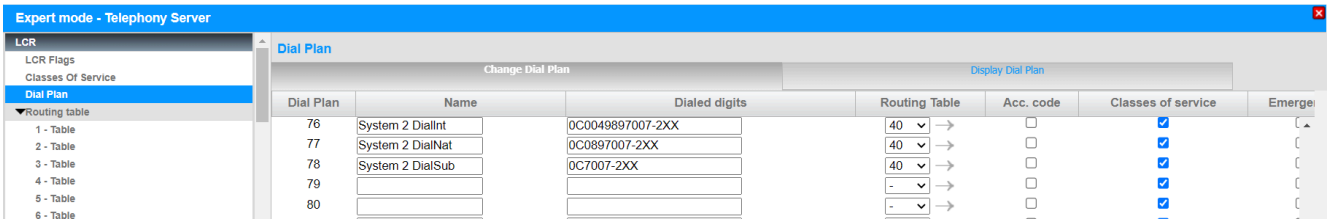
  Corto = 07007nnn

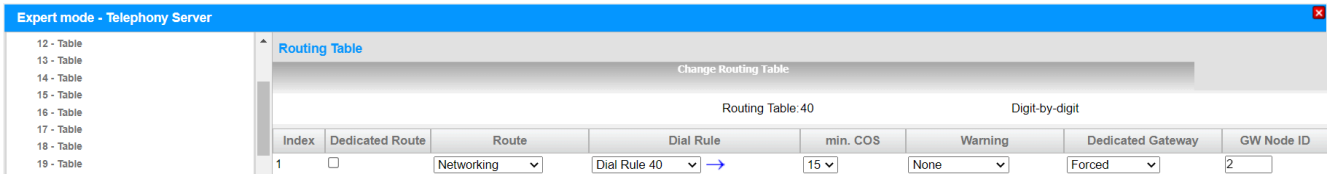
  El ejemplo parte del supuesto de que todos los números de marcación directa son extensiones del sistema 2.

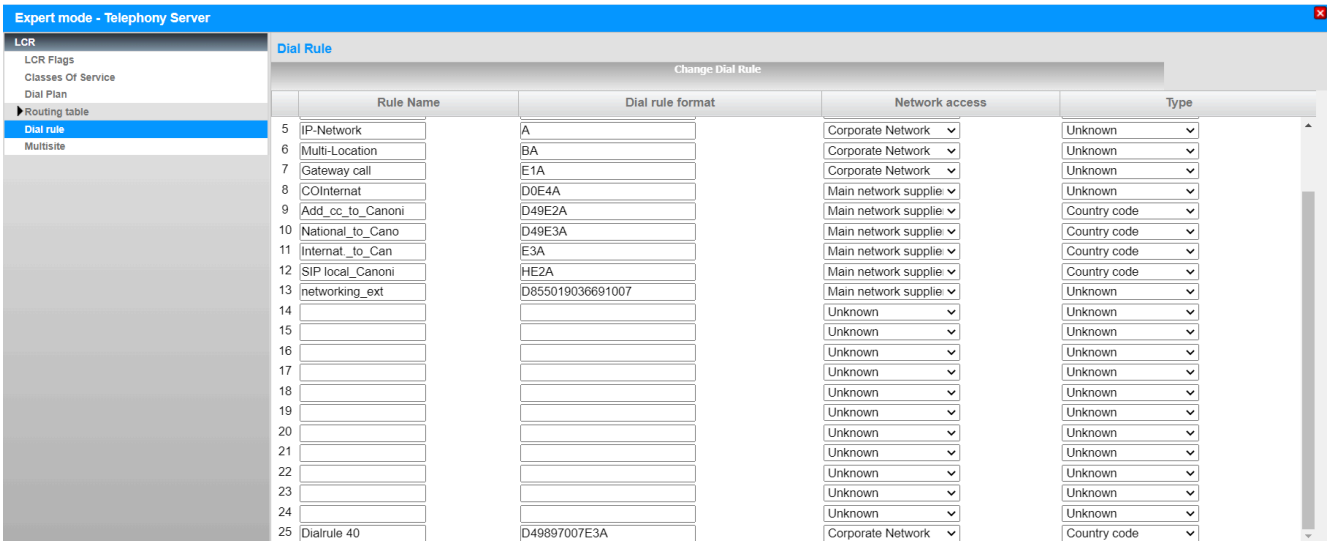
  Nota: Los registros de plan de marcación se deben configurar de forma que TODOS los números de teléfono afectados también pertenezcan al nodo secundario (interred). Según las peculiaridades del plan de numeración,

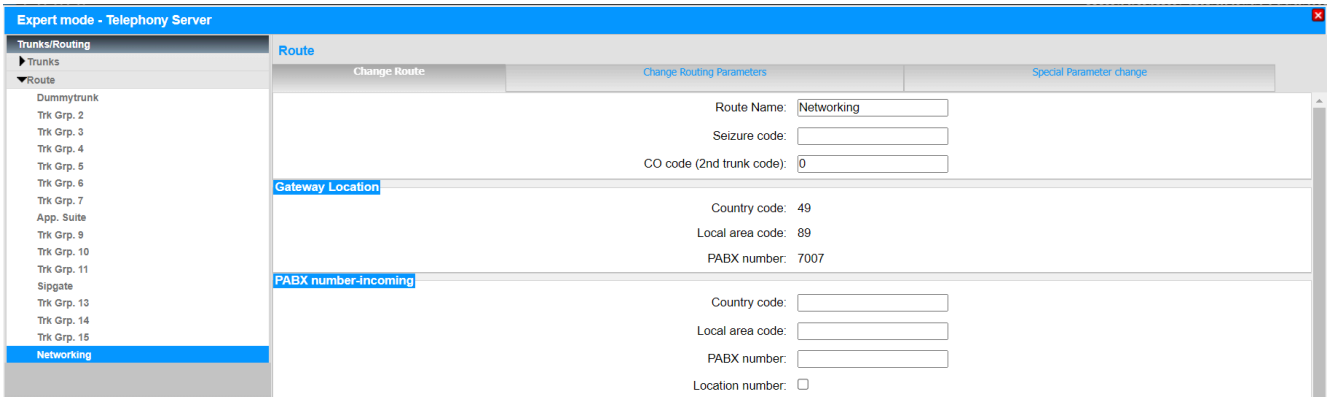
esto puede hacer necesario un gran número de registros (por ejemplo, si la conexión de línea urbana está compartida o hay una configuración de MSN).

- En el nodo 2 se registra un número de ubicación mediante una "ruta urbana dummy" con los datos de ubicación del nodo 1 (gateway), para que en caso de marcación pública se pueda descomponer el número de destino antes de buscar un destino interno en el nodo 2.

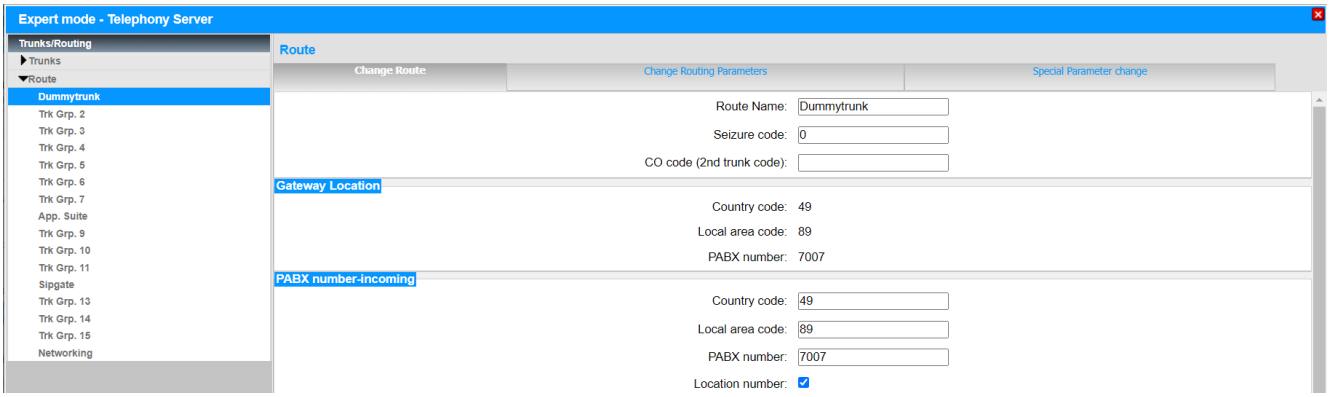








El tipo de ruta **PABX** debe introducirse en la pestaña **Editar parámetros de ruta**.



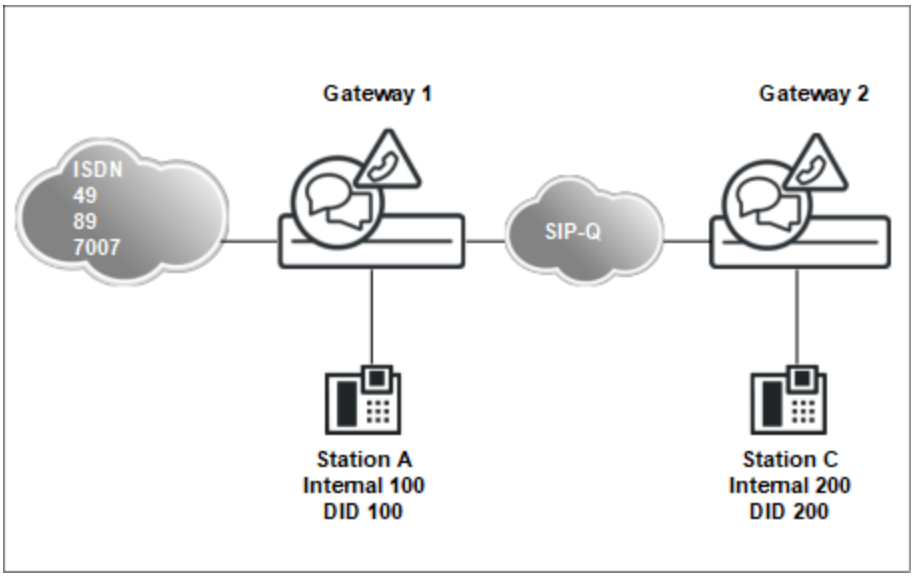
El tipo de ruta **CO** debe introducirse en la pestaña **Editar parámetros de ruta**.

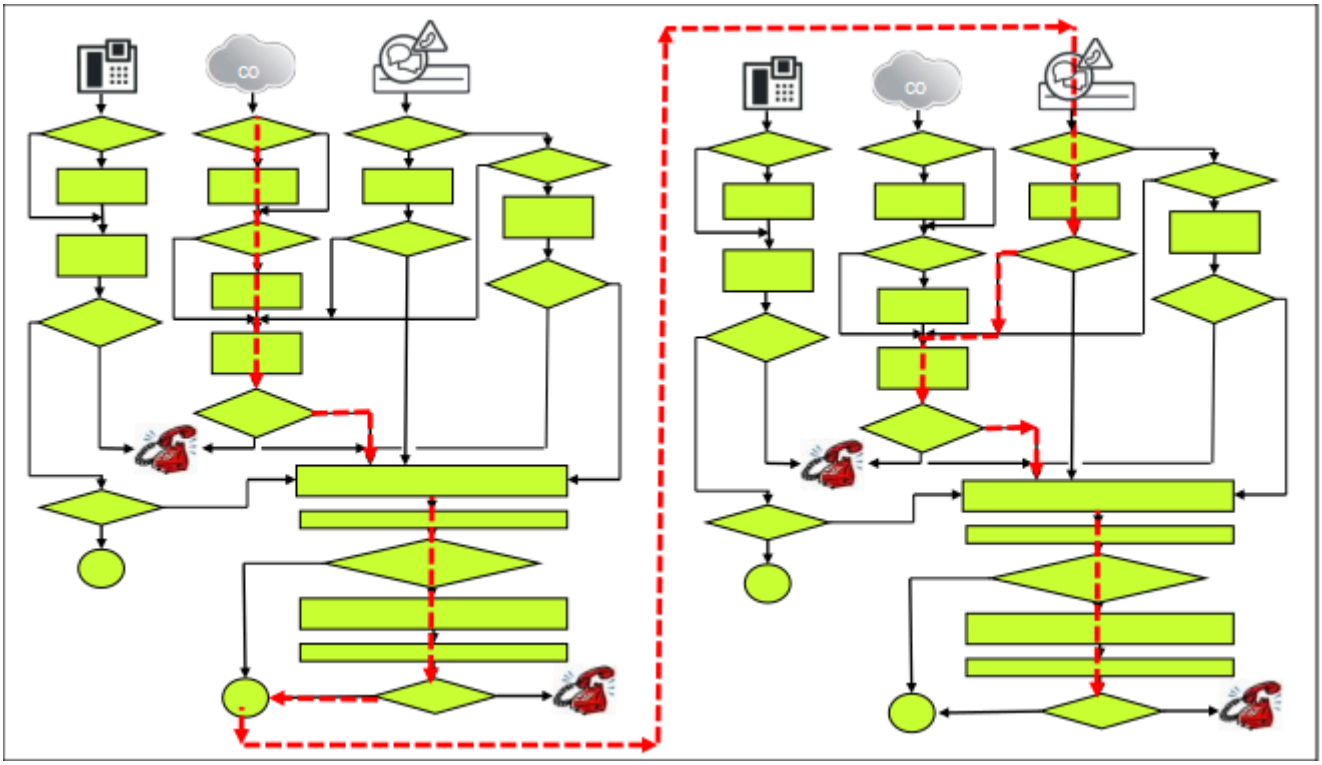
En el nodo 2 se encaminan al nodo 1 todos los números de teléfono públicos que no pertenecen al nodo propio (marcación estándar p. ej. 0CZ)

16.3.4.8 La línea urbana RDSI llama a la extensión C

Sistema interconectado como sistema secundario

Peculiaridades de esta configuración





Ejemplo: Llamada entrante con número de destino con TON = Extensión

- Hay que configurar el nodo 1 como en el escenario anterior.

  En ambos casos, el direccionamiento del nodo 2 se realiza con el número de teléfono público y es independiente de si el origen de la conexión está en el nodo 1 (extensión del sistema 1) o en la red pública.

  Consejo: Los registros de plan de marcación se deben configurar de forma que TODOS los números de teléfono afectados también pertenezcan al nodo secundario (interred). Según las peculiaridades del plan de numeración, esto puede hacer necesario un gran número de registros (por ejemplo, si la conexión de línea urbana está compartida o hay una configuración de MSN).

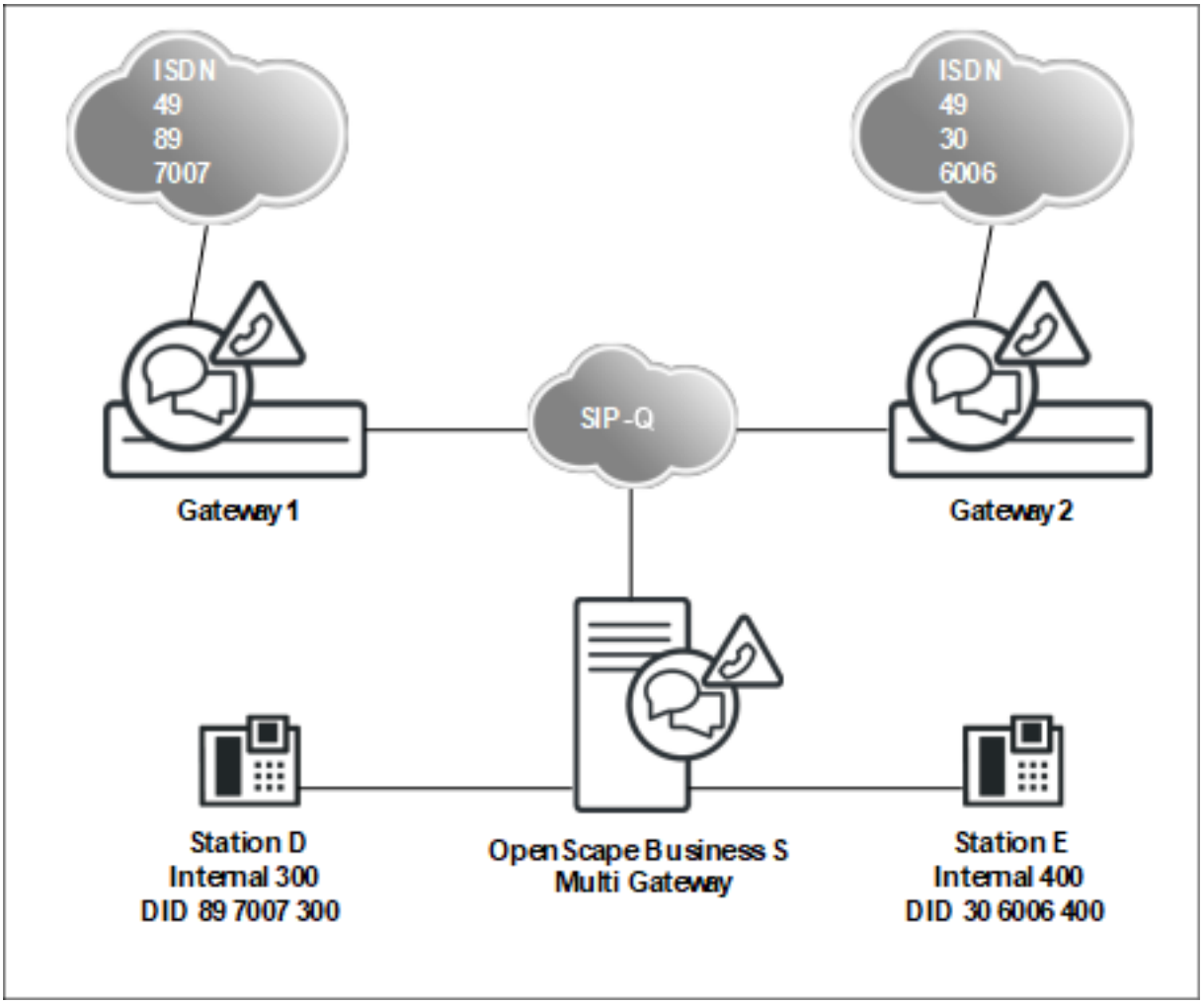
- También hay que configurar el nodo 2 como se describe en el escenario anterior.

16.3.4.9 El gateway 1 de línea urbana RDSI llama a la extensión D

Configuración de un sistema interconectado en una configuración multigateway

Configuración

Configuración del multigateway, OpenScape Business S

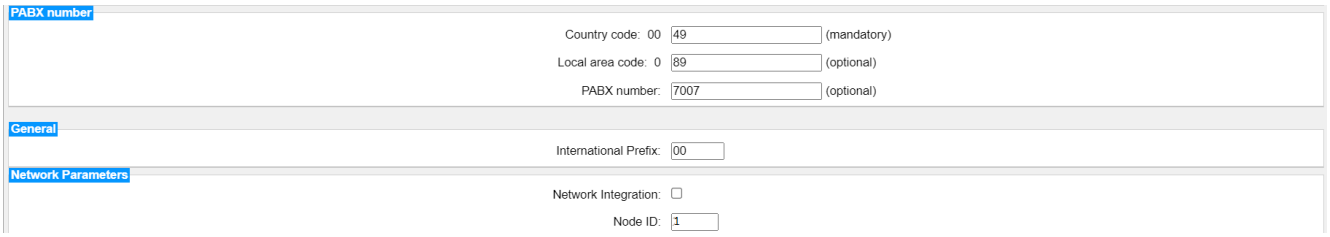


Ejemplo: Llamada entrante con número de destino con TON = extensión

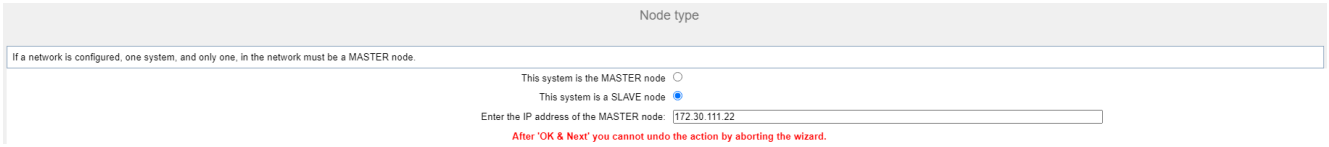
Peculiaridades de este escenario:

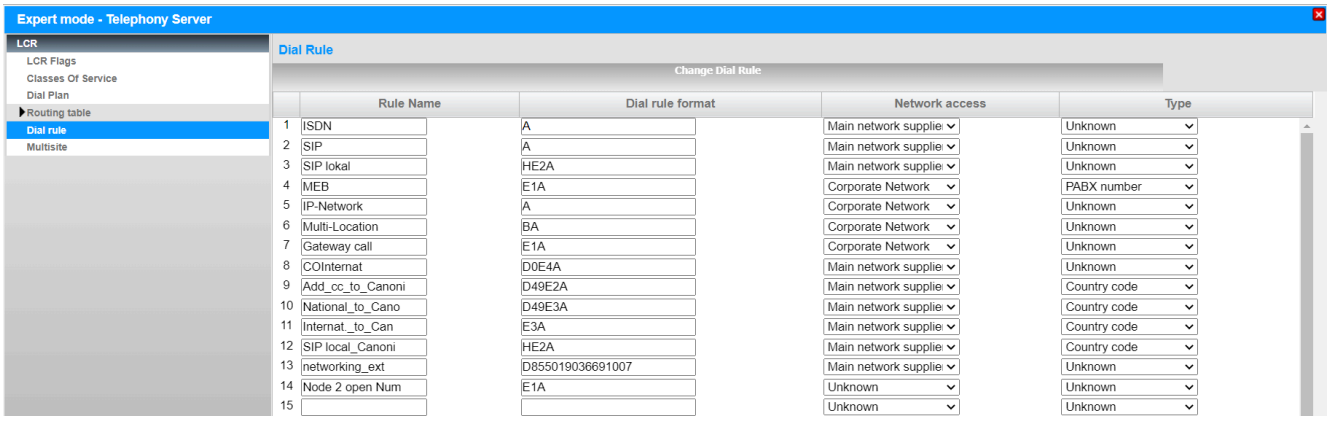
- En principio, el gateway 1 se configura como en el escenario anterior (gateway 1), es decir, primero instalación básica y luego ejecutar el asistente Redes. Diferencia esencial: Los gateways se configuran como esclavos y el OpenScape Business S, como maestro (rendimiento, ancho de banda, registro de licencia).
- En este ejemplo, solo se señalan las diferencias esenciales respecto al escenario anterior.

Instalación básica del gateway 1



Asistente Redes para el gateway 1





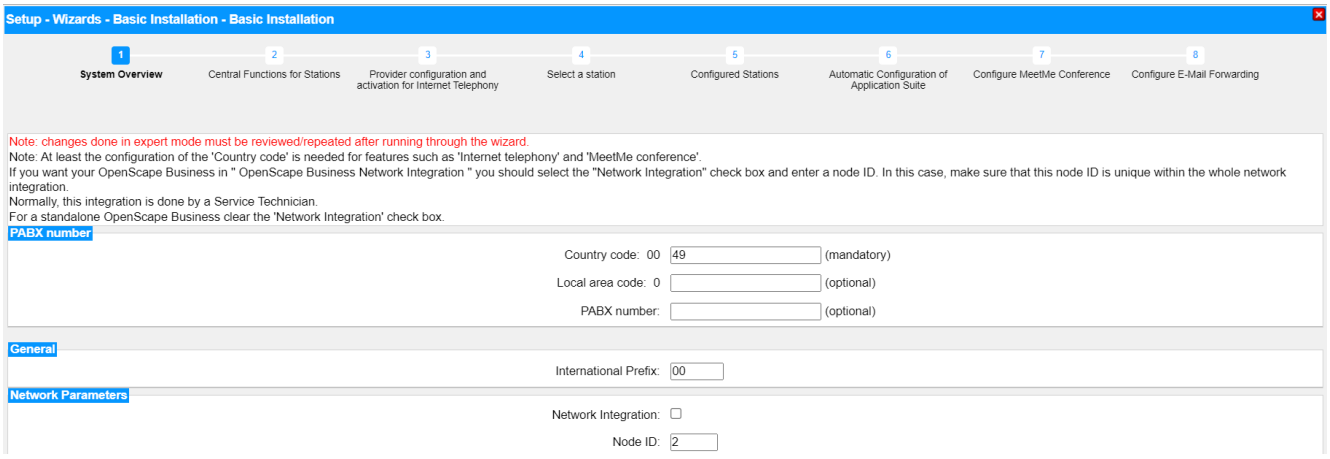
En OpenScape Business S el número de destino ya está registrado como número de marcación directa en el "formato nacional".

"BA" (Broaden all) solo es relevante en el gateway.

"BA" solo es necesario si "se ha recibido el número de destino original TON unknown, es decir, si solo contiene el "DID breve" = parte de la extensión.

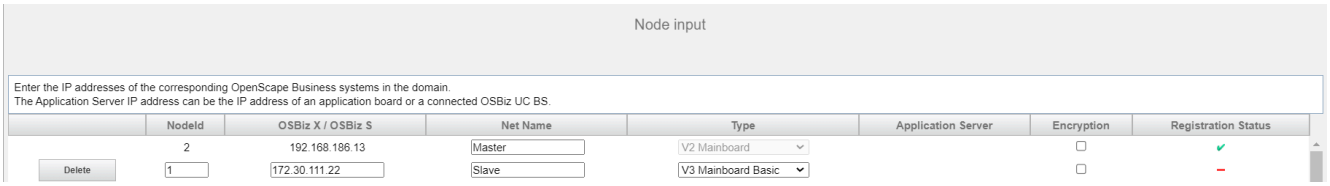
- Se realiza primero la instalación básica y luego se ejecuta el asistente Redes.
- Por cada extensión de OpenScape Business S se configura lo siguiente:
  - Número interno en formato abreviado (p. ej., 300)
  - Número de marcación directa en formato nacional (p. ej., 89 7007 300)
  - ID de nodo de gateway correspondiente

Instalación básica de OpenScape Business S, multigateway



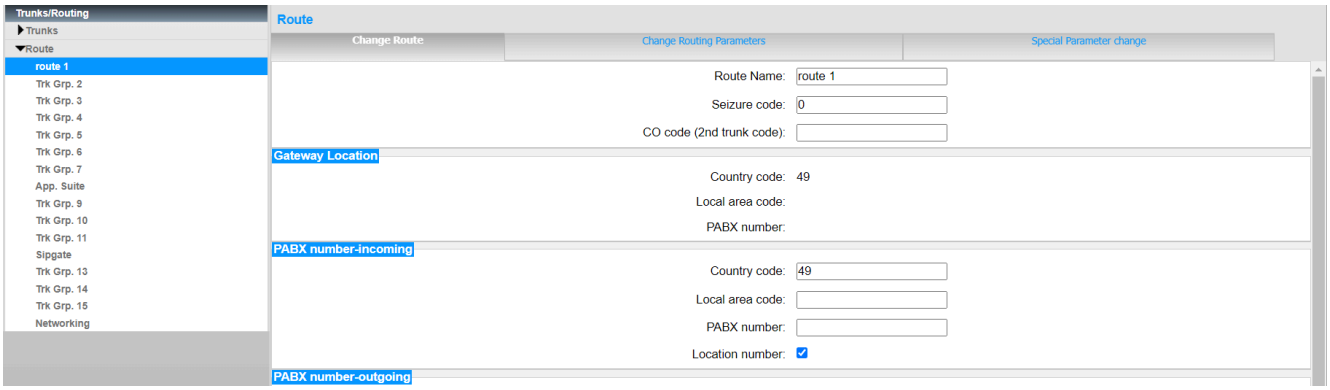
Consejo: En los datos de la instalación solo hay que introducir el código de país, el resto del número de teléfono está en la entrada de marcación directa de la extensión.

Asistente Redes de OpenScape Business S, multigateway



Seleccione Multigateway en la Configuración de red.

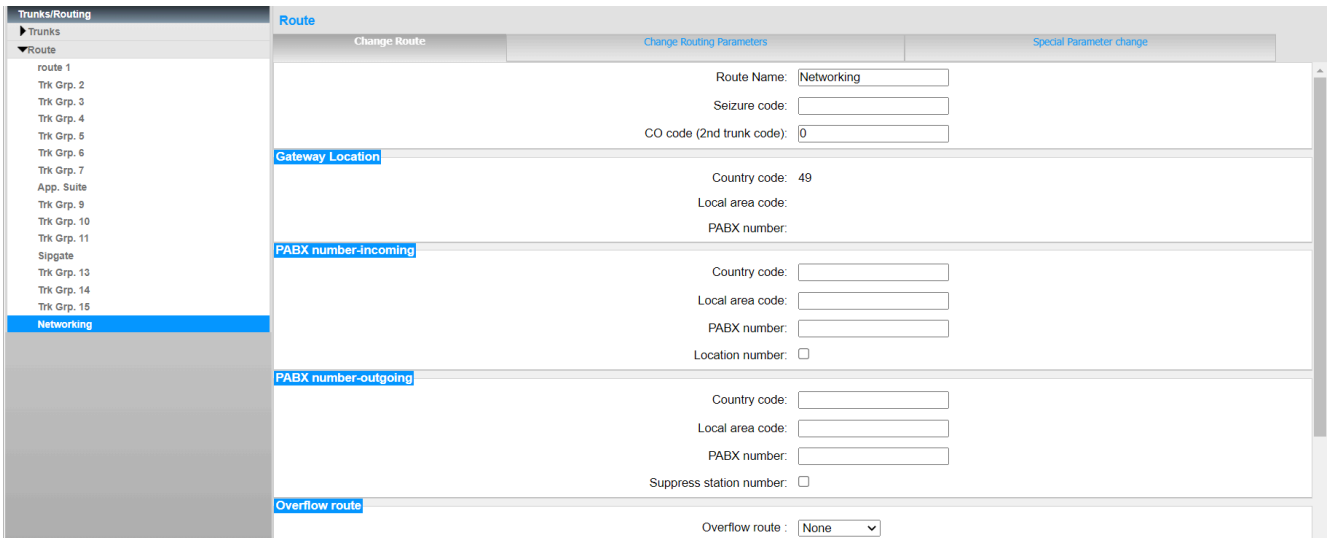
Rutas de OpenScape Business S, multigateway



El código del país ya se ha registrado en el asistente.

Parámetros de ruta: Tipo de ruta CO (Línea urbana)

Esta ruta recibe el tipo de ruta "Línea urbana".



Parámetro Encaminamiento: Tipo de número de llamada outgoing=Nacional, Tipo de ruta PABX

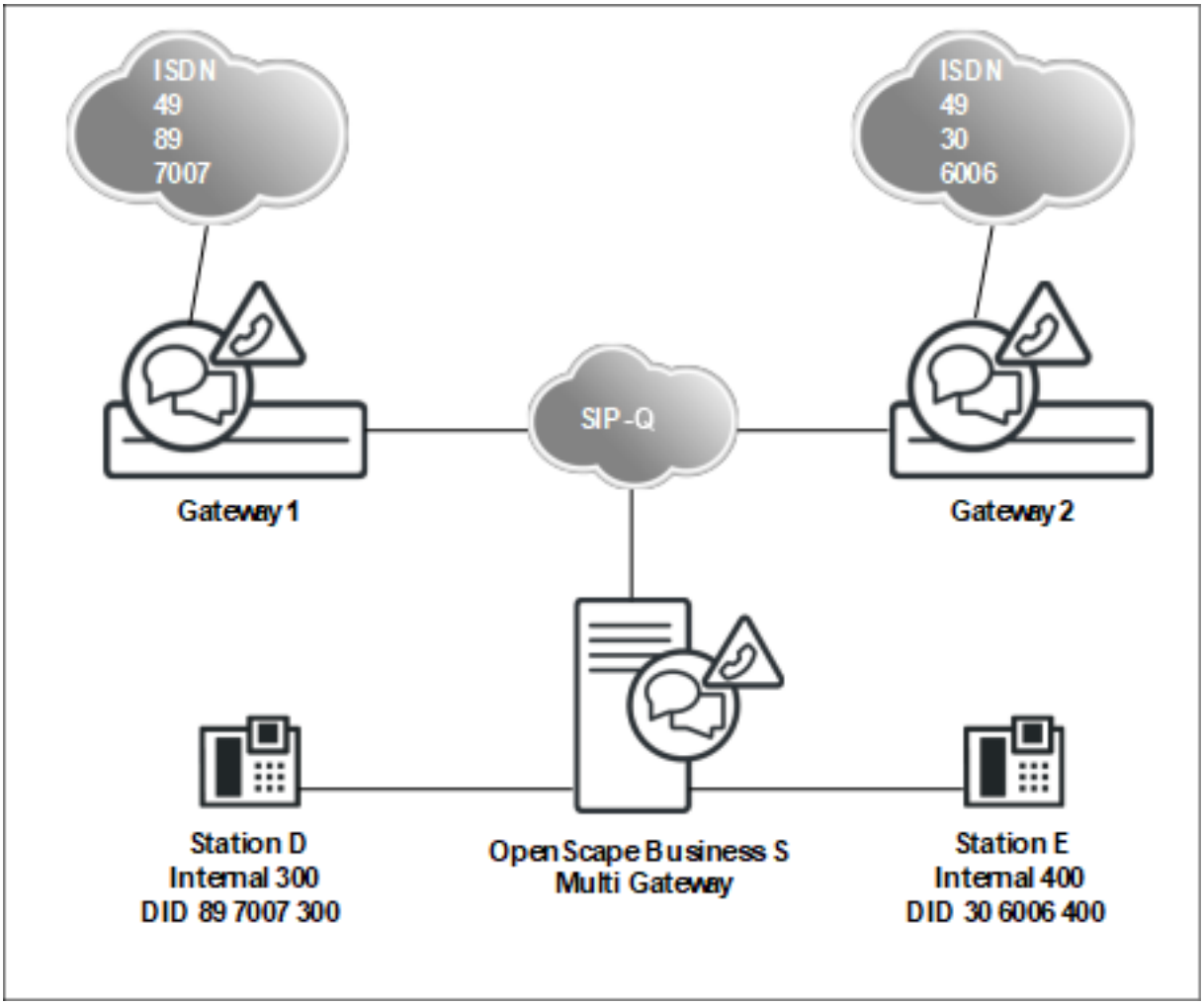
Esta ruta recibe el tipo de ruta "PABX" y el tipo de número de llamada, saliente debe configurarse con **Código de red local**.

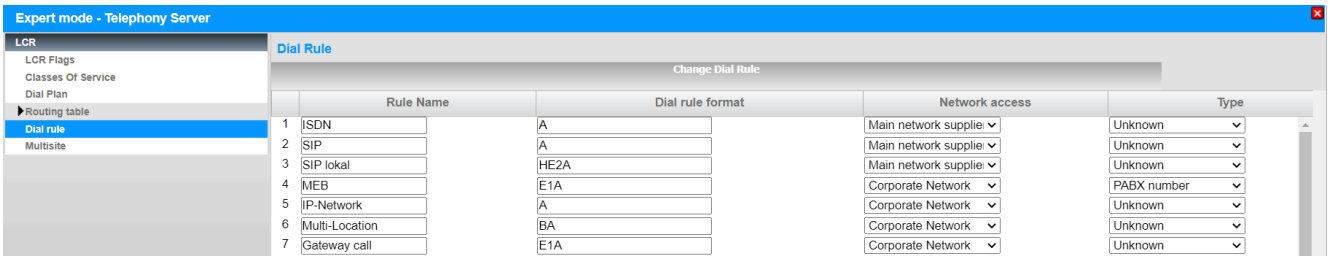
16.3.4.10 La extensión D llama a una extensión externa mediante la línea urbana

Sistema interconectado con configuración multigateway

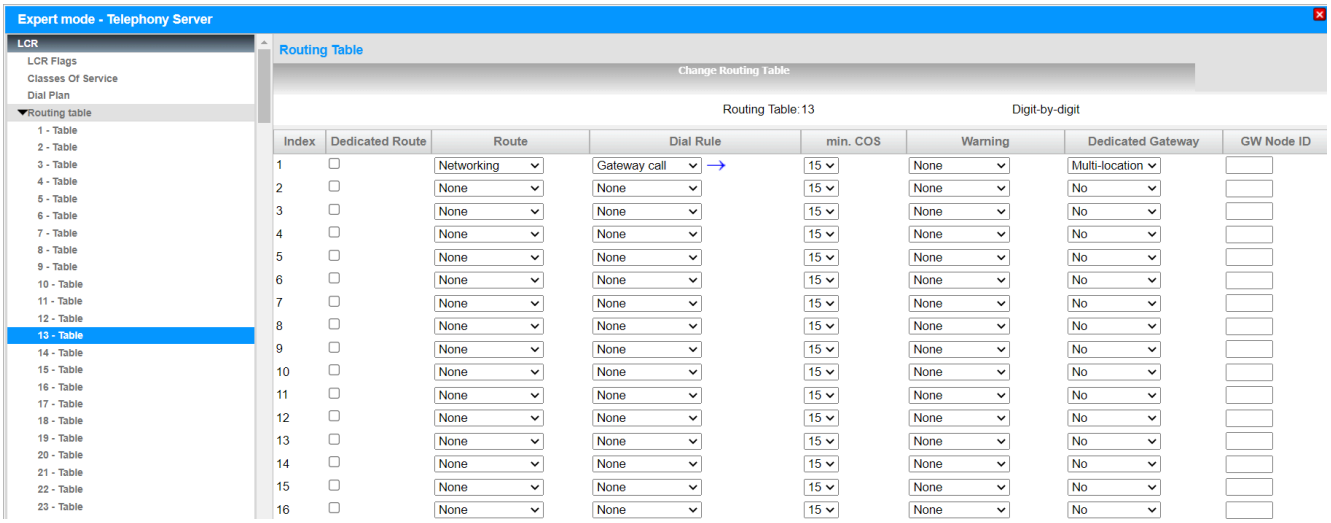
Configuración de OpenScape Business S, multigateway

Encaminamiento de OpenScape Business S, multigateway, a los gateways





	Rule Name	Dial rule format	Network access	Type
1	ISDN	A	Main network supplie	Unknown
2	SIP	A	Main network supplie	Unknown
3	SIP lokal	HE2A	Main network supplie	Unknown
4	MEB	E1A	Corporate Network	PABX number
5	IP-Network	A	Corporate Network	Unknown
6	Multi-Location	BA	Corporate Network	Unknown
7	Gateway call	E1A	Corporate Network	Unknown



El gateway 1 se configura como en el ejemplo anterior; lo mismo sucede con el gateway 2.

16.4 Llamadas de emergencia

El sistema de comunicación y los teléfonos conectados ofrecen distintas opciones para establecer una llamada de emergencia. El administrador puede configurar una hotline/llamada de socorro o un servicio de llamadas de emergencia.

Si el periodo de activación todavía no ha comenzado o el sistema de comunicación está en el periodo a prueba de fallos, las llamadas de emergencia siempre se pueden establecer desde los dos primeros teléfonos activos.

Requisitos

A la centralita de números de emergencia se accede marcando el código urbano (p.ej., 0) y el número de llamada de emergencia (p.ej., 112). Por ello, desde las aplicaciones la marcación del número de destino para las llamadas de emergencia se debe realizar introduciendo primero el código urbano.

Procedimiento básico

Caso 1: marcación de la llamada de emergencia a través de la línea PSTN

Caso 2: marcación de la llamada de emergencia a través de ITSP

Caso 3: acuerdo especial con el ITSP o con el proveedor PSTN

Caso 4: llamadas de emergencia con Mobile Logon (IP-Mobility)

Las llamadas de emergencia se inician desde una extensión del sistema de comunicación marcando el código de acceso a línea urbana y el número de llamada de emergencia. El sistema de comunicación transfiere el número de llamada de emergencia al proveedor correspondiente (PSTN o ITSP).

La llamada de emergencia se establece en la red local a la que está asignada la conexión del sistema de comunicación. Hay que tener en cuenta lo siguiente: todos los usuarios que no se encuentran en la misma ubicación que el sistema de comunicación (p.ej. extensiones Mobility, usuarios CallMe (teletrabajadores) o teléfonos conectados por WAN) deben marcar el número de emergencia con un teléfono móvil u otro teléfono de la red fija para realizar la llamada de emergencia en la red local de su ubicación.

No todos los ITSP admiten las llamadas de emergencia. En este caso, mediante la configuración LCR hay que garantizar el encaminamiento de las llamadas de emergencia a través de PSTN.

Por si se da el caso de que no todas las extensiones del sistema de comunicación tienen una ubicación, pero sí están asignadas de forma fija a una ubicación sin PSTN propio, se puede definir un procedimiento individualizado para la señalización de emergencia junto con el proveedor. P. ej. En función de la identificación de llamante, el proveedor puede encaminar la llamada de emergencia a la red local acordada. Estos acuerdos son individuales y no están sujetos a ninguna pauta general.

Mobile Logon (IP-Mobility) significa que los usuarios pueden cambiar de teléfono manteniendo su número de teléfono.

En este caso se pueden realizar llamadas de emergencia, siempre que los teléfonos estén registrados en las ubicaciones de los gateways. Todos los usuarios que no se encuentren en la ubicación del gateway (p.ej., extensiones Mobility, usuarios CallMe (teletrabajadores) o terminales conectados por WAN) deben marcar el número de emergencia con un teléfono móvil o con otro teléfono de la red fija para realizar la llamada de emergencia en la red local de su ubicación.

Consejo: Los escenarios de varios gateways en los que se utiliza la prestación Mobile Logon tienen requisitos especiales. La configuración correspondiente se describe en el capítulo "Llamadas de emergencia en combinación con Mobile Logon".

16.4.1 Llamada de socorro / Hotline

La función Hotline se puede activar para cada usuario. Al hacerlo se establece si al descolgar el microteléfono se establecerá conexión con el destino de hotline inmediatamente (Hotline) o transcurrido un determinado tiempo (llamada de socorro).

Llamada de socorro

Si el usuario marca en el tiempo predefinido (tiempo de llamada de socorro) una cifra cualquiera, **no** se establece conexión con el destino de hotline.

El administrador configura de forma centralizada este tiempo de llamada de socorro, y cada usuario lo puede activar y desactivar de forma individual.

Hot-line

Si la hotline está activada, los usuarios **no** pueden introducir un número de teléfono luego de descolgar el auricular. Es posible marcar un número antes de descolgar el auricular. Al descolgar el microteléfono acceden automáticamente al destino de hotline interno o externo predefinido.

Si el destino de hotline está ajustado para el desvío de llamadas o para la transferencia automática diferida, el usuario siempre es transferido.

Información específica de sistema

El administrador puede configurar 6 destinos de hotline y la duración del tiempo de llamada de socorro (de 0 a 99 segundos). Si el administrador introduce un tiempo de 0 segundos, se llama inmediatamente al destino de hotline.

Dependencias

Tema	Dependencia
No molestar	Si el destino tiene activado el estado No molestar, el llamante escucha el tono de ocupado

16.4.1.1 Cómo configurar y modificar el destino de hotline

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, desplácese hasta **Sistema** > **Interceptación/PO/Hot-line**.
4) En **Hot-line** se pueden registrar 6 destinos distintos (**N.º llam. destino**).
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.4.1.2 Cómo modificar el Tiempo de llamada de socorro

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema**.
4) Haga clic en **Interceptación/PO/Hot-line**.
5) En Hot-line puede modificar el **tiempo de llamada de socorro** (tiempo de retardo en segundos).
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.4.1.3 Cómo configurar la llamada de socorro o el hot-line para una extensión

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el grupo de menús, haga doble clic en **Extensiones**.
4) Haga clic, por ejemplo, en **Clientes IP**.
5) Haga clic, por ejemplo, en **Clientes sist**.
6) Marque la extensión correspondiente y en el campo de modo **Hot-line**, establezca **Llamada de socorro** o **Hot-line**.
7) Si ha seleccionado Hot-line, en el campo Hot-line deberá establecer también la **cantidad de destinos hot-line**.
8) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.4.2 Corte de línea para una llamada de emergencia

Si se hace una llamada de emergencia y no hay ninguna línea urbana libre, se ejecuta una desconexión forzosa. La línea libre se asigna automáticamente al usuario que ha realizado la llamada de emergencia.

El corte de línea funciona con líneas RDSI y ITSP.

Si todas las líneas están ocupadas el usuario puede ejecutar un corte de línea manual o automático.

- Automático: la prestación Ruta más económica (LCR) está activada y hay un número de llamada de emergencia en el LCR.
- Manual: la prestación siempre de liberación de línea está activa para el puesto de operadora y se ejecuta a través de una tecla o código.

Información específica de sistema

El administrador puede configurar tantos números de teléfono de emergencia como quiera.

Para que se realice un corte de línea cuando todas las líneas están ocupadas, el número de llamada de emergencia debe estar registrado en el plan de marcación del LCR y se debe establecer el flag de emergencia *Modo Experto*.

16.4.2.1 Cómo activar o desactivar Corte de línea para una llamada de emergencia

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Encaminamiento**.
3) En el árbol de navegación, desplácese hasta **LCR** > **Plan de marcación**.

4) En la ventana **Editar plan marcación** seleccione una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Número de llamada de emergencia** para el número de teléfono correspondiente.
   - Si desea desactivar la función, desactive la casilla de verificación **Número de llamada de emergencia** para el número de teléfono correspondiente.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.4.3 Solo para EE. UU., Canadá: Servicio de emergencia E911

Con el servicio de emergencia avanzado E911, al realizar una llamada de emergencia se transfiere, además del número de teléfono, informaciones sobre la ubicación geográfica (dirección almacenada) del llamante.

El puesto de rescate que reciba la llamada de emergencia, no tendrá que pedir al llamante que le indique verbalmente su ubicación.

El los EE. UU. esta prestación solo se activa al marcar el número de teléfono de emergencias 911.

Para el servicio de emergencia E911, el administrador debe asignar a cada conexión un LIN (Location Identification Number) con un número de marcación directa válido. A las líneas de extensión que se encuentran cercanas se les asigna un mismo LIN. Valiéndose del LIN transmitido, una base de datos de la central de emergencias (en la que están almacenados todos los LIN), identifica el nombre y la dirección del llamante.

Interdependencias

Tema	Interdependencia
CLIP	En los EE. UU., LIN está activado por defecto. Si la prestación CLIP (Calling Line Identification Presentation) está activada para los EE. UU., el LIN se desactiva automáticamente.

16.4.3.1 Cómo editar CLIP / Lin

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el grupo de menús, haga doble clic en **Extensiones**.
4) Haga clic, por ejemplo, en **Clientes IP**.
5) Haga clic en la pestaña **Modificar extensión**.
6) En el campo **Clip/Lin** de la extensión en cuestión, introduzca la LIN de 16 caracteres.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

16.4.4 Llamadas de emergencia en combinación con Mobile Logon

Si se utiliza la prestación Mobile Logon en una interred Multi-Gateway, al cambiar el teléfono también se puede cambiar la ubicación física. Por ello hay que realizar medidas especiales para encaminar las llamadas de emergencia.

Descripción del algoritmo para marcar una llamada de emergencia

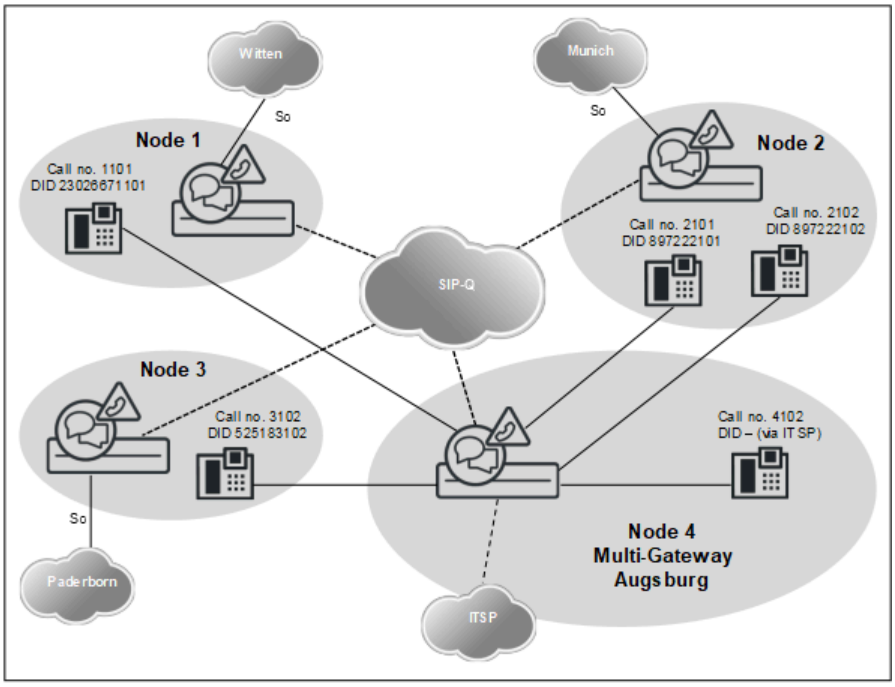
Si un usuario marca un número de llamada de emergencia (identificación del LCR), el algoritmo comprueba si en el teléfono hay configurado un número de llamada de emergencia. En tal caso se utilizará ese número para generar un número de teléfono derivado que se utilizará en la interred para encaminar la llamada a través del gateway correcto.

Todos los números identificados en el plan de marcación como números de llamada de emergencia, tienen también una referencia a un registro de la tabla de rutas. Todas las entradas de la tabla de rutas pertenecientes a un número de llamada de emergencia deben tener asignada una clase de servicio (COS) baja. Una clase de servicio baja significa que todos los usuarios están autorizados a restablecer un número de llamada de emergencia.

16.4.4.1 Configuración del escenario de llamada de emergencia

La configuración del escenario de llamada de emergencia muestra los pasos de configuración en una interred multigateway.

Tratamiento de números de llamada de emergencia



Mobile Logon solo se admite dentro de un nodo, es decir, los cambios de ubicación (y los requisitos especiales para las llamadas de emergencia) solo son relevantes en los teléfonos que operan en los nodos multigateway (4). Por norma general, todos los teléfonos correspondientes están registrados en el nodo 4, aunque físicamente se encuentran en diferentes ubicaciones.

- En todos los teléfonos correspondientes es necesario hacer una entrada para llamadas de emergencia (parte de conexión del número de teléfono canónico del nodo de la ubicación + código de ocupación de ruta de llamada de emergencia)
- La entrada LCR (Nodo_4local) de la siguiente tabla solo es necesaria si en el nodo 4 (multigateway) hay teléfonos presentes físicamente. También está disponible el número de ubicación aunque aquí está incompleto (solo con el prefijo de país). Para ello se requiere un acceso ITSP en el nodo 4 compatible con llamadas de emergencia en la red local.
- Al realizar la marcación en el teléfono se cumple una regla LCR identificada con la llamada de emergencia (p. ej. 0C11x).
- El número de llamada de emergencia guardado en el teléfono (y transferido al sistema al iniciar sesión en el sistema) se compara con los datos de ubicación del sistema (prefijo del país, código de red local, número de teléfono del sistema).

  Si los datos no coinciden se crea un número de llamada de emergencia "largo":

  – Eliminación del código de acceso: 0112 -> 112
  – Inserción de <código de ocupación LDAP><Prefijo internacional><Número de emergencias programado>: p. ej. 112 -> 0 00 49897220 112
- El número de llamada de emergencia "largo" se enruta a través del LCR y a través de las reglas LCR específicas se dirigir directamente a la línea urbana local o al nodo colateral correspondiente a través de una línea directa y, desde ahí, a la línea urbana.

Consejo: En el teléfono no se registra exactamente el número de emplazamiento completo del nodo local, por lo que en la ubicación multigateway también hay que registrar una regla LCR adecuada para la llamada de emergencia local.

Configuración de los datos de ubicación para el nodo 4

Parámetros de ruta

Nodo 4, Teléfonos

Resumen de las entradas relevantes para una llamada de emergencia en el LCR del nodo 4

Nodo 4	Nodos de gateway
G.-País de la ubicación	49
G.-Red local de la ubicación	
G.-Instalación de la ubicación	
Prefijo internacional	00
Prefijo nacional	0
Código de ocupación LDAP	0

Ruta	Tipo de número de llamada, saliente	Tipo RNR
Redes	Nacional	Int/marcación directa

Ruta (redes)	
Código urbano (2º AKZ)	0

Ubicación Witten	
Call Number (Número de teléfono)	1101
Emergency Number (Número de llamada de emergencia)	4923026670

Ubicación Múnich	
Call Number (Número de teléfono)	2101
Emergency Number (Número de llamada de emergencia)	49897220

Ubicación Paderborn	
Call Number (Número de teléfono)	3102
Emergency Number (Número de llamada de emergencia)	49525180

Ubicación Augsburgo	
Call Number (Número de teléfono)	4102
Emergency Number (Número de llamada de emergencia)	490

Plan de numeración			Tabla de rutas			Regla de marcación		
Nombre	Cifras marcadas	Servicio de emergencia	Ruta	Gateway dedicado	ID de gateway	Regla de marcación	Procedimiento	Tipo
Llamada_emergencia 5	0C112	X	Redes	Multigateway	1	E1A	Corp. Red	Desconocido
Llamada_emergencia 5	0C0110	X						
Línea urbana	0CZ							
Llamada de emergencia_a_1	0C00492302667-0-11X	X	Redes	Obligatorio	1	E3A	Corp. Red	Desconocido
Llamada de emergencia_a_2	0C004989722-0-11X	X			2			
Llamada_emergencia_a_3	0C004952518-0-11X	X			3			
Llamada_emergencia_4local 6	0C0049-0-11X	X	ITSP	No		E4A	Operador de red principal	Desconocido

16.4.5 Servicio de llamada de emergencia E112 para Europa

Con el servicio de emergencia avanzado E112, al realizar una llamada de emergencia se transfiere, además del número de teléfono, informaciones sobre la ubicación geográfica (dirección almacenada) del llamante.

La información geográfica se transmite en un documento XML estandarizado. La definición de los contenidos del documento depende del país y del ITSP. Por tanto, solo tiene que introducir el subconjunto de datos que le haya proporcionado su ITSP (por ejemplo, en Suiza solo se utiliza el campo NAM).

La prestación se activa con la configuración de números de emergencia en LCR y definiendo información de ubicación adecuada.

16.4.5.1 Cómo añadir un ID de ubicación ITSP a una extensión

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Gateway de voz**.
3) En el grupo de menús, haga clic en **ITSP Loc-ID Settings** (Ajustes de ID de ubicación ITSP).
4) Rellene el parámetro **Loc-ID Name** (Nombre de ID de ubicación) (obligatorio) y los parámetros definidos para la información de ubicación que le haya proporcionado su ITSP (por ejemplo, en Suiza solo se utiliza el campo NAM).
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

   Se asigna automáticamente un ID de índice al **ID de ubicación ITSP**.
6) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
7) En el grupo de menús, haga doble clic en **Extensiones**.
8) Haga clic, por ejemplo, en **Clientes IP**.
9) Haga clic en la pestaña **Modificar extensión**.
10) Introduzca el ID de índice correspondiente en el campo del ID de ubicación ITSP.
11) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

---

[5] En este ejemplo, con las reglas recogidas arriba se identifica la situación de llamada de emergencia, pero no se hace ningún encaminamiento. Para el encaminamiento de la llamada de emergencia se utiliza el número de teléfono "largo" derivado.

[6] En una ubicación multigateway las extensiones están conectadas físicamente por lo que hay que registrar una regla LCR propia para el acceso de llamada de emergencia local (a través de una ruta de ITSP).

16.5 Servicio de control de llamadas (Call Admission Control)

La prestación del servicio de control de llamadas (Call Admission Control CAC) permite restringir el ancho de banda utilizado a través del número de comunicaciones.

El sistema de comunicación ofrece res opciones para influir en el ancho de banda necesario:

- Restricción del número de llamadas simultáneas a través de ITSP
- Restricción del ancho de banda necesario en llamadas de gateway
- Restricción de la cantidad de comunicaciones en los escenarios de interconexión

16.5.1 Restricción del número de llamadas simultáneas por ITSP

La cantidad máxima de llamadas que se pueden realizar a través de un ITSP se puede restringir configurando el ancho de banda de carga disponible. Al reducir el número de estas llamadas (llamadas por Internet), se pueden reducir aún más los requisitos de ancho de banda.

La configuración para esto se puede realizar en los asistentes **Red/Internet** y **Telefonía Central**.

El número de llamadas posibles a través de un ITSP se puede ver en **modo Experto** en **Telefonía** >**Puerta de enlace de voz** > **Parámetros SIP**.

Las llamadas por Internet son:

- Llamadas ITSP
- Llamadas Unify Phone
- myPortal for Teams calls
- myPortal@work calls
- Llamadas de dispositivo a casa

Sólo las llamadas LAN myPortal@work y WebRTC puras no reservan ancho de banda porque la carga útil es directa.

16.5.2 Restricción del ancho de banda necesario en llamadas de gateway

Configurando los códecs admitidos en llamadas de gateway se puede modificar el ancho de banda.

Si solo se configuran códecs de compresión, el ancho de banda necesario es más bajo. Si se utilizan códecs mixtos, se puede reducir la prioridad de los códecs sin compresión para que se utilicen con menos frecuencia.

Los ajustes de configuración correspondientes se realizan en el **Modo Experto**, en **Telefonía** > **Gateway voz** > **Editar parámetros codec**.

16.5.3 Restricción del número de llamadas en los escenarios de interconexión

El sistema de comunicación ofrece dos opciones para controlar el ancho de banda en escenarios de interconexión.

Restricción mediante el número de líneas a otros nodos de red

Restricción del ancho de manda mediante selección de códec

Mediante la asignación de un número determinado de líneas a otros nodos de red se puede fijar un límite máximo para las llamadas simultáneas salientes y entrantes de los nodos.

El ancho de banda disponible se puede definir configurando los códecs utilizados desde y hacia el colateral (dirección IP de destino).

La configuración correspondiente se realiza en el **Modo Experto**, en **Telefonía** > **Gateway voz** > **Añadir parám. codec destino**.

16.6 Central compartida

Toda la capacidad del sistema de comunicación se puede dividir organizativamente en seis subsistemas como máximo. De esta forma, por ejemplo, varias empresas pueden utilizar conjuntamente un sistema de comunicación.

La prestación Central compartida se implementa mediante el uso de prestaciones existentes. Esto significa que no se realiza una configuración explícita de los sistemas individuales.

El control de conexiones autorizadas y prohibidas entre las distintas líneas y extensiones se realiza mediante grupos de relaciones de tráfico.

Prestaciones de la Central compartida:

- Interceptación
- Nº teléfono del sistema
- Lista de llamantes
- Intercalar
- DISA
- Mensaje directo
- Grabación de detalles de llamada
- Destinos hot-line
- Textos de información, mensajes por ausencia
- Llamadas internas
- Listín telefónico interno
- Impresión de la memoria de datos de cliente (KDS)
- Servicio nocturno
- Posición de aparcamiento
- Grupos de relaciones de tráfico
- Mensaje de voz
- Control de marcación

El sistema de comunicación se puede utilizar como Central compartida y, de esta forma, lo pueden utilizar varias empresas al mismo tiempo. La funcionalidad de todas las prestaciones se mantiene sin cambios en todas las extensiones.

Se excluyen aquí determinados recursos que se deben distribuir entre los suboperadores del sistema (empresas). Estos recursos se pueden asignar a uno, a varios o a todos los suboperadores. Estos son los recursos que se distribuyen:

- Extensiones
- Rutas
- Puesto de operadora
- Estación de interceptación
- Equipos de anuncios grabados, buzón de voz
- Grupos de relaciones de tráfico
- Abrepuertas
- Líneas DISA

Mediante los grupos VBZ se determina la accesibilidad de los suboperadores.

En cada área parcial se pueden configurar destinos de hotline propios.

Interdependencias

Tema	Interdependencias
GEZ	Solo hay un registro de tarifas central para todas las áreas parciales.
Llamadas internas	Se pueden realizar llamadas internas entre extensiones de "diferentes" áreas parciales, siempre que así lo permita la configuración de VBZ.
LCR	La ocupación automática de ruta solo se puede configurar a nivel de sistema.
Impresión de la memoria de datos de cliente (KDS)	La impresión de la base de datos solo se lleva a cabo para todo el sistema.
Listín telefónico interno	Se muestran los nombres de todas las extensiones y los números de marcación directa del sistema.
Conmutación	No se pueden conmutar líneas sin marcar.
Interceptación	Interceptación solo se puede programar a nivel de sistema.

16.6.1 Marcación abreviada central en centrales compartidas

Con la Marcación abreviada central en centrales compartidas se pueden seleccionar destinos de marcación abreviada en interdependencia de los grupos de relaciones de tráfico. Para ello, con la Gestión basada en Web (WBM) se puede asignar un área de destinos de marcación abreviada a los grupos de relaciones de tráfico correspondientes.

Interdependencias

Tema	Interdependencias
Números de teléfono externos	Los destinos de marcación abreviada solo pueden tener números de teléfono externo.
	El número de teléfono externo debe incluir código de ocupación de ruta o línea.

Tema	Interdependencias
Nombres KWZ	Se puede asignar un nombre a cada destino de marcación abreviada.
Portero eléctrico	El portero eléctrico no puede llamar a destinos de marcación abreviada.
Grupos VBZ	No es posible asignar a un grupo VBZ varias áreas de destinos de marcación abreviada.

17 Attendants

OpenScape Business ofrece funciones de conmutación para cualquier necesidad, como AutoAttendants y Attendants basados en teléfono y PC.

Vista general del Attendant ofrecido

	Se puede usar para	Hardware	Licencia
AutoAttendants			
Company AutoAttendant (UC Smart)	UC Smart	OpenScape Business X OpenScape Business S	necesario
Company AutoAttendant (UC Suite)	UC Suite	OpenScape Business X3/X5/ X8 con UC Booster Card o UC Booster Server OpenScape Business S	necesario
Attendants telefónicos			
OpenStage Attendant			
Attendants de PC			
OpenScape Business Attendant	UC Smart	PC y teléfono, UP_{0E}	necesario
- OpenScape Business BLF	UC Smart	Base IP	
myAttendant	UC Suite	OpenScape Business X3/X5/ X8 con UC Booster Card o UC Booster Server OpenScape Business S	necesario

17.1 AutoAttendant

Junto con el buzón de voz, el AutoAttendant constituye un servicio de puesto de operadora automático integrado y una memoria de mensajes, por ejemplo, para la central de empresa. El AutoAttendant reproduce a los llamantes un anuncio grabado de saludo. Durante el anuncio grabado o después de él, el llamante puede ser transferido a una extensión o a un buzón de voz automáticamente o introduciendo unos dígitos.

Para ello hay disponibles distintas funciones que permiten una conmutación personalizada con anuncios, por ejemplo, "Pulse el 1 para servicio técnico, 2 para ventas". Después de introducir la cifra deseada, el llamante es conectado automáticamente con empleados de ventas o de servicio técnico.

El Company AutoAttendant no tiene asignado ningún número de teléfono interno, sino que es una instancia central. Así, a una extensión se pueden asignar varios Company AutoAttendants o buzones. De esta forma, el usuario puede desviar llamadas de forma individualizada al Company AutoAttendant correspondiente. Después del desvío, el llamante puede escuchar un anuncio grabado del buzón personal o el anuncio de empresa central. No obstante, con

el Company AutoAttendant también se pueden reproducir anuncios grabados personalizados por extensión, independientemente del buzón personal.

Visión general de funciones

- Interceptar después de anuncio a un destino configurado
- Anuncios grabados en función del estado: se pueden reproducir diferentes anuncios grabados en función del estado de la extensión (libre u ocupada).
- Anuncios grabados diferentes para día/noche (conmutación manual o automática)
- Control central de calendario mediante servicio nocturno automático
- Marcación posterior de un número de teléfono cualquiera hasta una extensión configurada (desactivable)
- Marcación abreviada (= marcación directa desde el exterior) a destinos configurados (cualquier número de teléfono o buzón)

  En total puede haber 4 listas con un total de 10 destinos y un destino de interceptación. La lista activa se determina mediante el saludo seleccionado.
- Marcación posterior de un número de teléfono cualquiera hasta una extensión configurada. La función de Marcación posterior también se puede desactivar para evitar el abuso de tarifas.
- Multi Step AutoAttendant

  Los buzones de AutoAttendant se pueden configurar como destinos de marcación abreviada (manual 1 a 4, Día/noche). Esto permite encadenar buzones de voz.

  El Company AutoAttendant se comporta como con un desvío de llamadas; la llamada se transfiere de un buzón al siguiente y siempre se reproduce el anuncio grabado correspondiente. En total hay disponibles hasta 100 buzones de AutoAttendant.
- Marcación rápida

  Los anuncios grabados se pueden desactivar para garantizar una conmutación rápida.
- Anuncio grabado antes de contestar con señalización en paralelo (sin marcación abreviada)

  Si se reproduce un anuncio grabado de saludo al llamante, la llamada se señaliza al mismo tiempo en la extensión acústicamente (y visualmente). Si el usuario descuelga, se interrumpe el anuncio grabado y se le conecta con el llamante. Si el usuario no descuelga, se reproduce el anuncio grabado ininterrumpidamente hasta que llamante cuelga o se le transfiere mediante la Gestión de llamadas (Call Management).
- Identificación de tono de ocupado
- Transferencia de llamadas de fax (detección automática de tono de fax) a un destino de fax preconfigurado.
- Llamada recordatoria

  En caso de Llamada recordatoria (salvo una llamada de fax), el llamante es transferido al buzón de voz correspondiente, siempre que haya uno presente y que la grabación de mensajes esté activa.

Nota: Para garantizar que el sistema de buzón de voz realice una interceptación automática al puesto de operadora, hay que registrar internamente el código del puesto de operadora (valor estándar 9, EE. UU. 0).

Nota: El buzón de voz de AutoAttendant solo se puede administrar (TUI) desde un teléfono. Por ello, la contraseña para el buzón de voz de AutoAttendant debe ser diferente de la contraseña del buzón personal del teléfono.

Ejemplos de aplicación

- Ejemplo 1: **Anuncios grabados independientes para servicios de emergencia o de despliegue**

  Fuera del horario de oficina, el cliente desvía las llamadas al AutoAttendant (p.ej. Servicio nocturno). El AutoAttendant conecta al técnico de servicio de turno a demanda y ofrece dejar un mensaje en un buzón central. En este caso, un anuncio grabado lleva a la transferencia a los distintos números de teléfono móvil de los técnicos de servicio.
- Ejemplo 2: **Diferentes servicios de domingo para consultas médicas**

  No es necesario indicar el servicio de domingo correspondiente en el contestador ni cambiar de cinta. Así, el cliente configura tantos AutoAttendant como suplentes tiene. Los AutoAttendants se graban una vez y el fin de semana se activan con un desvío (servicio nocturno) al AutoAttendant correspondiente. Aquí sucede lo contrario: varios anuncios grabados diferentes llevan al mismo buzón.

17.1.1 Company AutoAttendant (UC Smart)

El Company AutoAttendant (UC Smart) es el AutoAttendant de la solución de Unified Communications UC Smart. Se puede utilizar como AutoAttendant personal y como AutoAttendant central. La configuración inicial se realiza mediante la Gestión basada en Web (WBM); a continuación se puede controlar y configurar con el teléfono.

El Company AutoAttendant (UC Smart) puede operar en dos modos:

- **AutoAttendant personal**

  El AutoAttendant personal está asignado a una extensión o a grupo y responde al número de teléfono de la extensión o del grupo a los que se ha llamado en origen (y que hace el desvío) (p.ej. `12345678-100`).

  Se puede acceder al AutoAttendant personal a través de la línea colectiva "Voicemail" (número de teléfono estándar: 351). El servicio se realiza mediante puertos SmartVM (puertos EVM) del tipo "PhoneMail" que deben estar asignados todos a esa línea colectiva.

  No se puede operar en paralelo con la UC Suite.
- **AutoAttendant central**

  El AutoAttendant central se utiliza como puesto de operadora central y responde a su número de teléfono propio (p.ej. `12345678-0`). El comportamiento es idéntico tanto si la llamada se realiza directamente al AutoAttendant como si está desviada.

  Se accede al AutoAttendant central a través de una o varias líneas colectivas propias (número de teléfono estándar: 352). El servicio se realiza

mediante puertos SmartVM (puertos EVM) del tipo "Estándar" que pueden estar asignados a una o varias líneas colectivas (máx. 100).

De forma predeterminada, hay configurado un Company Auto Attendant (índice de grupo 3) con 2 puertos SmartVM. Los nombres y los tipos de los puertos se pueden modificar con el asistente **Telefonía central** > **SmartVM** (véase también Cómo configurar el buzón de voz (SmartVM)).

La lista de marcación abreviada y la carga de saludos se puede modificar en el modo Experto **Telefonía** > **Conexiones** > **SmartVM** (véase Cómo cargar, guardar y borrar saludos sueltos). También se pueden configurar y activar más (máx. 99) Company AutoAttendants (UC Smart).

Se puede operar en paralelo con la UC Suite.

El Company AutoAttendant (UC Smart) requiere licencia (licencia Company AutoAttendant). Si no hay disponible ninguna licencia, se ignoran las "reglas" del Company AutoAttendant y las llamadas se desvían al puesto de interceptación central.

17.1.1.1 Cómo configurar un Company AutoAttendant

Por ejemplo, para las llamadas diurnas habría que configurar un anuncio grabado antes de contestar con opción de grabación (p.ej. buzón de voz 100). Por la noche, después del anuncio grabado correspondiente se debe hacer directamente una interceptación al buzón nocturno con opción de aceptar la llamada (también buzón de voz 100).

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

UC Smart está activado.

De forma predeterminada, después del anuncio grabado se hace una interceptación al puesto de interceptación en el servicio nocturno/diurno.

De forma predeterminada, la función Speeddial y la Marcación posterior no están activadas.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Conexión**.
3) En el grupo de menús, haga clic en **Equipo auxiliar** > **SmartVM**.
4) En el grupo de menús, haga clic en **Puesto de operadora automático (AutoAttendant)**.
5) En la línea del AutoAttendant deseado (p.ej. `352`) desactive la casilla de verificación **Interceptar después de anuncio**, para poder introducir dígitos de marcación abreviada después del anuncio grabado de saludo.
6) Active la casilla de verificación **ninguna marcación de sufijo**. Esto solo permite la entrada de dígitos de marcación abreviada (no se pueden introducir números de teléfono internos).
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
8) En el grupo de menús, haga clic en **AutoAttendant** y a continuación en la entrada del AutoAttendant deseado (p.ej. `352`).

9) Haga clic en la pestaña **Editar marcación abreviada/Dest. interceptación (día)**.
10) En la línea **Marc. abr. 0** de la lista desplegable **Seleccionar**, seleccione la extensión para el puesto de interceptación (p.ej. la extensión 100) y en la lista desplegable **Tipo**, la entrada **Buzón de voz**.
11) En la línea **Interceptación** de la lista desplegable **Seleccionar**, seleccione la extensión para el puesto de interceptación (p.ej., la extensión 100).
12) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
13) Haga clic en la pestaña **Editar marcación abreviada/Dest. interceptación (noche)**.
14) En la línea **Interceptación** de la lista desplegable **Seleccionar**, seleccione la extensión para el puesto de interceptación (p.ej. la extensión 100) y en la lista desplegable **Tipo**, la entrada **Buzón de voz**.
15) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
16) En el grupo de menús, haga clic en **SmartVM**.
17) Para evitar que haya saludos duplicados en el buzón de puesto de interceptación, en la lista del puesto de interceptación deseado (p.ej. la extensión 100) de la lista desplegable **Saludo** seleccione la entrada **Ninguno**. De esta forma, inmediatamente después del saludo del Company AutoAttendant se emitirá el tono de señal para la grabación.
18) El saludo del Company AutoAttendant se puede modificar mediante un teléfono o mediante **Modo Experto** > **Mantenimiento** > **SmartVM** (véase Configuración del buzón de voz (SmartVM)).

17.1.1.2 Cómo configurar un Company AutoAttendant nuevo

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

UC Smart está activado.

Licencias necesarias

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En primer lugar, configure la línea colectiva:

a) En el árbol de navegación, haga clic en **Telefonía** > **Llamadas entrantes**.

b) En el árbol de navegación, haga clic en **Llamadas entrantes** > **Llam. grupo / lín. colectiva**.

c) Haga clic en la pestaña **Añadir grupo**.

d) En el campo **Número de teléfono de extensión**, introduzca el número de teléfono del nuevo AutoAttendant (p.ej. `353`).

e) En el campo **Número de marcación directa**, introduzca el número de marcación directa del nuevo AutoAttendant (p.ej. `353`).

: Si desea utilizar DID 879, 890 o 891, debe hacer la configuración a través de ManagerE y no a través de WBM.

---

f) En el campo **Nombre**, introduzca el nombre del nuevo AutoAttendant (p.ej. `AutoAttendant 353`).

g) En la lista desplegable **Tipo**, seleccione la entrada **Lín. colectiva cíclica**.

h) En el área **Miembro grupo** de la lista desplegable Número de llamada, seleccione el puerto de AutoAttendant deseado (p.ej. **745 SmartVM 7**).

i) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

j) Para añadir otro puerto de AutoAttendant a la línea colectiva, en el árbol de navegación de **Llam. grupo / lín. colectiva**, haga clic en el AutoAttendant deseado y, a continuación, en la pestaña **Añadir miembro**. En esta pestaña, en **Número de teléfono de extensión**, seleccione otro puerto de AutoAttendant (p.ej. **746 SmartVM 8**).

k) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

3) Configure el buzón del AutoAttendant:

a) En el árbol de navegación, haga clic en **Telefonía** > **Conexiones**.

b) En el árbol de navegación, haga clic en **Conexiones** > **SmartVM**.

c) En el árbol de navegación, haga clic en **AutoAttendant**.

d) En la línea del AutoAttendant deseado (p.ej. `353`), defina las dos casillas de verificación según sea necesario:

Interceptar después de anuncio: si está activada, el llamante puede introducir una cifra de marcación abreviada de una opción de conmutación durante el saludo.

Ninguna marcación de sufijo: si está activada, solo se pueden introducir cifras de marcación abreviada y no números de llamada internos.

e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

f) En el árbol de navegación, haga clic en **SmartVM**.

g) Haga clic en

h) En la pestaña **Editar buzones SmartVM**, y en la opción **Saludo** de la línea del AutoAttendant deseado, seleccione el saludo deseado.

i) En la línea del AutoAttendant deseado, active la casilla de verificación **AutoAttendant**.

j) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

4) Configure las opciones de conmutación (p.ej. "0" para conectar y "1" para un anuncio grabado):
   a) En el árbol de navegación, haga clic en **SmartVM** y a continuación en **AutoAttendant**.
   b) En el árbol de navegación, en **AutoAttendant**, haga clic en la entrada del AutoAttendant deseado (p. ej. 352).
   c) Haga clic en la pestaña **Editar marcación abreviada/Dest. interceptación (día)**.
   d) En la línea **Marc. abr.0** y en **Número de llamada**, introduzca el número de teléfono con el que desea establecer conexión. En la lista desplegable **Tipo**, seleccione la entrada **Número de llamada**.
   e) En la línea **Marc. abr. 1** de la lista desplegable **Seleccionar**, seleccione la extensión para el puesto de interceptación (p.ej. la extensión 100) y en la lista desplegable **Tipo**, la entrada **Buzón de voz**.
   f) En la línea **Interceptación** de la lista desplegable **Seleccionar**, seleccione el Company AutoAttendant (p.ej. 353).
   g) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
   h) Si el flag **ninguna marcación de sufijo** está desactivado, también se pueden marcar números internos durante el anuncio grabado. Para evitar abuso de tarifas, hay que comprobar o limitar la **Limitación longitud nº llamada** para que no se puedan marcar números de teléfono externos (véase **Modo experto** > **Telefonía** > **SmartVM** > **Editar parámetros de SmartVM**).

17.1.2 Company AutoAttendant (UC Suite)

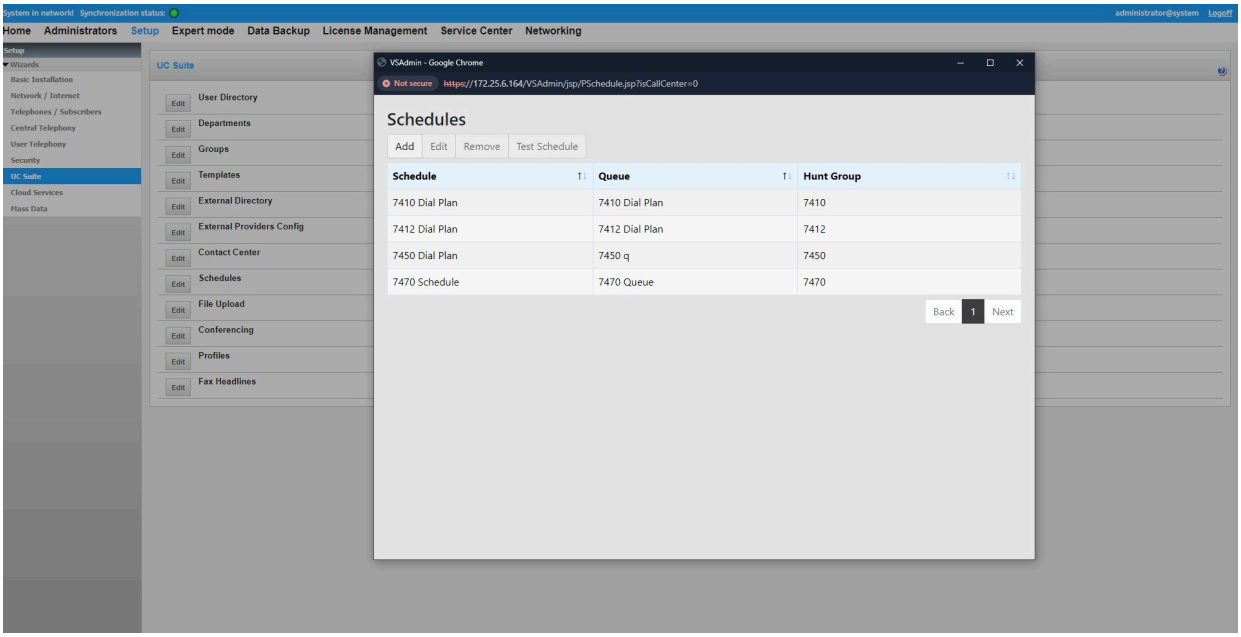
El Company AutoAttendant central (UC Suite) es un puesto de operadoras que solo puede configurar el administrador. Para facilitar la instalación y la configuración, hay disponibles cinco plantillas que puede adaptar el administrador.

El administrador puede configurar el Company AutoAttendant (UC Suite) mediante planes horarios en base a reglas. Los planes horarios ofrecen opciones de selección ampliadas como, por ejemplo, marcación por nombre.

17.1.2.1 Planes horarios

El plan horario y las reglas en él incluidas (CCV, Call Control Vector) permiten definir cómo se administrarán las llamadas entrantes en determinados días y horas.

Por ejemplo, en los días laborables se puede definir una regla para el primer turno (de 06:00 h a 14:00 h), otra para el turno central (de 14:00 a 22:00 h) y otra para el turno de noche (de 22:00 a 06:00 h). Para el fin de semana se puede definir una regla de fin de semana. Para cada una de estas reglas se puede indicar, por ejemplo, si se reproducirán anuncios grabados y/o adonde serán transferidas las llamadas.



Se debe asignar al menos una regla (Call Control Vector CCV) a un plan horario. Las reglas determinan cómo se gestionarán las llamadas entrantes durante el tiempo de vigencia de un plan horario. Las reglas se aplican exclusivamente a llamadas, no a faxes ni correos electrónicos.

Las reglas se crean con el editor de reglas gráfico (Editor CCV) mediante la vinculación de objetos CCV predefinidos y se pueden guardar con cualquier nombre una vez finalizadas.

Las reglas guardadas se pueden asignar a uno o varios planes horarios como reglas estándar (CCV estándar) o como reglas de excepción (CCV de excepción). El editor de reglas permite la apertura, modificación y guardado en cualquier momento.

Si se ha asignado una regla estándar (CCV estándar) a un plan horario, ese plan se puede guardar con un nombre de selección libre. Los planes horarios con una regla estándar, tras ser asignados a una cola de espera, se aplican 24 horas al día, 365 días al año. Si desea aplicar otras reglas en determinados momentos (Pausa, Fin de semana, Festivo, Vacaciones, etc.), puede asignarlas al plan horario correspondiente como reglas de excepción (CCV de excepción). De esta forma, se puede definir cómo se administrarán las llamadas entrantes, por ejemplo, durante las vacaciones. Los planes horarios vacacionales tienen prioridad frente a otros planes horarios y reglas.

Editor de reglas (Editor CCV)

Con el editor de reglas se pueden crear reglas a partir de objetos CCV predefinidos. La asignación de los objetos CCV y de sus propiedades determina cómo serán administradas las llamadas entrantes.

Nota: Una regla tiene un límite superior de 500 objetos CCV.

Están disponibles los siguientes objetos predefinidos:

Consejo: A todos los objetos CCV indicados se les aplican, además, estas dos propiedades generales:

Descripción: describe de forma opcional el objeto CCV, por ejemplo, "Saludo de bienvenida".

Iniciar proceso después de marcar los dígitos: indica los dígitos necesarios, sin espacios en blanco, comas ni otros caracteres. La indicación se refiere al objeto CCV anterior. Si en Dígitos aceptados se ha introducido un 9, también aquí se debe introducir esta cifra.

- **Reproducir mensaje**

  Hace que se reproduzca el anuncio grabado deseado. Se puede seleccionar un archivo de sonido presente en la UC Suite. Además, se puede importar un nuevo archivo de sonido a la UC Suite o se puede grabar un nuevo anuncio grabado y, a continuación, importarlo como archivo de sonido a la UC Suite.

  Al reproducir un anuncio grabado se ocupa un canal Media Stream.

  Propiedades:

  – **Nombre archivo**: selección de un anuncio grabado (archivo de sonido en formato wav)
  – **Dígitos de interrupción**: indicación de una tecla o combinación de teclas en el teclado de marcación con el que el llamante puede interrumpir la reproducción del anuncio grabado.
  – **Administrador de archivos**: este botón permite cargar un archivo de sonido en formato wav o crear un nuevo archivo de voz con el grabador.
- **Finalizar llamada**

  Hace que finalice la conexión

  Después de este objeto CCV no se pueden insertar más objetos CCV.
- **A CCV**

  Crea un bucle a otro objeto CCV

  Propiedad:

  – **CCV de destino**: selección del objeto CCV

- **Iniciar proceso después de marcar los dígitos**

  Hace que el siguiente objeto u objetos CCV se ejecuten en función de las cifras aquí indicadas (Iniciar proceso después de marcar los dígitos).

  Propiedades:

  – **Nombre archivo**: selección de uno o varios anuncios grabados (archivo de sonido en formato wav).
  – **Lista de reproducción**: lista de reproducción de los anuncios grabados seleccionados (archivo de sonido en formato wav) en el orden de reproducción.
  – **Tiempo excedido al introducir dígitos**: tiempo excedido al introducir tiempo en segundos que espera el sistema de comunicación a la entrada de cifras.

    Si la entrada completa de dígitos no se produce dentro del tiempo indicado, se vuelve a reproducir el mensaje (anuncio grabado).
  – **Enlace con**: listado de los números con destino.

    Las cifras y los destinos se pueden añadir, editar y eliminar.
  – **Administrador de archivos**: este botón permite cargar un archivo de sonido en formato wav o crear un nuevo archivo de voz con el grabador.

  El contenido de la lista de reproducción se muestra en el editor de reglas mediante una información sobre herramientas al sostener el cursor sobre el objeto CCV.
- **Transferencia de un solo paso**

  Esta función depende del ajuste **SST de puesto de operadora automático normal** (WBM, **Modo experto**: **Aplicaciones** > **OpenScape Business UC Suite** > **Servidor** > **Ajustes generales**):

  – **SST de puesto de operadora automático normal** habilitado (configuración estándar; no para EE. UU.): se transfiere una llamada, tanto si el destino está libre como ocupado.

    Consejo: En el caso de una extensión con bloqueo de avisos de llamada en espera, la llamada solo se transfiere cuando la extensión de destino está libre. No se produce un aviso de llamada en espera en caso de ocupado.
  – **SST de puesto de operadora automático normal** deshabilitado (configuración estándar; solo para EE. UU.): la llamada se transfiere si el destino está libre.

    Si el destino está ocupado y el bloqueo de avisos de llamada en espera está desactivado, o si el destino no está disponible, el llamante escucha la reproducción de un anuncio grabado. Con ello, el llamante puede

decidir dejar un mensaje en el buzón de voz de la extensión o marcar el número de teléfono de otro destino.

Si el destino está ocupado y el bloqueo de avisos de llamada en espera está activado, la llamada no se transfiere.

Después de este objeto CCV no se pueden insertar más objetos CCV.

Propiedad:

– **Extensión de destino**: indicación del número de teléfono interno o del número de marcación directa externo con número de línea urbana. No se permite el uso de caracteres vacíos, comas ni otros caracteres.

El número de teléfono de la extensión de destino se muestra en el objeto CCV.

Nota: Después de la transferencia de un solo paso, el sistema desconecta la llamada después de señalizarla durante 5 minutos.

- **Grabar en buzón de voz**

  Hace que la llamada se transfiera al buzón de voz de una extensión o de un grupo de buzón de voz

  Después de este objeto CCV no se pueden insertar más objetos CCV.

  Propiedad:

  – **Buzón de voz del usuario**: indicación del número de teléfono del buzón de voz de una extensión o de un grupo de buzón de voz.

  El número de teléfono y el nombre del buzón de voz o del grupo de buzón de voz se muestran en el editor de reglas mediante una información sobre herramientas al dejar el cursor sobre el objeto CCV.

- **Transferencia supervisada**

  Hace que la llamada se transfiera a un destino interno. Durante la transferencia, el llamante escucha la música en espera (Music On Hold MOH de la UC Suite).

  Frente a la transferencia de un solo paso al objeto CCV, aquí hay que introducir otros dos objetos CCV. En concreto, hay que definir cuál será el comportamiento del sistema cuando el destino de la llamada esté ocupado o cuando no se responda a la llamada. Normalmente, en estos casos el llamante escucha la reproducción de un anuncio grabado.

  Propiedades:

  – **Extensión de destino**: indicación del número de teléfono interno.

    Solo se admiten números de teléfono internos en el nodo propio. No se admite el desvío a destinos externos, extensiones virtuales, otros

AutoAttendants, UCD incl. Contact Center o destinos CallMe externos. En estos casos hay que utilizar SST (transferencia en un paso).

– **Tiempo de espera de tono de llamada (seg.)**: tiempo en segundos en el que se debe aceptar la llamada.

  Si la llamada no se acepta dentro del tiempo indicado, es restablecida en el sistema de comunicación y se utiliza el siguiente objeto CCV.

  Consejo: El tiempo aquí indicado debe ser menor que el tiempo configurado para la transferencia automática diferida (configuración estándar para la transferencia automática diferida = 15 segundos). Consulte Cómo configurar una transferencia automática diferida.

– **Devolver llamada si el dispositivo de destino está transferido / desviado** Opción (solo se aplica a número de llamada interno).

  Si la opción está activa se comprueba el destino de la llamada. Si en el destino de llamada hay activada una transferencia automática diferida de llamadas o un desvío de llamadas, la llamada se restablece en el sistema de comunicación y se utiliza el siguiente objeto CCV.

– **Comprobar estado de presencia al transferir llamadas**: Opción

  Si esta opción está activada, se comprueba el estado de presencia del destino de la llamada; si el estado no es Oficina, la llamada se devuelve al sistema de comunicación y se utiliza el siguiente objeto CCV.

  Nota: Si una llamada entrante procede de un número suprimido o desconocido, la contesta AutoAttendant (UC Suite) y la transfiere mediante Transferencia supervisada, el número del llamante que se mostrará será el de UC Suite.

• **Marcar por nombre**

  Se solicita al llamante indicar las tres primeras letras del apellido del usuario deseado a través del teclado de marcación.

  Si hay una extensión con las letras iniciales indicadas, se establece una conexión.

  Si hay varias extensiones con las letras iniciales indicadas, el llamante escucha sus nombres (10 extensiones como máximo). Si una extensión no ha grabado ningún anuncio de nombre, se escuchará en su lugar la reproducción del número de teléfono. Después de seleccionar la extensión deseada se establece una conexión.

  Si por el contrario ningún usuario se corresponde con las letras iniciales especificadas, el llamante recibe un mensaje al respecto.

  Consejo: Las teclas del teclado de marcación responden a la primera pulsación de teclas. Cada vez que se pulsa una tecla se comprueba si hay apellidos de usuario con las letras asignadas a las teclas.

  Ejemplo: en el directorio interno están presentes los siguientes cinco apellidos con las letras iniciales t, u y v:

Taylor, Taler, Ullrich, Vasquez y Volterra. Para establecer una conexión con el usuario Taylor, pulse estas teclas: 8 2 9

Después de este objeto CCV no se pueden insertar más objetos CCV.

Propiedades:

– **Método**: selección de **Transferir a extensión** o **Grabar en buzón de voz**.

  En función del método seleccionado, se establecerá una conexión con la extensión deseada o con su buzón de voz. Solo se admiten extensiones internas registradas en el directorio interno con nombre y apellidos.

- **Marcar por extensión**

Se solicita al llamante indicar el número de teléfono de la extensión deseada a través del teclado de marcación.

Si el llamante marca el número de teléfono de una extensión virtual, se le solicitará introducir otro número de teléfono de extensión. A continuación, se establece una conexión. Si la extensión deseada no responde, la llamada será atendida por su buzón de voz.

Después de este objeto CCV no se pueden insertar más objetos CCV.

Propiedades:

– **Método**: selección de **Transferir a extensión** o **Grabar en buzón de voz**.

  En función del método seleccionado, se establecerá una conexión con la extensión deseada o con su buzón de voz. Recuerde que solo se admiten extensiones internas cuyos números de teléfono estén registrados en el directorio interno.

- **Definir idioma**

Permite seleccionar el idioma de los anuncios estándares, en función del número de teléfono del llamante. Hay que tener en cuenta que solo afecta a anuncios estándar (anuncios del sistema) y no a anuncios personales.

Se puede definir, por ejemplo, que para un número de teléfono con el prefijo nacional +49 se reproduzca un anuncio en alemán, y que para los números de teléfono con el prefijo +33 se reproduzca un anuncio grabado en francés.

Propiedades:

– **Idioma predeterminado**: lista desplegable para seleccionar un idioma.

  El idioma seleccionado aquí se utiliza para todos los números de teléfono para los que no se ha definido un idioma propio.

– **Patrón**: indicación del número de teléfono al que se asignará un idioma determinado.

  Se pueden utilizar los siguientes marcadores de posición: * = cualquier número, ? = cualquier cifra.

– **Idioma**: lista desplegable para seleccionar el idioma que se asignará al número de teléfono correspondiente (**Patrón**).

Un idioma se puede asignar a tantos números de teléfono diferentes como se desee (**Patrón**).

- **Encaminamiento CLI**

  Permite desviar una llamada a uno o varios objetos CCV consecutivos, mediante el número de teléfono del llamante.

  Por ejemplo, se puede definir que un número de teléfono con el prefijo nacional +49 escuche, en primer lugar, un anuncio en alemán (objeto CCV **Reproducir mensaje**) y que, a continuación, la llamada se transfiera a un teléfono interno (objeto CCV **Transferencia de un solo paso**). También se puede utilizar el código de red (p. ej., 089 para Munich)

  En el contexto de UC Suite y CLI Routing, los usuarios deben considerar escenarios específicos, como llamadas entrantes desde MS Teams Native SIP Trunk. Si tiene la intención de enviar a OpenScape Business los números de la persona que llama en formato canónico, incluido el código de país, debe establecer reglas de enrutamiento CLI adicionales.

  Por ejemplo, si las personas que llaman desde MS Teams tienen números en el formato 49777555XXXX y 777555 es la parte común de estos números, los usuarios deben crear reglas de enrutamiento CLI relevantes que incorporen esta parte común (777555).

  Propiedades:

  – **Estándar**: lista desplegable para seleccionar el objeto CCV.

    El objeto CCV seleccionado aquí se utiliza para todos los números de teléfono para los que no hay definido ningún destino propio.
  – **Patrón**: indicación del número de teléfono al que se debe asignar como destino un determinado objeto CCV.

    Se pueden utilizar los siguientes marcadores de posición: * = cualquier número, ? = cualquier cifra.
  – **Descripción**

    entrada de una explicación.

    Para el **Patrón** +49 (=prefijo del país Alemania) se puede introducir, por ejemplo, Alemania.

    El texto aquí introducido se muestra en el editor de reglas.
  – **Destino**: lista desplegable para seleccionar el objeto CCV al que se asignará el número de teléfono correspondiente (**Patrón**) como destino.

  Un objeto CCV se puede asignar tantos números de teléfonos diferentes (**Patrón**) como destino como se desee.
- **Bifurcar con variable**

  Desvía una llamada a uno o varios objetos CCV consecutivos en base a una condición.

  Se puede definir por ejemplo que los llamantes escuchen la reproducción de un anuncio grabado (Vuelva a llamar más tarde...) en cuando haya más de 20 llamadas en una cola de espera.

  Propiedades:

  – **Variable**: selección de **Llamadas** o **Agentes disponibles**.

    En función de la variable seleccionada se utiliza como condición definida el número de llamadas en espera dentro de una cola o el número de agentes disponibles (incluidos los agentes que se encuentren en el tiempo administrativo o de tratamiento posterior) de una cola. En la lista desplegable correspondiente hay que seleccionar la condición

(**menor que**, **mayor que**, **menor o igual que**, **mayor o igual que**, **igual a**) e introducir el valor de comparación en el campo de entrada correspondiente.

– **Bifurcar con True**: lista desplegable para seleccionar el objeto CCV que se debe utilizar como destino si se cumple la condición.
– **Bifucar con False**: lista desplegable para seleccionar el objeto CCV que se debe utilizar como destino si no se cumple la condición.

El número de agentes disponibles en una cola de espera está determinado por los siguientes cambios de estado de los agentes:

– Inicio de sesión de un agente en la cola de usuario mediante "Inicio de sesión/Login": --> +1
– Fin de sesión de un agente de la cola de espera mediante "Fin de sesión/ Logout": --> -1
– Agente en estado "Pausa":-->-1
– Agente en estado "Disponible después del descanso":--> 1

El número de agentes disponibles en una cola de espera **no** está determinado por los siguientes cambios de estado de los agentes:

– Agente en el estado "Sonando"
– Agente en el estado "En conversación"
– Agente en el estado "Tratamiento posterior"
– Agente en el estado "Llamada perdida"
– Agente en el estado "Tiempo excedido"

17.1.2.1.1 Cómo añadir una Excepción en CCV

Si desea aplicar otras reglas en determinados momentos (Pausa, Fin de semana, Festivo, Vacaciones, etc.), puede asignarlas al plan horario correspondiente como reglas de excepción como CCV de excepción. De esta forma, se puede definir cómo se administrarán las llamadas entrantes, por ejemplo, durante las vacaciones. Los planes horarios vacacionales tienen prioridad frente a otros planes horarios y reglas.

Paso a paso

1) Vaya a **Modo experto > Aplicaciones > OpenScape Business UC Suite**.
2) Haga clic en **Planes horarios**, seleccione uno de los horarios disponibles y haga clic en **Editar**.

Puede hacer clic en **Agregar** para crear un Nuevo plan horario.

3) Haga clic en **Agregar** en el área **Excepciones**.
4) Rellene el campo **Descripción**, si lo desea.
5) Seleccione el tipo de excepción entre las opciones disponibles:

- **Dentro del intervalo de hora**: seleccione una hora, un día y una recurrencia específicos para la excepción
- **Dentro del intervalo de fecha y hora**: seleccione una fecha, hora, día y recurrencia específicos para la excepción
- **Planes horarios vacacionales**: seleccione una fecha específica de vacaciones para la excepción
- **Repetición anual**: seleccione si la excepción se repetirá cada año

6) Haga clic en **Guardar**.

17.1.2.2 Plantillas

Las siguientes plantillas son plantillas estándar y preconfiguradas para el Company AutoAttendant (UC Suite), que se pueden modificar en caso necesario según las necesidades específicas.

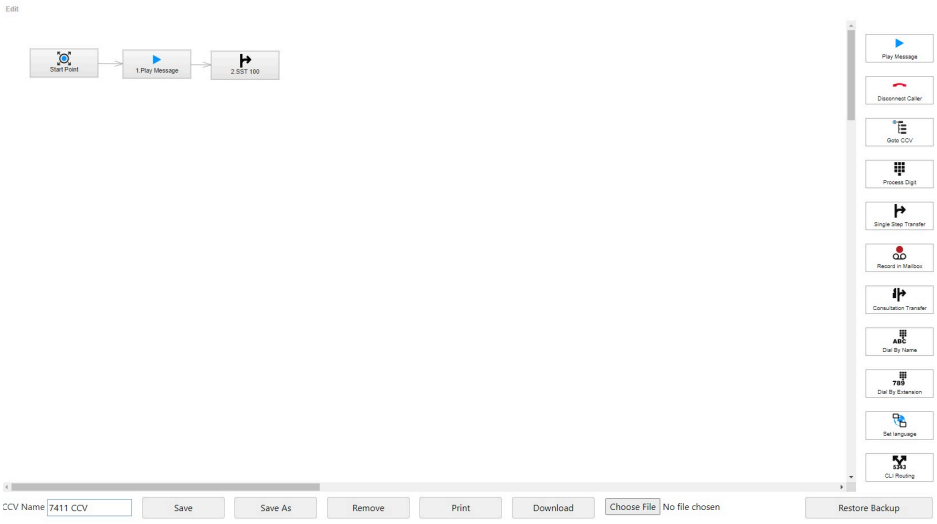
Plantilla 1 - 7410 CCV: Llamada con conmutación (sin correo de voz)

El llamante escucha la reproducción de un anuncio grabado. A continuación, se le indica que pulse una tecla (de cifra) y se le transfiere a una extensión. Si el llamante no pulsa ninguna tecla, se le transfiere al puesto de interceptación (valor predeterminado 100).



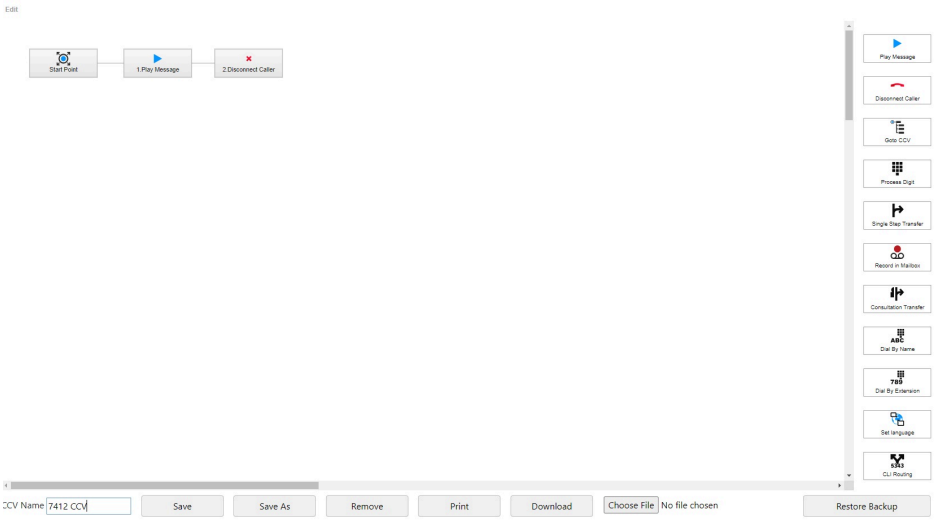
Plantilla 2 - 7411 CCV: Anuncio antes de responder

El llamante escucha la reproducción de un anuncio grabado. A continuación se le desvía al puesto de interceptación 100.



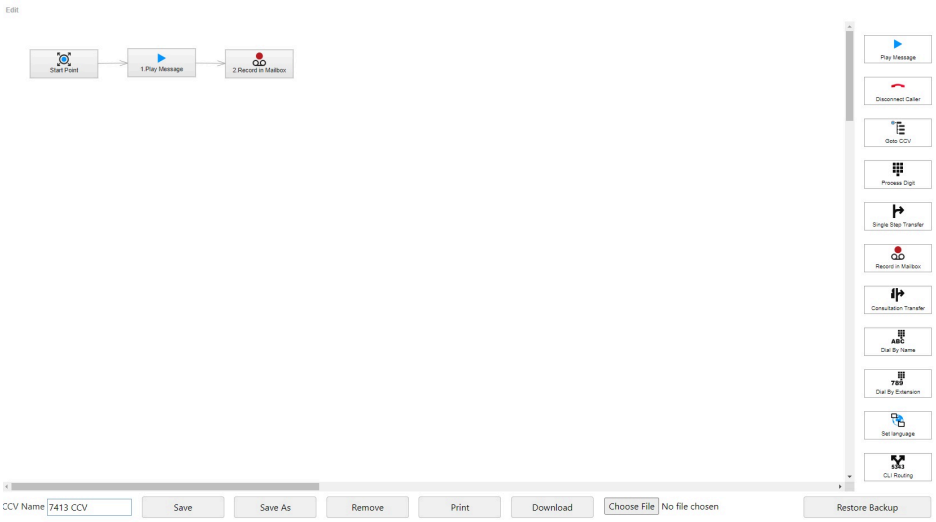
Plantilla 3 - 7412 CCV: Horario fuera del horario comercial

Si se realiza una llamada entrante fuera del horario de oficina, se reproduce un anuncio grabado al llamante. A continuación se interrumpe la conexión.



Plantilla 4 - 7413 CCV: Llamada fuera del horario comercial con transferencia automática diferida a un buzón de voz

Si se realiza una llamada entrante fuera del horario de oficina, se reproduce un anuncio grabado al llamante. A continuación, el llamante puede grabar y dejar un mensaje en un buzón de voz.



17.2 OpenStage Attendant

Las funciones de conmutación se pueden ejecutar con un teléfono OpenStage con una configuración especial. El OpenStage Attendant sirve al mismo tiempo como puesto de interceptación.

Distribución del teclado

Al OpenStage Attendant llegan todas las llamadas que no tienen opción de marcación directa o en las que no se ha localizado ninguna extensión que cumpla los criterios de asignación de llamadas (Interceptación). El personal de conmutación retransmite entonces las llamadas entrantes a las extensiones deseadas.

Se pueden utilizar como Attendant estos teléfonos OpenStage:

- OpenStage 30
- OpenStage 40
- OpenStage 60
- OpenStage 80

Si hay configurado un teléfono OpenStage como puesto de operadora, las teclas de función programables están asignadas del siguiente modo:

- Servicio nocturno
- Listín telefónico
- Llamadas en espera
- Intercalar
- Retener
- Externo 1
- Externo 2 (no con OpenStage 40)
- (Tecla vacía, no preasignada) (no con OpenStage 40)

17.3 OpenScape Business Attendant

OpenScape Business Attendant ofrece funciones de conmutación e integra un listín telefónico para OpenScape Business. OpenScape Business Attendant se puede ampliar mediante la interconexión, para mostrar informaciones de presencia y BLF a nivel de red.



Funciones de conmutación importantes:

- Administrar llamadas contestadas y pendientes
- Datos de la llamada activa
- Llamadas aparcadas y retenidas
- Lista de llamadas
- Diario de llamadas aceptadas, perdidas y salientes
- Buzón de voz personal

Aplicación de listín:

- Contactos Outlook
- LDAP (Conexión mediante OpenDirectory Service)
- Directorio personal

Estado del campo de lámparas de ocupado:

- Libre, Ocupado, En una llamada, Desviado

Visibilidad de presencia:

- oficina, reunión, enfermo, pausa, fuera de oficina, vacaciones, pausa de mediodía, en mi domicilio

  Nota: El estado de presencia “enfermo” puede no estar disponible, según la configuración del sistema realizada por el administrador.

- Cambiar el estado de presencia para las extensiones del nodo propio (por ahora, no para extensiones de otros nodos)

Hay dos "estilos" diferentes disponibles para personalizar la interfaz de usuario de OpenScape Business Attendant.

Se pueden conectar como máx. ocho OpenScape Business Attendant por cada sistema de comunicación (máx. ocho licencias por cada OpenScape BusinessX1/X3/X5/X8 y OpenScape Business S).

OpenScape Business Attendant tiene licencia a través de WBM.

Requisitos técnicos

- PC con Windows estándar
- Terminal Server se puede emplear con teléfonos HFA (para obtener información sobre los requisitos, consulte Requisitos para los clientes de PC de UC Suite)
- Interfaz USB o LAN, en función del terminal utilizado
- Pantalla con una resolución mín. de 1024x768, opcional una segunda pantalla para mostrar el segundo BLF
- Tarjeta gráfica con color de 16 bits (mín. 256 colores)
- Acceso a Internet para soporte y actualizaciones

Sistema operativo

- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bits o 64 bits)
- Microsoft Windows Vista (32 bits)
- Microsoft Windows Server 2015 (32 bits / 64 bits) como Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bits / 64 bits) como Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bits) como Microsoft Terminal Server

El soporte de OpenScape Business Attendant para Microsoft Windows XP y Microsoft Windows Server 2003 termina al mismo tiempo que la asistencia de Microsoft. El producto seguirá soportado, pero ya no se harán pruebas exhaustivas.

Teléfonos compatibles

- OpenStage 40/60/80 HFA
- openStage 30T/40T/60T/80T
- OpenScape DeskPhone CP 100/200/205/400/600/600E/700/700X
- OpenScape DeskPhone CP 110/210/410/710

Nota: En el caso de OpenScape DeskPhone CP 200/205/210, el nombre del usuario no se muestra en una llamada externa.

Sigue habiendo compatibilidad parcial para dispositivos más antiguos (por ejemplo, optiPoint 410/420/500). Consulte cuáles son los dispositivos probados y autorizados en las notas de la versión correspondientes.

Conexión Plug and Play sencilla en la instalación

OpenScape Business Attendant se configura inicialmente mediante un asistente. que abre los cuadros de configuración necesarios.

p. ej.:

- Consulta del tipo de terminal
- Consulta y comprobación del acceso al sistema
- Consulta y comprobación de posibles interredes
- Integración automática de los BLF.

17.3.1 OpenScape Business BLF

Buy Lamp Field (panel de lámparas de ocupado) de OpenScape Business BLF es una aplicación independiente para indicar estados de ocupado. Funciones adicionales son la indicación y la definición del estado de presencia, y el establecimiento de conexión para el teléfono asignado.

Requisitos técnicos

Funciones esenciales:

- OpenScape Business BLF se puede ampliar y se puede personalizar
  - de 10 a 350 campos BLF (botones de usuario), en función de la resolución de pantalla
- Funciones de teléfono
  - Marcar
  - Aceptar llamadas
  - Desconectar
- Definir el estado de presencia (para la extensión propia)
- Listín telefónico (Listín del sistema)
- Diario de llamadas

Para el funcionamiento de cada OpenScape Business BLF se requiere una licencia OpenScape Business BLF y una licencia UC User.

- PC con Windows estándar
- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bits o 64 bits)
- Microsoft Windows Vista (32 bits)
- Microsoft Windows Server 2015 (32 bits / 64 bits) como Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bits / 64 bits) como Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bits) como Microsoft Terminal Server
- Pantalla con una resolución mínima de 1024x768
- Tarjeta gráfica con color de 16 bits (mín. 256 colores)
- Interfaz LAN
- Ratón y teclado estándar
- Acceso a Internet para soporte y actualizaciones

17.3.2 Ejemplos de configuración para OpenScape Business Attendant y OpenScape Business BLF

En los siguientes capítulos encontrará ejemplos para la configuración general de OpenScape Business Attendant y OpenScape Business BLF.

17.3.2.1 Escenario 1: OpenScape Business Attendant conectado a un sistema único OpenScape Business

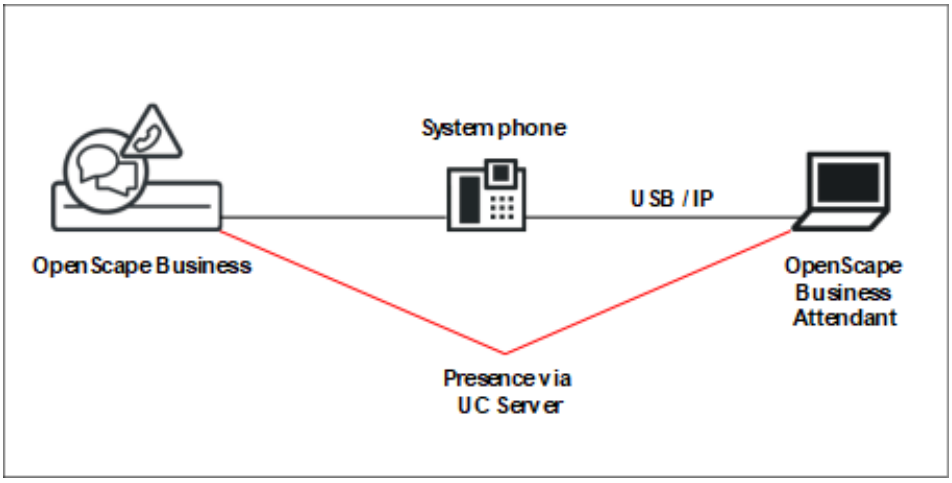
Requisitos previos

Hay licencia para OpenScape Business Attendant

Terminal con licencia válida

Licencia para UC Smart o UC Suite para información de presencia (opcional)

La dirección IP para usar la interfaz de servicio web (WSI, "Web Service Interface) es diferente según se use UC Smart o la UC Suite. En el caso de UC Smart, WSI siempre se ejecuta en el sistema de comunicación; para UC Suite, por el contrario, se ejecuta en la placa de aplicación o en el servidor de aplicaciones (consulte UC Smart y UC Suite). Si Booster Server está en uso, se debe usar la dirección IP del Booster Server, y si OCAB está en uso, se debe usar la dirección IP de OCAB. Solo se debe usar la IP del sistema de comunicación cuando estos componentes no están conectados.



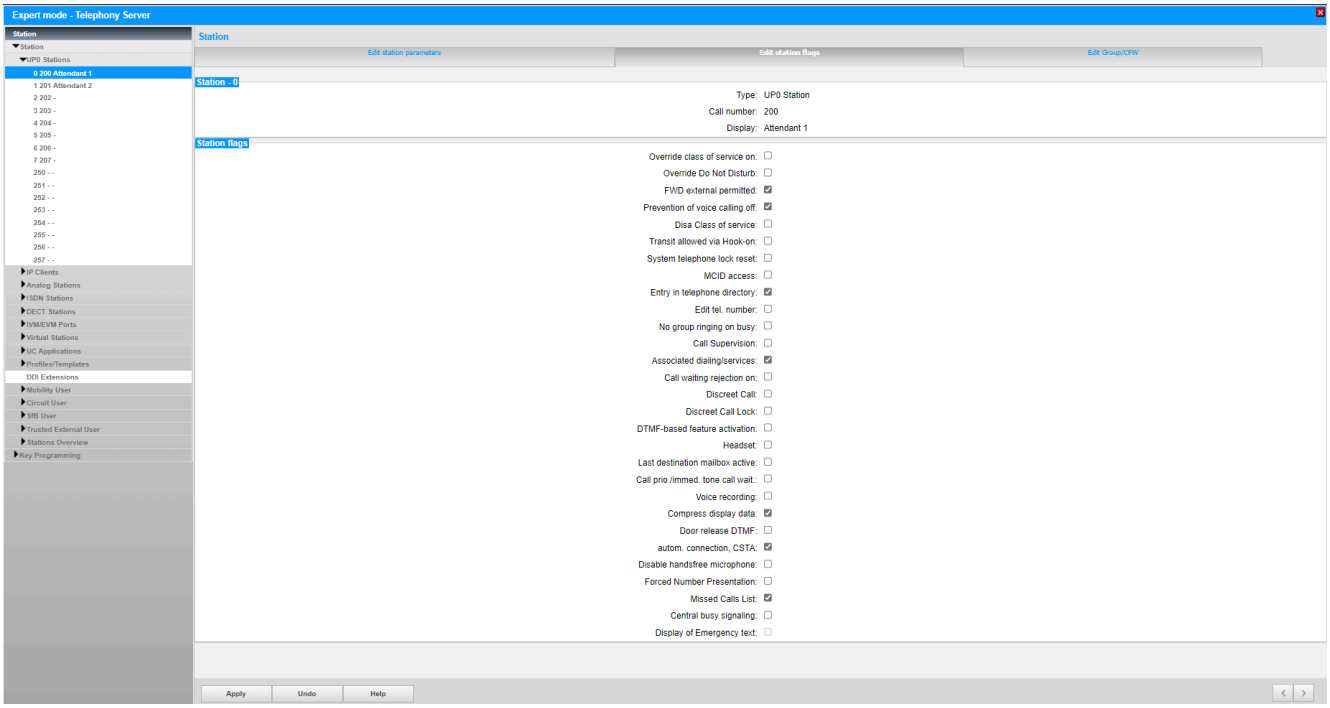
Paso a paso

1) Configure una estación como operadora mediante WBM o Manager E (optiPoint 500, OpenStage 30T, 40T, 60T, 80T u OpenStage 40HFA, 60HFA, 80 HFA).

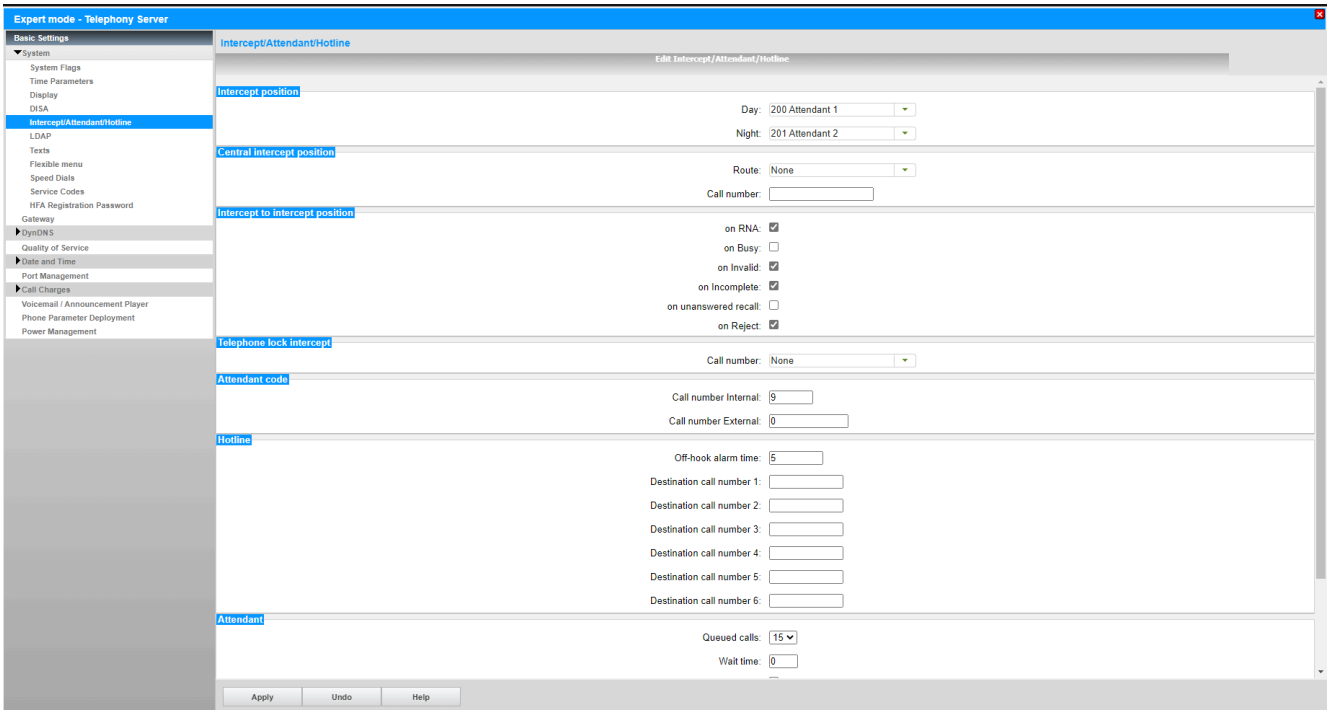
   Consejo: No se admite el uso de teléfonos SIP o CMI.

2) Active la prestación **Servicios asociados**. Es necesario en OpenScape Business Attendant, para activar y desactivar prestaciones para otras extensiones.

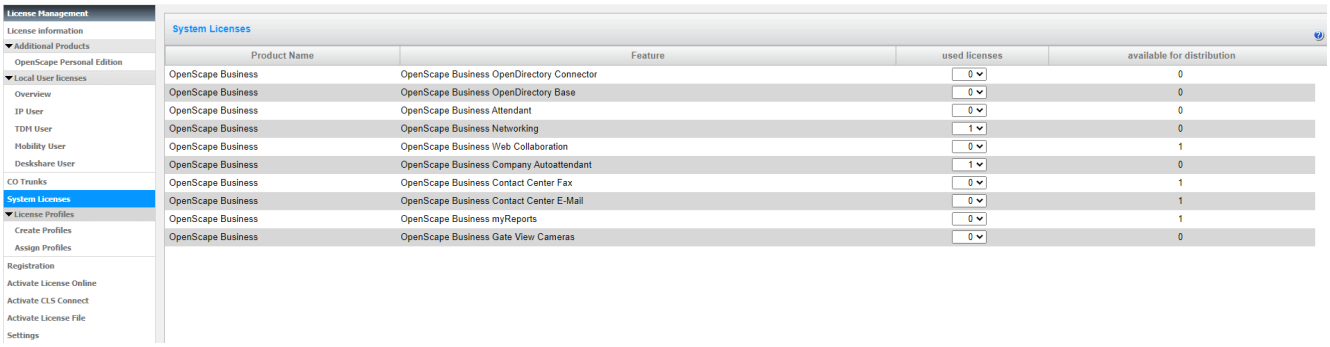
3) Activar **Anular No molestar** y deshabilite **Rechazo de llamada en espera activado**.



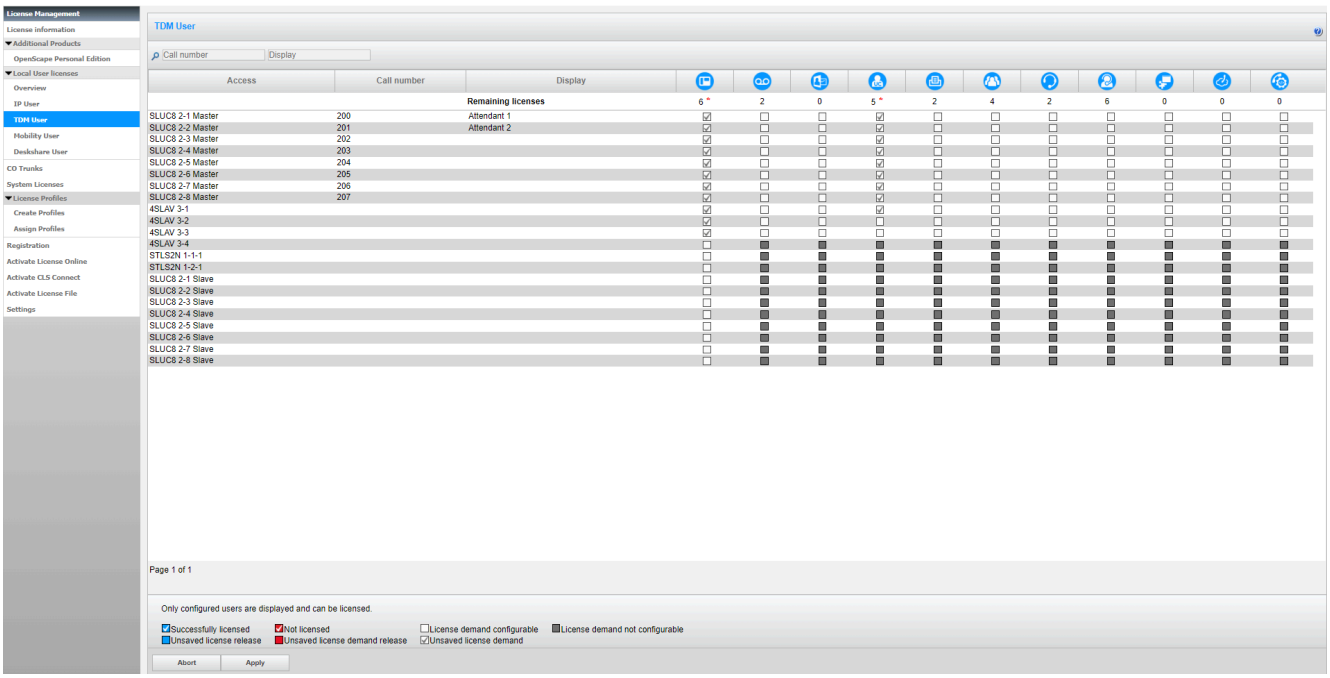
4) Configure criterios de interceptación y códigos de puesto (defina las opciones de interceptación y los números de teléfono del puesto de operadora).



5) Registro de licencia de OpenScape Business Attendant



6) Licencia del estado de presencia



7) Opcional: Al configurar un Attendant como extensión IP, en el teléfono hay que configurar una contraseña para el acceso de usuarios.

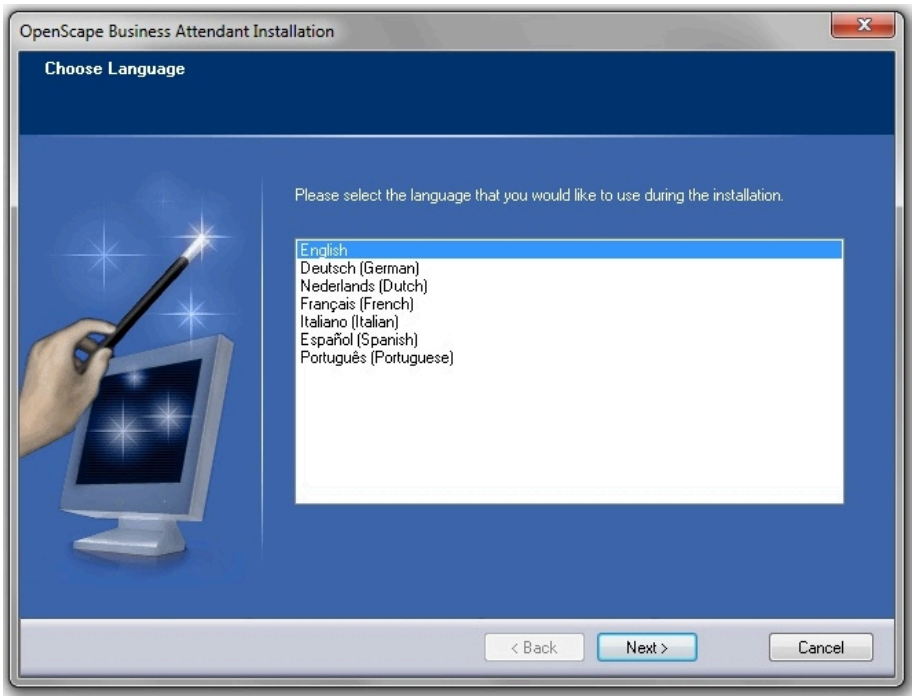


8) Instalar el controlador USB

USB - Controlador COM (CallBridge) para optiPoint 500, OpenStage 30T y OpenStage 40T

USB - Controlador RNDIS para OpenStage 60T y OpenStage 80T

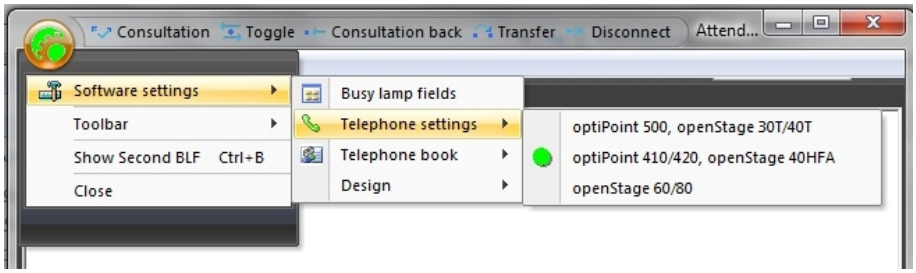
9) Instalar OpenScape Business Attendant con la rutina de instalación (aceptar el Acuerdo de licencia, indicación de la ubicación de almacenamiento y del idioma de OpenScape Business Attendant).

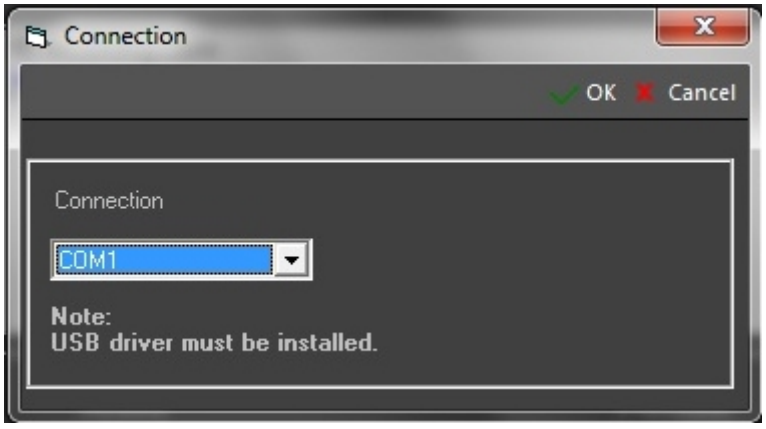


Después de la instalación y de iniciar por primera vez el programa, se inicia automáticamente el asistente de configuración inicial, que consulta estos ajustes:

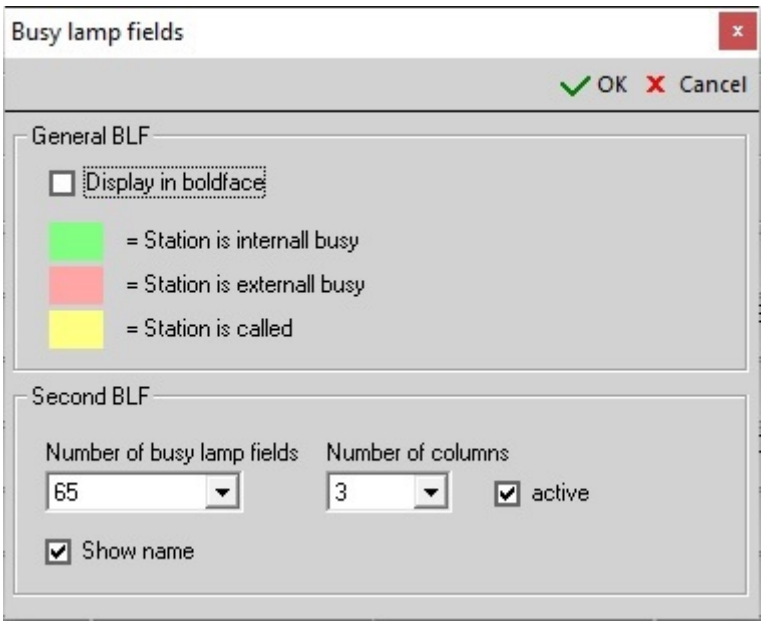
- Tipo de teléfono
- Si se quiere utilizar la función de presencia

Configuración para el acceso en el Attendant:

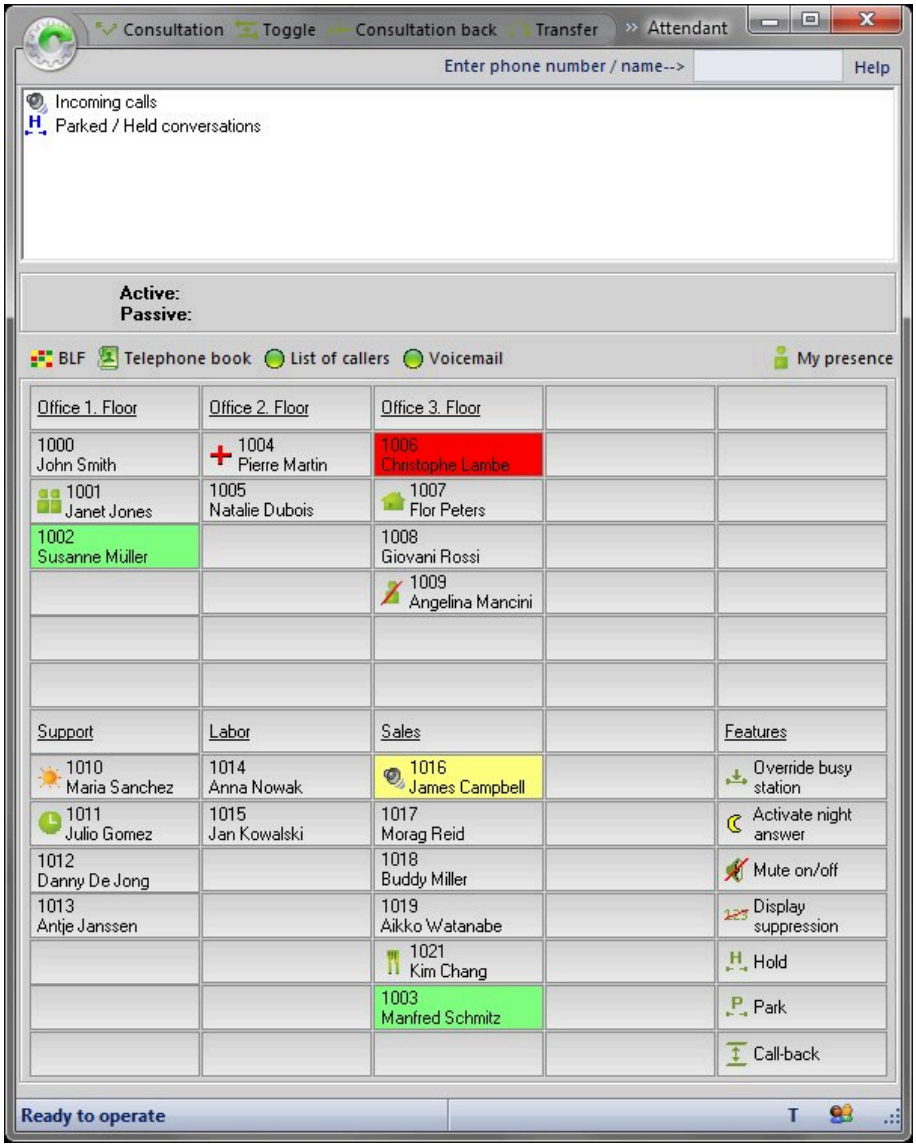




Después de iniciar sesión en el sistema de comunicación es posible llenar automáticamente el BLF.



Consejo: Asigne o compruebe la configuración de seguridad (http o https) en la Gestión basada en Web (WBM).



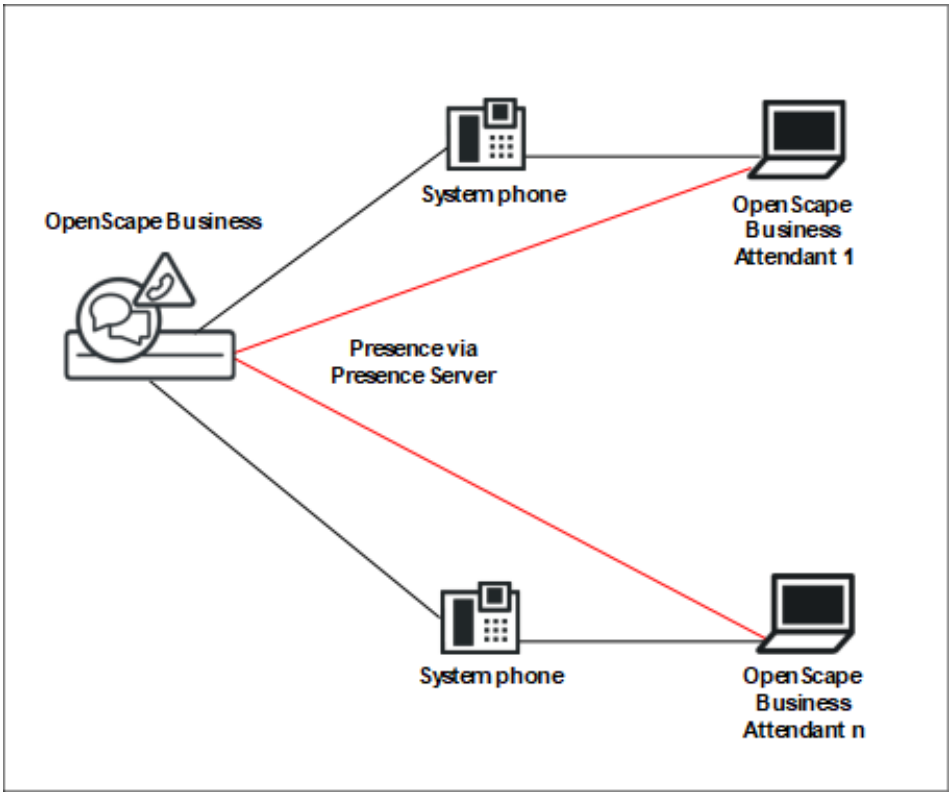
17.3.2.2 Escenario 2: Dos o más OpenScape Business Attendant con un sistema individual OpenScape Business

Requisitos previos

Además de los definidos en el escenario 1, hay que cumplir estos requisitos:

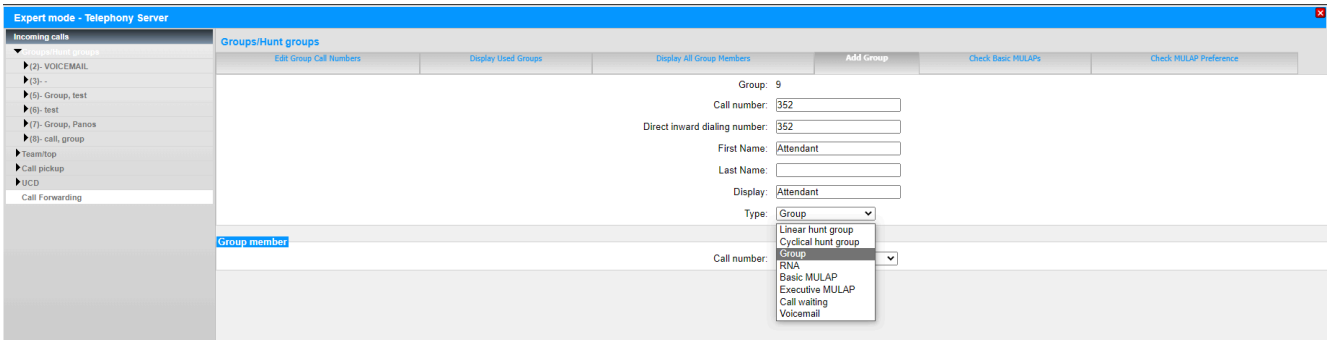
Licencias suficientes para UC Smart o UC Suite para información de presencia (opcional)

Configuración de grupos

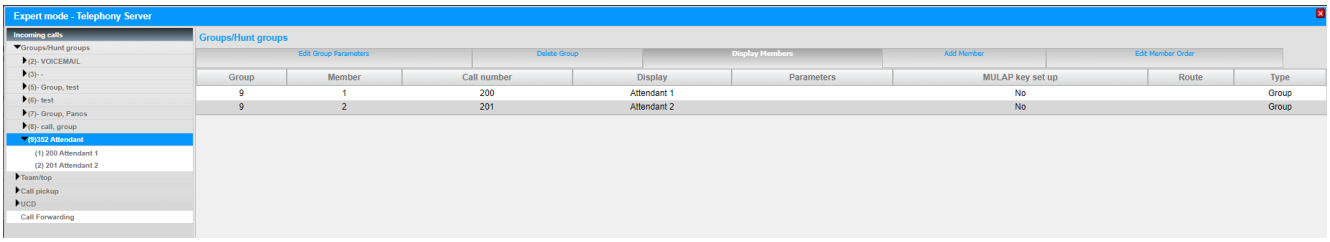


Paso a paso

1) Configuración de una extensión como Attendant mediante la Gestión basada en Web (WBM) (véase el ejemplo de configuración 1).
2) Defina un grupo; se pueden utilizar líneas colectivas (lineales y cíclicas) y grupos de llamada.



3) Asigne los Attendants (de las extensiones correspondientes) al grupo.



Consejo: Configure criterios de interceptación y códigos de puesto (defina las opciones de interceptación y los números de teléfono del puesto de operadora). En estos casos, el puesto de interceptación es el número de teléfono del grupo.

17.3.2.3 Escenario 3: Interconexión de OpenScape Business con Attendants OpenScape Business propios (estado de presencia y BLF a nivel de red mediante WSI)

Requisitos previos

Licencia de UC Smart para información de presencia (opcional)

Solo se pueden utilizar varios Attendants OpenScape Business en redes UC Smart. El WSI (servidor de presencia de OpenScape Business) proporciona estados de conexión e información de presencia a nivel de red. Las redes UC Suite necesitan myAttendant para la funcionalidad a nivel de red.

17.3.2.4 Escenario 4: Interconexión de OpenScape Business con el Attendant central de OpenScape Business (estado de presencia y BLF a nivel de red mediante WSI)

Requisitos previos

Licencia de UC Smart para información de presencia (opcional)

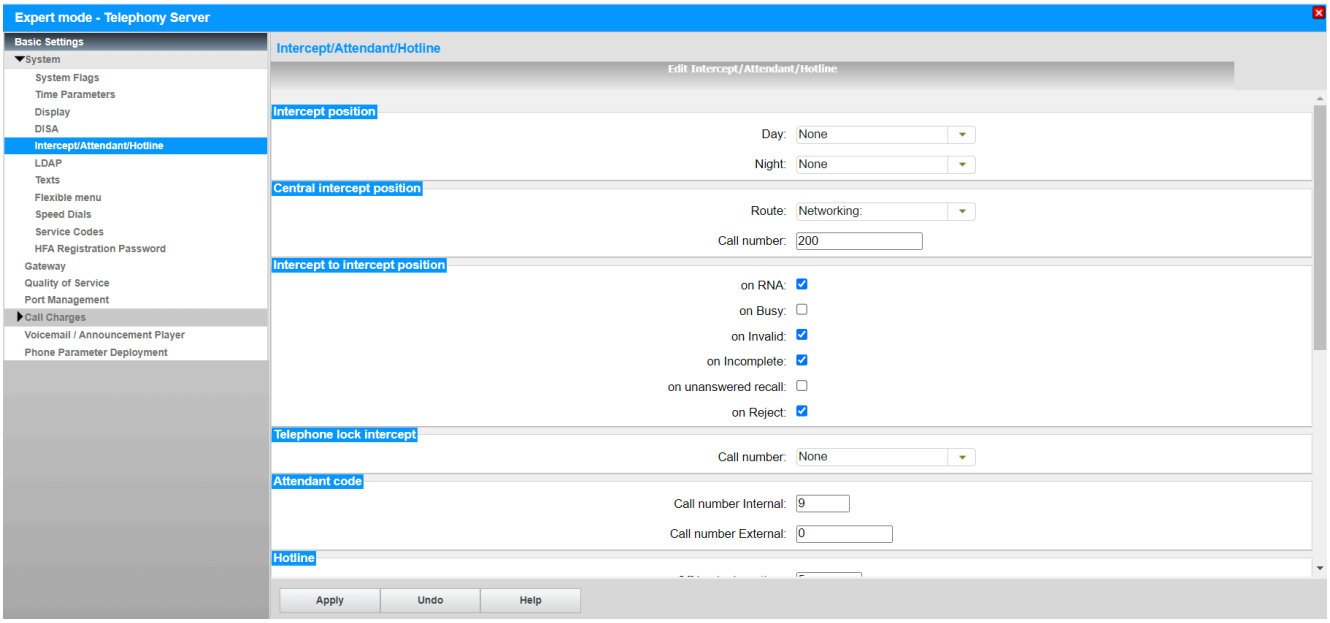
Sólo se pueden utilizar varias operadoras OpenScape Business en redes UC-Smart. El WSI (servidor de estado de presencia de OpenScape Business) proporciona estados Hook para toda la red e información sobre presencia. Las redes UC-Suite necesitan myAttendant para funcionar en toda la red.

Puesto de interceptación central (en el nodo en el que no haya configurado ningún OpenScape Business Attendant)

Paso a paso

1) Configuración de OpenScape Business Attendant según el ejemplo de configuración 1.

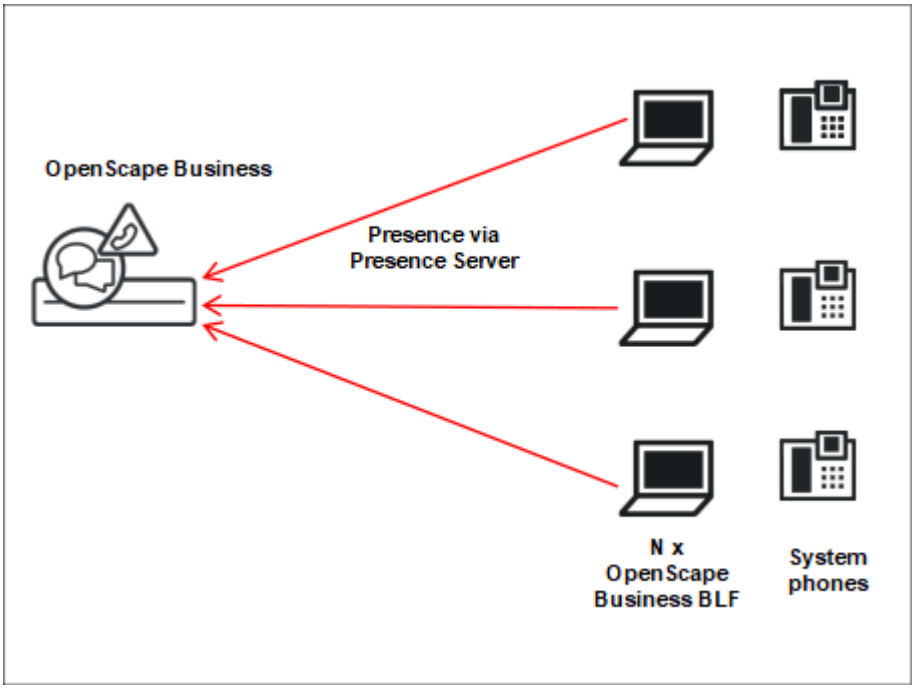
2) En el nodo (en el que no haya configurado ningún OpenScape Business Attendant) registre el puesto de interceptación central.



17.3.2.5 Escenario 5: OpenScape Business BLF conectado a un sistema individual OpenScape Business

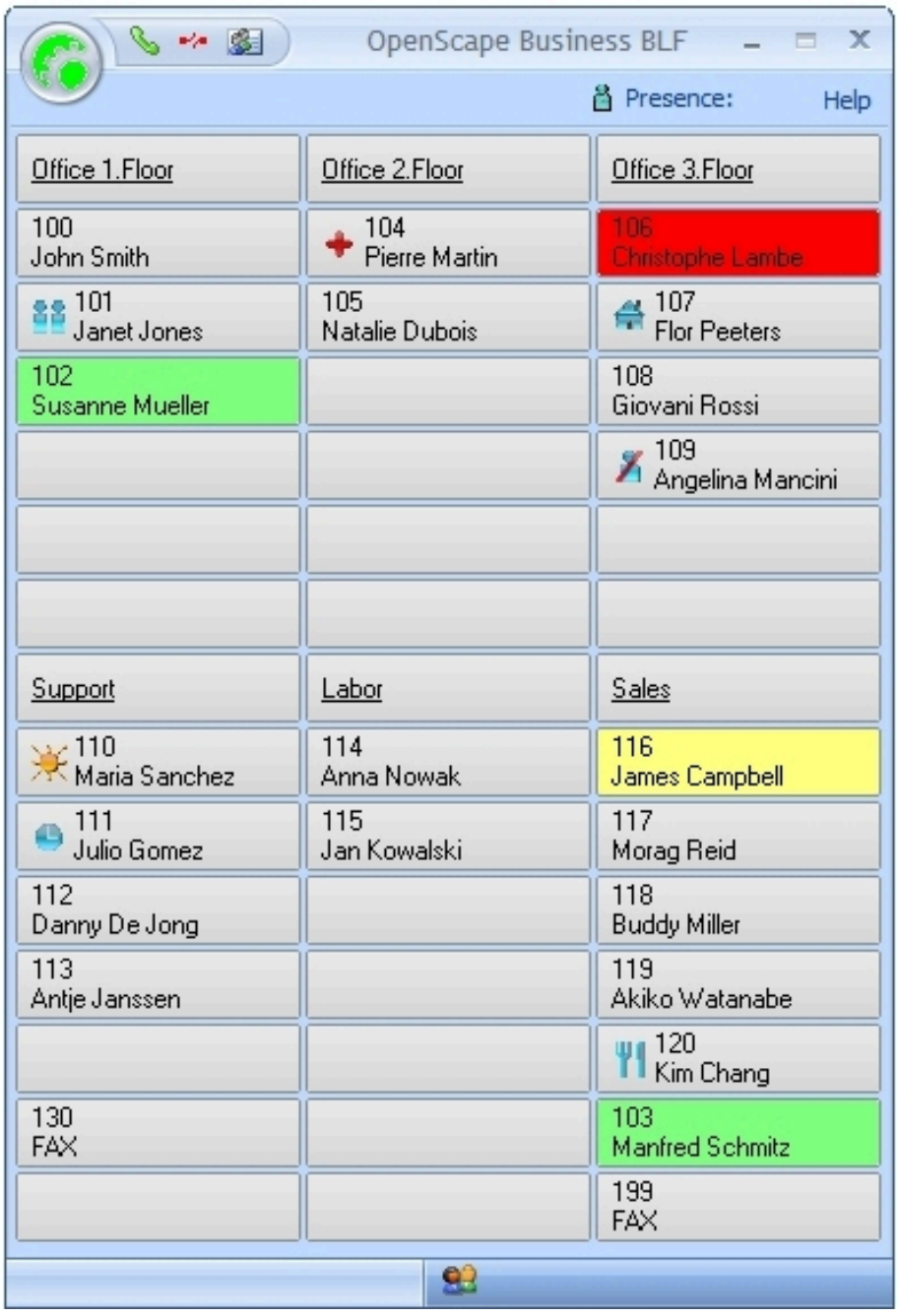
Requisitos previos

- Hay disponible una licencia OpenScape Business BLF por cada extensión
- Los teléfonos ya están asignados
- Hay disponible una licencia UC User para cada extensión telefónica



Paso a paso

1) Configurar teléfonos mediante WBM
2) Configurar el servidor de presencia mediante Gestión basada en Web (WBM)
3) Instalar e iniciar OpenScape Business BLF
4) Después de iniciar el sistema por primera vez, se realiza (opcional) la asignación automática del OpenScape Business BLF.



17.3.2.6 Escenario 6: OpenScape Business BLF conectado en una interred OpenScape Business (estado de presencia y BLF mediante WSI)

Requisitos previos

- Hay disponible una licencia de OpenScape Business-BLF por cada extensión
- Los teléfonos ya están asignados
- Hay disponible una licencia UC User para cada extensión
- OpenScape Business BLF se puede usar en redes UC Smart, pero no en redes UC Suite. El WSI (servidor de estado de presencia de OpenScape Business) proporciona estados Hook para toda la red e información sobre presencia.

Paso a paso

1) Configurar teléfonos mediante WBM

2) Instalar e iniciar OpenScape Business BLF

3) Después de iniciar el sistema por primera vez, se establece conexión con WSI y el BLF se asigna de forma manual. En este caso, el BLF se puede ocupar con extensiones a nivel de red.

17.4 myAttendant

myAttendant le ofrece amplias funciones de conmutación. Las extensiones se administran cómodamente mediante botones de usuario. Para la transmisión de mensajes (mensajes de voz, fax, mensajes instantáneos, SMS y correo electrónico) dispone del centro de mensajes.

Funciones de conmutación esenciales

Por cada sistema de comunicación (por nodo de red) se pueden conectar 20 myAttendant como máximo. La ampliación máxima de una interred es la suma de las capacidades de los sistemas de comunicación interconectados. El estado de presencia y el estado del teléfono se muestran para todas las extensiones de la red. En el centro de mensajes de myAttendant se muestran las extensiones del sistema de comunicación propio.

- Administrar llamadas contestadas y pendientes
- Se muestran datos de la llamada activa
- Se muestran las llamadas aparcadas y retenidas
- Lista de llamadas
- Diario para llamadas pendientes, programadas, internas, externas, respondidas, perdidas y salientes
- Aplicación de listín
  - LDAP (p. ej. ODS)
  - Listín personal/Contactos Outlook
  - Directorio interno, con interconexión de todas las extensiones de la red.

- Estado del campo de lámparas de ocupado de todas las extensiones internas del sistema propio y todas las extensiones de la red
  - Estado del teléfono: libre, ocupado, llamado, desviado, no molestar
  - Estado de presencia: oficina, CallMe, reunión, enfermo, pausa, fuera de oficina, vacaciones, pausa de mediodía, en cada (a nivel de red)

  Nota: El estado de presencia “enfermo” puede no estar disponible, según la configuración del sistema realizada por el administrador.
- Hay tres estilos de interfaz para elegir.
- Se pueden conectar como máximo 20 myAttendant por cada sistema de comunicación (máx. 20 licencias por cada OpenScape Business X3/X5/X8 y OpenScape Business S). El registro de licencia de myAttendant se hace con la gestión WBM.

Requisitos técnicos (para obtener información detallada, véase la información de ventas)

- PC con Windows estándar
- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bits o 64 bits)
- Microsoft Windows Vista (32 bits)
- Se puede utilizar Terminal Server

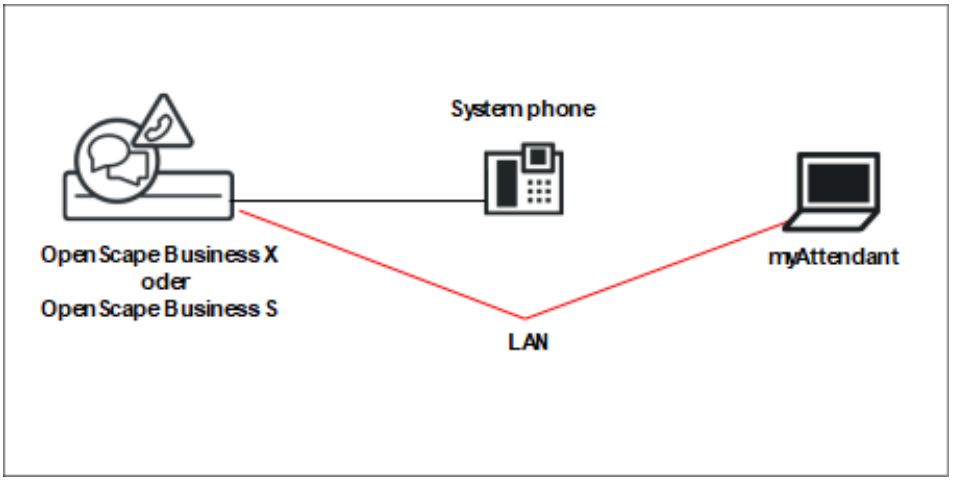
Software adicional

- Debe estar instalado Oracle Java 8 o superior o, como alternativa, OpenJDK 8 (véase **Centro de servicios** > **Software**)

Teléfonos compatibles

- OpenStage 40/60/80 HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/410/710 HFA
- SIP phones con RFC 3725 soporte, e.g., OpenScape Desk Phone IP 35G/55G SIP, OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X SIP, OpenScape Desk Phone CP 110/210/410/710 SIP
- OpenStage 30T/40T/60T/80T

Sencillo Plug and Play en la instalación; el sistema envía al usuario (si ha configurado su dirección de correo) los primeros pasos de la instalación.



17.4.1 Administración de extensiones

Para la administración de extensiones en myAttendant están disponibles los botones de usuario, el directorio interno, el directorio externo y el directorio personal.

Botones de usuario

Los botones de usuario se encuentran en la pestaña **Estándar** y forman parte de la ventana principal de myAttendant.

En una pestaña de botones de usuario hay disponibles 100 botones de usuario. Puede cambiar el número predeterminado de botones de usuario por pestaña cuando lo desee.

De forma predeterminada, los botones de usuario están ordenados alfabéticamente por apellidos.

Se pueden configurar varias pestañas para botones de usuarios. Los nombres de los botones son libres.

A los botones de usuario se les pueden asignar extensiones internas y externas, y contactos personales (usuarios).

17.4.2 Centro de mensajes

En el **Centro de mensajes** de myAttendant se administran y registran los mensajes de voz y fax, los mensajes instantáneos, SMS y correos electrónicos.

Se pueden administrar los mensajes de otras extensiones. No obstante, éstas deberán concedido el permiso requerido.

En la lista de extensiones aparecen enumeradas todas las extensiones del sistema de comunicación, con su estado de presencia/ausencia. En la parte superior, aparece su estado propio con un resumen de mensajes desplegado. Siguen las demás extensiones en orden alfabético.

En función de la selección realizada en el resumen de mensajes aparece información sobre los mensajes. Esta información se presenta en forma de tabla y permite seleccionar los mensajes para proceder a su edición.

Los distintos tipos de mensajes se pueden editar de esta forma:

- Los **mensajes de voz** se pueden escuchar, eliminar y reenviar,
- Los **Mensajes LAN** se pueden leer, modificar y borrar.
- Los **mensajes de fax** se pueden reenviar.

Mensajes LAN

Solo los usuarios de myAttendant pueden crear mensajes LAN. Sirven como una especie de "tablón de notas" para el usuario, para que pueda dejar anotaciones (sobre las distintas extensiones). Estos mensajes se pueden ver, modificar o borrar, pero no se pueden enviar a otras extensiones.

17.4.3 Escenario 1: Cómo configurar myAttendant en un sistema individual OpenScape Business

Requisitos previos

Hay una licencia para myAttendant

Teléfono con licencia válida

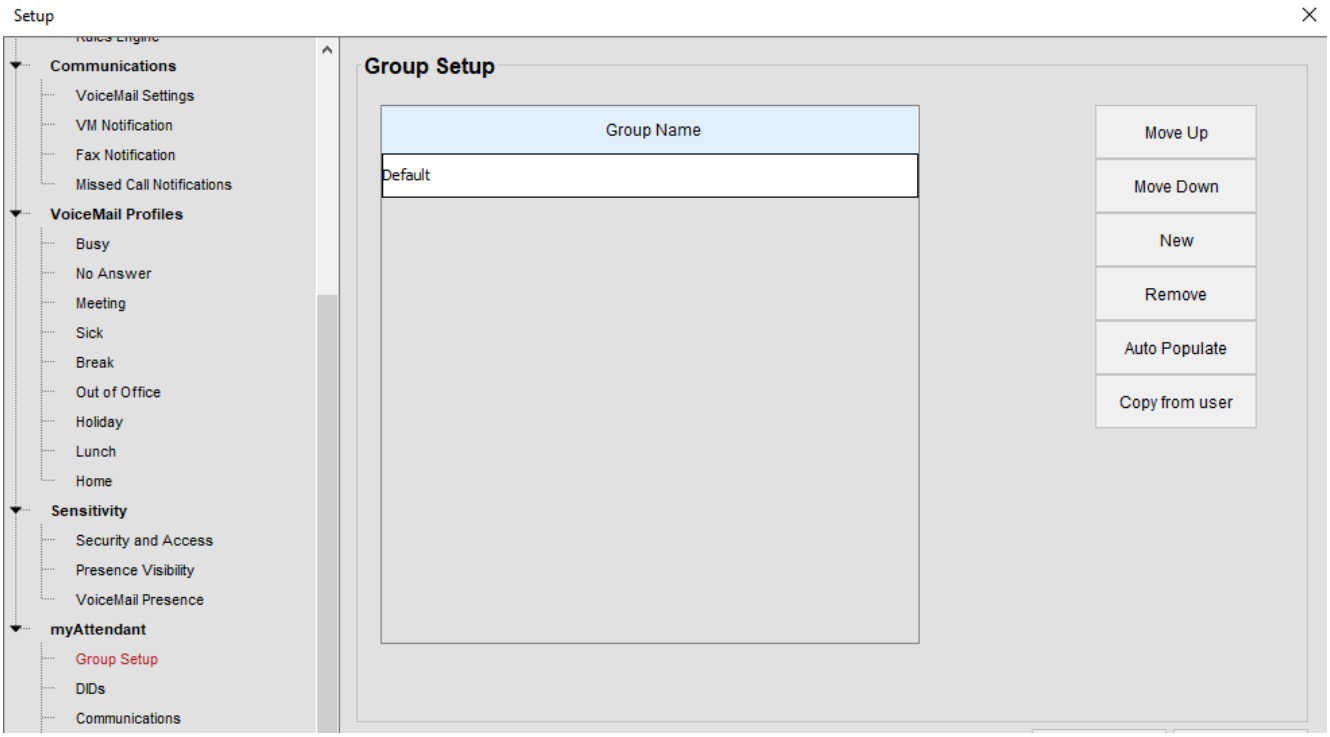
Servidor de aplicaciones o Tablero de aplicaciones disponible

La UC Suite está activada con el asistente de instalación básica

Paso a paso

1) Configurar un teléfono para el puesto de operadora mediante la Gestión basada en Web (WBM)
2) Desactive el **Bloqueo de avisos de llamada en espera** en el **Modo Experto**, en **Extensiones**>**Clientes IP**>**Clientes de sistema**>**Extensiones**>**Editar flags de extensión**.
3) Active la función de **Aviso de llamada en espera inmediato para llamadas de puesto de operadora** en el **Modo Experto** en **Servidor de telefonía**>**Configuración básica**>**Sistema**>**Interceptación**>**Puesto de operadora**>**Hotline**.
4) Compruebe o modifique los criterios de interceptación y los códigos de posición (definición de las opciones de interceptación y de los números de teléfono para el puesto de operadora).
5) Registro de licencia de myAttendant

6) Después de iniciar sesión en el sistema de comunicación es posible llenar automáticamente el BLF. Esto se puede configurar en myAttendant en **Configuración > myAttendant > Configuración de grupo**.



17.4.4 Escenario 2: Cómo configurar uno o varios myAttendant en un sistema individual OpenScape Business

El escenario 2 se basa en el escenario 1 y se construye por ampliación.

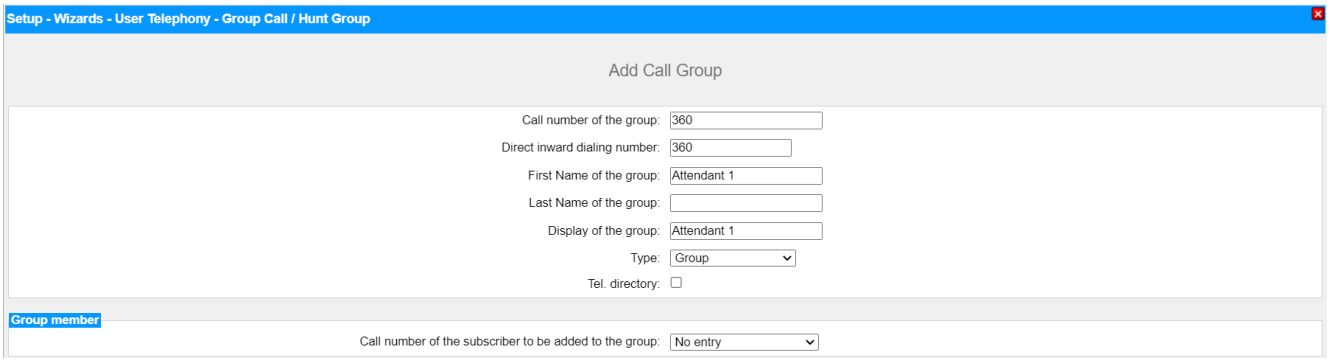
Requisitos previos

Licencias suficientes para myAttendant

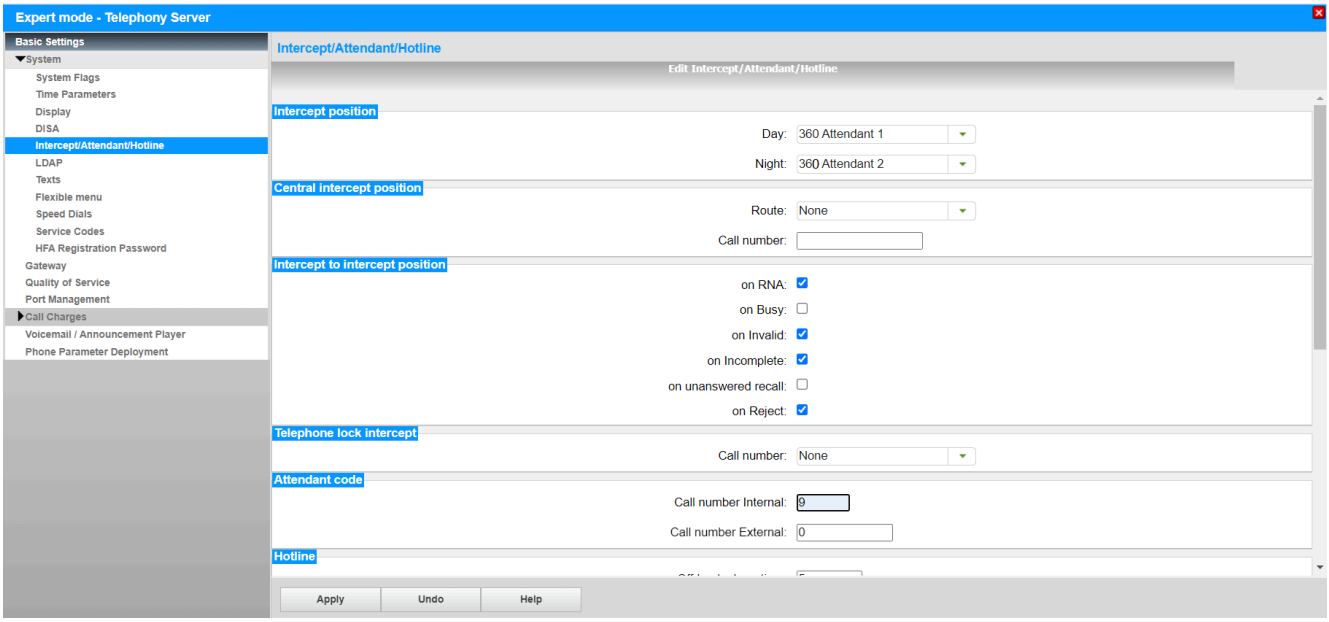
Teléfono con licencia válida

Paso a paso

1) Configure un grupo (formado solo por puestos de operadora) en el WBM en **Configuración** > **Telefonía de Usuario** > **Llamada de grupo / Línea colectiva** >**Añadir**.



2) Seleccione este grupo al configurar los teléfonos de puesto de operadora OpenSgate.



17.4.5 Escenario 3: Cómo configurar una interconexión OpenScape Business con myAttendant central

El escenario 3 se basa en el escenario 1 y 2 y se configura por ampliación. El nodo 1 está vinculado al nodo 2. El puesto de operadora central está en el nodo 2.

Requisitos previos

Hay suficientes licencias para myAttendant

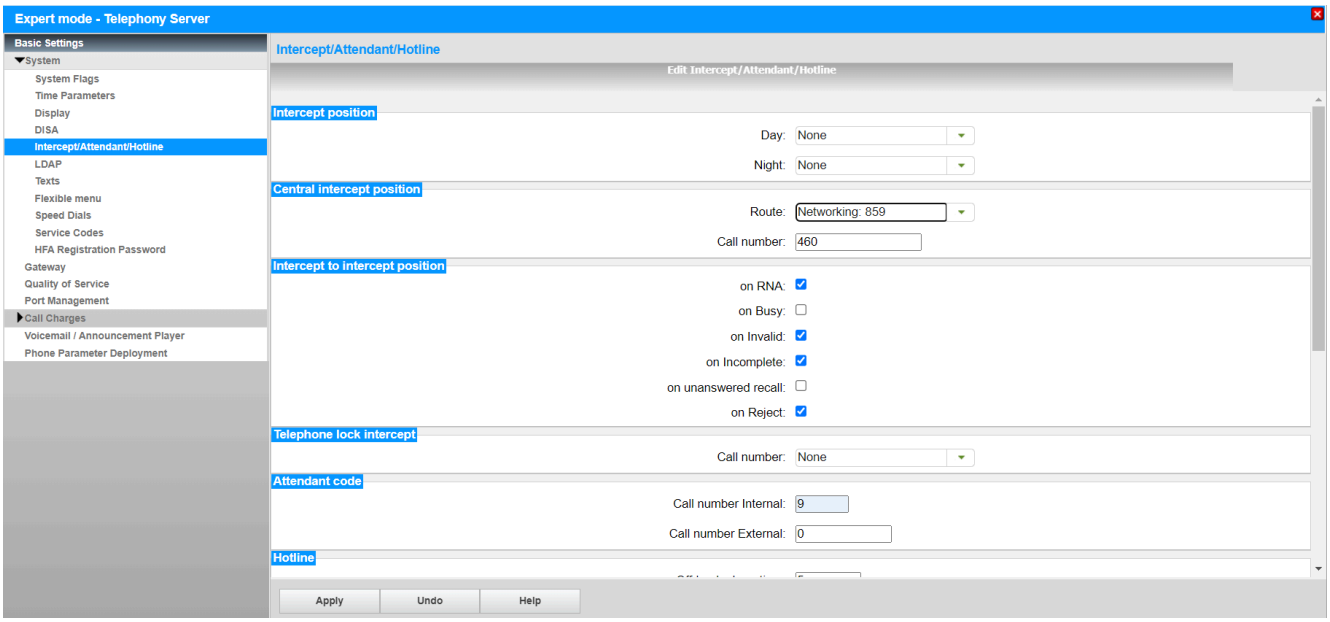
Hay licencias para la interconexión

Teléfono con licencia válida

LCR está configurado

Paso a paso

1) Establezca una posición de interceptación central en el nodo 1. El puesto de interceptación central debe crearse en un nodo en el que NO haya configurado ningún puesto de operadora.



2) Configure el puesto de operadora para el sistema 2 (tal y como se describe en el escenario 2).
3) Instale myAttendant con los datos de usuario del nodo 2.

17.5 Puesto de interceptación

El sistema de comunicación permite desviar llamadas externas que no están asignadas a ningún usuario o a las que no se responde a un puesto de interceptación definido para que no se pierda ninguna llamada. Puede configurar los criterios de interceptación como administrador.

El puesto de interceptación puede ser una extensión individual, un grupo o un equipo de anuncios grabados:

- Puesto de interceptación (Puesto de operadora)
- Extensiones
- Línea colectiva
- Grupos MULAP
- Llamada de grupo
- Equipo de anuncios grabados externo

Como puesto de interceptación no se puede seleccionar un grupo UCD.

Si se ha configurado un puesto de interceptación, en caso de interceptación las llamadas se desvían a este puesto de interceptación. Si no se ha configurado ningún puesto de interceptación, las llamadas interceptadas se señalizan en la primera extensión IP.

Si una extensión interna está configurada como puesto de interceptación, se le asigna automáticamente la ocupación de teclas predeterminada. Además, se puede autorizar al puesto de interceptación para la prestación "Intercalación".

Como administrador puede asignar un código del puesto de operadora (2 posiciones) para el puesto de interceptación para comunicaciones internas y externas. A través de ese código se puede acceder directamente al puesto de interceptación.

Una interceptación actúa a nivel de sistema, es decir, en las centrales compartidas se aplica por igual a todas las extensiones. Véase también "Puesto de interceptación central en la interred" del capítulo Interconexión.

Criterios de interceptación

A través de los criterios de interceptación, el administrador establece en qué situaciones se debe proceder a una interceptación. Estos son los posibles criterios de interceptación:

- En caso de libre

  La llamada sigue las entradas de la Gestión de llamadas (Call Management) (p.ej., una transferencia automática diferida configurada). Si ningún usuario acepta la llamada, se transfiere al puesto de interceptación.
- En caso de ocupado, si ya no es posible la transferencia diferida

  Se comprueba en primer lugar si se puede efectuar o no el aviso de llamada en espera. Si no se puede efectuar el aviso de llamada en espera, la llamada sigue las entradas de la Gestión de llamadas (Call Management) (p.ej., una transferencia automática diferida configurada). Si ningún usuario acepta la llamada, se transfiere al puesto de interceptación. La Interceptación en caso de ocupado solo se refiere a la primera llamada, no a llamadas conmutadas o a enlaces salientes. La llamada recordatoria de una extensión externa no se intercepta inmediatamente en una extensión de destino ocupada, sino que se indica con aviso de llamada en espera.
- En caso de marcación errónea

  Si el número de teléfono marcado no está configurado o activo.
- En caso de marcación incompleta

  Si el número marcado es demasiado corto. Si hay un puesto de interceptación central, no se evalúa la marcación incompleta.
- En caso de llamada recordatoria no atendida

  Si después de la transferencia antes de contestar no se consulta una llamada externa y después de la llamada recordatoria al destino original tampoco resulta ninguna contestación, se efectúa una interceptación después de transcurrido el tiempo establecido.
- Con llamada rechazada

  Si la llamada ha sido rechazada por una extensión interna, la llamada sigue las entradas de la Gestión de llamadas (Call Management) (p.ej. una transferencia automática diferida configurada). Si ningún usuario acepta la llamada, se transfiere al puesto de interceptación.
- En caso de número de llamada no existente

  Como en caso de marcación errónea.
- En caso de transferencia diferida de llamada con encadenamiento

  Si una llamada desviada se encuentra con otro desvío de llamadas en el destino del desvío y, de esta forma, se supera la cantidad de interconexiones autorizadas, se realiza una interceptación. interceptación. El número de interconexiones depende de las entradas de la transferencia automática diferida, como máximo se permiten tres interconexiones.

- En caso de candado telefónico

  Si un usuario marca un código de ruta en un teléfono que tenga activado el candado telefónico, se produce una interceptación. Para este tipo de casos, el administrador establece un destino de interceptación independiente.
- Con anuncio grabado (solo con UC Suite)

  Si un usuario marca el código de puesto de operadora (2 posiciones) mientras escucha un anuncio grabado del buzón de voz o del puesto de operadora automático (AutoAttendant), se produce una interceptación. Para este tipo de casos, el administrador establece un destino de interceptación independiente.

Dependencias

Tema	Dependencia
Llamadas de datos	Las llamadas de datos no se interceptan sino que se cortan.
Línea colectiva	En una línea colectiva no se lleva a cabo la interceptación. La llamada se vuelve a transferir a la primera extensión, es decir, queda siempre dentro de la línea colectiva.
Ocupación de teclas predeterminada	La ocupación de teclas predeterminada contiene además la tecla **Indicar cantidad de llamadas**. Esta solo puede asignarse en 6 terminales. Cuando se ha alcanzado el límite ya no se asignan más ocupaciones de teclas predeterminadas. La programación de las teclas predeterminadas no se borra cuando un terminal ya no está definido como puesto de interceptación.
Líneas S_0	La evaluación de líneas S_0 solo tiene lugar cuando no se ha establecido ningún puesto de interceptación de día/noche.
Servicio nocturno	A fin de conseguir alcanzar el mismo destino tanto desde líneas con marcación directa como desde líneas analógicas mientras está activado el servicio nocturno, deben ser idénticos los valores introducidos de Interceptación > PO y de **Número de llamada nocturno** en **Asignación de llamadas por línea**.

17.5.1 Cómo configurar criterios de interceptación y puesto de interceptación

Con el asistente **Puesto de operadora** puede configurar los números de teléfono del puesto de interceptación y criterios de interceptación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Puesto de operadora**.
4) En las secciones **Puesto de operadora** y **Código del puesto de operadora** (2 dígitos), establezca los números de teléfono deseados para el puesto de interceptación.
5) En la sección **Criterios de interceptación**, establezca los valores deseados.
6) Haga clic en**OK & Continuar** y, a continuación, en **Salir**.

17.5.2 Cómo configurar puesto de interceptación central

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **Interceptación/PO/Hot-line**.
4) En la sección **Puesto de interceptación central**, dentro de la lista desplegable **Ruta**, seleccione la entrada deseada.
5) En el área **Puesto de interceptación central** introduzca el **Número de teléfono** deseado para **Día** y **Noche**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

17.5.3 Cómo configurar la interceptación en caso de candado telefónico

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **Interceptación/PO/Hot-line**.
4) En la sección **Interceptación en caso de candado telefónico**, dentro de la lista desplegable **Número de teléfono**, seleccione la entrada deseada.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

17.5.4 Cómo configurar interceptación en caso de anuncio grabado

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor** en el menú contextual.
4) Haga clic en la pestaña **Ajustes generales**.
5) Introduzca el número de teléfono del puesto de interceptación en el campo **Número de destino** de la sección **Núm. de tel. de puesto de interceptación**.
6) Haga clic en **Guardar** y cierre la ventana.

18 Multimedia Contact Center

El Contact Center es una potente solución para la distribución y tratamiento de llamadas, faxes y correos electrónicos entrantes. La distribución inteligente y basada en capacidades garantiza que los llamantes se pongan en contacto con el agente de Contact Center más cualificado, independientemente del medio de contacto. La aplicación myReports ofrece a los agentes de Contact Center cómodas funciones para la edición y el tratamiento posterior de llamadas, faxes y correos electrónicos. myReports ofrece numerosas plantillas de informe para la evaluación del servicio de Contact Center.

El Multimedia Contact Center está totalmente integrado en el software de la UC Suite. Se incluyen todos los componentes de software necesarios. Las funciones de Contact-Center se liberan a través de licencias.

El Contact Center utiliza los recursos del sistema de comunicación como, por ejemplo, colas de espera para llamadas entrantes y funciones de Comunicaciones Unificadas para la grabación y reproducción de anuncios grabados.

Los componentes de software centrales del Contact Center controlan todas las funciones de encaminamiento para llamadas, faxes y correos electrónicos entrantes, además controla los puestos de trabajo de PC conectados mediante LAN de los agentes y los tableros.

En los puestos de trabajo de PC de los agentes se instala la aplicación myAgent. De forma opcional, también se puede instalar la aplicación myReports para generar y enviar informes. El software necesario se puede descargar directamente en el área de descarga del sistema de comunicación para instalarlo en el PC cliente.

Mediante la Gestión basada en Web (WBM) se realiza la configuración de las funciones básicas de Contact Center, de los planes horarios, de las reglas de distribución y de los agentes. Los ajustes de configuración para el servicio diurno del Contact Center (por ejemplo, la asignación de agentes a las colas de espera) también se pueden realizar directamente mediante myAgent.

Si el Contact Center no está disponible (caída, error de conexión u otros problemas), se puede implementar una solución de respaldo mediante la función UCD del sistema de comunicación. Se debe atender a las reglas de distribución para el servicio de emergencia al configurar los grupos UCD durante la configuración inicial del Contact Center.

Consejo: Puede consultar información sobre la UC Suite y las funciones de Comunicaciones Unificadas en el capítulo sobre la UC Suite.

18.1 Clientes de Contact Center

A través de la aplicación myAgent, los agentes de Contact Center disponen de cómodas funciones para la edición y el tratamiento posterior de llamadas, faxes y correos electrónicos. A través de la aplicación integrada myReports, se pueden generar informes sobre llamadas, colas, agentes, rendimiento, nivel de servicio y códigos de tratamiento posterior del Contact Center. Hay disponibles más de 100 plantillas de informe predefinidas.

18.1.1 myAgent

Todos los agentes disponen, a través de myAgent, de cómodas funciones para la edición y tratamiento posterior de llamadas, faxes y correos electrónicos.

myAgent ofrece las siguientes prestaciones:

- Procesamiento de
  - Realizar llamada
  - Faxes
  - Correos electrónicos
- Función de devolución de llamadas para agentes
- Indicación y modificación del estado de agentes
- Indicación y modificación del estado de presencia de las extensiones internas del sistema de comunicación
- Presentación de las colas de espera en tiempo real
- Grabación de llamadas, siempre que la opción esté activada en el sistema de comunicación
- Mensajería instantánea
- Solicitud de asistencia mediante
  - Supervisión de llamadas (en función del país)
  - Intercalación de llamadas
  - Mensajería instantánea
- Integración del directorio interno, del directorio externo, del directorio offline externo (LDAP) y de contactos Outlook para buscar nombres
- Creación de informes sobre la base de plantillas de informe predefinidas

En función del nivel de clase de servicio asignado, los agentes dispondrán de funciones estándar (Agente) o avanzadas (Supervisor o Administrador) en myAgent (véase Funciones en función de la clase de servicio para agentes).

La asignación de agentes a colas de espera se realiza mediante la aplicación myAgent. Esta asignación solo la pueden realizar los agentes con el nivel de clase de servicio Supervisor o Administrador. Es posible asignar a los agentes las siguientes propiedades (Asignación de agentes). Estas propiedades influyen en la distribución de llamadas, faxes y correos electrónicos dentro de una cola:

- **Agente principal** o **Agente de desbordamiento**

  Llamadas se distribuyen homogéneamente entre los agentes principales. Los agentes de desbordamiento solo reciben llamadas si las llamadas han superado un determinado número o si una llamada ha superado un determinado tiempo de espera en cola.
- **Activar devolución de llamada de agente**

  La devolución de llamadas de agente permite a un llamante de la cola dejar un mensaje de voz para los agentes. En cuanto un agente está disponible, recibe una llamada, escucha el mensaje de voz del llamante y puede devolverle la llamada.
- **Nivel de habilidad**

  El nivel de habilidad controla la distribución de llamadas entre agentes en una cola: los agentes con un nivel de habilidad alto tienen la prioridad en la distribución. Cuando todos los agentes tienen el mismo nivel de habilidad, el agente que lleve más tiempo libre recibirá la llamada.

- **Tiempo de actividad**

  El tiempo de actividad permite a los agentes realizar tareas administrativas después de finalizar una llamada y antes de recibir la siguiente.
- **Desbordamiento tras llamadas en cola**

  Los agentes de desbordamiento reciben las llamadas que superan el número máximo.
- **Desbordamiento tras segundos en cola**

  Los agentes de desbordamiento reciben las llamadas que superan este tiempo de espera.

La zona **Lista de asignaciones de agentes** muestra a los agentes con la clase de servicio Supervisor o Administrador, qué agentes están asignados a cada cola. Los agentes con la clase de servicio Agente solo pueden ver las colas a las que están asignados.

18.1.2 Requisitos para myAgent

Para poder utilizar myAgent, el PC cliente de la extensión debe tener un equipamiento de software y hardware adecuado.

Consejo: Siga siempre las indicaciones del archivo `Readme first`, que puede encontrar en el directorio de almacenamiento de los archivos de instalación.

Teléfonos

myAgent se puede utilizar junto con los siguientes teléfonos:

- OpenStage HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/410/710 HFA
- OpenStage T
- OpenScape Personal Edition HFA
- OpenStage M3 (OpenScape Business inalámbrico)
- Teléfono OpenScape DECT S6/SL6/R6 (OpenScape Business inalámbrico)

Se admiten dispositivos más antiguos (como optiPoint 410/420/500 y Gigaset M2/SL3/S4/SL4/S5). No se pueden operar dispositivos Optiset E. myAgent no se puede utilizar con extensiones SIP, Mobility o virtuales, con grupos ni con extensiones MULAP. En las notas de la versión puede consultar cuáles son los teléfonos comprobados y autorizados.

Sistemas operativos

myAgent se puede utilizar junto con los siguientes sistemas operativos:

- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bits o 64 bits)
- Microsoft Windows Vista (32 bits)

Consejo: El sistema operativo utilizado requiere siempre la última versión de todas las actualizaciones disponibles (Service Packs y parches).

El soporte de myReports para Microsoft Windows XP y Microsoft Windows Server 2003 finalizará al mismo tiempo que la asistencia de Microsoft. El producto seguirá soportado, pero ya no se harán pruebas exhaustivas.

Software adicional

- Debe estar instalado Oracle Java 8 o superior o, como alternativa, OpenJDK 8 (véase **Centro de servicios** > **Software**)
- Adobe Reader 9 o superior (para informes en formato PDF)

Requisitos mínimos de hardware

- 2 GHz CPU
- RAM: 2GB
- LAN de 100 MBit/s
- Resolución de pantalla XGA (1024x768), myPortal for Outlook: Resolución de pantalla SVGA (800x600)

Microsoft Terminal Server, Citrix XenApp Server

myAgent puede ejecutarse en entornos Microsoft Terminal Server y Citrix Server siempre que se cumplan los requisitos indicados a continuación:

Consejo: Los entornos de Terminal Server y CitrixServer (incluidos entornos virtuales y de Hosted Services) son responsabilidad del cliente.

Consejo: Los entornos Citrix-Server no pueden decodificar correctamente algunos caracteres regionales (p.ej., las diéresis del alemán).

Sistemas operativos:

- Microsoft Windows Server 2015 (32 bits / 64 bits) como Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bits / 64 bits) como Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bits) como Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bits) con Citrix XenApp 6.5 Server (modo escritorio)

El soporte de myAgent para Microsoft Windows XP y Microsoft Windows Server 2003 finalizará al mismo tiempo que la asistencia de Microsoft. El producto seguirá soportado, pero ya no se harán pruebas exhaustivas.

Requisitos de hardware: El número de clientes que se pueden instalar depende del rendimiento del servidor y de la memoria de trabajo disponible. Si en el servidor se utilizan otras aplicaciones hay que atender a su consumo de memoria de trabajo.

Puede obtener más información sobre la configuración en Citrix XenApp Server en:

`http://wiki.unify.com/wiki/OpenScape_Business`.

Archivos de instalación

Para poner los archivos de instalación a disposición de los usuarios existen las siguientes opciones:

- El administrador Servicio los archivos de instalación desde el **Centro de servicios** y los pone a disposición de los usuarios (por ejemplo, a través de una unidad de red).

Siga las indicaciones del archivo `ReadMe first`, que puede encontrar en el directorio de almacenamiento de los archivos de instalación.

Consejo: No se admite la distribución automática del archivo MSI a través de un servicio de implementación con Microsoft Windows Server.

18.1.3 myReports

Los agentes con el nivel de clase de servicio Supervisor o Administrador pueden crear informes sobre agentes y sus actividades, llamadas, colas, rendimiento, nivel de servicio y códigos de tratamiento posterior con myReports.

myReports ofrece las siguientes prestaciones:

- Más de 100 plantillas de informe predefinidas y ordenadas por áreas temáticas (grupos de informes) para la creación de informes
- Planes horarios para la creación controlada por tiempo de informes
- Envío inmediato o controlado por tiempo de informes por correo electrónico
- Exportación de informes controlada por tiempo
- Formatos de salida para la vista preliminar de informes, correos electrónicos enviados e informes exportados: Excel, PDF y Word
- Vista previa de informes para comprobar si los informes se van a crear en el formato de salida deseado.

Roles de usuario

myReports tiene una administración de usuarios propia que regula el acceso a las funciones de myReports mediante roles de usuario. Se diferencia para ello entre usuarios de myReports (usuarios estándar) y administrador de myReports.

Su rol de usuario actual se establece en el inicio de sesión en myReports.

Las diferencias entre los roles de usuario se resumen en la siguiente tabla.

myReports:	**Rol de usuario**	
Acción	myReports Usuario	myReports Administrador
Informes		

myReports: Acción	Rol de usuario	
	myReports Usuario	myReports Administrador
Vista preliminar de informe	X	X
Enviar informes por correo electrónico de forma inmediata	X	X
Agregar plantilla de informe	X	X
Borrar plantilla de informe agregada	X	X
Definir nueva plantilla de informe		X
Actualizar plantillas de informe predefinidas		X
Planes horarios		
Agregar plan horario	X	X
Mostrar un plan horario	X	X
Editar plan horario	X	X
Borrar plan horario	X	X
Configuración		
Cambiar el idioma de la interfaz de usuario	X	X
Modificar el color de la interfaz de usuario	X	X
Configurar una plantilla de correo electrónico	X[7]	X
Cómo modificar la dirección de servidor	X	X
Cambiar la contraseña de administrador		X
Configurar prefijos para números de teléfono externos		X
Activar o desactivar la protección de datos		X
Configurar el lugar de almacenamiento para la exportación de informes controlados por tiempo		X
Configurar idioma		X[8]
Configurar idioma estándar		X[8]

7 Es necesario introducir la contraseña de administrador para configurar la plantilla de correo electrónico

8 Para configurar el idioma y el idioma estándar es necesario iniciar sesión como administrador de myReports con una contraseña especial.

18.1.3.1 Cómo restablecer la contraseña de administrador de myReports

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor**.
4) Haga clic en **Mantenimiento**.
5) Haga clic en **Restablecer contraseña**, en la sección **Informes**.

Pasos siguientes

Informe al administrador o administradores de myReports de que ha restablecido la contraseña del administrador al valor por defecto `reports`.

18.1.4 Requisitos para myReports

Para poder utilizar myReports, el PC cliente de la extensión debe tener un equipamiento de software y hardware adecuado.

Consejo: Siga siempre las indicaciones del archivo `ReadMe first`, que se ubica en el directorio de almacenamiento de los archivos de instalación.

Sistemas operativos

myReports se puede utilizar junto con los siguientes sistemas operativos:

- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bits o 64 bits)
- Microsoft Windows Vista (32 bits)

Consejo: El sistema operativo utilizado requiere siempre la última versión de todas las actualizaciones disponibles (Service Packs y parches).

El soporte de myReports para Microsoft Windows XP y Microsoft Windows Server 2003 finalizará al mismo tiempo que la asistencia de Microsoft. El producto seguirá soportado, pero ya no se harán pruebas exhaustivas.

Software adicional

- Oracle Java 8 o superior, o bien OpenJDK 8 (véase**Service Center** > **Software**)
- Adobe Reader 9 o superior (para informes en formato PDF)
- Microsoft Excel 16 / 2013 / 2010 (para informes en formato Excel)
- Microsoft Word 16 / 2013 / 2010 (para informes en formato Word)

Requisitos mínimos de hardware

- CPU de 2 GHz
- RAM: 2 GB
- LAN de 100 Mbit/s (LAN de 1 Gbit/s recomendada)
- Resolución de pantalla XGA (1024x768), myPortal for Outlook: resolución de pantalla SVGA (800x600)

PC multiusuario

En Microsoft Windows 7 con PC multiusuario y Microsoft Windows Vista con PC multiusuario, todos los usuarios locales pueden utilizar myReports con su configuración personalizada si el primer usuario local lo instala con derechos de administración locales. Solo el primer usuario local con derechos de administración locales puede realizar una actualización mediante actualización automática (AutoUpdate).

Microsoft Terminal Server, Citrix XenApp Server

myReports puede ejecutarse en entornos Microsoft Terminal Server y Citrix Server siempre que se cumplan los requisitos indicados a continuación:

Consejo: Los entornos de Terminal Server y CitrixServer (incluidos entornos virtuales y de Hosted Services) son responsabilidad del cliente.

Consejo: Los entornos Citrix-Server no pueden decodificar correctamente algunos caracteres regionales (p.ej., las diéresis del alemán).

Sistemas operativos:

- Microsoft Windows Server 2015 (32 bits / 64 bits) como Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bits / 64 bits) como Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bits) como Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bits) con Citrix XenApp 6.5 Server (modo escritorio)

Requisitos de hardware: el número de clientes que se pueden instalar depende del rendimiento del servidor y de la memoria de trabajo disponible. Si en el servidor se utilizan otras aplicaciones hay que atender a su consumo de memoria de trabajo.

Puede obtener más información sobre la configuración en Citrix XenApp Server en:

`http://wiki.unify.com/wiki/OpenScape_Business`.

Archivos de instalación

Para poner los archivos de instalación a disposición de los usuarios existen las siguientes opciones:

- El administrador descarga los archivos de instalación desde el **Centro de servicios** y los pone a disposición de los usuarios (por ejemplo, a través de una unidad de red).

Siga las indicaciones del archivo `ReadMe first`, que puede encontrar en el directorio de almacenamiento de los archivos de instalación.

Consejo: No se admite la distribución automática del archivo MSI a través de un servicio de implementación con Microsoft Windows Server.

18.1.5 Observaciones sobre el uso simultáneo de myAgent y clientes de UC Suite

Si se utiliza de forma simultánea myAgent y clientes de UC Suite mediante una cuenta de usuario de UC Suite, no puede excluirse la posibilidad de que se afecten mutuamente.

En esta sección, el término myPortal se utiliza para hacer referencia a myPortal for Desktop, myPortal for Outlook, myPortal @work y myPortal to go.

Ejemplos de influencia mutua:

- modificar estado de presencia mediante myPortal

  Los ejemplos se aplican al ajuste estándar **Mensaje de voz** para todos los destinos de reenvío.

  – myAgent: el agente ha iniciado sesión.

    myPortal: el restablecimiento automático del estado de presencia a Oficina está desactivado.

    Si se modifica el estado de presencia mediante myPortal, se cierra inmediatamente la sesión del agente de las colas de espera. Cuando el agente inicia sesión a través de myAgent, el estado de presencia de myPortal se vuelve a establecer en **Oficina**.

    Si el estado del agente se modifica mediante myAgent (por ejemplo, **Pausa**) se registra con myPortal, a excepción de **Inicio de sesión**, **Finalizar sesión** y **Tiempo de actividad**.

  – myAgent: el agente ha iniciado sesión.

    myPortal: el restablecimiento automático del estado de presencia a Oficina está activado.

    Si el agente modifica su estado mediante myAgent a **Pausa**, vuelve a estar disponible de forma automática una vez finalizado el tiempo de pausa.

    Si se modifica el estado de presencia a través de myPortal a **Pausa**, se cierra inmediatamente la sesión del agente de la cola o colas de espera.

  – myAgent: el agente ha iniciado sesión.

    Si se modifica el estado de presencia a través de myPortal a **No molestar**, se cierra inmediatamente la sesión del agente de la cola o colas de espera.

- Llamadas salientes mediante myPortal

  El estado de presencia de la extensión se puede ver mediante myAgent.

  Las llamadas solo aparecen en el diario de myPortal. No se incluyen en las estadísticas del centro de contactos, ya que no se trata de llamadas de centro de contactos.
- Llamadas entrantes al número de extensión del agente

  El estado de presencia de la extensión se puede ver mediante myAgent.

  Las llamadas solo aparecen en el diario de myPortal. No se incluyen en las estadísticas del centro de contactos, ya que no se trata de llamadas de centro de contactos.
- Grabar una llamada

  myAgent no registra la grabación de llamadas mediante myPortal. myAgent ofrece esta función aun cuando las llamadas ya se estén grabando mediante myPortal.

18.2 Agentes

Los agentes (extensiones) que pertenecen a una cola forman un grupo de trabajo que, por ejemplo, puede ponerse en uso en las hotlines técnicas o en el procesamiento de pedidos o consultas. Las llamadas, faxes y correos electrónicos entrantes se distribuyen homogéneamente entre los agentes disponibles de una cola.

Para utilizar una extensión del sistema de comunicación como agente, debe estar configurada como tal. Los derechos del agente se definen en la selección del nivel de clase de servicio (agente, supervisor o administrador). Los agentes con el nivel de clase de servicio Supervisor o Administrador disponen de autorizaciones ampliadas (véase Funciones en función de la clase de servicio para agentes).

Los agentes se pueden definir como agente permanente. Permanecerán disponibles para llamadas, faxes y correos electrónicos, aunque no acepten una llamada, un fax o un correo electrónico.

18.2.1 Funciones según la clase de servicio para agentes

Al configurar una extensión como agente, los derechos del agente se definen seleccionando el nivel de clase de servicio (Agente, Supervisor o Administrador). Los agentes con el nivel de clase de servicio Supervisor o Administrador tienen autorizaciones ampliadas.

Las diferencias entre clases de servicio aparecen resumidas en la siguiente tabla.

myAgent:	**Nivel de autorización (clase de servicio)**		
Acción	**Agente**	**Supervisor**	**Administrador**
Asignar agente a una cola	–	X	X
Mover un agente a otra cola	–	X	X
Eliminar agente de una cola	–	X	X

myAgent:	Nivel de autorización (clase de servicio)		
Acción	**Agente**	**Supervisor**	**Administrador**
Cambiar el estado de un agente	–	X	X
Mostrar/ocultar la lista de asignaciones de agentes	Colas asignadas	Todas las colas	Todas las colas
Editar la asignación de un agente	–	X	X
Mostrar lista de Llamadas en directo	Colas asignadas	Todas las colas	Todas las colas
En caso de alarma, activar myAgent automáticamente en primer plano	–	X	X
Activar el tono de alarma	–	X	X
Mostrar el tablero	Colas asignadas	Todas las colas	Todas las colas
Mostrar el diagrama de nivel de servicio	Colas asignadas	Todas las colas	Todas las colas
Mostrar el diagrama de Tiempos medios	Colas asignadas	Todas las colas	Todas las colas
Mover una llamada a la primera posición de una cola de espera	–	X	X
Grabar una llamada	Llamada actual	Todas las llamadas	Todas las llamadas
Guardar la grabación de una llamada como archivo WAV o enviarla como archivo WAV por correo electrónico	–	X	X
Guardar fax como archivo TIFF o enviarlo por correo electrónico	–	X	X
Guardar un correo electrónico como archivo EML o enviarlo como archivo EML por correo electrónico	–	X	X
Supervisión de llamadas (en función del país)	–	X	X
Intercalar una Llamada	–	X	X
Aceptar una solicitud de asistencia	–	X	X
Crear informes	–	X	X
Abrir WBM	–	X	X

18.2.2 Agentes preferidos

A cada llamante (por ejemplo, a cada cliente llamante) se le pueden asignar uno o varios agentes preferidos de una cola. En tal caso, el sistema de comunicación intenta transferir al llamante y sus solicitudes de devolución de llamada a un agente favorito en primer lugar. Si se han establecido varios agentes preferidos, se puede definir una prioridad (orden) con la que son transferidos los agentes preferidos.

Si no hay disponible ningún agente preferido, la llamada se transfiere a cualquier otro agente disponible.

18.2.3 Agente en varias colas de espera

Un agente puede estar asignado a varias colas con distintos niveles de capacidades. Para ello hay que definir si los agentes actuarán como agentes principales o como agentes de desbordamiento.

18.2.4 Pausas de Contact Center

Para permitir a todos los agentes pausas definidas, pueden definirse pausas de Contact Center de distinta duración (por ejemplo, pausa de mediodía, pausa para fumar, etc.). Las pausas de Contact Center están disponibles a nivel de sistema y, si es necesario, los agentes pueden seleccionarlas a través de myAgent.

18.2.5 Inicio/Cierre de sesión de agente mediante el teléfono

En el Contact Center también se puede iniciar y cerrar sesión a través del teléfono, sin necesidad de ejecutar myAgent para acceder a las funciones de Contact Center. Si un agente ha iniciado sesión a través del teléfono, solo se procesan llamadas de voz. En este caso, no se admiten entradas de código de tratamiento posterior ni de ventana emergente. Esto también es aplicable si myAgent está activo y el agente inicia sesión en el Contact Center por teléfono. Para recuperar la funcionalidad completa de myAgent, el agente debe cerrar sesión a través del teléfono y conectarse de nuevo con myAgent.

Requisitos previos y restricciones

- Las funciones de OpenScape Business Contact Center a través del teléfono solo están disponibles para agentes que tienen asignada una licencia de myAgent en OpenScape Business
- Todas las funciones solamente son compatibles con teléfonos homologados para el uso con OpenScape Business Contact Center
- Si se ha iniciado sesión por teléfono correctamente y el cliente myAgent asociado no está activo, solo se encaminan al agente llamadas de voz
- Si se ha iniciado sesión por teléfono correctamente, el cliente myAgent asociado está activo y el agente inicia sesión por teléfono, no se le comunican los mensajes de voz, los faxes ni las devoluciones de llamada. En este caso, las ventanas emergentes y el tratamiento posterior funcionan de la forma habitual, pero solo se pasan al agente las llamadas de voz. Para disponer de la funcionalidad completa, el agente debe cerrar sesión con el teléfono y conectarse de nuevo con myAgent

Inicio de sesión en el Contact Center mediante el teléfono

Si los agentes inician sesión en OpenScape Business Contact Center por teléfono, con independencia del cliente myAgent, y Contact Center está activo:

- Las funciones UCD para el inicio de sesión se utilizan en el teléfono
- La función de inicio de sesión se puede ejecutar mediante un código de prestación o con una tecla programada

- El agente inicia sesión en todas las colas a las que está asignado en la configuración de Contact Center
- La pantalla del teléfono informa al agente sobre el estado de cierre de sesión
- Solo aparece información de colas UCD (por ejemplo, información sobre llamadas en cola) a demanda

El agente puede utilizar las funciones siguientes:

- Iniciar/Cerrar sesión (con ID de agente UCD)
- Resumen
- Disponible/No disponible
- Visualización de llamadas en cola UCD a las que está asignado el ID de agente UCD

Nota: El agente no debe utilizar Servicio nocturno UCD.

Nota: La marca permanente de myAgent es compatible para iniciar sesión usando el teléfono. Esto significa que en caso de que un agente haya iniciado sesión con su teléfono y se haya perdido una llamada, este agente sigue disponible para la próxima llamada. Este es el mismo comportamiento que con el uso del cliente myAgent.

Si Contact Center tiene un fallo mientras el agente está conectado, se mantiene la sesión abierta en UCD y las llamadas de voz se encaminan según la configuración del encaminamiento UCD. Si el agente no ha iniciado sesión, puede conectarse a UCD por teléfono.

Cierre de sesión del Contact Center mediante el teléfono

Si los agentes cierran sesión del OpenScape Business Contact Center a través del teléfono, con independencia del cliente myAgent, y Contact Center está activo:

- Las funciones UCD de cierre de sesión se pueden utilizar en el teléfono
- La función de inicio de sesión se puede ejecutar mediante un código de prestación o con una tecla programada
- El agente cierra sesión de todas las colas a las que está asignado en la configuración de Contact Center
- La pantalla del teléfono informa al agente sobre el estado de inicio de sesión
- No aparece más información de Contact Center/UCD (por ejemplo, información sobre llamadas en cola)

Marcar un agente como disponible/no disponible mediante el teléfono

Si un agente define su estado en “Disponible” o “No disponible” para el encaminamiento de contactos de OpenScape Business Contact Center a través del teléfono, con independencia del cliente myAgent, y Contact Center está activo:

- La pantalla del teléfono informa al agente sobre el estado de cierre de sesión
- Si myAgent no está activo, solo se encaminan al agente llamadas de voz

Definir/Restablecer el estado "Trabajo posterior a llamada" (Tratamiento posterior) mediante el teléfono

Si un agente define su estado en "Trabajo posterior a llamada" (Tratamiento posterior) a través del teléfono, con independencia del cliente myAgent, y Contact Center está activo, no se encaminan llamadas al agente hasta que termine el tiempo de Tratamiento posterior específico configurado en OpenScape Business Contact Center para él, o hasta que reinicie el Tratamiento posterior a través del teléfono.

Asignación de estado

El cambio de estado del agente mediante el teléfono se asigna al estado del agente myAgent de la manera siguiente:

Dispositivo telefónico			myAgent			
Código de característi	**Código de característi**	**Descripción**	Texto en pantalla del teléfono	**Estado**	**Texto adicional**	Observación
*401	ID de agente UCD	Dar de alta agentes UCD	Disponible	Disponible	-	El agente se marca como “disponible” en todas las colas asignadas
#401	–	Dar de baja agente UCD	No disponible	No disponible	-	El agente deja de estar disponible en todas las colas asignadas
*402	–	Agente UCD disponible	Disponible	-	-	Disponible (final de tiempo de trabajo)
#402	–	Agente UCD no disponible	No disponible	Tiempo de actividad	Cuenta atrás de 999.999 segundos	-
*403	–	Tiempo administrativo UCD act.	Resumen	Tiempo de actividad	Cuenta atrás de tiempo de trabajo configurado	El tiempo de trabajo debe terminarse antes de que pueda comenzar de nuevo. No se acumula tiempo de trabajo como en myAgent. Una vez finalizado el tiempo de trabajo, el agente se marca como “disponible” automáticamente.

Dispositivo telefónico			myAgent			
Código de característi	**Código de característi**	**Descripción**	Texto en pantalla del teléfono	**Estado**	**Texto adicional**	Observación
#403	–	Tiempo administrativo UCD des.	Disponible	Disponible	-	-
*404	Objetivo de servicio nocturno	Servicio nocturno UCD act.	–	No compatible	-	Servicio nocturno UCD no debe utilizarse
#404	–	Servicio nocturno UCD des.	–	No compatible	-	Servicio nocturno UCD no debe utilizarse
*405	–	Consultar estado cola de llamadas UCD	-	-	-	Solo aparece la cola a la que está asignado el ID de agente UCD, aunque el agente esté asignado a varias colas en el Contact Center

18.3 Colas de espera y planes horarios

Las colas de espera son la base del Contact Center. Las llamadas, faxes y correos electrónicos de la cola se pueden administrar en función del nivel de capacidad de los agentes, de la prioridad y del tiempo de espera. Las llamadas que se encuentran en estado de espera pueden escuchar la reproducción de anuncios grabados. Mediante un plan horario se define cómo se van a administrar las llamadas entrantes en determinados días y a horas determinadas.

18.3.1 Colas de espera

Por norma general, la distribución de llamadas se realiza de forma que las llamadas, faxes o correos electrónicos entrantes dirigidos a un grupo UCD son transferidos a aquellas extensiones del grupo (agentes) que lleven más tiempo sin atender llamadas. También se pueden establecer otras reglas de distribución (por ejemplo en función de los distintos niveles de habilidad de los agentes). Si todos los agentes están ocupados, las nuevas llamadas, faxes y correos electrónicos entrantes son puestos en espera y, a continuación, se distribuyen a los agentes que se van liberando en función de su prioridad y tiempo de espera.

Mediante los planes horarios y las reglas incluidas en ellos (= CCV, Call Control Vector) se puede definir cómo se gestionará una llamada dirigida a una cola en una hora o día determinados. Las reglas definen, por ejemplo, qué anuncios grabados se reproducen a los llamantes o el destino de transferencia de una llamada.

Los faxes, correos electrónicos y devoluciones de llamada de los agentes se asignan directamente a las colas de espera, con independencia de los planes horarios.

En la asignación de agentes a colas de espera, los agentes pueden tener asignadas distintas propiedades (asignación de agentes) que influyen en la distribución de las llamadas en una cola de espera (por ejemplo, agente principal o agente de desbordamiento, nivel de habilidad). Se pueden asignar agentes a las colas de espera

- a través de la Gestión basada en Web (WBM) por parte de un administrador con el perfil **Avanzado**.
- a través de la aplicación myAgent por parte de un agente con el nivel de clase de servicio Supervisor o Administrador.

Si un agente está asignado a varias colas, a través de la prioridad de cola se puede establecer si las llamadas dirigidas a una cola deberán ser transferidas al agente con una prioridad más elevada que las llamadas dirigidas a otras colas.

En las colas se pueden realizar los siguientes ajustes básicos a través de la herramienta la Gestión basada en Web (WBM):

- Activar, desactivar o borrar colas de espera

  Advertencia: después de borrar una cola de espera no se pueden crear informes sobre periodos de tiempo pasados. No se deben desactivar más colas necesarias.
- Configurar alarmas de cola

  Existen estas opciones:

  – Recuento de alarma de cola (número de umbral de alarma): si se supera el número aquí indicado de llamadas en espera, el sistema de cola de los agentes cambia de color verde a naranja. Los agentes con la clase de servicio Supervisor o Administrador pueden configurar si desean ser advertidos mediante un tono de alarma y si desean que myAgent aparezca automáticamente en primer plano.
  – Hora de alarma de cola (tiempo de umbral de alarma): si se supera el tiempo de espera de una llamada en la cola, la entrada correspondiente de la lista de llamadas del Contact Center de los agentes pasa a color rojo. Los agentes con la clase de servicio Supervisor o Administrador pueden configurar si desean ser advertidos mediante un tono de alarma y si desean que myAgent aparezca automáticamente en primer plano.
- Definición del tiempo excedido de llamadas, faxes y correos electrónicos salientes

  Si no se acepta una llamada, un fax o un correo electrónico en el tiempo aquí indicado, la llamada, el fax o el correo electrónico se transfiere al siguiente agente libre.
- Definir el valor umbral de llamada abandonada

  En función del tiempo indicado se establece si una llamada abandonada será o no incluida en las estadísticas (en los informes). Se registran de forma estadística todas las llamadas abandonadas una vez finalizado el tiempo indicado.
- Configurar la profundidad de cola

  Control del número máximo de llamadas activas y en espera en una cola determinada. El Contact Center indica al sistema que se ha alcanzado el

umbral definido del tamaño de la cola. En consecuencia, el sistema rechaza todas las llamadas entrantes nuevas para la cola correspondiente antes que la llamada se conecte con el sistema y hasta que el número de llamadas baje del límite definido.

El tamaño máximo de cola está determinado por los parámetros siguientes:

– Número máximo de posiciones en espera en la cola. (WLS = Tamaño de bucle de espera)
– Número máximo de llamadas activas y en espera de la cola (tamaño de profundidad de cola).

- Configurar pilotos de fax entrante

  Si esta opción está configurada, se pueden seleccionar números de teléfono para mensajes de fax entrantes. Los faxes dirigidos a esas direcciones se depositan en la cola de espera y se gestionan como llamadas entrantes.
- Configurar el servicio de email entrante

  Se pueden configurar varias direcciones de correo electrónico para una cola. Los correos electrónicos dirigidos a esas direcciones se depositan en la cola de espera y se gestionan como llamadas entrantes.
- Configurar la dirección de email de devolución

  Dirección de correo electrónico de la cola que puede visualizar el destinatario cuando un agente envía un correo electrónico.
- Activar el encaminamiento de llamadas inteligente

  Las llamadas entrantes se transfieren al último agente conectado con el llamante. Para ello es necesario que no haya definido ningún agente preferido para ese llamante.

18.3.2 Planes horarios

El plan horario y las reglas en él incluidas (CCV, Call Control Vector) de cada cola permiten definir cómo se administrarán las llamadas entrantes en determinados días y horas.

Por ejemplo, en los días laborables se puede definir una regla para el primer turno (de 06:00 h a 14:00 h), otra para el turno central (de 14:00 a 22:00 h) y otra para el turno de noche (de 22:00 a 06:00 h). Para el fin de semana se puede definir una regla de fin de semana. Para cada una de estas reglas se puede indicar, por ejemplo, si se reproducirán anuncios grabados y/o adonde serán transferidas las llamadas.

Los planes horarios son la pieza clave de la configuración del Contact Center. Si no se define al menos un plan de horario no se puede finalizar correctamente la configuración de un Contact Center. Cada cola debe estar asignada al menos a un plan horario. También puede ser siempre el mismo plan horario.

Se debe asignar al menos una regla (Call Control Vector CCV) a un plan horario. Las reglas determinan qué llamadas entrantes se gestionarán en una determinada cola durante el tiempo de vigencia de un plan horario. Las reglas se aplican exclusivamente a llamadas, no a faxes ni correos electrónicos.

Las reglas se crean con el editor de reglas gráfico (Editor CCV) mediante la vinculación de objetos CCV predefinidos y se pueden guardar con cualquier nombre una vez finalizadas.

Las reglas guardadas se pueden asignar a uno o varios planes horarios como reglas estándar (CCV estándar) o como reglas de excepción (CCV de excepción). El editor de reglas permite la apertura, modificación y guardado en cualquier momento.

Si se ha asignado una regla estándar (CCV estándar) a un plan horario, ese plan se puede guardar con un nombre de selección libre. Los planes horarios con una regla estándar, tras ser asignados a una cola de espera, se aplican 24 horas al día, 365 días al año. Si desea aplicar otras reglas en determinados momentos (Pausa, Fin de semana, Festivo, Vacaciones, etc.), puede asignarlas al plan horario correspondiente como reglas de excepción (CCV de excepción). De esta forma, se puede definir cómo se administrarán las llamadas entrantes, por ejemplo, durante las vacaciones. Los planes horarios vacacionales tienen prioridad frente a otros planes horarios y reglas de una cola.

Editor de reglas (Editor CCV)

Con el editor de reglas se pueden crear reglas a partir de objetos CCV predefinidos. La asignación de los objetos CCV y de sus propiedades determina cómo serán administradas las llamadas entrantes.

Nota: Una regla tiene un límite superior de 500 objetos CCV.

Están disponibles los siguientes objetos predefinidos:

Consejo: A todos los objetos CCV indicados se les aplican, además, estas dos propiedades generales:

Descripción: describe de forma opcional el objeto CCV, por ejemplo, "Saludo de bienvenida".

Iniciar proceso después de marcar los dígitos: indica los dígitos necesarios, sin espacios en blanco, comas ni otros caracteres. La indicación se refiere al objeto CCV anterior. Si en Dígitos aceptados se ha introducido un 9, también aquí se debe introducir esta cifra.

- **Reproducir mensaje**

  Hace que se reproduzca el anuncio grabado deseado. Se puede seleccionar un archivo de sonido presente en la UC Suite. Además, se puede importar un nuevo archivo de sonido a la UC Suite o se puede grabar un nuevo anuncio grabado y, a continuación, importarlo como archivo de sonido a la UC Suite.

  Al reproducir un anuncio grabado se ocupa un canal Media Stream.

  Propiedades:

  – **Nombre archivo**: selección de un anuncio grabado (archivo de sonido en formato wav)
  – **Dígitos de interrupción**: indicación de una tecla o combinación de teclas en el teclado de marcación con el que el llamante puede interrumpir la reproducción del anuncio grabado.
  – **Administrador de archivos**: este botón permite cargar un archivo de sonido en formato wav o crear un nuevo archivo de voz con el grabador.

- **Música en espera**

  Hace que se reproduzca música en espera (Music On Hold, MOH, del sistema de comunicación) a un llamante externo durante un tiempo configurado

  Propiedad:

  – **Valor de hora**: tiempo en segundos durante el que se reproducirá la música en espera.
- **Finalizar llamada**

  Hace que finalice la conexión

  Después de este objeto CCV no se pueden insertar más objetos CCV.
- **Reproducir información sobre posición de cola**

  Ofrece información al llamante sobre su posición actual en la cola
- **Tiempo de espera estimado**

  ofrece información sobre el Tiempo de espera estimado para el llamante.

  El tiempo de espera estimado se calcula según:

  1) Tiempo histórico promedio en cola para todas las colas
  2) Tiempo histórico promedio en cola para la cola en particular
  3) Tiempo histórico promedio de conversación para el agente en particular
- **A CCV**

  Crea un bucle a otro objeto CCV

  Propiedad:

  – **CCV de destino**: selección del objeto CCV
- **Grabar devolución de llamada**

  Permite a un llamante de una cola activar una devolución de llamada de agente (grabación de un mensaje de voz). La devolución de llamadas de agente permanece en la cola de espera en lugar del llamante. La devolución de llamadas de agente muestra a los agentes con la propiedad **Activar devolución de llamada de agente** en la lista de llamadas del Contact Center.

  Después de este objeto CCV no se pueden insertar más objetos CCV.

  Propiedades:

  – **Tipo**: selección de **Devolución de llamada simple** o **Devolución de llamada amplia**.

    Frente a lo que ocurre en la devolución de llamada simple, en el caso de las devoluciones ampliadas los llamantes cuentan con opciones e información adicionales sobre la disponibilidad (confirmación o modificación del número de teléfono para la devolución, confirmación del mensaje de voz).
  – **Longitud máxima del mensaje**: longitud de tiempo en segundos durante el que se puede realizar la grabación de un mensaje de voz.

- **Iniciar proceso después de marcar los dígitos**

  Hace que el siguiente objeto u objetos CCV se ejecuten en función de las cifras aquí indicadas (Iniciar proceso después de marcar los dígitos).

  Propiedades:

  – **Nombre archivo**: selección de uno o varios anuncios grabados (archivo de sonido en formato wav).
  – **Lista de reproducción**: lista de reproducción de los anuncios grabados seleccionados (archivo de sonido en formato wav) en el orden de reproducción.
  – **Tiempo excedido al introducir dígitos**: tiempo excedido al introducir tiempo en segundos que espera el sistema de comunicación a la entrada de cifras.

    Si la entrada completa de dígitos no se produce dentro del tiempo indicado, se vuelve a reproducir el mensaje (anuncio grabado).
  – **Enlace con**: listado de los números con destino.

    Las cifras y los destinos se pueden añadir, editar y eliminar.
  – **Administrador de archivos**: este botón permite cargar un archivo de sonido en formato wav o crear un nuevo archivo de voz con el grabador.

  El contenido de la lista de reproducción se muestra en el editor de reglas mediante una información sobre herramientas al sostener el cursor sobre el objeto CCV.
- **Transferencia de un solo paso**

  Esta función depende del ajuste **SST de puesto de operadora automático normal** (WBM, **Modo experto**: **Aplicaciones** > **OpenScape Business UC Suite** > **Servidor** > **Ajustes generales**):

  – **SST de puesto de operadora automático normal** habilitado (configuración estándar; no para EE. UU.): se transfiere una llamada, tanto si el destino está libre como ocupado.

    Consejo: En el caso de una extensión con bloqueo de avisos de llamada en espera, la llamada solo se transfiere cuando la extensión de destino está libre. No se produce un aviso de llamada en espera en caso de ocupado.
  – **SST de puesto de operadora automático normal** deshabilitado (configuración estándar; solo para EE. UU.): la llamada se transfiere si el destino está libre.

    Si el destino está ocupado y el bloqueo de avisos de llamada en espera está desactivado, o si el destino no está disponible, el llamante escucha la reproducción de un anuncio grabado. Con ello, el llamante puede

decidir dejar un mensaje en el buzón de voz de la extensión o marcar el número de teléfono de otro destino.

Si el destino está ocupado y el bloqueo de avisos de llamada en espera está activado, la llamada no se transfiere.

Después de este objeto CCV no se pueden insertar más objetos CCV.

Propiedad:

– **Extensión de destino**: indicación del número de teléfono interno o del número de marcación directa externo con número de línea urbana. No se permite el uso de caracteres vacíos, comas ni otros caracteres.

El número de teléfono de la extensión de destino se muestra en el objeto CCV.

Nota: Después de la transferencia de un solo paso, el sistema desconecta la llamada después de señalizarla durante 5 minutos.

- **Transferir a cola**

  Hace que la llamada se transfiera a la cola

  Después de este objeto CCV no se pueden insertar más objetos CCV.

  Propiedad:

  – **Cola**: selección de la cola
- **Grabar en buzón de voz**

  Hace que la llamada se transfiera al buzón de voz de una extensión o de un grupo de buzón de voz

  Después de este objeto CCV no se pueden insertar más objetos CCV.

  Propiedad:

  – **Buzón de voz del usuario**: indicación del número de teléfono del buzón de voz de una extensión o de un grupo de buzón de voz.

  El número de teléfono y el nombre del buzón de voz o del grupo de buzón de voz se muestran en el editor de reglas mediante una información sobre herramientas al dejar el cursor sobre el objeto CCV.
- **Transferencia supervisada (también llamada transferencia controlada)**

  Hace que la llamada se transfiera a un destino interno. Durante la transferencia, el llamante escucha la música en espera (Music On Hold MOH de la UC Suite).

  Frente a la transferencia de un solo paso al objeto CCV, aquí hay que introducir otros dos objetos CCV. En concreto, hay que definir cuál será el comportamiento del sistema cuando el destino de la llamada esté ocupado o cuando no se responda a la llamada. Normalmente, en estos casos el llamante escucha la reproducción de un anuncio grabado.

  Propiedades:

  – **Extensión de destino**: indicación del número de teléfono interno.

    Solo se admiten números de teléfono internos en el nodo propio. ¡No se permite el desvío a destinos externos, estaciones virtuales, operadoras

automáticas adicionales, usuarios de Mobility ni destinos externos de CallMe!

Para estos escenarios se debe utilizar la SST (transferencia de un solo paso). Para transferir una llamada a otro UCD que sea parte del Contact Center, se debe utilizar el objeto CCV **Transferir a Cola**.

– **Tiempo excedido de timbre**: tiempo en segundos en el que se debe aceptar la llamada.

Si la llamada no se acepta dentro del tiempo indicado, es restablecida en el sistema de comunicación y se utiliza el siguiente objeto CCV.

Consejo: El tiempo aquí indicado debe ser menor que el tiempo configurado para la transferencia automática diferida (configuración estándar para la transferencia automática diferida = 15 segundos). Consulte Cómo configurar una transferencia automática diferida.

– **Devolver llamada si el dispositivo de destino está transferido / desviado** Opción (solo se aplica a número de llamada interno).

Si la opción está activa se comprueba el destino de la llamada. Si en el destino de llamada hay activada una transferencia automática diferida de llamadas o un desvío de llamadas, la llamada se restablece en el sistema de comunicación y se utiliza el siguiente objeto CCV.

– **Comprobar estado de presencia al transferir llamadas**: Opción

Si esta opción está activada, se comprueba el estado de presencia del destino de la llamada; si el estado no es Oficina, la llamada se devuelve al sistema de comunicación y se utiliza el siguiente objeto CCV.

• **Marcar por nombre**

Se solicita al llamante indicar las tres primeras letras del apellido del usuario deseado a través del teclado de marcación.

Si hay una extensión con las letras iniciales indicadas, se establece una conexión.

Si hay varias extensiones con las letras iniciales indicadas, el llamante escucha sus nombres (10 extensiones como máximo). Si una extensión no ha grabado ningún anuncio de nombre, se escuchará en su lugar la reproducción del número de teléfono. Después de seleccionar la extensión deseada se establece una conexión.

Si por el contrario ningún usuario se corresponde con las letras iniciales especificadas, el llamante recibe un mensaje al respecto.

Consejo: Las teclas del teclado de marcación responden a la primera pulsación de teclas. Cada vez que se pulsa una tecla se comprueba si hay apellidos de usuario con las letras asignadas a las teclas.

Ejemplo: en el directorio interno están presentes los siguientes cinco apellidos con las letras iniciales t, u y v:

Taylor, Taler, Ullrich, Vasquez y Volterra. Para establecer una conexión con el usuario Taylor, pulse estas teclas: 8 2 9

Después de este objeto CCV no se pueden insertar más objetos CCV.

Propiedades:

– **Método**: selección de **Transferir a extensión** o **Grabar en buzón de voz**.

  En función del método seleccionado, se establecerá una conexión con la extensión deseada o con su buzón de voz. Solo se admiten extensiones internas registradas en el directorio interno con nombre y apellidos.

- **Marcar por extensión**

Se solicita al llamante indicar el número de teléfono de la extensión deseada a través del teclado de marcación.

Si el llamante marca el número de teléfono de una extensión virtual, se le solicitará introducir otro número de teléfono de extensión. A continuación, se establece una conexión. Si la extensión deseada no responde, la llamada será atendida por su buzón de voz.

Después de este objeto CCV no se pueden insertar más objetos CCV.

Propiedades:

– **Método**: selección de **Transferir a extensión** o **Grabar en buzón de voz**.

  En función del método seleccionado, se establecerá una conexión con la extensión deseada o con su buzón de voz. Recuerde que solo se admiten extensiones internas cuyos números de teléfono estén registrados en el directorio interno.

- **Definir idioma**

Permite seleccionar el idioma de los anuncios estándares, en función del número de teléfono del llamante. Hay que tener en cuenta que solo afecta a anuncios estándar (anuncios del sistema) y no a anuncios personales.

Se puede definir, por ejemplo, que para un número de teléfono con el prefijo nacional +49 se reproduzca un anuncio en alemán, y que para los números de teléfono con el prefijo +33 se reproduzca un anuncio grabado en francés.

Propiedades:

– **Idioma predeterminado**: lista desplegable para seleccionar un idioma.

  El idioma seleccionado aquí se utiliza para todos los números de teléfono para los que no se ha definido un idioma propio.

– **Patrón**: indicación del número de teléfono al que se asignará un idioma determinado.

  Se pueden utilizar los siguientes marcadores de posición: * = cualquier número, ? = cualquier cifra.

– **Idioma**: lista desplegable para seleccionar el idioma que se asignará al número de teléfono correspondiente (**Patrón**).

Un idioma se puede asignar a tantos números de teléfono diferentes como se desee (**Patrón**).

- **Encaminamiento CLI**

  Permite desviar una llamada a uno o varios objetos CCV consecutivos, mediante el número de teléfono del llamante.

  Por ejemplo, se puede definir que un número de teléfono con el prefijo nacional +49 escuche, en primer lugar, un anuncio en alemán (objeto CCV **Reproducir mensaje**) y que, a continuación, la llamada se transfiera a un teléfono interno (objeto CCV **Transferencia de un solo paso**). También se puede utilizar el código de red (p. ej., 089 para Munich)

  En el contexto de UC Suite y CLI Routing, los usuarios deben considerar escenarios específicos, como llamadas entrantes desde MS Teams Native SIP Trunk. Si tiene la intención de enviar a OpenScape Business los números de la persona que llama en formato canónico, incluido el código de país, debe establecer reglas de enrutamiento CLI adicionales.

  Por ejemplo, si las personas que llaman desde MS Teams tienen números en el formato 49777555XXXX y 777555 es la parte común de estos números, los usuarios deben crear reglas de enrutamiento CLI relevantes que incorporen esta parte común (777555).

  Propiedades:

  – **Estándar**: lista desplegable para seleccionar el objeto CCV.

    El objeto CCV seleccionado aquí se utiliza para todos los números de teléfono para los que no hay definido ningún destino propio.
  – **Patrón**: indicación del número de teléfono al que se debe asignar como destino un determinado objeto CCV.

    Se pueden utilizar los siguientes marcadores de posición: * = cualquier número, ? = cualquier cifra.
  – **Descripción**

    entrada de una explicación.

    Para el **Patrón** +49 (=prefijo del país Alemania) se puede introducir, por ejemplo, Alemania.

    El texto aquí introducido se muestra en el editor de reglas.
  – **Destino**: lista desplegable para seleccionar el objeto CCV al que se asignará el número de teléfono correspondiente (**Patrón**) como destino.

  Un objeto CCV se puede asignar tantos números de teléfonos diferentes (**Patrón**) como destino como se desee.
- **Bifurcar con variable**

  Desvía una llamada a uno o varios objetos CCV consecutivos en base a una condición.

  Se puede definir por ejemplo que los llamantes escuchen la reproducción de un anuncio grabado (Vuelva a llamar más tarde...) en cuando haya más de 20 llamadas en una cola de espera.

  Propiedades:

  – **Variable**: selección de **Llamadas** o **Agentes disponibles**.

    En función de la variable seleccionada se utiliza como condición definida el número de llamadas en espera dentro de una cola o el número de agentes disponibles (incluidos los agentes que se encuentren en el tiempo administrativo o de tratamiento posterior) de una cola. En la lista desplegable correspondiente hay que seleccionar la condición

(**menor que**, **mayor que**, **menor o igual que**, **mayor o igual que**, **igual a**) e introducir el valor de comparación en el campo de entrada correspondiente.

– **Bifurcar con True**: lista desplegable para seleccionar el objeto CCV que se debe utilizar como destino si se cumple la condición.
– **Bifucar con False**: lista desplegable para seleccionar el objeto CCV que se debe utilizar como destino si no se cumple la condición.

El número de agentes disponibles en una cola de espera está determinado por los siguientes cambios de estado de los agentes:

– Inicio de sesión de un agente en la cola de usuario mediante "Inicio de sesión/Login": --> +1
– Fin de sesión de un agente de la cola de espera mediante "Fin de sesión/ Logout": --> -1
– Agente en el estado "Pausa": --> -1
– Agente en el estado "Disponible después de una pausa": --> + 1

El número de agentes disponibles en una cola de espera **no** está determinado por los siguientes cambios de estado de los agentes:

– Agente en el estado "Sonando"
– Agente en el estado "En conversación"
– Agente en el estado "Tratamiento posterior"
– Agente en el estado "Llamada perdida"
– Agente en el estado "Tiempo excedido"

• **Bifurcar con datos**

Desvía una llamada a uno o varios objetos CCV consecutivos en base a una condición.

Se puede definir por ejemplo que los llamantes escuchen la reproducción de un anuncio grabado (Vuelva a llamar más tarde...) en cuando haya más de 20 llamadas en una cola de espera.

Propiedades:

– **Variable**: Selección de **LDAP data1 (xmpp)** o **LDAP data2 (localizador)**.

La consulta de datos se realiza mediante LDAP ya sea directamente a una base de datos con capacidad LDAP o indirectamente a través de Directory Service (ODS) a una base de datos SQL / ODBC. Los resultados de la consulta se asignan mediante el campo UC Suite LDAP que se asigna a los criterios adecuados de Contact Center. En la lista desplegable correspondiente hay que seleccionar la condición (**menor que**, **mayor que**, **menor o igual que**, **mayor o igual que**, **igual a**) e introducir el valor de comparación en el campo de entrada correspondiente. Es necesario asignar las palabras claves "localizador" e "info".

– **Tiempo de espera**: Tiempo en segundos para que se produzca un tiempo de espera.
– **Tiempo de espera de sucursal**: lista desplegable para seleccionar el objeto CCV que se debe utilizar como destino cuando se produce el tiempo de espera.
– **Bifurcar con True**: lista desplegable para seleccionar el objeto CCV que se debe utilizar como destino si se cumple la condición.

- **Bifucar con False**: lista desplegable para seleccionar el objeto CCV que se debe utilizar como destino si no se cumple la condición.
- **Descripción**: entrada de una explicación.

18.3.3 Terminar

En función de los motivos de tratamiento posterior las llamadas entrantes se pueden asignar a distintos temas (pedido, reclamación, servicio técnico, etc.). La asignación la realiza un agente después de completar la llamada (durante el tiempo de trabajo) ingresando el motivo de finalización apropiado usando myAgent.

Se pueden definir motivos de tratamiento posterior para cada cola por separado.

En este punto se distingue entre:

- Tratamiento posterior simple

  En las colas con el modo de Tratamiento posterior "Tratamiento posterior simple" se pueden definir uno o varios motivos de tratamiento posterior.

  Ejemplo: Se definieron para una cola los dos motivos de conclusión, "problema de hardware" y "problema de software". Un agente asigna a cada llamada uno de estos motivos de conclusión durante el tiempo de trabajo. De esta forma, por ejemplo, se puede generar un informe que incluya una visión general de todas las llamadas sobre el tema "Problema de hardware".

- Tratamiento posterior múltiple

  En las colas con el modo de tratamiento posterior "Tratamiento posterior múltiple" se pueden definir uno o varios motivos de tratamiento posterior y reunirlos en grupos o grupos secundarios.

  Debajo de cada grupo o subgrupo (si lo hubiera) también se debe configurar al menos un elemento para que el agente pueda finalizar una llamada. No es posible finalizar una llamada si un grupo o subgrupo está vacío. Esto se aplica solo a las colas que tienen habilitada la configuración de conclusión múltiple.

  Ejemplo: Se definieron para una cola un grupo de Hardware con los motivos de resumen Placa base y Fuente de alimentación y un grupo de Software con los motivos de resumen Sistema operativo y Controladores. Un agente asigna a cada llamada uno de estos motivos de conclusión durante el tiempo de trabajo. De esta forma, por ejemplo, se puede generar un informe que incluya una visión general de todas las llamadas sobre problemas de hardware o sobre todas las llamadas sobre problemas relacionados con el hardware de la placa base.

18.3.4 Nivel de servicio

Los niveles de servicio permiten evaluar la calidad de transferencia de una cola. Esto es posible mediante la comparación del tiempo de espera de los llamantes en la cola de espera con valores nominales que se pueden predefinir de forma individual para cada cola.

Los valores nominales del nivel de servicio (Grade of Service, GoS) se pueden determinar libremente en función del tiempo de espera de los llamantes en una cola. Por cada llamada a la cola de espera en cuestión se transmite el nivel de servicio al finalizar la llamada y se aplica a la base de datos. Los agentes con el nivel de clase de servicio "Supervisor" o "Administrador" pueden evaluar el nivel de servicio mediante la aplicación myAgent.

18.3.5 Tablero (Wallboard)

A través de myAgent se puede consultar la indicación de los detalles de cola de espera. La indicación incluye una tabla con información estadística sobre las colas de espera en tiempo real para el intervalo actual de 24 horas. La indicación, por ejemplo, se puede visualizar a través de un gran monitor LCD o a través de un beamer (proyector de pantalla).

Los agentes con el nivel de clase de servicio Agente reciben información sobre las colas de espera a las que están asignados. Los agentes con el nivel de clase de servicio Supervisor o Administrador reciben información sobre todas las colas de espera.

Para el tablero hay que configurar una extensión independiente. Para ello se requiere una licencia de extensión (IP User o TDM User) y una licencia de myAgent.

18.3.6 Devolución de llamadas de agentes

Si un llamante pasa demasiado tiempo en la cola de espera y el plan horario correspondiente incluye el objeto CCV **Grabar devolución de llamada**, puede dejar una solicitud de devolución de llamada. Esta solicitud de devolución de llamada incluye la posición del llamante original en la cola de espera. El agente recibe la solicitud en forma de mensaje de voz. Después de escuchar el mensaje de voz, el agente puede devolver la llamada al llamante a través de una ventana emergente.

Si se ha definido un agente preferido para un llamante, las solicitudes de devolución de llamada de ese llamante se conmutan, en primer lugar, al agente preferido. Si al agente preferido no está disponible, la solicitud de devolución de llamada se transfiere a cualquier otro agente disponible.

18.4 Asesoramiento VIP

En cada cola de espera se puede definir de forma personalizada si determinados llamantes o llamantes cuyo número responda a patrones configurables deberán ser tratados de forma preferente. Este tratamiento les permite entrar en contacto más rápidamente con un agente libre.

Si todos los agentes están asignados a una cola de espera, se conecta a los llamantes VIP de forma preferente con el siguiente agente libre.

18.4.1 Prioridad de llamantes VIP

Mediante la prioridad de llamantes VIP se puede definir, de forma individualizada para cada cola, si los llamantes incluidos en la lista de llamadas VIP (por ejemplo, clientes) deben ser tratados con preferencia.

Los valores de prioridad de llamantes VIP se puede determinar libremente en función del tiempo de espera del llamante en una cola. De esta forma, el nivel de prioridad de los llamantes VIP se define frente al de los llamantes normales.

Si un llamante VIP activa una devolución de llamadas de agentes (grabación de un mensaje de voz con solicitud de devolución de llamada), en la cola de espera permanece la devolución de llamadas de agentes en lugar del llamante VIP. En este caso no se aplica la prioridad de llamantes VIP.

Los llamantes VIP deben estar incluidos en la lista de llamadas VIP (véase Lista de llamadas VIP).

18.4.2 Lista de llamadas VIP

Los llamantes (directorio externo) ya registrados en el sistema de comunicación se pueden incluir en la lista de llamadas VIP. Se pueden seleccionar varias opciones o utilizar la función "**Seleccionar todo**". Además se pueden introducir patrones de números de teléfono. Los patrones de números de teléfono se componen de una determinada secuencia de cifras y de un comodín (marcador de posición). De esta forma, por ejemplo, se puede incluir a todos los empleados de una empresa en la lista de llamadas VIP.

Por cada cola, la prioridad de llamantes VIP permite definir si

- los llamantes incluidos en la lista de llamadas VIP y
- los llamantes que se correspondan con uno de los patrones de números de teléfono incluidos en una lista de llamadas VIP serán tratados de forma preferente.

No se pueden introducir patrones de números de teléfono en formato canónico. Tampoco se pueden utilizar abreviaturas de prefijos de país (p. ej. +49 en lugar de 0049). Siempre hay que indicar los patrones de números de teléfono.

Ejemplos de patrones de números de teléfono:

- 089 7577* (089 = Código de red local de Múnich, 7577 = Número de teléfono del sistema de una empresa, * = Comodín para números). Al introducir este patrón de números de teléfono en la lista de llamadas VIP todos los llamantes de Múnich cuyo número comience por 7577 reciben un tratamiento preferente.
- 0039* (0039 = Prefijo del país Italia, * = Comodín para números). Al introducir este patrón de números de teléfono en la lista de llamadas VIP, todos los llamantes de Italia pueden recibir un trato preferente.

En un patrón de números de teléfono se pueden utilizar como comodines (marcadores de posición) los siguientes caracteres:

- * = comodín para números
- ? = comodín para cifras

18.5 Solución de respaldo (solución Fallback)

Si el Contact Center no está disponible por distintos problemas (caída, falta de conexión o similar), se conmuta automáticamente a la prestación "Uniform Call Distribution UCD" del sistema de comunicación. Esta prestación sirve así como solución de respaldo para el Contact Center.

En caso de caída del Contact Center, las llamadas entrantes se distribuyen según la solución de respaldo. No se pueden distribuir faxes ni correos electrónicos.

Sí, en función de los requisitos se puede configurar una de las soluciones de respaldo descritas a continuación.

Solución de respaldo estándar

En este caso, la solución de respaldo se basa en los ID UCD (ID de agentes) de los agentes:

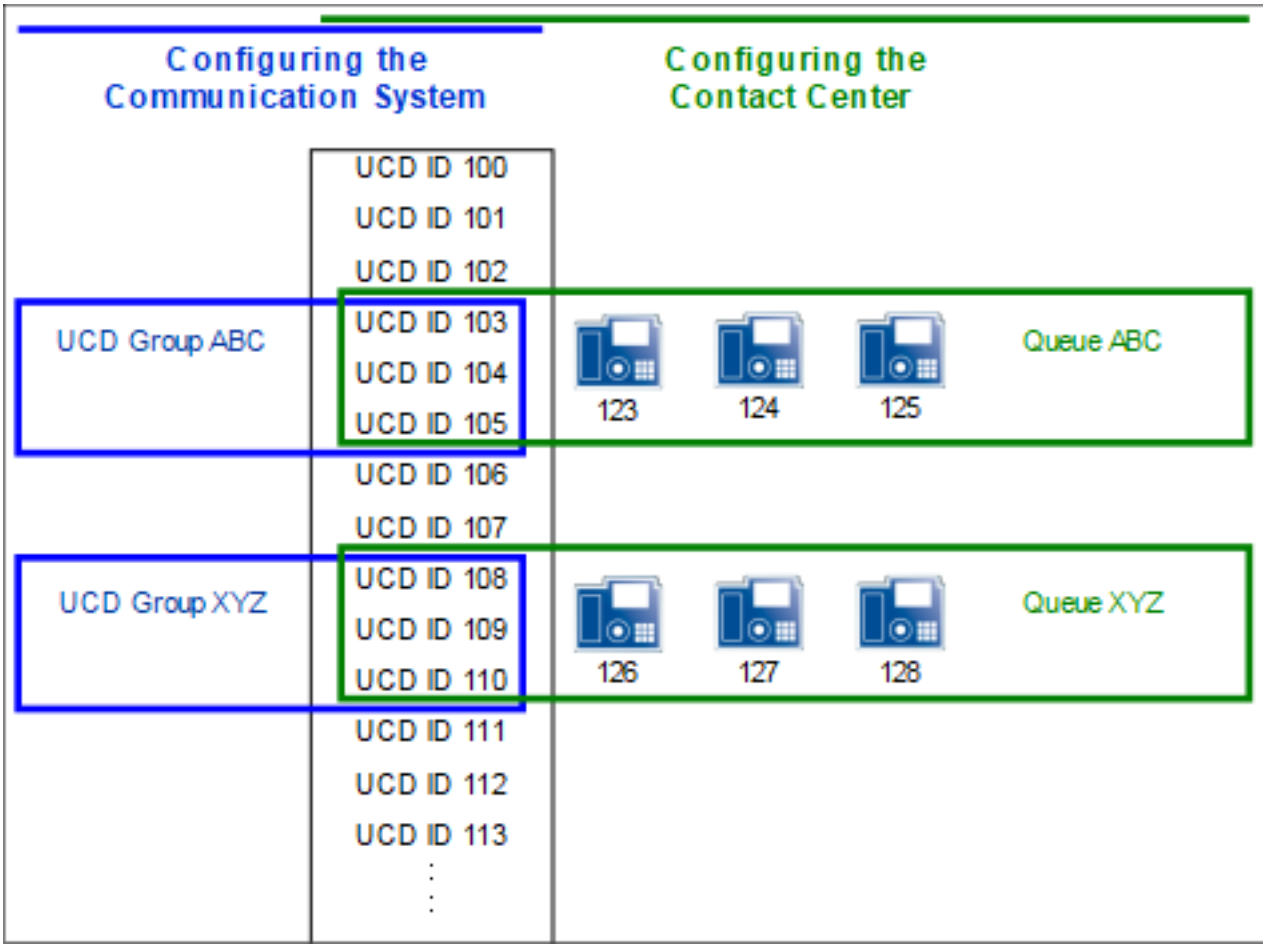
- Se han asignado agentes a los grupos UCD del sistema de comunicación mediante ID UCD. El ID UCD determina qué grupo UCD se asigna al agente en caso de caída del Contact Center.

Para garantizar el correcto funcionamiento de la solución de respaldo estándar, a cada cola de espera se deben asignar los agentes de Contact Center con los ID UCD que fueron asignados a los grupos UCD correspondientes.

En caso de caída del Contact Center, las llamadas entrantes se distribuyen entre los agentes registrados a través de los distintos grupos UCD.

Ejemplo:

- El grupo UCD ABC recibe asignados los ID UCD 103, 104 y 105. El grupo UCD XYZ tiene asignados los ID UCD 108, 109 y 110.
- Las extensiones 123, 124 y 125 se configuran como agentes con los identificadores UCD 103, 104 y 105. Las extensiones 126, 127 y 128 se configuran como agentes con los identificadores UCD 108, 109 y 110.
- En la asignación de agentes a colas de espera, las extensiones 123, 124 y 125 deben asignarse a la cola ABC y las extensiones 126, 127 y 128 a la cola XYZ.



Solución de respaldo básica

En este caso, todos los agentes del Contact Center se asignan al grupo UCD de respaldo mediante sus ID UCD. Al asignar los agentes correspondientes, los ID UCD se utilizan también en las colas de espera del Contact Center. De esta forma se garantiza que en caso de caída del Contact Center los sistemas no tengan que volver a registrarse en su teléfono con otro ID de forma manual. Este grupo UCD de respaldo se define como destino de transferencia automática diferida para todos los grupos UCD del sistema de comunicación.

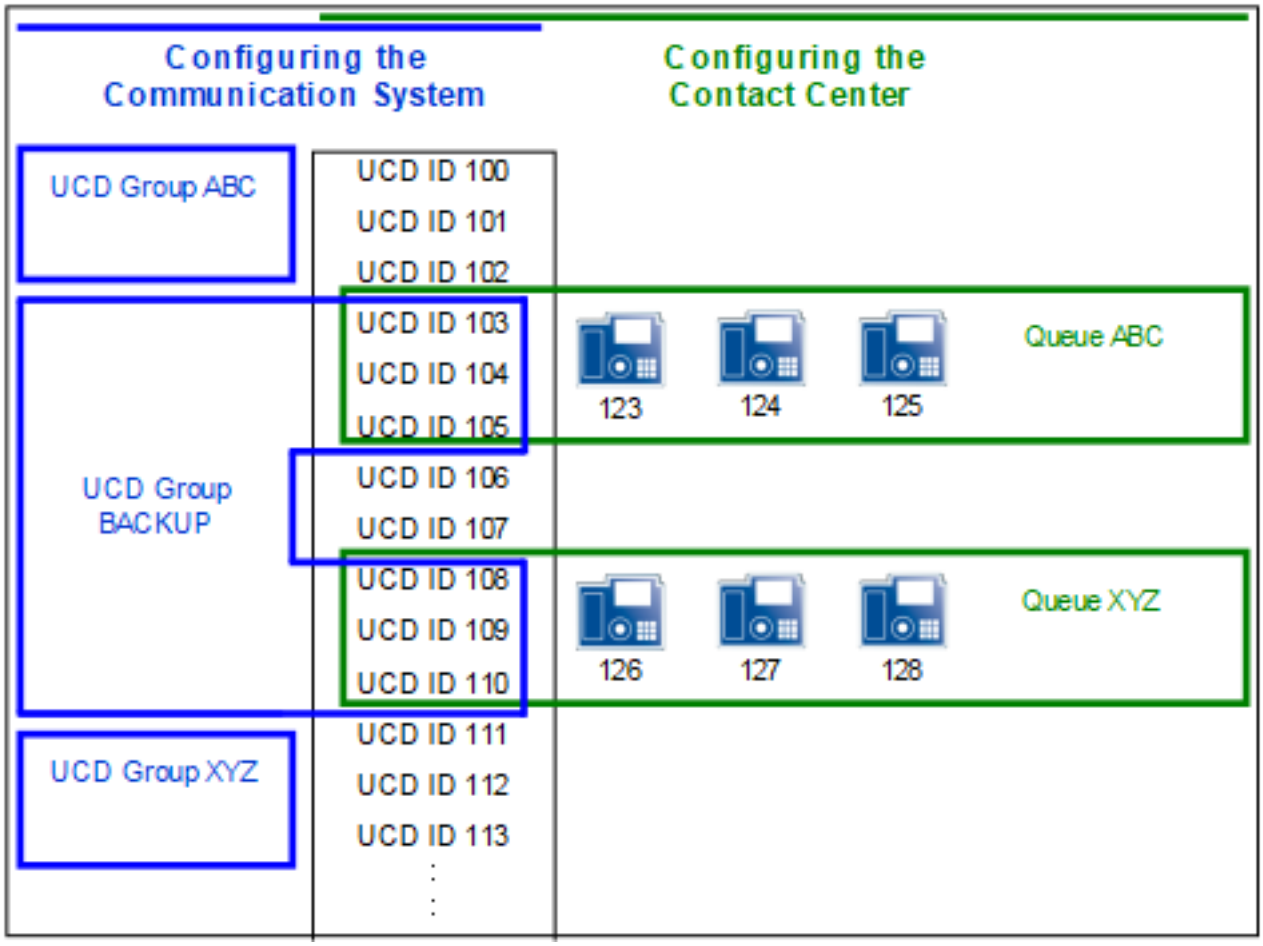
Nota: El grupo UCD Respaldo configurado también debe configurarse como grupo en el Contact Center. Solo así se garantiza que este grupo también esté controlado.

En caso de caída del Contact Center, las llamadas entrantes se distribuyen entre todos los agentes del grupo UCD de respaldo.

Ejemplo:

- No se ha asignado un ID UCD a los grupos UCD ABC y XYZ. El grupo UCD RESPALDO recibe asignados los ID UCD 103 a 105 y 108 a 110.
- Las extensiones 123, 124 y 125 se configuran como agentes con los identificadores UCD 103, 104 y 105. Las extensiones 126, 127 y 128 se configuran como agentes con los identificadores UCD 108, 109 y 110.

- En la asignación de agentes a colas de espera, las extensiones 123, 124 y 125 se asignan a la cola ABC y las extensiones 126, 127 y 128 a la cola XYZ.



Solución de respaldo específica del cliente

En este caso, la configuración específica del cliente del Contact Center se restablece a través de varios grupos UCD.

En caso de caída del Contact Center se consigue un comportamiento similar de la solución de respaldo.

Para obtener información sobre la configuración de una distribución de llamadas a través de la prestación "Uniform Call Distribution, UCD" del sistema de comunicación, véase UCD (Uniform Call Distribution).

Una ventaja fundamental de la solución de respaldo específica del cliente es la precisa representación del Contact Center en la solución de respaldo.

Una desventaja de la solución de respaldo específica del cliente es lo complejo de su configuración. Además, todos los cambios realizados en la configuración del Contact Center deben restablecerse en la solución de respaldo para garantizar un comportamiento similar de la transferencia de llamadas.

Una ventaja fundamental de la solución de respaldo básica y estándar es lo sencillo de su configuración.

18.6 Configuración del Contact Center

Al configurar el Contact Center, hay que definir en primer lugar los grupos UCD. Las colas del Contact Center son grupos de trabajo basados en los grupos UCD del sistema de comunicación. A continuación se puede realizar la configuración propia del Contact Center (planes horarios, colas, etc.).

Antes de configurar el Contact Center, se deben acordar con el cliente los procedimientos de distribución de llamadas en modo de servicio normal y de emergencia.

Consejo: El Contact Center solo se debe configurar una vez haya finalizado la configuración del sistema de comunicación y de la UC Suite.

Si se realizan cambios en la configuración de los grupos UCD, hay que reiniciar la UC Suite a través del Centro de servicios de la Gestión basada en Web (WBM).

Las siguientes licencias son prerrequisito para el servicio de un Contact Center:

- Un número pertinente de licencias para agentes (myAgent)
- Licencia de fax de Contact-Center (para la recepción y envío de faxes), si es necesario
- Licencia de correo electrónico de Contact-Center (para la recepción y envío de correos electrónicos), si es necesario

18.6.1 Ejemplo de configuración de Contact Center

El principio operativo del Contact Center con OpenScape Business se muestra mediante un ejemplo. La estructura y configuración del ejemplo se basan en un escenario de clientes ficticio con funciones estándar de Contact Center.

Escenario de ejemplo de un Contact Center

La empresa XYZ opera un Contact Center con los siguientes números de teléfono (colas de espera):

- Número de teléfono 440 para el área Servicio
- Número de teléfono 444 para el área Ventas
- Número de teléfono 456 para las llamadas gratuitas (Hotline). Los llamantes reciben un anuncio grabado y, a continuación, pueden ponerse en contacto con el área de Servicio o con el área de Ventas marcando un determinado dígito.

El Contact Center consta de seis empleados (agentes). De ellos, tres son empleados del área de Servicio y tres del área de Ventas.

Las colas de espera para las áreas de Servicio y Ventas deben estar accesibles de forma directa en el horario de 09:00 a 17:00 horas. Ambas colas de espera disponen de un buzón de fax y de una dirección de correo electrónico.

Si todos los agentes están al teléfono o no están disponibles, se notificará al usuario y escuchará la música en espera. Si tras un tiempo determinado no hay ningún agente libre, el llamante puede dejar una solicitud de devolución de llamada o acceder al puesto de operadora marcando un determinado

dígito. Si no se marca ningún dígito, el llamante es transferido de nuevo automáticamente a la cola.

Fuera del horario comercial se debe reproducir un anuncio grabado que permita la grabación de una solicitud de devolución de llamada (Devolución de llamadas de agentes).

Nota: La reproducción de anuncios grabados solo es posible mediante líneas urbanas. Para reproducir el anuncio grabado, la llamada debe proceder de una línea urbana o bien OpenScape Contact Center debe supervisar a la persona que llama.

Durante la pausa de mediodía (de 12:00 a 13:00 h) se reproducirá un anuncio grabado en las colas de espera de las áreas Servicio y Ventas. Este anuncio grabado permite la grabación de una solicitud de devolución de llamada.

Solución de respaldo (solución Fallback) a través del grupo UCD de respaldo: si el Contact Center no está disponible por problemas (caída, falta de conexión o similar) se conmutará automáticamente a la prestación "Uniform Call Distribution UCD" del sistema de comunicación. Para ello, todos los agentes del Contact Center se deben asignar a un único grupo UCD de respaldo. Este grupo UCD de respaldo se debe definir como destino de transferencia automática diferida para todos los grupos UCD del sistema de comunicación. En caso de caída del Contact Center, las llamadas entrantes se distribuyen entre los agentes del grupo UCD de respaldo.

Configuración del escenario de ejemplo

Se pueden ejecutar las siguientes tareas para el escenario de ejemplo:

- Configuración de grupos UCD

  Las colas del Contact Center son grupos de trabajo basados en los grupos UCD del sistema de comunicación. Antes de proceder a la configuración del Contact Center propiamente dicha, hay que definir los grupos UCD.

  En el presente ejemplo de Contact Center de la empresa XYZ hay que configurar tres grupos UCD (Servicio, Ventas, Hotline).
- Configuración de la solución de respaldo (solución Fallback)

  En el ejemplo presente hay que configurar un grupo UCD de respaldo que debe definirse como destino de transferencia automática diferida de todos los grupos UCD del sistema de comunicación.
- Configuración de extensiones como agentes

  En este ejemplo hay que configurar seis extensiones como agentes.
- Grabación de anuncios grabados individuales

  En este ejemplo hay que grabar distintos anuncios. Son, por ejemplo, anuncios grabados para el caso de que no haya ningún agente disponible o para informar a los llamantes sobre opciones (**Ejecutar acción tras dígito**).
- Carga de anuncios grabados personalizados

  En este ejemplo hay que cargar los anuncios grabados en el sistema de comunicación.

- Definición de planes horarios

  Por cada intervalo de tiempo de un plan de horario se define a través de reglas (Call Control Vector CCV) cómo se gestionarán las llamadas entrantes en determinados días y a determinadas horas.

  En el presente ejemplo, hay que definir un plan horario (Standard Schedule XYZ) con una regla para las horas fuera del horario comercial y excepciones para el horario comercial y para la pausa de mediodía. Además, hay que definir un segundo plan horario (Standard Schedule Hotline) con una regla para llamadas gratuitas (Hotline).

Plan horario	Regla (CCV)	
Standard Schedule XYZ	Out Of The Office	Horario fuera del horario comercial
	Open	Horario comercial de 08:00 a 11:59 horas = Open1
		Horario comercial de 13:00 a 17:00 horas = Open2
	Lunch Break (Pausa de mediodía)	Pausa de mediodía de 12:00 a 12:59 horas
Standard Schedule Hotline	Hot-line	24 horas

- Agregar tres colas de espera

  En este ejemplo hay que configurar una cola de espera para el área Servicio y otra cola para el área Ventas. Además, hay que configurar otra cola (Hotline) para las llamadas gratuitas.
- Asignar agentes a las colas

  En este ejemplo hay que asignar a tres agentes a la cola Servicio y otros tres agentes a la cola Ventas.

Para obtener información sobre la configuración de todas las funciones del Contact Center, consulte los Procedimiento de configuración .

18.6.1.1 Cómo configurar grupos UCD para el ejemplo de Contact Center

El asistente **UCD** permite definir tres grupos UCD (Servicio, Ventas, Hotline) con los números de teléfono 440, 444 y 456 para el ejemplo de Contact Center de la empresa XYZ.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.

3) Haga clic en **Editar** para iniciar el asistente **UCD**. Podrá ver una lista de todos los grupos UCD posibles.
4) Para configurar un grupo UCD, en la fila del grupo UCD deseado haga clic en **Editar**.
5) En el campo **Número de teléfono**, introduzca el número de teléfono `440` del grupo UCD Servicio.
6) En el campo **Número de marcación directa**, introduzca el número de marcación directa `440` del grupo UCD Servicio.
7) En el campo **Nombre** introduzca el nombre `Servicio`.
8) Haga clic en **OK & Continuar**. Se abre la ventana **Asignación de agentes UCD**.
9) Haga clic en **OK & Continuar**, ya que no se pueden asignar ID UCD al grupo UCD Servicio.

   Dado que en el Contact Center de ejemplo de la empresa XYZ se va a configurar una solución de respaldo a través de un grupo UCD de respaldo, a los tres grupos UCD Servicio, Ventas y Hotline no se les pueden asignar identificadores UCD.
10) Haga clic en **OK & Continuar**. Se abre la ventana **Editar anuncio grabado/desbordamiento**.
11) Haga clic en **Aceptar**, puesto que los parámetros mostrados no son relevantes para la configuración del grupo UCD.
12) Repita los pasos del 4 al 11 para el grupo UCD Ventas con el número de teléfono 444 y para el grupo UCD Hotline con el número de teléfono 456.
13) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

18.6.1.2 Cómo configurar una solución de respaldo (solución Fallback) para el ejemplo de Contact Center

El asistente **UCD** permite configurar un grupo UCD de respaldo con el número de teléfono 400 para el ejemplo de Contact Center de la empresa XYZ. En este ejemplo se utilizan los la ID de agentes UCD 101 a 106. Además, define el grupo UCD de respaldo como destino de transferencia automática diferida de todos los grupos UCD del ejemplo de Contact Center de la empresa XYZ.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

El grupo UCD Respaldo con el número de teléfono 400 debe configurarse en las colas de UC Suite Contact Center.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **UCD**. Podrá ver una lista de todos los grupos UCD posibles.
4) Para configurar un grupo UCD, en la fila del grupo UCD deseado haga clic en **Editar**.

5) En el campo **Número de teléfono**, introduzca el número de teléfono `400` del grupo UCD Respaldo.
6) En el campo `Número de marcación directa`, introduzca el número de marcación directa **400** del grupo UCD Respaldo.
7) En el campo **Nombre** introduzca el nombre `Respaldo`.
8) Haga clic en **OK & Continuar**. Se abre la ventana **Asignación de agentes UCD**.
9) Seleccione los ID de agente UCD deseados en **Selección** y asigne los agentes al grupo UCD Respaldo. Para hacerlo, haga clic en **Agregar**.
10) Haga clic en **OK & Continuar**. Se muestra la ventana **Asignar extensiones**.
11) Asigne todos los ID de agente UCD a las extensiones deseadas.
12) Haga clic en **OK & Continuar**. Se abre la ventana **Editar anuncio grabado/desbordamiento**.
13) Haga clic en **Aceptar**, ya que los parámetros mostrados no son relevantes para la configuración del grupo UCD Respaldo.
14) Para configurar el nuevo grupo UCD Respaldo como destino de transferencia automática diferida del grupo UCD Servicio, en la línea del grupo UCD Servicio, haga clic en **Editar**.
15) Haga clic en **OK & Continuar** varias veces, hasta que se abra la ventana **Editar anuncio grabado/desbordamiento**.
16) En la lista desplegable **Destino de desbordamiento**, seleccione el grupo UCD Respaldo con el número de teléfono 400 como destino de transferencia automática diferida.
17) Haga clic en **Aceptar**.
18) Repita los pasos del 14 al 17 para configurar el nuevo grupo UCD Respaldo como destino de transferencia automática de los grupos UCD Ventas y Hotline.
19) Clic **OK & Continuar** y luego **Salir**.

18.6.1.3 Cómo configurar extensiones como Agente para el ejemplo de Contact Center

El asistente **Directorio de usuario** permite configurar extensiones como agentes para el ejemplo de Contact Center de la empresa XYZ. En este ejemplo, las extensiones con los números de teléfono 101 a 106 se configuran como agentes. Las extensiones con los números de teléfono 101 y 104 reciben el nivel de clase de servicio **Supervisor** y las demás extensiones el nivel de clase de servicio **Agente**.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Directorio de usuario**.
4) Marque el usuario con la **Extensión** 101 y haga clic en **Editar**.

5) En el grupo de menús, haga clic en **Detalles personales** > **Nivel de usuario**.
6) Active la casilla de verificación **Agente disponible de forma permanente**. De esta forma, el agente también permanecerá disponible para llamadas, faxes y correos electrónicos aunque no acepte una llamada, un fax o un correo electrónico.
7) En la lista desplegable **Nivel** seleccione el nivel de clase de servicio **Supervisor**.
8) Haga clic en **Guardar**.
9) Repita los pasos del 4 al 8 para configurar las extensiones con los números de teléfonos del 102 al 106 como agentes.

18.6.1.4 Cómo grabar anuncios grabados para el ejemplo de Contact-Center

El asistente Grabadora permite grabar anuncios para el ejemplo de Contact Center de la empresa XYZ. Los anuncios grabados son necesarios, entre otras cosas, por si no se puede acceder a ningún agente.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en Editar para iniciar el asistente Carga de archivo.
4) Active el campo de opción **Seguridad**.
5) En la lista desplegable Extensión seleccione el número del teléfono a través del que se realizará la grabación.
6) Haga clic en Realizar llamada. Se llama al número de teléfono seleccionado.
7) Descuelgue el auricular, y en el campo Nombre de archivo, introduzca un nombre para el anuncio grabado.
8) Haga clic en Grabar, para iniciar la grabación del anuncio.
9) Haga clic en Detener, en cuanto termine la grabación del anuncio.
10) Si desea escuchar un nuevo anuncio grabado, haga clic en Reproducir.
11) Haga clic en Cerrar, para guardar los anuncios grabados.

Consejo:

Después de grabar y guardar un anuncio grabado ya no se puede borrar. No obstante, si se utiliza el mismo nombre de archivo se puede sobrescribir un anuncio grabado ya guardado. Por ejemplo, al guardar el archivo de sonido anuncio1.wav se sobrescribe el archivo anuncio1.wav ya existente.

---

12) Repita los pasos del 3 al 10 para grabar nuevos anuncios grabados para el ejemplo de Contact Center de la empresa XYZ.

18.6.1.5 Cómo cargar anuncios grabados para el ejemplo de Contact Center

El asistente Carga de archivo permite cargar anuncios grabados para el ejemplo de Contact Center de la empresa XYZ.

Requisitos previos

Hay disponible un archivo de sonido en formato wav con las siguientes propiedades: monoaural, tasa de muestreo de sonido 8 kHz, tamaño de muestreo de sonido 16 bit, tamaño marco 2.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en Editar para iniciar el asistente Carga de archivo.
4) Haga clic en la pestaña **Administrador de archivos de audio** .
5) En la lista desplegable Destino de carga seleccione el destino Puesto de operadora.
6) Seleccione el botón de radio **Uploader** y haga clic en **Choose File**, navegue hasta la ubicación de almacenamiento deseada del archivo de audio y haga clic en **Open**.
7) Haga clic en Carga.

Consejo:

Después de la carga de archivo ya no se puede borrar un archivo de sonido. No obstante, si se utiliza el mismo nombre de archivo se puede sobrescribir un archivo de sonido ya cargado. Por ejemplo, al cargar el archivo de sonido anuncio1.wav se sobrescribe el archivo anuncio1.wav ya existente.

---

8) Repita los pasos del 4 al 7 para cargar más anuncios grabados para el ejemplo de Contact Center de la empresa XYZ.

18.6.1.6 Cómo agregar el plan horario Standard Schedule XYZ para el ejemplo de Contact Center

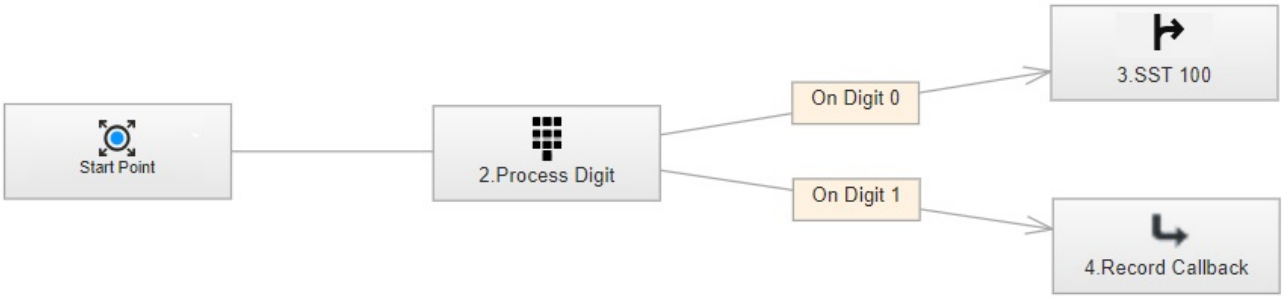
Este ejemplo le muestra cómo utilizar el asistente del **Contact Center** para definir un cronograma con reglas para descansos y horarios comerciales para el Contact Center de muestra de la empresa XYZ. Para ello hay que definir un plan horario (Standard Schedule XYZ) con una regla para el horario fuera del horario comercial (Out Of The Office) y excepciones para el horario comercial (de 08:00 a 11:59 h = Open1, de 13:00 a 17:00 h = Open2) y la pausa de mediodía (de 12:00 a 12:59 h = Lunch Break).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Plan horario**. Aparecen todos los planes horarios existentes.
5) Haga clic en **Agregar**.
6) Haga clic en **Agregar** en el área **Programación**.
7) Defina la regla representada para las horas fuera del horario comercial.



En la lista de herramientas CCV haga clic en uno de los objetos CCV incluidos en las reglas representadas y arrástrelo al editor de reglas. Ingrese las propiedades indicadas a continuación en la ventana del objeto CCV que aparece y confírmelo haciendo clic en **Guardar**. Repita el procedimiento para todos los demás objetos CCV. Conecte siempre los objetos CCV. Para ello, haga clic con el botón secundario del ratón en el primero de los dos objetos CCV que quiera conectar. En el menú desplegable, utilice la opción **Link To** para seleccionar el segundo de los objetos CCV que desea conectar. Repita el procedimiento para todos los demás objetos CCV que desee conectar.

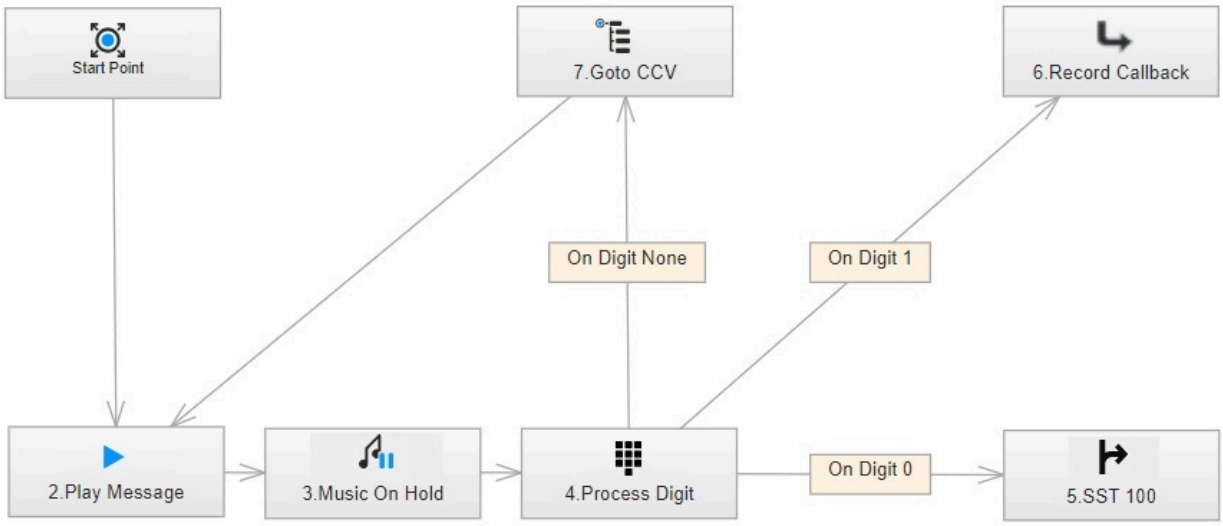
Propiedad	Valor
1st. Objeto CCV: **Ejecutar acción tras dígito**	
Lista de reproducción	Archivo de sonido en formato wav
Tiempo excedido al introducir dígitos	5
Descripción	Anuncio: "Presione el dígito 0 para...; Presione el dígito 1 para...
2.° Objeto CCV: **Transferencia de un solo paso**	
Extensión de destino	100
Descripción	Pasar al puesto de operadora
Iniciar proceso después de marcar los dígitos	0
Objeto 3er CCV: **Grabar devolución de llamada**	
Tipo	Devolución de llamada amplia
Longitud máxima del mensaje	20

Propiedad		Valor
	Descripción	Solicitud de devolución de llamada (Devolución de llamadas de agentes)
	Iniciar proceso después de marcar los dígitos	1

Haga clic en **Guardar**. Ingrese `Fuera de la oficina` como **nombre CCV** de la regla y luego haga clic en **Guardar**. Si la nueva regla es errónea, no se podrá guardar. El objeto u objetos CCV erróneos aparecen marcados en rojo en el editor de reglas. Cierre la ventana que permite configurar el guardado de la regla.

Seleccione la regla `Fuera de la oficina` en la lista desplegable **CCV predeterminado**.

8) Ingrese el nombre `Horario estándar XYZ` en el campo **Nombre del horario**.
9) Haga clic en **Guardar**.
10) Haga clic en **Agregar** en el área **Programación**.
11) Defina la regla representada para el horario comercial.



En la lista de herramientas CCV haga clic en uno de los objetos CCV incluidos en las reglas representadas y arrástrelo al editor de reglas. Ingrese las propiedades indicadas a continuación en la ventana del objeto CCV que aparece y confírmelo haciendo clic en **Guardar**. Repita el procedimiento para todos los demás objetos CCV. Conecte siempre los objetos CCV. Para ello, haga clic con el botón secundario del ratón en el primero de los dos objetos CCV que quiera conectar. En el menú desplegable, utilice la opción **Link To** para seleccionar el segundo de los objetos CCV que desea conectar. Repita el procedimiento para todos los demás objetos CCV que desee conectar.

Propiedad		Valor
1st. Objeto CCV: **Reproducir mensaje**		
	Nombre del archivo	Archivo de sonido en formato wav

Propiedad		Valor
	Dígitos de interrupción	5
	Descripción	Anuncio grabado: Agentes no disponibles
2.° Objeto CCV: **Música en espera**		
	Valor de hora	30
	Descripción	Música en espera durante 30 segundos
3rd. Objeto CCV: **Ejecutar acción tras dígito**		
	Lista de reproducción	Archivo de sonido en formato wav
	Tiempo excedido al introducir dígitos	5
	Descripción	Anuncio: "Presione el dígito 0 para...; Presione el dígito 1 para...
4th. Objeto CCV **Transferencia de un solo paso**		
	Extensión de destino	100
	Descripción	Pasar al puesto de operadora
	Iniciar proceso después de marcar los dígitos	0
5th. Objeto CCV: **Grabar devolución de llamada**		
	Tipo	Devolución de llamada amplia
	Longitud máxima del mensaje	20
	Descripción	Solicitud de devolución de llamada (Devolución de llamadas de agentes)
	Iniciar proceso después de marcar los dígitos	1
6.° Objeto CCV: **A CCV**		
	CCV de destino	1. Reproducir mensaje
	Descripción	Volver al anuncio grabado

Haga clic en **Guardar**. Ingrese `Abrir` como **Nombre CCV** para la nueva regla y luego haga clic en **Guardar**. Cierre la ventana que permite configurar el guardado de la regla.

En la lista desplegable, seleccione la regla `Abrir` para la excepción Open1.

12) En el área **Excepciones**, haga clic en **Agregar** para definir la primera excepción para el horario comercial.

13) Ingrese **Abrir1** en el campo `Descripción`.

14) Defina a qué hora se aplicará la excepción Open1:

Habilite el botón de opción **Dentro del rango de tiempo**. Seleccione **08:00** como hora de inicio en el cuadro de lista `Hora de inicio` y **11:59** como

`hora de finalización` en el cuadro de lista Hora de finalización para definir el período de tiempo diario.

Seleccione los días de la semana en los que se aplicará la regla en la ventana **Seleccionar días.** Haga clic en **Guardar**.

15) En el área **Excepciones**, haga clic en **Agregar** para definir la segunda excepción para el horario comercial.

16) Ingrese `Open2` en el campo **Descripción**.

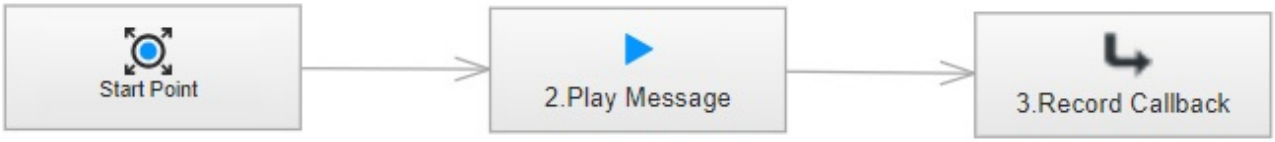
17) En la lista desplegable, seleccione la regla `Abrir` para la excepción Open2.

18) Defina a qué hora se aplicará la excepción Open2:

Seleccione **Dentro del rango de tiempo** en la lista desplegable **Tipo**. Seleccione **13:00** como hora de inicio en el cuadro de lista `Hora de inicio` y **17:00** como `hora de finalización` en el cuadro de lista Hora de finalización para definir el período de tiempo diario.

Seleccione los días de la semana en los que se aplicará la regla en la ventana **Seleccionar días.** Haga clic en **Guardar**.

19) Defina la regla representada para la pausa de mediodía.



En la lista de herramientas CCV haga clic en uno de los objetos CCV incluidos en las reglas representadas y arrástrelo al editor de reglas. Ingrese las propiedades indicadas a continuación en la ventana del objeto CCV que aparece y confírmelo haciendo clic en **Guardar**. Repita el procedimiento para todos los demás objetos CCV. Conecte siempre los objetos CCV. Para ello, haga clic con el botón secundario del ratón en el primero de los dos objetos CCV que quiera conectar. En el menú desplegable, utilice la opción **Link To** para seleccionar el segundo de los objetos CCV que desea conectar. Repita el procedimiento para todos los demás objetos CCV que desee conectar.

Propiedad	Valor
1st. Objeto CCV: **Reproducir mensaje**	
Nombre del archivo	Archivo de sonido en formato wav
Dígitos de interrupción	Seleccionar servicio
Descripción	Anuncio grabado: Agentes no disponibles
Objeto 2º CCV: **Grabar devolución de llamada**	
Tipo	Devolución de llamada amplia
Longitud máxima del mensaje	20
Descripción	Solicitud de devolución de llamada (Devolución de llamadas de agentes)

Propiedad		Valor
	Iniciar proceso después de marcar los dígitos	1

Haga clic en **Guardar**. Ingrese `Pausa para el almuerzo` como **Nombre CCV** de la regla. Cierre la ventana que permite configurar el guardado de la regla.

En la lista desplegable, seleccione la regla `Pausa para el almuerzo` para la excepción de Pausa para el almuerzo.

20) En el área **Excepciones**, haga clic en **Agregar** para definir la excepción para la pausa del almuerzo.

21) Ingrese la **pausa para el almuerzo** en el campo `Descripción`.

22) Defina a qué hora se aplicará la excepción "Lunch Break":

Seleccione **Dentro del rango de tiempo** en la lista desplegable **Tipo**. Seleccione `12:00` como **hora de inicio** en el cuadro de lista Hora de inicio y `12:59` como hora de finalización en el cuadro de lista **Hora de finalización** para definir el período de tiempo diario.

Seleccione los días de la semana en los que se aplicará la regla en la ventana **Seleccionar días.** Haga clic en **Guardar**.

23) Si desea comprobar qué regla (CCV) del plan horario se ejecutará en un momento determinado, haga clic en **Probar plan horario**. En la lista desplegable **Fecha**, seleccione el día deseado y en la lista desplegable **Hora**, la hora. Haga clic en **Probar plan horario**. A continuación, se muestra qué regla (CCV) está activa ese día a esa hora. Haga clic en **Cerrar** para cerrar la ventana **Probar plan horario**.

24) Haga clic en **Guardar**.

25) Cierre la ventana.

18.6.1.7 Cómo agregar el plan horario Standard Schedule Hotline para el ejemplo de Contact Center

Puede definir el horario con una regla para llamadas gratuitas (Hotline) para el Contact Center de muestra de la empresa XYZ con el asistente **Contact Center**.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.

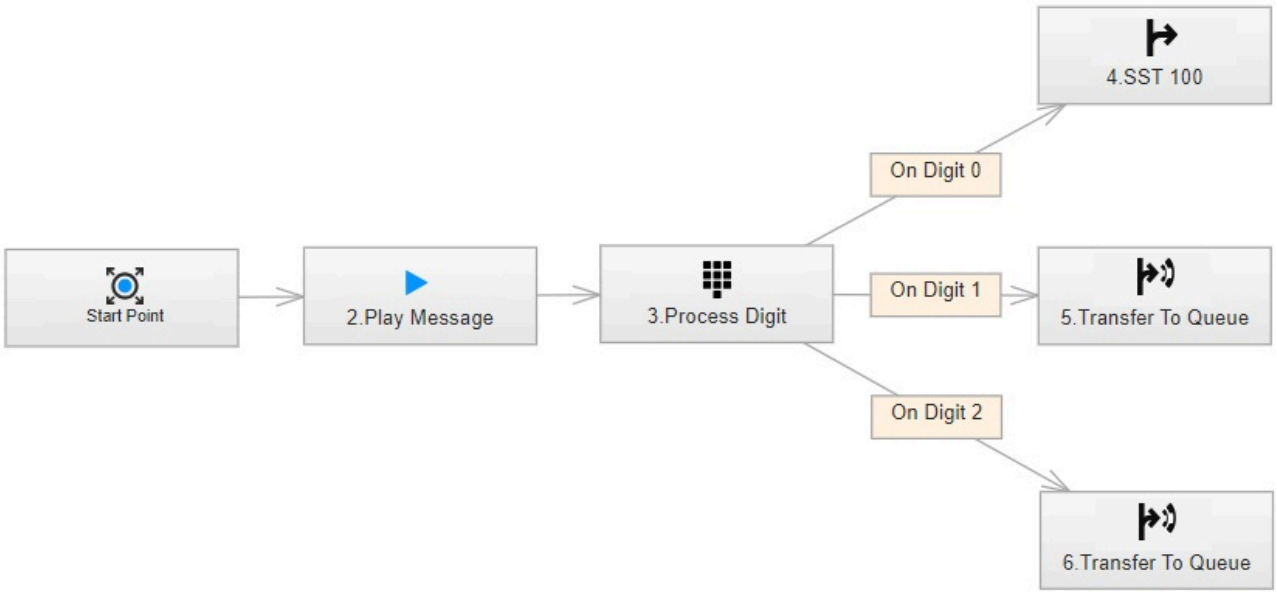
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.

4) Haga clic en **Plan horario**. Aparecen todos los planes horarios existentes.

5) Haga clic en **Agregar**.

6) Haga clic en **Agregar** en el área **Programación**.

7) Defina la regla representada para las llamadas gratuitas (Hotline).



En la lista de herramientas CCV haga clic en uno de los objetos CCV incluidos en las reglas representadas y arrástrelo al editor de reglas. Ingrese las propiedades indicadas a continuación en la ventana del objeto CCV que aparece y confírmelo haciendo clic en **Guardar**. Repita el procedimiento para todos los demás objetos CCV. Conecte siempre los objetos CCV. Para ello, haga clic con el botón secundario del ratón en el primero de los dos objetos CCV que quiera conectar. En el menú desplegable, utilice la opción **Link To** para seleccionar el segundo de los objetos CCV que desea conectar. Repita el procedimiento para todos los demás objetos CCV que desee conectar.

Propiedad	Valor
1st. Objeto CCV: **Reproducir mensaje**	
Nombre del archivo	Archivo de sonido en formato wav
Dígitos de interrupción	5
Descripción	Anuncio: Saludo
2.° Objeto CCV: **Ejecutar acción tras dígito**	
Lista de reproducción	Archivo de sonido en formato wav
Tiempo excedido al introducir dígitos	5
Descripción	Anuncio: "Presione el dígito 0 para...; Presione el dígito 1 para...
3rd. Objeto CCV: **Transferencia de un solo paso**	
Extensión de destino	100
Descripción	Pasar al puesto de operadora
Iniciar proceso después de marcar los dígitos	0

Propiedad	Valor
4th. Objeto CCV **Transferir a cola**	
Cola	440
Descripción	Pasar e la cola de espera Servicio
Iniciar proceso después de marcar los dígitos	1
5th. Objeto CCV **Transferir a cola**	
Cola	444
Descripción	Pasar a la cola de espera Ventas
Iniciar proceso después de marcar los dígitos	2

Haga clic en **Guardar**. Ingrese a la `línea directa` como el **nombre CCV** para la regla y luego haga clic en **Guardar**. Si la nueva regla es errónea, no se podrá guardar. El objeto u objetos CCV erróneos aparecen marcados en rojo en el editor de reglas. Cierre la ventana que permite configurar el guardado de la regla.

Seleccione la regla **Línea directa** en la lista desplegable `CCV predeterminad`o.

8) Ingrese el nombre `Línea directa de horario estándar` en el campo **Nombre del programa**.

9) Haga clic en **Guardar horario**.

18.6.1.8 Cómo agregar colas de espera para el ejemplo de Contact Center

Este ejemplo muestra cómo usar el asistente **Contact Center** para configurar colas para el Contact Center de ejemplo de la compañía XYZ. En este ejemplo hay que configurar una cola para el área Servicio (número de teléfono 440) y otra cola para el área Ventas (número de teléfono 444). Hay que configurar otra cola (Hotline, número de teléfono 456) para llamadas gratuitas.

Requisitos previos

Se han configurado los grupos UCD **Servicio**, **Ventas** y **Hotline** para el Contact Center de ejemplo.

Se han configurado los planes horarios **Plan horario estándar XYZ** y **Hotline de plan horario estándar** para el Contact Center de ejemplo.

Hay disponible al menos una cuenta de correo electrónico para la recepción de correo electrónico.

El envío de correo electrónico está configurado en el sistema de comunicación.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.

3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.

4) Haga clic en **Cola**.
5) Haga clic **Agregar**.
6) Haga clic en la pestaña **Ajustes generales**.
7) Introduzca el nombre `Servicio` en el campo **Nombre de cola**.
8) En la lista desplegable **Cola activa**, seleccione la opción **Activa**.
9) Introduzca el número **440** en el campo `Línea colectiva`.
10) Seleccione la opción **CSP** en la lista desplegable **Conmutación telefónica**.
11) Seleccione la opción **Plan horario estándar XYZ** en la lista desplegable **Plan horario**.
12) En el campo **Recuento de alarma de cola**, introduzca el valor `20`, por ejemplo.

    Si hay más de 20 llamantes en espera en la cola de espera, el símbolo de cola de los agentes pasa de verde a naranja.
13) En el campo **Hora de alarma de cola**, introduzca el valor `300`, por ejemplo.

    Si el tiempo de espera de una llamada en la cola supera los 300 segundos, la entrada correspondiente de la lista de llamadas del Contact Center del agente pasa a color rojo.
14) En el campo **Tiempo excedido de llamadas perdidas**, introduzca el valor `100`, por ejemplo, para que cualquier llamada no contestada en 100 segundos se desvíe al siguiente agente libre.
15) Introduzca un número en el campo **Umbral de llamada abandonada**; por ejemplo, `120`. De esta forma se registran en una estadística (en un informe) las llamadas abandonadas tras 120 segundos.
16) Seleccione la casilla de verificación **Ventana emergente activada**. para que cuando se produzcan llamadas entrantes en myAgent, se abra una ventana emergente con indicación y entrada de datos de cliente.
17) Active la opción **Sin tratamiento posterior**.
18) Seleccione la opción **Estático** en la lista desplegable **Modo de profundidad de cola**.
19) Introduzca un número en el campo **Tamaño de profundidad de cola**; por ejemplo, `5`.
20) Haga clic en la pestaña **Pilotos de cola**.
21) En la lista desplegable **Pilotos de fax entrantes**, seleccione las opciones que corresponda para los pilotos deseados (números de teléfono), de forma que los faxes se pongan en cola.

    Los faxes dirigidos a este número o números de teléfono se incluyen en la cola y se administran como llamadas entrantes.

22) Seleccione una de las siguientes opciones en el área **Servicio de correo electrónico entrante**, para que los correos electrónicos se incluyan en la cola:

- Si desea configurar una nueva dirección de correo electrónico, haga clic en **Agregar**. Se abre la ventana **Agregar**.

  Seleccione el método de autenticación para su servidor de correo electrónico en la lista desplegable **Método de autenticación**. Puede elegir entre **Básico** y **OAuth 2.0**.

  En el campo **Servidor**, introduzca la designación del servidor de correo electrónico que se utilizará para la recepción de los correos electrónicos (por ejemplo, `pop3.web.de`).

  En el campo **Puerto**, introduzca el número de puerto del servidor de correo electrónico (por ejemplo, `110`, el número de puerto estándar para POP3).

  Si el método de autenticación seleccionado es **Básico**, introduzca los datos de acceso al servidor de correo electrónico en los campos **Nombre de usuario** y **Contraseña**.

  Si el método de autenticación seleccionado es **OAuth 2.0**, introduzca el nombre de usuario para acceder al servidor de correo electrónico en los campos **Nombre de usuario**, **ID de tenencia**, **ID de aplicación** y **Contraseña de cliente**. El ID de tenencia, el ID de aplicación y la contraseña del cliente corresponden a la aplicación que se ha registrado en Azure AD para las colas de correo electrónico. Puede obtenerlas de su administrador de Azure AD. Introduzca el alcance de la aplicación en el campo **Alcance** (valor por defecto: https://outlook.office365.com/.default).

  Seleccione si desea realizar el envío de correo electrónico a través de una conexión SSL (Secure Socket Layer). Si desea usar una conexión SSL, active la casilla de verificación **Usar conexión SSL** (con ello se modifica, en su caso, el número de puerto del servidor de correo electrónico. Número de puerto estándar para POP3 mediante SSL = 995). Si no desea utilizar una conexión SSL, desactive la casilla de verificación **Usar conexión SSL**.

  Haga clic en **Guardar**. A continuación, la nueva dirección de correo aparecerá en la sección **Servicio de correo electrónico entrante**.
- Si desea editar una dirección de correo electrónico ya existente, marque la dirección deseada y haga clic en **Editar**. Se abre la ventana **Editar**.

  Cambie los parámetros deseados y, a continuación, haga clic en **Guardar**.
- Si desea eliminar una dirección de correo electrónico existente, marque la dirección deseada y haga clic en **Eliminar email**.

23) Haga clic en la pestaña **Varios**.

24) En el campo **Dirección de email de devolución**, indique la dirección de correo electrónico que podrá ver el destinatario en el envío de correos electrónicos por un agente.

25) Si activa la casilla de verificación **Encaminamiento de llamadas inteligente**, las llamadas entrantes se desvían automáticamente al agente con el que la persona que llama estuvo conectada por última vez.

26) Haga clic en **Guardar**.

27) Repita los pasos del 5 al 23 para configurar la cola de ventas. Repita los pasos del 5 al 17 y el paso 23 para configurar la cola Hotline.

18.6.1.9 Cómo asignar agentes a las colas del ejemplo de Contact-Center

El asistente **Contact Center** permite asignar a los agentes a colas de espera para el ejemplo de Contact Center de la empresa XYZ. En este ejemplo, hay que asignar tres agentes a la cola de espera Servicio y tres agentes a la cola de espera Ventas.

Requisitos previos

Se han configurado las colas de espera **Servicio** y **Ventas** para el ejemplo de Contact Center.

Se han configurado seis agentes para el ejemplo de Contact Center.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.

3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.

4) Haga clic en **Enlaces de cola**. Se muestran las colas de **Servicio** y **Ventas**.

5) Seleccione la cola a la que desea asignar un agente y haga clic en **Editar**. Se muestran todos los agentes asignados.

6) Seleccione el primer agente para la cola de **Servicio** de la tabla y haga clic en **Editar**. Aparecerá la ventana **Editar**.

7) Elija una de estas opciones:

- Si el agente debe recibir llamadas sin tener en cuenta la carga de la cola de **Servicio**, seleccione el **Agente principal** en la lista desplegable **Tipo**.
- Si el agente debe recibir llamadas solo cuando se desborde la cola de **Servicio**, seleccione el **Agente de desbordamiento** en la lista desplegable **Tipo**.

8) Si ha seleccionado **Agente de** desbordamiento:

a) En el campo **Desbordamiento tras segundos en cola** indique el tiempo tras el cual las llamadas dirigidas a un agente se transferirán con desbordamiento.

b) En el campo **Desbordamiento tras llamadas en cola** introduzca el número máximo de llamadas. Los agentes de desbordamiento reciben las llamadas que superan este valor máximo.

9) Establezca un valor porcentual para el **Nivel de habilidad** del agente.

El nivel de habilidad permite controlar la distribución de las llamadas a los agentes de la cola de espera **Servicio**. Los agentes con un nivel de habilidad elevado tienen prioridad en la distribución de llamadas. Cuando todos los agentes tienen el mismo nivel de habilidad, el agente que lleve más tiempo libre recibirá la llamada.

10) Elija una de estas opciones:
    - Si desea que el agente reciba las solicitudes de devolución de llamada en forma de mensajes de voz, active la casilla de verificación **Activar devolución de llamada de agente**.
    - Si no desea que el agente reciba solicitudes de devolución de llamada, desactive la casilla de verificación **Activar devolución de llamada de agente**.
11) Introduzca el tiempo de trabajo automático en segundos para el agente de la cola de **Servicio** en el campo **Tiempo de trabajo**.
12) Haga clic en **Aceptar**.
13) Repita los pasos del 5 al 12 para asignar todos los agentes a las colas del Contact Center de muestra.

18.6.2 Procedimiento de configuración

Aquí puede consultar una visión general sobre las tareas a realizar en la configuración del Contact Center.

- Configuración de grupos UCD

  Las colas del Contact Center son grupos de trabajo basados en los grupos UCD del sistema de comunicación. Antes de proceder a la configuración del Contact Center propiamente dicha, hay que definir los grupos UCD.
- Configuración de una solución de respaldo (solución Fallback)

  Si el Contact Center no está disponible por distintos problemas (caída, falta de conexión o similar), se conmuta automáticamente a la prestación "Uniform Call Distribution UCD" del sistema de comunicación. Esta prestación sirve así como solución de respaldo para el Contact Center (véase Solución de respaldo (solución Fallback)).
- Configuración de extensiones como agentes
- Grabación de anuncios grabados individuales para el Contact Center
- Carga de anuncios grabados personalizados para el Contact Center

  Nota: La reproducción de anuncios grabados solo es posible mediante líneas urbanas. Para reproducir el anuncio grabado, la llamada debe proceder de una línea urbana o bien OpenScape Contact Center debe supervisar a la persona que llama.
- Agregar planes horarios
- Agregar colas de espera
- Definición de valores de software para el nivel de servicio
- Definición de la prioridad de llamantes VIP
- Edición de la lista de llamadas VIP
- Definición de agentes favoritos
- Agregar pausas de Contact Center
- Agregar códigos de tratamiento posterior
- Asignación de agentes a colas de espera

18.6.2.1 Cómo configurar grupos UCD para el Contact Center

El asistente **UCD** permite configurar grupos UCD para el Contact Center.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **UCD**. Podrá ver una lista de todos los grupos UCD posibles.
4) Para configurar un grupo UCD, en la fila del grupo UCD deseado haga clic en **Editar**.
5) En el campo **N.° de llamada**, indique el número de teléfono del grupo UCD.
6) En el campo **Número de marcación directa**, indique el número de marcación directa del grupo UCD.
7) En el campo **Nombre**, indique el nombre del grupo UCD.
8) Haga clic en **OK & Continuar**. Se abre la ventana **Asignación de agentes UCD**.
9) Seleccione las ID de agente UCD deseadas en **Selección** y asigne los agente al grupo UCD. Para hacerlo, haga clic en **Agregar**.
10) Haga clic en **OK & Continuar**. Se muestra la ventana **Asignar extensiónes**.
11) Asigne todos los ID de agente UCD a las extensiones deseadas.
12) Haga clic en **OK & Continuar**. Se abre la ventana **Editar anuncio grabado/desbordamiento**.
13) Haga clic en **Aceptar**, puesto que los parámetros mostrados no son relevantes para la configuración del grupo UCD.
14) Si desea configurar más grupos UCD para el Contact Center, repita los pasos del 4 al 11.
15) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

18.6.2.2 Cómo configurar extensiones como agentes

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Directorio de usuario**.
4) Seleccione la extensión deseada en el directorio de usuarios y haga clic en **Editar**.

5) En el grupo de menús, haga clic en **Detalles personales** > **Nivel de usuario**.
6) Elija una de estas opciones:

   Si desea que el agente esté disponible de forma permanente, active la casilla de verificación **Agente disponible de forma permanente**. De esta forma, el agente también permanecerá disponible para llamadas, faxes y correos electrónicos aunque no acepte una llamada, un fax o un correo electrónico.

   Si no desea que el agente esté disponible de forma permanente, desactive la casilla de verificación **Agente disponible de forma permanente**. El agente deja de estar disponible si no acepta una llamada, un fax o un correo electrónico.
7) En la lista desplegable **Nivel** seleccione el nivel de clase de servicio.
8) Haga clic en **Guardar**.
9) Si desea configurar otras extensiones como agente, repita el paso 4 al paso 8.

18.6.2.3 Cómo grabar un anuncio grabado personalizado para el Contact Center

El asistente Grabadora permite grabar anuncios personalizados para el Contact Center.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en Editar para iniciar el asistente Carga de archivo.
4) Active el campo de opción **Seguridad**.
5) En la lista desplegable Extensión seleccione el número del teléfono a través del que se realizará la grabación.
6) Haga clic en Realizar llamada. Se llama al número de teléfono seleccionado.
7) Descuelgue el auricular, y en el campo Nombre de archivo, introduzca un nombre para el anuncio grabado.
8) Haga clic en Grabar, para iniciar la grabación del anuncio.
9) Haga clic en Detener, en cuanto termine la grabación del anuncio.
10) Si desea escuchar un nuevo anuncio grabado, haga clic en Reproducir.
11) Haga clic en Cerrar, para guardar los anuncios grabados.

Consejo:

Después de grabar y guardar un anuncio grabado ya no se puede borrar. No obstante, si se utiliza el mismo nombre de archivo se puede sobrescribir un anuncio grabado ya guardado. Por ejemplo, al guardar el archivo de sonido

anuncio1.wav se sobrescribe el archivo anuncio1.wav ya existente.

18.6.2.4 Cómo cargar un anuncio grabado personalizado para el Contact Center

El asistente Carga de archivo permite cargar anuncios grabados personalizados para el Contact Center.

Requisitos previos

Hay disponible un archivo de sonido en formato wav con las siguientes propiedades: monoaural, tasa de muestreo de sonido 8 kHz, tamaño de muestreo de sonido 16 bit, tamaño marco 2.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en Editar para iniciar el asistente Carga de archivo.
4) Haga clic en la pestaña **Administrador de archivos de audio** .
5) En la lista desplegable Destino de carga seleccione el destino Puesto de operadora.
6) Seleccione el botón de radio **Uploader** y haga clic en **Choose File**, navegue hasta la ubicación de almacenamiento del archivo de audio deseado y haga clic en **Open**.
7) Haga clic en Carga.

Consejo: Después de la carga de archivo ya no se puede borrar un archivo de sonido. No obstante, si se utiliza el mismo nombre de archivo se puede sobrescribir un archivo de sonido ya cargado. Por ejemplo, al cargar el archivo de sonido anuncio1.wav se sobrescribe el archivo anuncio1.wav ya existente.

18.6.2.5 Cómo agregar un plan horario

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Plan horario**. Aparecen todos los planes horarios existentes.
5) Haga clic en **Agregar**.

6) Para seleccionar la regla (CCV), elija una de estas opciones:

- Si desea asignar al plan horario una regla ya definida, en la lista desplegable **CCV estándar** seleccione la regla deseada.
- Si desea asignar una nueva regla que aún no se ha definido al programa, haga clic en **Editar** en el área **Programación** y proceda de la siguiente manera:

  En la lista de herramientas CCV, haga clic en el objeto CCV deseado y arrástrelo al editor de reglas. Ingrese las propiedades deseadas en la ventana del objeto CCV que aparece y haga clic en **Guardar**. Si es necesario, arrastre más objetos CCV al editor de reglas y defina sus propiedades. Para conectar dos objetos CCV, haga clic con el botón secundario del ratón sobre el primero de los dos objetos que desee conectar. En el menú desplegable, utilice la opción **Link To** para seleccionar el segundo de los objetos CCV que desea conectar.

  Si desea borrar un objeto CCV del editor de reglas, haga clic con el botón secundario del ratón sobre él y, en el menú desplegable, seleccione **Eliminar**.

  Haga clic en **Guardar**. Ingrese un nombre para la nueva regla y luego haga clic en **Guardar**. Cierre la ventana que permite configurar el guardado de la regla. Si la nueva regla es errónea, no se podrá guardar. El objeto u objetos CCV erróneos aparecen marcados en rojo en el editor de reglas.

  En la lista desplegable **CCV estándar**, seleccione la nueva regla guardada.
- Si desea asignar al plan horario una nueva regla basada en una regla ya definida, siga este procedimiento:

  En la lista desplegable **CCV estándar**, seleccione la regla deseada y haga clic en **Editar**. La regla aparece en el editor de reglas. Modifique la regla.

  En la lista de herramientas CCV, haga clic en el objeto CCV deseado y arrástrelo al editor de reglas. Ingrese las propiedades deseadas en la ventana del objeto CCV que aparece y haga clic en **Guardar**. Si es necesario, arrastre más objetos CCV al editor de reglas y defina sus propiedades. Para conectar dos objetos CCV, haga clic con el botón secundario del ratón sobre el primero de los dos objetos que desee conectar. En el menú desplegable, utilice la opción **Link To** para seleccionar el segundo de los objetos CCV que desea conectar.

  Haga clic en **Guardar**. Introduzca un nombre CCV para la nueva regla y luego haga clic en **Guardar**. Cierre la ventana que permite configurar el guardado de la regla. Si la nueva regla es errónea, no se podrá guardar. El objeto u objetos CCV erróneos aparecen marcados en rojo en el editor de reglas.

  En la lista desplegable **CCV estándar**, seleccione la nueva regla guardada.

7) Si desea imprimir la regla o enviarla por correo electrónico, puede guardar la regla como archivo PDF. Para hacer esto, haga clic en **Imprimir**. Aparece la ventana **Imprimir**.

Introduzca el nombre del archivo y seleccione el directorio en el que desea guardar el archivo. Haga clic en **Guardar**.

8) En el campo **Nombre de plan horario**, indique el nombre del nuevo plan horario.

9) Haga clic en **Guardar**.

10) Si desea asignar otra regla (CCV) a un determinado periodo de tiempo del plan horario, en la sección **Excepciones**, haga clic en **Agregar**. A continuación, se muestran los campos para esta excepción.

11) En el campo **Descripción**, introduzca el nombre de la excepción.

12) Para seleccionar la regla (CCV), elija una de estas opciones:

- Si desea asignar una regla ya definida a este periodo de tiempo del plan horario, en la lista desplegable de la excepción seleccione la regla deseada.
- Si desea asignar una nueva regla aún no definida a este periodo de tiempo del plan horario, siga este procedimiento:

  Haga clic en **Agregar** en el área **Programación**.

  En la lista de herramientas CCV, haga clic en el objeto CCV deseado y arrástrelo al editor de reglas. Ingrese las propiedades deseadas en la ventana del objeto CCV que aparece y haga clic en **Guardar**. Si es necesario, arrastre más objetos CCV al editor de reglas y defina sus propiedades. Para conectar dos objetos CCV, haga clic con el botón secundario del ratón sobre el primero de los dos objetos que desee conectar. En el menú desplegable, utilice la opción **Link To** para seleccionar el segundo de los objetos CCV que desea conectar.

  Si desea borrar un objeto CCV del editor de reglas, haga clic con el botón secundario del ratón sobre él y, en el menú desplegable, seleccione **Eliminar**.

  Haga clic en **Guardar**. Ingrese un nombre para la nueva regla y luego haga clic en **Guardar**. Cierre la ventana que permite configurar el guardado de la regla. Si la nueva regla es errónea, no se podrá guardar. El objeto u objetos CCV erróneos aparecen marcados en rojo en el editor de reglas.

  En la lista desplegable de esta excepción, seleccione la nueva regla guardada.
- Si desea asignar una nueva regla basada en una regla ya definida a este periodo de tiempo del plan horario, siga este procedimiento:

  En la lista desplegable de esta excepción, seleccione la regla deseada y haga clic en **Editar**. La regla aparece en el editor de reglas. Modifique la regla.

  En la lista de herramientas CCV, haga clic en el objeto CCV deseado y arrástrelo al editor de reglas. Ingrese las propiedades deseadas en la ventana del objeto CCV que aparece y haga clic en **Guardar**. Si es necesario, arrastre más objetos CCV al editor de reglas y defina sus propiedades. Para conectar dos objetos CCV, haga clic con el botón secundario del ratón sobre el primero de los dos objetos que desee conectar. En el menú desplegable, utilice la opción **Link To** para seleccionar el segundo de los objetos CCV que desea conectar.

  Haga clic en **Guardar**. Ingrese un nombre para la nueva regla y luego haga clic en **Guardar**. Cierre la ventana que permite configurar el guardado de la regla. Si la nueva regla es errónea, no se podrá

guardar. El objeto u objetos CCV erróneos aparecen marcados en rojo en el editor de reglas.

En la lista desplegable de esta excepción, seleccione la nueva regla guardada.

13) Seleccione una de las siguientes opciones para establecer a qué hora se aplicará la excepción:

- Si la excepción es solicitar un período de tiempo ilimitado durante todo el año, seleccione **Dentro del rango de tiempo** en la lista desplegable **Tipo**. Seleccione el inicio y el fin del periodo diario en los cuadros de lista **Hora de inicio** y **Hora de fin**.

  Seleccione los días de la semana en los que se aplicará la excepción. Haga clic en **Guardar**.
- Si la excepción es solicitar por un período de tiempo limitado durante el año, seleccione **Dentro del rango de tiempo** en la lista desplegable **Tipo**. En el campo **Fecha de inicio**, indique la fecha para el comienzo y en el campo **Fecha de fin**, la fecha de finalización del periodo de tiempo (en el formato dd.mm.aaaa). Seleccione la hora exacta de la fecha de inicio y la hora exacta de la fecha de fin en los cuadros de lista **Hora de inicio** y **Hora de fin**. La excepción se aplicará entre la fecha/hora de inicio y la fecha/hora de finalización del periodo cubierto.

  Seleccione los días de la semana en los que se aplicará la excepción. Haga clic en **Guardar**.
- Si la excepción se aplica en días festivos, seleccione **Horarios de días festivos** en la lista desplegable **Tipo**. En el campo **Fecha de inicio**, indique la fecha para el comienzo y en el campo **Fecha de fin**, la fecha de finalización del horario vacacional. En la lista de selección **Hora de inicio**, indique la hora de inicio y en la lista de selección **Hora de fin**, seleccione el final del tiempo vacacional.

  Consejo: Los planes horarios vacacionales tienen prioridad frente a otros planes horarios y reglas de una cola.

- Si la excepción se aplica todos los años, seleccione **Recurrencia anual** en la lista desplegable **Tipo**. Ingrese las fechas de inicio y finalización para la recurrencia anual en los campos **Fecha de inicio** y **Fecha de finalización**, respectivamente. Seleccione las horas de inicio y finalización de la periodicidad anual en los cuadros de lista **Hora de inicio** y **Hora de finalización**, respectivamente.

14) Haga clic en **Guardar**.

15) Repita los pasos del 10 al 14 para definir más excepciones para determinados periodos.

16) Si desea comprobar qué regla (CCV) del plan horario se ejecutará en un momento determinado, haga clic en **Probar plan horario**. En la lista desplegable **Fecha**, seleccione el día deseado y en la lista desplegable **Hora**, la hora. Haga clic en **Probar plan horario**. A continuación, se muestra qué regla (CCV) está activa ese día a esa hora. Haga clic en **Cerrar** para cerrar la ventana **Probar plan horario**.

17) Si desea asignar este horario a una o más colas, seleccione las casillas de verificación para las colas deseadas en el área **Colas**.

> **Nota:** Una cola seleccionada solo se puede asignar a un horario, pero se pueden asignar varias colas diferentes a un horario seleccionado.

18) Cierre la ventana.

18.6.2.6 Cómo modificar un plan horario

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Plan horario**. Aparecen todos los planes horarios existentes.
5) Marque el horario a editar y haga clic en **Editar**.
6) Modifique los ajustes de configuración deseados para el CCV estándar:
   - Si desea asignar alguna otra regla (CCV) además de la que se muestra actualmente en la lista desplegable **CCV predeterminado**, seleccione la regla deseada en la lista **CCV predeterminado**.
   - Si desea editar la regla (CCV) que se muestra en el **CCV predeterminado** lista, **Editar** bajo el área **Programa**. La regla aparece en el editor de reglas. Modifique la regla. Haga clic en **Guardar**. Ingrese un nombre para la nueva regla y luego haga clic en **Guardar**. Cierre la ventana que permite configurar el guardado de la regla.

     En la lista desplegable **CCV estándar**, seleccione la nueva regla guardada.
7) Haga clic en **Guardar**.
8) Cambie la configuración deseada en el área de **Excepciones**:
   - Si desea asignar otra regla (CCV) a un período de tiempo específico dentro del cronograma, haga clic en **Agregar** en el área de **Excepción**. En la lista desplegable de esta excepción, seleccione la regla deseada. Mediante los campos de opción y las listas desplegables, seleccione la hora en la que se aplicará la excepción. En el campo **Descripción**, introduzca el nombre de la excepción. Haga clic en **Guardar**.
   - Si desea editar esta excepción o una de las excepciones mostradas, haga clic en **Editar** bajo la **excepción** después de seleccionar la excepción deseada y luego use botones de opción, listas desplegables y campos para especificar cuándo se aplicará esta excepción y en qué regla (CCV). Además, puede hacer clic en **Editar CCV** en el área de **Excepción** para editar la regla asociada (CCV). La regla aparece en el editor de reglas. Modifique la regla. Haga clic en **Guardar**. Ingrese

un nombre para la nueva regla y luego haga clic en **Guardar**. Cierre la ventana que permite configurar el guardado de la regla.

En la lista desplegable, seleccione la nueva regla guardada. Mediante los campos de opción y las listas desplegables seleccione el periodo de tiempo en que se aplicará la regla (CCV). Haga clic en el símbolo verde Guardar.

- Si desea eliminar esta excepción o una de las excepciones mostradas, haga clic en **Eliminar** después de la selección de la excepción deseada.

9) Si desea comprobar qué regla (CCV) del plan horario se ejecutará en un momento determinado, haga clic en **Probar plan horario**. En la lista desplegable **Fecha**, seleccione el día deseado y en la lista desplegable **Hora**, la hora. Haga clic en **Probar plan horario**. A continuación, se muestra qué regla (CCV) está activa ese día a esa hora. Haga clic en **Cerrar** para cerrar la ventana **Probar plan horario**.

10) Si desea asignar este horario a una o más colas, seleccione las casillas de verificación para las colas deseadas en el área **Colas**.

Nota: Una cola seleccionada solo se puede asignar a un horario, pero se pueden asignar varias colas diferentes a un horario seleccionado.

---

11) Cierre la ventana.

18.6.2.7 Cómo borrar un plan horario

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.

3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.

4) Haga clic en **Plan horario**. Aparece un listado de todos los planes horarios disponibles.

5) Marque el horario deseado y haga clic en **Eliminar**.

Consejo: Los planes horarios no se pueden borrar mientras estén asignados a una cola de espera. Antes de borrar hay que eliminar la asignación del plan horario a la cola o colas de espera.

18.6.2.8 Cómo guardar reglas (CCV) como archivo PDF

El asistente **Contact Center**, permite guardar reglas (CCV) como archivos PDF. A continuación, el archivo se puede imprimir o enviar por correo electrónico, por ejemplo.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Plan horario**. Aparecen todos los planes horarios existentes.
5) Seleccione el plan horario que incluya la regla deseada y haga clic en **Editar**.
6) Seleccione la regla deseada en la lista desplegable y haga clic en **Editar**. La regla aparece en el editor de reglas.
7) Haga clic en **Imprimir**. Se muestra la ventana Guardar.
8) Introduzca el nombre del archivo y seleccione el directorio en el que desea guardar el archivo.
9) Haga clic en **Guardar**.
10) Cierre la ventana y confirme la acción con **Sí**.

18.6.2.9 Cómo guardar reglas (CCV) como archivo PDF

El asistente Contact Center, permite guardar reglas (CCV) como archivos PDF.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Plan horario**. Aparecen todos los planes horarios existentes.
5) Seleccione el plan horario que incluya la regla deseada y haga clic en Editar.
6) Seleccione la regla deseada en la lista desplegable **CCV** y haga clic en **Editar** bajo el área de **Programación** . La regla aparece en el editor de reglas.
7) Haga clic en **Descargar**.

La regla deseada (CCV) se descarga ahora como archivo de respaldo.

18.6.2.10 Cómo cargar una regla descargada (CCV) en un formato de archivo de copia de seguridad

El asistente **del Centro de** Contacto le permite cargar reglas (CCV) que se descargan previamente en formato de archivo de copia de seguridad.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Descargue una regla (CCV) en formato de archivo de copia de seguridad.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Plan horario**. Aparecen todos los planes horarios existentes.
5) Seleccione el plan horario que incluya la regla deseada y haga clic en Editar.
6) Seleccione la regla deseada de la lista desplegable **CCV** y haga clic en **Editar** bajo el área de **Programación** . La regla aparece en el editor de reglas.
7) Haga clic en Examinar, desplácese hasta el lugar de almacenamiento del archivo de sonido deseado y haga clic en Abrir.

   Si eliges un archivo que no está en formato de copia de seguridad se produce un error.
8) Haga clic en Recuperar copia de seguridad.

La regla deseada (CCV) está ahora cargada en el sistema.

18.6.2.11 Cómo agregar una cola

Requisitos previos

Hay configurado al menos un grupo UCD.

Hay configurado al menos un plan horario.

Hay disponible al menos una cuenta de correo electrónico para la recepción de correo electrónico si desea que los correos electrónicos se capturen en la cola de espera.

El envío de correo electrónico se ha configurado en el sistema de comunicación, si se desea que los agentes de la cola de espera puedan enviar correos electrónicos.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Cola**.
5) Haga clic **Agregar**.
6) Haga clic en la pestaña **Ajustes generales**.
7) Introduzca el nombre de la cola en el campo **Nombre de cola**.

   Recomendación: utilice el nombre de uno de los grupos UCD que haya configurado.

Consejo: Para que en las evaluaciones (informes) se muestre el nombre completo de la cola, seleccione

denominaciones cortas y no compuestas. Ejemplo: Grupo de ventas nacionales 1 (no: DomesticSalesGroup 1)

8) Elija una de estas opciones para el estado de la cola:

- Si desea activar la nueva cola, seleccione la opción **Activa** en la lista desplegable **Cola activa**.
- Si desea desactivar la nueva cola, seleccione la opción **No activa** en la lista desplegable **Cola activa**.

  Si se desactiva una cola de espera, se activa la solución de respaldo por parte del grupo UCD correspondiente. Si ningún agente se ha registrado en el grupo UCD y no se registra ningún otro destino de transferencia automática diferida para el grupo UCD, los llamantes reciben la señal de ocupado.

9) En el campo **Línea colectiva**, indique el número de llamada de un grupo UCD que haya configurado en la configuración básica del Contact Center.

10) Seleccione la opción **CSP** en la lista desplegable **Conmutación telefónica**.

11) Seleccione el plan horario deseado en la lista desplegable **Plan horario**.

12) Introduzca el valor umbral de alarma en el campo **Recuento de alarma de cola**.

Si se supera el número de llamadas en espera aquí indicado, el símbolo de cola del agente cambia del color verde al naranja.

13) Introduzca el valor de umbral de alarma en segundos en el campo **Hora de alarma de cola**.

Si se supera el tiempo de espera de una llamada en la cola aquí indicado, la entrada correspondiente de la lista de llamadas del Contact Center del agente pasa a color rojo.

14) En el campo **Tiempo excedido de llamadas**, introduzca el tiempo (en segundos) transcurrido el cual una llamada sin contestar se transferirá al siguiente agente libre.

15) En el campo **Umbral de llamada abandonada**, indique el tiempo (en segundos) que determina si una llamada abandonada será incluida o no en las estadísticas (es decir, en los informes).

Se registran de forma estadística todas las llamadas abandonadas una vez finalizado el tiempo indicado.

16) Elija una de estas opciones para la visualización de ventanas emergentes en la aplicación myAgent:

Consejo: Las ventanas emergentes son necesarias para aceptar y realizar devoluciones de llamada y para aceptar faxes y correos electrónicos.

- Si, en caso de llamadas entrantes, desea que aparezca una ventana emergente en myAgent para ver e introducir los datos de cliente, active la casilla de verificación **Ventana emergente activada**.
- Si, en caso de llamadas entrantes, no desea que aparezca una ventana emergente en myAgent, desactive la casilla de verificación **Ventana emergente activada**.

17) Elija una de estas opciones para el modo de Tratamiento posterior:

En las colas con modo de Tratamiento posterior, los agentes puede asignar sus llamadas a distintos temas valiéndose de códigos de tratamiento posterior (pedido, reclamación, servicio técnico, etc.).

- Si desea configurar una cola con el modo Tratamiento posterior simple, seleccione la opción **Tratamiento posterior simple**.
- Si desea configurar una cola con el modo Tratamiento posterior múltiple, seleccione la opción **Tratamiento posterior múltiple**.
- Si desea configurar una cola sin modo Tratamiento posterior, seleccione la opción **Sin tratamiento posterior**.

18) Si desea modificar la prioridad de la cola, haga clic en **Prioridades**.

Haga clic en los puntos rojos de la sección **Prioridad de cola con el paso del tiempo** y arrástrelos a la posición deseada. El eje horizontal indica el tiempo de espera de la cola y el eje vertical la prioridad de las colas seleccionadas respecto a las demás colas. Si un agente está asignado a varias colas, se puede establecer si las llamadas dirigidas a una cola deberán ser transferidas a ese agente con mayor prioridad que las llamadas dirigidas a otras colas.

Arrastre las barras deslizantes de la sección **Prioridades de tipo de llamada** a la posición deseada. De esta forma puede definir la prioridad de los distintos tipos de llamada dentro de la cola seleccionada. Cuanto más a la derecha esté la barra, mayor será la prioridad.

Consejo: En las llamadas de voz debe seleccionarse una prioridad más alta que para los demás tipos de llamada. De lo contrario, las devoluciones de llamada, faxes o correos electrónicos ocuparán el lugar de los llamantes en espera.

---

19) Seleccione una de las siguientes opciones para el modo de profundidad de cola:

La profundidad de cola se puede establecer individualmente para cada cola en el cuadro de diálogo de configuración de la cola.

- Si el **Modo de profundidad de cola** se define como **Estático**, se pueden configurar los parámetros **WLS** y **Tamaño de profundidad de cola**.
- Si el **Modo de profundidad de cola** se define como **Ninguno**, el parámetro **WLS** se podrá configurar, y en este caso afectará también a la configuración de UCD, pero el parámetro **Tamaño de profundidad de cola** no se podrá configurar.

20) Introduzca el tamaño del bucle de espera en el campo **WLS**. El valor de **WLS**, que es el número de llamadas de voz a la espera de ser conectadas a un agente, afecta directamente a la configuración del parámetro Llamadas en cola del grupo UCD asignado.

21) Si el **Modo de profundidad de cola** está configurado como **Estático**, introduzca la cantidad de profundidad de la cola en el campo **Tamaño de profundidad de cola**. El tamaño de profundidad de cola es el resumen del tamaño del bucle en espera (WLS) y las llamadas al agente.

22) Haga clic en la pestaña **Pilotos de cola**.

23) Si desea incluir los faxes en la cola, seleccione las casillas de verificación de los pilotos deseados (números de teléfono) en la sección **Pilotos de fax entrante**.

Los faxes dirigidos a este número o números de teléfono se incluyen en la cola y se administran como llamadas entrantes.

24) Seleccione una de las siguientes opciones en el área **Servicio de correo electrónico entrante**, para que los correos electrónicos se incluyan en la cola:

- Si desea configurar una nueva dirección de correo electrónico, haga clic en **Agregar**. Se abre la ventana **Agregar**.

  Seleccione el método de autenticación para su servidor de correo electrónico en la lista desplegable **Método de autenticación**. Puede elegir entre **Básico** y **OAuth 2.0**.

  En el campo **Servidor**, introduzca la designación del servidor de correo electrónico que se utilizará para la recepción de los correos electrónicos (por ejemplo, `pop3.web.de`).

  En el campo **Puerto**, introduzca el número de puerto del servidor de correo electrónico (por ejemplo, `110`, el número de puerto estándar para POP3).

  Si el método de autenticación seleccionado es **Básico**, introduzca los datos de acceso al servidor de correo electrónico en los campos **Nombre de usuario** y **Contraseña**.

  Si el método de autenticación seleccionado es **OAuth 2.0**, introduzca el nombre de usuario para acceder al servidor de correo electrónico en los campos **Nombre de usuario**, **ID de tenencia**, **ID de aplicación** y **Contraseña de cliente**. El ID de tenencia, el ID de aplicación y la contraseña del cliente corresponden a la aplicación que se ha registrado en Azure AD para las colas de correo electrónico. Puede obtenerlas de su administrador de Azure AD. Introduzca el alcance de la aplicación en el campo **Alcance** (valor por defecto: https://outlook.office365.com/.default).

  Seleccione si desea realizar el envío de correo electrónico a través de una conexión SSL (Secure Socket Layer). Si desea usar una conexión SSL, active la casilla de verificación **Usar conexión SSL** (con ello se modifica, en su caso, el número de puerto del servidor de correo electrónico; número de puerto estándar para POP3 mediante SSL = 995). Si no desea utilizar una conexión SSL, desactive la casilla de verificación **Usar conexión SSL**.

  Haga clic en **Guardar**. A continuación, la nueva dirección de correo aparecerá en la sección **Servicio de correo electrónico entrante**.
- Si desea editar una dirección de correo electrónico ya existente, marque la dirección deseada y haga clic en **Editar**. Se abre la ventana **Editar**.

  Cambie los parámetros deseados y, a continuación, haga clic en **Guardar**.
- Si desea eliminar una dirección de correo electrónico existente, marque la dirección deseada y haga clic en **Eliminar**.

25) Haga clic en la pestaña **Varios**.

26) En el campo **Dirección de email de devolución**, indique la dirección de correo electrónico que podrá ver el destinatario en el envío de correos electrónicos por un agente.

27) Elija una de estas opciones para el encaminamiento de llamadas inteligente dentro de una cola:

- Si desea transferir las llamadas entrantes automáticamente al último agente conectado con ese llamante, active la casilla de verificación **Buscar último agente de cliente si no se ha localizado el agente preferido**. Para ello es necesario que no haya definido un agente preferido para el llamante.
- Si no desea que las llamadas entrantes sean transferidas al último agente conectado con el llamante, desactive la casilla de verificación **Buscar último agente de cliente si no se ha localizado el agente preferido**.

28) Haga clic en **Guardar**.

18.6.2.12 Cómo modificar una cola

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.

3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.

4) Haga clic en **Cola**.

5) Marque la cola deseada y haga clic en **Editar**.

6) Haga clic en la pestaña **Ajustes generales**.

7) Modifique los ajustes de configuración deseados.

8) Elija una de estas opciones para el estado de la cola:

- Si desea activar la cola, seleccione la opción **Activa** en la lista desplegable **Cola activa**.
- Si desea desactivar la cola, seleccione la opción **No activa** en la lista desplegable **Cola activa**.

  Si se desactiva una cola de espera, se activa la solución de respaldo por parte del grupo UCD correspondiente. Si ningún agente se ha registrado en el grupo UCD y no se registra ningún otro destino de transferencia automática diferida para el grupo UCD, los llamantes reciben la señal de ocupado.

9) Elija una de estas opciones para la visualización de ventanas emergentes en la aplicación myAgent:

> **Consejo:** Las ventanas emergentes son necesarias para aceptar y realizar devoluciones de llamada y para aceptar faxes y correos electrónicos.

- Si, en caso de llamadas entrantes, desea que aparezca una ventana emergente en myAgent para ver e introducir los datos de cliente, active la casilla de verificación **Ventana emergente activada**.
- Si, en caso de llamadas entrantes, no desea que aparezca una ventana emergente en myAgent, desactive la casilla de verificación Ventana emergente activada.

10) Elija una de estas opciones para el modo de Tratamiento posterior:

En las colas con modo de Tratamiento posterior, los agentes puede asignar sus llamadas a distintos temas valiéndose de códigos de tratamiento posterior (pedido, reclamación, servicio técnico, etc.).

- Si desea configurar el modo de tratamiento posterior simple para la cola, seleccione la opción **Tratamiento posterior simple**.
- Si desea configurar el modo de tratamiento posterior múltiple para la cola, seleccione la opción **Tratamiento posterior múltiple**.
- Si no desea configurar ningún modo de tratamiento posterior para la cola, active la opción **Sin tratamiento posterior**.

11) Si desea modificar la prioridad de la cola, haga clic en **Prioridades**.

Haga clic en los puntos rojos de la sección **Prioridad de cola con el paso del tiempo** y arrástrelos a la posición deseada. El eje horizontal indica el tiempo de espera de la cola y el eje vertical la prioridad de las colas seleccionadas respecto a las demás colas. Si un agente está asignado a varias colas, se puede establecer si las llamadas dirigidas a una cola deberán ser transferidas a ese agente con mayor prioridad que las llamadas dirigidas a otras colas.

Arrastre las barras deslizantes de la sección **Prioridades de tipo de llamada** a la posición deseada. De esta forma puede definir la prioridad de los distintos tipos de llamada dentro de la cola seleccionada. Cuanto más a la derecha esté la barra, mayor será la prioridad.

> **Consejo:** En las llamadas de voz debe seleccionarse una prioridad más alta que para los demás tipos de llamada. De lo contrario, las devoluciones de llamada, faxes o correos electrónicos ocuparán el lugar de los llamantes en espera.

12) Haga clic en la pestaña **Pilotos de cola**.

13) Seleccione los ajustes deseados en la sección **Pilotos de fax entrantes**:

- Si desea incluir los faxes en la cola, seleccione las casillas de verificación de los pilotos deseados (números de teléfono) en la sección **Pilotos de fax entrante**.
- Si no desea incluir faxes en la cola, desactive la casilla o casillas de verificación de la sección **Pilotos de fax entrantes**.

14) Seleccione la configuración deseada en la sección **Servicio de correo electrónico entrante**:

- Si desea configurar una nueva dirección de correo electrónico, haga clic en **Agregar**. Se abre la ventana **Agregar**.

  Seleccione el método de autenticación para su servidor de correo electrónico en la lista desplegable **Método de autenticación**. Puede elegir entre **Básico** y **OAuth 2.0**.

  En el campo **Servidor**, introduzca la designación del servidor de correo electrónico que se utilizará para la recepción de los correos electrónicos (por ejemplo, `pop3.web.de`).

  En el campo **Puerto**, introduzca el número de puerto del servidor de correo electrónico (por ejemplo, `110`, el número de puerto estándar para POP3).

  Si el método de autenticación seleccionado es **Básico**, introduzca los datos de acceso al servidor de correo electrónico en los campos **Nombre de usuario** y **Contraseña**.

  Si el método de autenticación seleccionado es **OAuth 2.0**, introduzca el nombre de usuario para acceder al servidor de correo electrónico en los campos **Nombre de usuario**, **ID de tenencia**, **ID de aplicación** y **Contraseña de cliente**. El ID de tenencia, el ID de aplicación y la contraseña del cliente corresponden a la aplicación que se ha registrado en Azure AD para las colas de correo electrónico. Puede obtenerlas de su administrador de Azure AD. Introduzca el alcance de la aplicación en el campo **Alcance** (valor por defecto: https://outlook.office365.com/.default).

  Seleccione si desea realizar el envío de correo electrónico a través de una conexión SSL (Secure Socket Layer). Si desea usar una conexión SSL, active la casilla de verificación **Usar conexión SSL** (con ello se modifica, en su caso, el número de puerto del servidor de correo electrónico. Número de puerto estándar para POP3 mediante SSL = 995). Si no desea utilizar una conexión SSL, desactive la casilla de verificación **Usar conexión SSL**.

  Haga clic en **Guardar**. A continuación, la nueva dirección de correo aparecerá en la sección **Servicio de correo electrónico entrante**.
- Si desea editar una dirección de correo electrónico ya existente, marque la dirección deseada y haga clic en **Editar**. Se abre la ventana **Editar**.

  Cambie los parámetros deseados y, a continuación, haga clic en **Guardar**.
- Si desea eliminar una dirección de correo electrónico existente, marque la dirección deseada y haga clic en **Eliminar**.

15) Haga clic en la pestaña **Varios**.

16) Modifique los ajustes de configuración deseados.

17) Haga clic en **Guardar**.

18.6.2.13 Cómo activar o desactivar la cola de espera

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Cola**.
5) Haga clic en **Editar**.
6) Haga clic en la pestaña **Ajustes generales**.
7) Elija una de estas opciones para el estado de la cola:
   - Si desea activar la cola, en la lista desplegable **Cola activa**, seleccione la entrada **Activo**.
   - Si desea desactivar la cola, en la lista desplegable **Cola activa**, seleccione la entrada **Inactivo**.

     Si se desactiva una cola de espera, se activa la solución de respaldo por parte del grupo UCD correspondiente. Si ningún agente se ha registrado en el grupo UCD y no se registra ningún otro destino de transferencia automática diferida para el grupo UCD, los llamantes reciben la señal de ocupado.
8) Haga clic en **Guardar**.

18.6.2.14 Cómo configurar un piloto para los mensajes de fax entrantes en colas

Requisitos previos

Hay disponible al menos un número de teléfono de fax para la recepción de faxes.

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Extensiones**.
3) En el grupo de menús, haga clic en **Extensiones** > **UC Applications** > **Contact Center Fax**. Se muestran los números de puerto lógicos previstos para los buzones de fax.
4) En el grupo de menús, haga clic en el número de puerto deseado.
5) Haga clic en la pestaña **Editar parámetros exten.**.
6) En el campo **Número de teléfono**, introduzca el número de teléfono del nuevo piloto para los mensajes de fax entrantes.
7) En el campo **Nombre**, introduzca el nombre del nuevo piloto para los mensajes de fax entrantes.
8) En el campo **Marcación directa**, introduzca el número de marcación directa del nuevo piloto para los mensajes de fax entrantes.

9) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

El piloto para los mensajes de fax entrantes ya se puede activar para una de las colas deseadas.

18.6.2.15 Cómo establecer valores nominales para el nivel de servicio

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Nivel de servicio**.
5) Seleccione la cola deseada y haga clic en **Editar**.
6) Haga clic en los puntos rojos y arrástrelos a la posición deseada.

   El eje horizontal indica el tiempo de espera en la cola en intervalos de diez segundos, y el eje vertical indica el valor nominal del nivel de servicio en valores porcentuales.

   De esta forma, se preestablecen los valores nominales para la calidad de transferencia de la cola. Comparando los valores nominales con los tiempos de espera reales de los llamantes se puede determinar el grado de calidad.
7) Haga clic en **Guardar**.

18.6.2.16 Cómo definir la prioridad de llamantes VIP

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Prioridades de llamantes VIP**.
5) Seleccione la cola deseada y haga clic en **Editar**.
6) Haga clic en los puntos rojos y arrástrelos a la posición deseada.

   De esta forma puede definir la prioridad de los llamantes normales frente a los llamantes VIP.

   El eje horizontal indica el tiempo de espera en la cola en intervalos de 30 segundos, y el eje vertical indica la prioridad de los llamantes normales que no están incluidos en la lista de llamadas VIP.

   Por ejemplo, puede establecer los puntos rojos de forma que transcurridos 180 segundos se alcance una prioridad del 100 por cien. En este caso,

transcurridos 180 segundos, los llamantes normales serán tratados de igual forma que los llamantes VIP. Las llamadas de llamantes VIP que hayan entrado antes se gestionan con prioridad en la cola.

De forma alternativa, también puede introducir los valores para los distintos intervalos de tiempo de espera en los campos de entrada a la derecha del diagrama.

7) Haga clic en **Guardar**.

18.6.2.17 Cómo editar la lista de llamantes VIP

Requisitos previos

El llamante previsto para la lista de llamadas VIP está en el directorio externo.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.

3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.

4) Haga clic en **Lista de llamadas VIP**.

5) Seleccione la cola deseada y haga clic en **Editar**.

6) Elija una de estas opciones:

- Si desea añadir un llamante a la lista de llamadas VIP, en la parte superior de la ventana haga clic en **Agregar**. Marque la entrada deseada. Defina la prioridad de ese llamante VIP frente a los demás llamantes VIP. Para ello, desplace la barra deslizante a la posición deseada. Cuanto más a la derecha esté la barra, mayor será la prioridad.
- Si desea añadir un patrón de números de teléfono a la lista de llamadas VIP, en la parte inferior de la ventana haga clic en **Agregar**. En el campo Patrón introduzca el patrón de número de teléfono deseado (por ejemplo, `089 7577*`). Defina la prioridad de todos los llamantes VIP con ese patrón de números de teléfono frente a los demás llamantes VIP. Para ello, desplace la barra deslizante a la posición deseada. Cuanto más a la derecha esté la barra, mayor será la prioridad.

  No se pueden introducir patrones de números de teléfono en formato canónico. Tampoco se pueden utilizar abreviaturas de prefijos de país (p. ej. +49 en lugar de 0049). Siempre hay que indicar los patrones de números de teléfono.

  Ejemplo de patrón de números de teléfono: `089 7577*` (089 = Código de red local de Múnich, 7577 = Número de teléfono del sistema de una empresa, * = Comodín para números). Al introducir este patrón de números de teléfono en la lista de llamadas VIP todos los llamantes de Múnich cuyo número comience por 7577 reciben un tratamiento preferente.

  En un patrón de números de teléfono se pueden utilizar como comodines (marcadores de posición) los siguientes caracteres:

  – * = comodín para números
  – ? = comodín para cifras

- Si desea editar una de las entradas de la lista de llamantes VIP, marque la entrada deseada y haga clic en **Editar**. Modifique los ajustes de configuración deseados.
- Si desea eliminar un entrada de la lista de llamadas VIP, marque la entrada deseada y haga clic en **Eliminar**.

7) Haga clic en **Guardar**.

18.6.2.18 Cómo establecer agentes preferidos

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en Agentes preferidos.
5) Seleccione la cola deseada y haga clic en Editar.
6) Marque el llamador deseado en el área de **Clientes** , que es la superior de las dos tablas.
7) Haga clic en Agregar agente.
8) Seleccione el agente deseado y haga clic en Aceptar.

A continuación, el nombre del agente seleccionado aparece en la sección Agentes preferidos.

9) Si desea definir más agentes como agentes preferidos, repita los pasos 7 y 8.
10) Si ha establecido varios agentes preferidos, defina su prioridad. Tiene las siguientes opciones:

- Si desea asignar una prioridad más alta, seleccione el agente deseado y desplácelo mediante el botón Subir a una posición superior de la lista.
- Si desea asignar una prioridad más baja, seleccione el agente deseado y desplácelo mediante el botón Bajar a una posición inferior de la lista.

18.6.2.19 Cómo borrar agentes preferidos

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Agentes preferidos**.
5) Seleccione la cola deseada y haga clic en **Editar**.

6) En la sección **Agentes preferidos**, seleccione el agente o los agentes que desea borrar.
7) Haga clic en **Eliminar agente**.

18.6.2.20 Cómo agregar una pausa de Contact Center

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en Pausas de Contact Center.
5) Haga clic **Agregar**.
6) En el campo Nombre, introduzca el nombre de la nueva pausa de Contact Center.
7) En el campo Duración (Minutos), indique la duración de la nueva pausa de Contact Center en minutos.
8) Active la casilla de verificación Activo, para activar la pausa de Contact Center a nivel de sistema.
9) Haga clic en **Guardar**.
10) Si desea agregar una nueva pausa de Contact Center, repita los pasos 5 a 9.

18.6.2.21 Cómo modificar la pausa de Contact Center

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Pausas de Contact Center**.
5) Seleccione la pausa de Contact Center deseada y haga clic en **Editar**.
6) Modifique los parámetros deseados
7) Elija una de estas opciones:
   - Si desea que la pausa de Contact Center esté a disposición de los agentes, active la casilla de verificación **Activo**.
   - Si no desea que la pausa de Contact Center esté a disposición de los agentes, desactive la casilla de verificación **Activo**.
8) Haga clic en **Guardar**.

18.6.2.22 Cómo borrar pausas de Contact Center

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Pausas de Contact Center**.
5) Seleccione la pausa de Contact Center deseada y haga clic en **Eliminar**.

18.6.2.23 Cómo agregar un motivo de tratamiento posterior para el "Tratamiento posterior simple"

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Códigos de tratamiento posterior de Contact Center**.
   Se muestran todas las colas para las que se ha definido un motivo de tratamiento posterior para el "Tratamiento posterior simple".
5) Haga clic en **Agregar**.
6) En la lista desplegable **Cola**, seleccione la cola a la que desea agregar un motivo de tratamiento posterior.
7) En el campo **Descripción**, introduzca una designación para el nuevo motivo de tratamiento posterior.
8) Haga clic en **Guardar**.
9) Si desea agregar un nuevo motivo de tratamiento posterior, repita los pasos del 5 al 8.

18.6.2.24 Cómo modificar el motivo de tratamiento posterior para el "Tratamiento posterior simple"

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.

3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Códigos de tratamiento posterior de Contact Center**. Se muestran todas las colas para las que se ha definido un motivo de tratamiento posterior para el "Tratamiento posterior simple".
5) Seleccione la entrada deseada y haga clic en **Editar**.
6) Si desea asignar el motivo de tratamiento posterior de otra cola, en la lista desplegable **Cola** seleccione la nueva cola.
7) Si desea modificar la designación del motivo de tratamiento posterior, en el campo **Descripción** introduzca el nuevo nombre.
8) Haga clic en **Guardar**.

18.6.2.25 Cómo borrar el motivo de tratamiento posterior para el "Tratamiento posterior simple"

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Códigos de tratamiento posterior de Contact Center**. Se muestran todas las colas para las que se ha definido un motivo de tratamiento posterior para el "Tratamiento posterior simple".
5) Marque la entrada deseada y haga clic en **Eliminar**.

18.6.2.26 Cómo agregar un motivo de tratamiento posterior para el "Tratamiento posterior múltiple"

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Código de resumen múltiple**.
5) Seleccione la cola deseada en la lista desplegable **Cola del Contact Center**. Se muestran los grupos y grupos secundarios definidos para la cola de espera.

Nota: Debajo de cada grupo o subgrupo (si lo hay), también se debe configurar al menos un elemento para que el agente pueda finalizar una llamada. No es posible finalizar una llamada si un grupo o subgrupo está vacío.

---

6) Si desea recoger el nuevo motivo de tratamiento posterior en un grupo con otros códigos de tratamiento posterior, elija una de estas opciones:
   - Si desea asignar el nuevo motivo de finalización a un grupo o subgrupo existente, seleccione el grupo o subgrupo deseado y haga clic en **Agregar elemento**. Ingrese una designación para el nuevo motivo de resumen en el campo **Nuevo elemento de resumen** y haga clic en **Aceptar**.
   - Si desea asignar el nuevo motivo de finalización a un nuevo grupo, haga clic en **Agregar grupo**. Ingrese una designación para el nuevo grupo en el campo **Nombre del grupo** y haga clic en **Aceptar**.

     Seleccione el nuevo grupo y haga clic en **Agregar elemento**. Ingrese una designación para el nuevo motivo de resumen en el campo **Nuevo elemento de resumen** y haga clic en **Aceptar**.
   - Si desea asignar el nuevo motivo de conclusión a un nuevo subgrupo, seleccione el grupo deseado y haga clic en **Agregar grupo**. Ingrese una designación para el nuevo subgrupo en el campo **Nombre del grupo** y haga clic en **Aceptar**.

     Seleccione el nuevo subgrupo y haga clic en **Agregar elemento**. Ingrese una designación para el nuevo motivo de resumen en el campo **Nuevo elemento de resumen** y haga clic en **Aceptar**.
7) Si desea agregar otro motivo de finalización, repita los pasos 5 y 6.

18.6.2.27 Cómo modificar el motivo de tratamiento posterior para el "Tratamiento posterior múltiple"

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Código de tratamiento posterior múltiple**.
5) En la lista desplegable **Cola de centro de contactos**, seleccione la cola deseada. Se muestran los grupos y grupos secundarios definidos para la cola de espera.
6) Seleccione el grupo o grupo secundario que está asignado al motivo de tratamiento posterior que desea modificar. Se muestran todos los motivos de tratamiento posterior (elementos) asignados al grupo.
7) Marque el motivo de tratamiento posterior que desea modificar y haga clic en **Cambiar nombre de elemento**.
8) En el campo **Cambiar nombre de código de tratamiento posterior**, introduzca una nueva designación para el motivo de tratamiento posterior y haga clic en **Aceptar**.
9) Si desea modificar la designación del grupo o del grupo secundario, haga clic en **Cambiar nombre de grupo**.
10) En el campo **Nombre grupo**, introduzca una nueva designación para el grupo o grupo secundario y haga clic en **Aceptar**.

18.6.2.28 Cómo borrar el motivo de tratamiento posterior para el "Tratamiento posterior múltiple"

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Código de tratamiento posterior múltiple**.
5) En la lista desplegable **Cola de centro de contactos**, seleccione la cola deseada. Se muestran los grupos y grupos secundarios definidos para la cola de espera.
6) Seleccione el grupo o grupo secundario que esté asignado al motivo de tratamiento posterior que desea borrar. Se muestran todos los motivos de tratamiento posterior (elementos) asignados al grupo.
7) Marque el motivo de tratamiento posterior que desea borrar y haga clic en **Eliminar elemento**.
8) Si desea borrar el grupo o grupo secundario, haga clic en **Eliminar grupo**.

18.6.2.29 Cómo asignar un agente a una cola

El asistente **Contact Center** permite asignar agentes a una o varias colas de espera.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Enlaces de cola**. Se mostrarán todas las colas existentes.
5) Seleccione la cola a la que desea asignar un agente y haga clic en **Editar**. Se muestran todos los agentes asignados.
6) Haga clic en **Añadir** para añadir el agente correspondiente a la cola deseada. Aparecerá la ventana **Añadir**.
7) Elija una de estas opciones:
   - Si el agente debe recibir llamadas sin tener en cuenta la carga de la cola, seleccione **Agente principal** en la lista desplegable **Tipo**.
   - Si el agente debe recibir llamadas solo cuando se desborde la cola, seleccione **Agente de desbordamiento** en la lista desplegable **Tipo**.

8) Si ha seleccionado **Agente de** desbordamiento:
   a) En el campo **Desbordamiento tras segundos en cola** indique el tiempo tras el cual las llamadas dirigidas a un agente se transferirán con desbordamiento.
   b) En el campo **Desbordamiento tras llamadas en cola** introduzca el número máximo de llamadas. Los agentes de desbordamiento reciben las llamadas que superan este valor máximo.
9) Establezca un valor porcentual para el **Nivel de habilidad** del agente.

   El nivel de habilidad permite controlar la distribución de llamadas a los agentes de una cola de espera. Los agentes con un nivel de habilidad elevado tienen prioridad en la distribución de llamadas. Cuando todos los agentes tienen el mismo nivel de habilidad, el agente que lleve más tiempo libre recibirá la llamada.
10) Elija una de estas opciones:
   - Si desea que el agente reciba las solicitudes de devolución de llamada en forma de mensajes de voz, active la casilla de verificación **Activar devolución de llamada de agente**.
   - Si no desea que el agente reciba solicitudes de devolución de llamada, desactive la casilla de verificación **Activar devolución de llamada de agente**.
11) Introduzca el tiempo de trabajo automático en segundos para el agente de esta cola en el campo **Tiempo de trabajo**.
12) Haga clic en **Guardar**.
13) Si desea asignar más agentes a las colas, repita los pasos del 5 al 12.

18.6.2.30 Cómo eliminar un agente de una cola

El asistente **Contact Center** permite eliminar agentes de una o varias colas de espera.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Contact Center**.
4) Haga clic en **Enlaces de cola**. Se mostrarán todas las colas existentes.
5) Seleccione la cola de la que desea eliminar un agente y haga clic en **Editar**. Se muestran todos los agentes asignados.
6) Seleccione el agente deseado y haga clic en **Eliminar**.
7) Si desea eliminar más agentes de las colas, repita los pasos 5 y 6.

18.7 Observaciones sobre el uso del Contact Center

Aquí le ofrecemos información sobre peculiaridades y posibles limitaciones al usar el Contact Center.

18.7.1 Restricciones de servicio del Contact Center

Hay determinadas condiciones para el servicio del Contact Center. Además, hay restricciones en el uso de las prestaciones de sistema por parte de los agentes.

Condiciones para el servicio del Contact Center

Hay que tener en cuenta las siguientes condiciones para el servicio del Contact Center:

- Líneas

  El Contact Center no es compatible con líneas urbanas analógicas (HKZ). Todas las conexiones externas del Contact Center se deben realizar a través de RDSI o telefonía IP. Hay que tener en cuenta que la conexión mediante teléfonos IP solo se puede realizar a través de un ITSP (proveedor de servicios de telefonía por Internet) certificado.
- Interconexión

  En una interconexión, todos los agentes deben estar conectados con el sistema de comunicación en el que está configurado el Contact Center.
- Teléfonos de agente

  Los agentes pueden usar todos los teléfonos del sistema (teléfonos IP (HFA), como por ejemplo, OpenStage 40, o teléfonos $U_{P0/E}$, como por ejemplo, OpenStage 40 T) y teléfonos DECT. Hay que tener en cuenta que solo se pueden utilizar los teléfonos DECT habilitados actualmente para operar con OpenScape Business Cordless.

  No se pueden utilizar teléfonos analógicos, RDSI y SIP.

  Los agentes no pueden ser miembros de un grupo (llamada de grupo, línea colectiva) ni un MULAP. Esta restricción también se aplica para las prestaciones del sistema utilizadas junto con MULAP: "Configuración de equipo (grupo Team)", "Jefe/Secretaria (grupo Top)" y "Mobility Entry".
- myAgent

  No conviene utilizar myAgent al mismo tiempo que otros clientes de UC ya que los estados de presencia pueden afectarse mutuamente (véase Observaciones para el uso simultáneo de myAgent y clientes de UC Suite). En el modo de servicio normal del Contact Center, los agentes utilizan exclusivamente myAgent para modificar su estado (iniciar sesión, finalizar sesión, estado Disponible, etc.).
- Conexión de aplicaciones a través de la interfaz CSTA

  Siempre que se mantengan las siguientes condiciones, las aplicaciones se pueden conectar a través de la interfaz CSTA:

  – La aplicación no puede crear una carga adicional notable en la interfaz CSTA.

    En consecuencia, no se permite la conexión de soluciones de Comunicaciones Unificadas o de distribución de llamadas, marcadores

CTI-Power ni de soluciones CTI con muchos clientes individuales CTI de uso intensivo.

– La aplicación no puede controlar ningún teléfono de agente a través de la interfaz CSTA ni configurar desvíos para los teléfonos de agente.

  En consecuencia, no se permite la conexión de aplicaciones CTI para agentes, asistentes de reglas o asistentes personales.

Por norma general, está autorizada la conexión de TAPI 120/170. Para cargar el sistema de comunicación se aplican las mismas condiciones que para la conexión de otras aplicaciones mediante la interfaz CSTA. En combinación con el Contact Center, el TAPI 120/170 120/170 se debería utilizar preferentemente para la conexión de sistemas CRM (Customer Relationship Management, o Gestión de relaciones con los clientes) y ERP (Enterprise Ressource Planning, o Planificación de recursos empresariales), siempre que estos sistemas sean compatibles con TAPI.

Restricciones de uso de prestaciones del sistema

Las prestaciones de sistema indicadas a continuación no están a disposición de los agentes, o lo están con restricciones. No obstante, estas prestaciones no son obligatorias para los agentes ya que la asignación de llamadas se realiza automáticamente mediante el Contact Center. La asignación depende de las reglas configuradas y de la disponibilidad de los agentes.

- Prestaciones bloqueadas

  La activación de prestaciones del sistema con myAgent y con el teléfono de agente correspondiente no se admite para los agentes disponibles del Contact Center. Los agentes solo pueden activar prestaciones del sistema con myAgent.

  Por ello, en combinación con myAgent no se admiten las siguientes prestaciones del sistema:

  – Aviso llam. en espera
  – Segunda llamada
  – Aparcar
  – Llamada de grupo
  – No molestar (para agentes registrados)
  – Intercalación en una comunicación de agente (excepción: agentes con el nivel de clase de servicio Supervisor o Administrador)
  – Prestaciones relativas al encaminamiento de llamadas y conexiones activas

- Prestaciones con efectos en el encaminamiento de llamadas

  Las siguientes prestaciones pueden modificar el encaminamiento de las llamadas del Contact Center y, por ello, no deberían ejecutarlas los agentes.

  – Desvío de llamadas

    Si un agente registrado inicia un desvío de llamadas, se cierra sesión en la cola.

    El desvío de llamadas se desactiva en cuanto el agente inicia sesión en una cola de espera.
  – No molestar

    Si un agente registrado activa el estado No molestar mediante un cliente de UC, se cierra la sesión.

    El estado No molestar se desactiva en cuanto el agente inicia sesión en una cola.
  – Reasignación

    Al reasignar un teléfono se modifica la asignación lógica de números de teléfono. La nueva asignación de números de teléfono solo se transmite tras reiniciar (Restart) el Contact Center.
  – Servicio nocturno

    En la configuración de un servicio nocturno en el sistema de comunicación hay que tener en cuenta que la configuración de los parámetros relevantes del Contact Center (agentes, colas, etc.) es idéntica para el servicio nocturno y diurno.
- Prestaciones con efectos en los informes

  La ejecución de estas prestaciones desde un teléfono de agente puede falsear la información de los informes.

  – Telecaptura de llamadas de Contact-Center por extensiones que no son de agente
  – Telecaptura (por ejemplo a través de la tecla de llamada directa) de llamadas del Contact Center a usuarios que no sean agentes
  – Conferencia
  – Alternar
  – Aparcar

  Consejo: La prestación "Consulta" no es relevante para la presentación de llamadas de Contact Center en informes y la pueden utilizar los agentes, con independencia del destino de la consulta.
- Funciones no relevantes para los agentes

  Las siguientes funciones no son relevantes, ya que la prestación "Aviso de llamada en espera" está bloqueada para los agentes.

  – Puesto de operadora
  – Destino de Hot-line

18.8 Observaciones sobre el uso de teléfonos DECT

Los teléfonos DECT se pueden utilizar como teléfonos para los agentes de Contact Center. Hay que tener en cuenta las diferencias en el procedimiento de control respecto a los teléfonos con cable.

Requisitos para usar teléfonos DECT

- Solo se pueden utilizar los teléfonos DECT habilitados actualmente para el funcionamiento con HiPath Cordless Office y OpenScape Business Cordless.
- La zona por la que se mueven los agentes del Contact Center debe tener plena cobertura móvil.
- El número de la extensión base debe ser adecuado para que haya disponibles suficientes canales B para los teléfonos DECT de los agentes del Contact Center.
- Los agentes de Contact Center no deben abandonar la zona de recepción inalámbrica mientras estén registrados en una cola del Contact Center.

Diferencias en el procedimiento de control respecto a los teléfonos con cable

- Solo se puede iniciar sesión en una cola de espera del Contact Center a través de myAgent.
- En la pantalla de los teléfonos DECT no se muestran mensajes, como por ejemplo **Disponible** o **Pausa**.
- Un teléfono DECT no se puede controlar a través de myAgent (por ejemplo, a través del área **Telefonía** de la ventana principal de myAgent o a través de la ventana emergente de la llamada de myAgent entrante).
- Las llamadas entrantes solo se pueden aceptar a través del teléfono DECT.
- Las llamadas salientes se deben iniciar a través del teléfono DECT.

Efectos que tener en cuenta al usar teléfonos DECT:

- Tiempo de búsqueda

  Si se produce una llamada entrante, el tiempo hasta que se localiza el teléfono DECT puede durar varios segundos (en el peor caso hasta 20 segundos) antes de que la llamada se señalice en el teléfono DECT. Durante el tiempo de búsqueda, el oyente escucha el tono de llamada.

  El Contact Center evalúa este tiempo como tiempo transcurrido hasta la aceptación de la llamada. El tiempo propiamente dicho hasta que un agente del Contact Center acepte la llamada se compone así del tiempo de búsqueda y del tiempo de duración del timbre.

  Si un agente del Contact Center abandona el área de cobertura con su teléfono DECT, pueden darse tiempos de búsqueda más largos.
- No se puede encontrar el teléfono DECT

  Si una llamada de Contact Center supera el tiempo preestablecido hasta que la llamada es respondida por el agente (por ejemplo, si el agente del Contact Center se encuentra fuera de la zona de cobertura inalámbrica), se cierra automáticamente la sesión del agente en la cola o colas de espera. Solo se puede volver a iniciar sesión a través de myAgent.

18.9 Informes

Los informes permiten obtener el estado actual del Contact Center y analizar los puntos fuertes y débiles de los componentes correspondientes. Permite, por ejemplo, optimizar la configuración del Contact Center y un uso más eficaz de los recursos del Contact Center. El Contact Center ofrece a los usuarios informes en tiempo real e informes de historial.

Informes en tiempo real

Los informes en tiempo real se actualizan permanentemente. Ofrecen información importante, por ejemplo, datos sobre carga de los agentes, nivel de servicio, tasas de cancelación y tiempos de tramitación medios. Las listas de llamantes actualizadas constantemente y con capacidad de filtro permiten examinar gradualmente la evolución de un contacto con el cliente. Además, se pueden comprobar las actividades de todos los agentes. Esta información se puede utilizar, por ejemplo, para fines de formación o para actividades de seguimiento o de comprobación de contactos.

Los agentes con el nivel de clase de servicio Supervisor o Administrador pueden recibir avisos visuales o sonoros si se superan determinados tamaños de servicio ajustables. Los valores umbral correspondientes se pueden definir por separado para cada una de las colas.

Informes de historial

Al seleccionar elementos de datos y parámetros de informe específicos del usuario se pueden configurar rápidamente informes de historial y consultarlos en forma de gráfico o de tabla.

La aplicación myAgent permite utilizar más de 20 plantillas de informe predefinidas para informes estándar.

La aplicación opcional myReports amplía las opciones de creación de informes históricos mediante más de 100 plantillas de informe predefinidas. La creación de informes se puede planificar de forma individual. Los informes creados se pueden enviar en momentos programados a destinatarios de correo electrónico previamente establecidos o un lugar de almacenamiento configurado por el administrador de myReports. Se enviarán en los formatos de exportación habituales.

Consejo: Los informes se basan en el historial de llamadas almacenado en el sistema de comunicación. El tiempo de retención máximo del historial de llamadas es de 365 días (ajuste estándar). Los administradores con el perfil **Experto** pueden ajustar el tiempo de retención del historial de llamadas a nivel de sistema.

Ejemplo: el tiempo de retención se ha configurado en 100 días. Con ello, para crear informes se pueden consultar datos con una antigüedad máxima de 100 días.

Protección de datos

Si al configurar myReports, el administrador de myReports ha activado la protección de datos, en todos los informes correspondientes, las cuatro

últimas posiciones de los números de teléfono (columna CLI) se sustituyen por asteriscos (****).

Si una extensión interna ha identificado como no visible su número de teléfono privado, su número de teléfono móvil, su número externo 1 o su número externo 2, estos números de teléfono no se mostrarán en los informes correspondientes.

18.9.1 Plantillas de informe predefinidas

myReports ofrece más de 100 plantillas de informe predefinidas para crear informes.

Estas plantillas están asignadas a los siguientes temas (grupos de informes):

- **Actividad del agente**
- **Agentes**
- **CLI**
- **Historial de llamadas**
- **Llamadas**
- **Fax/Correo electrónico**
- **Otros**
- **Rendimiento**
- **Colas de espera**
- **Estado de presencia del usuario**
- **Códigos de tratamiento posterior**

19 Mobility

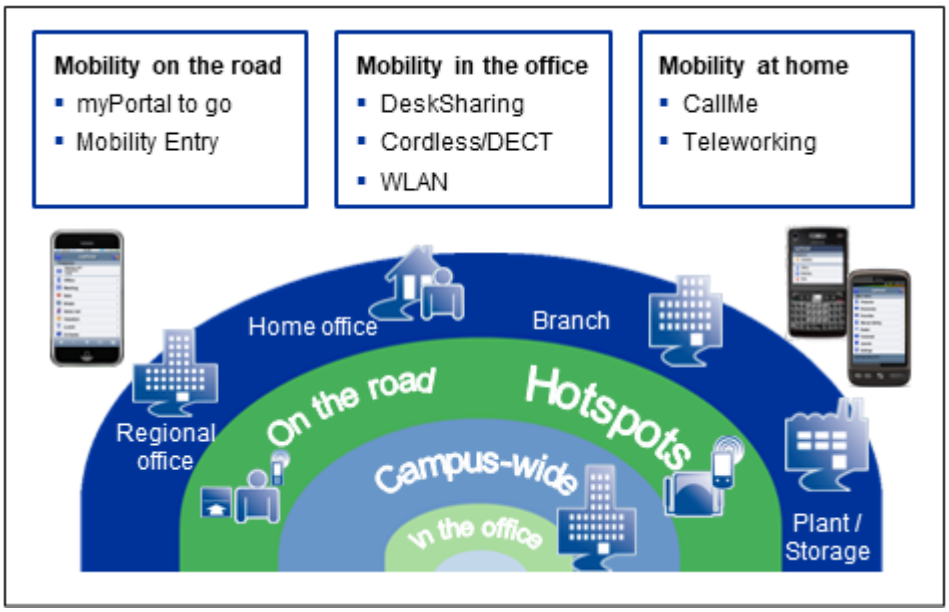
OpenScape Business ofrece soluciones de movilidad integradas para cada empresa. Incluye, por ejemplo, la integración de teléfonos móviles/ smartphones, el uso de teléfonos Cordless/DECT y WLAN, DeskSharing o teletrabajo, entre otros. Mobility incluye Movilidad fuera de casa/la oficina, Movilidad en la oficina y Movilidad en casa.

Conceptos relacionados

Estaciones en la página 432

19.1 Soluciones de movilidad integradas

Las soluciones de movilidad integradas en el sistema de comunicación brindan una comunicación eficaz global y con todo tipo de terminales.



19.2 Movilidad fuera de casa/la oficina

La movilidad fuera de casa/la oficina se consigue a través de la integración de teléfono móvil mediante myPortal to go o Mobility Entry. El One Number Service (Servicio de número único) permite acceder a una extensión a través de un único número de teléfono desde todo el mundo. La telefonía Dual-Mode permite ahorrar costes adicionales cuando la extensión se encuentra en el alcance de una WLAN.

Movilidad fuera de casa/la oficina es la combinación de:

- Teléfono de oficina y smartphone (myPortal to go)
  - Accesibilidad con un número de teléfono (One Number Service)
  - Control de prestaciones mediante el cliente web
  - Funciones de UC como, por ejemplo, control de presencia

- Teléfono de oficina y teléfono móvil (Mobility Entry)
  - Accesibilidad con un número de teléfono (One Number Service)
  - Control de prestaciones con códigos MF

Además de la combinación de teléfono móvil y teléfono de oficina también es posible configurar un teléfono móvil únicamente (es decir, sin teléfono de oficina en paralelo) para la accesibilidad con un número de la red de telefonía fija.

Con los teléfonos del sistema (HFA) se tiene todo el abanico de funciones. Se pueden utilizar teléfonos SIP, pero con restricciones.

19.2.1 myPortal to go

myPortal to go es una potente aplicación de Unified Communications para smartphones y tabletas y permite acceder a los usuarios a las prestaciones de Unified Communications del sistema de comunicación. Ofrece cómodas ayudas de marcación mediante directorios y favoritos e información sobre el estado de presencia de los usuarios. Pero, además, también ofrece acceso a mensajes de voz, por ejemplo.

myPortal to go está disponible en tres versiones:

- como app Mobile UC para el sistema operativo Android (versión 5.0 o superior)
- como app Mobile UC para el sistema operativo iOS de Apple (versión 12.5 o superior)
- como Web Edition para navegadores web móviles compatibles con HTML5, por ejemplo, sistemas operativos Windows Phone (versión 8.0 o superior) o Blackberry (versión 10 o superior):

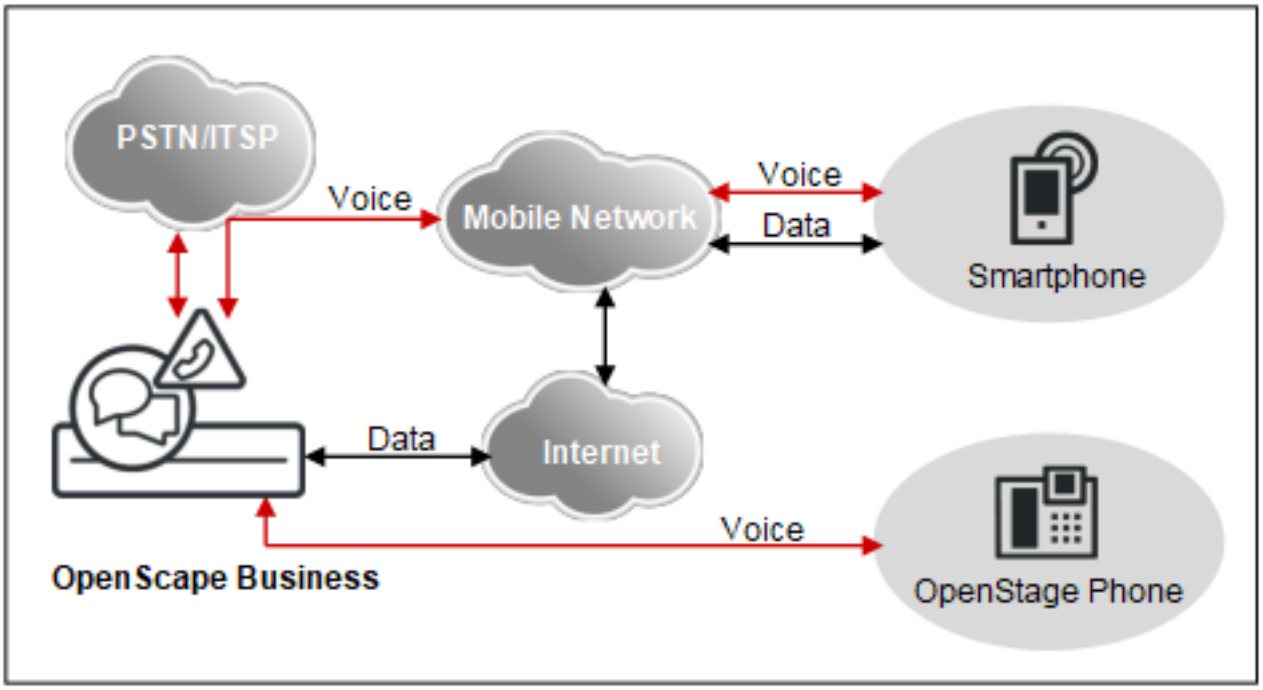
  `http://<Dirección IP del sistema de comunicación>:8801`

  `https://<Dirección IP del sistema de comunicación>:8802`

  Por motivos de seguridad, se recomienda utilizar exclusivamente https. Para ello, en el router hay que configurar un redireccionamiento de puertos del TCP/443 externo al TCP/8802 interno.

  Nota: Recuerde que al usar myPortal to go Web Edition con el modo de servicio de Teléfono de sobremesa, no se pueden utilizar funciones de telefonía desde el cliente. Puede realizar llamadas, pero el payload pasará por el teléfono de sobremesa que esté conectado.

myPortal to go se puede utilizar tanto en teléfonos móviles GSM como en teléfonos Dual-Mode. Para myPortal to go se requiere un contrato de telefonía móvil que permita la transmisión de datos (se recomienda una tarifa plana).



El abanico de funciones para las versiones es el mismo, salvo contadas excepciones (p.ej., acceso a datos de contactos del teléfono móvil).

myPortal to go admite las siguientes prestaciones:

- Estado de presencia
- Desvío de llamadas basado en el estado
- Servicio CallMe (solo con UC Suite)
- Directorios
- Lista de favoritos
- Diario
- Búsqueda de números de teléfono y nombres
- Funciones de llamada
- One Number Service (Servicio de número único)
- Buzón de voz
- Mensajes de texto

Prestaciones CTI durante una llamada:

- Consulta
- Alternar
- Conmutación
- En conferencia
- Desconectar

myPortal to go se puede utilizar con la soluciones de Unified Communications UC Smart y UC Suite. En función de la solución de UC y de las licencias que tenga asignadas, las prestaciones disponibles pueden variar ligeramente.

myPortal to go admite dos modos operativos:

- Mobility:

  Acceso ilimitado a las prestaciones de telefonía y de UC, desde cualquier ubicación (incl. One Number Service).

- Teléfono de sobremesa:

  Uso de las prestaciones de UC y como ayuda a la marcación para el teléfono de oficina (sin One Number Service).

Puede utilizar otras prestaciones con los clientes de UC (p.ej. myPortal for Desktop).

myPortal to go establece una conexión cifrada (https) con el servidor de UC de OpenScape Business. Si la conexión se interrumpe (modo sin conexión), las entradas del Diario y de la lista de favoritos que estén en el portapapeles se pueden marcar por GSM; también se puede realizar una marcación GSM manual.

Nota: Para respaldar la movilidad, myPortal to go debe registrarse como usuario VoIP (HFA) de forma que se active el puerto correspondiente por parte del sistema Openscape Business System.

Procedimiento de marcación de myPortal to go

Con las llamadas salientes, el usuario de smartphone puede utilizar distintos procedimientos de marcación en función del modo de servicio:

- Call through (Llamada directa) (solo en el modo de servicio Mobility)
- Enlace de devol. llam. preferido (solo en el modo de servicio Mobility)
- Marc. asoc. (solo modo serv. Teléf. sobremesa)

  myPortal to go controla el establecimiento de conexión para el teléfono en el puesto de trabajo. Si se controla un teléfono SIP o un softclient SIP mediante la marcación asociada, algunas prestaciones CTI como Consulta y Conferencia no están disponibles.

19.2.1.1 RequisitosmyPortal to go

Para utilizar myPortal to go, el smartphone debe tener el equipamiento de hardware y software adecuado.

Se aplican los siguientes requisitos:

- myPortal to go como app Mobile UC: Sistema operativo Android (versión 5.0 o superior) o Apple iOS (versión 12.5 o superior)
- myPortal to go como Web Edition: navegadores web móviles compatibles con HTML5, por ejemplo, sistemas operativos Windows Phone (versión 8.1 o superior) o Blackberry (versión 10 o superior). Ya no se admiten navegadores web que no son compatibles con TLS 1.2.

  Para el acceso, en el router hay que configurar un redireccionamiento de puertos del externo TCP/443 al interno TCP/8802 (https) o TCP/8801 (http). Por motivos de seguridad, se recomienda utilizar exclusivamente https.
- myPortal to go cliente iOS:
  - Se debe configurar un servidor DNS adecuado y se debe otorgar acceso a Internet para que se puedan resolver los nombres de dominio público y se puedan enviar mensajes de notificación automática al dispositivo iOS a través de los servidores APNS de Apple.

  - Si el firewall de la empresa limita el acceso a Internet saliente, asegúrese de que el firewall esté abierto para APNS en el puerto TCP/443.
  - Para las notificaciones push de iOS, es obligatorio mantener actualizado el software del sistema, ya que los certificados obligatorios para la comunicación con el servicio APNS de Apple se actualizarán con frecuencia con las versiones principales y secundarias del sistema y las versiones de reparación.
  - Las últimas versiones de myPortal to go (iOS) son compatibles con la API CallKit de Apple. CallKit es un marco de trabajo que tiene como objetivo mejorar la experiencia de VoIP permitiendo a myPortal to go (iOS) integrarse con las funciones de llamada nativas del dispositivo. La versión mínima requerida del software del sistema es V3R2.

    Los clientes actuales de myPortal to go (iOS) no podrán iniciar sesión en versiones anteriores de OpenScape Business.
  - Al conectarse al servidor de comunicación se aplican los requisitos de seguridad de iOS. El actual certificado autofirmado generado por OpenScape Business no es suficiente si la aplicación se conecta al servidor de comunicación utilizando un nombre de dominio en lugar de una dirección IP del servidor. Apple ha revisado sus requisitos de seguridad para los certificados de servidor TLS https://support.apple.com/en-us/HT210176.

    Para evitar problemas cuando myPortal to go (iOS) no puede establecer una conexión con el servidor de comunicación, recomendamos conectarse al servidor de comunicación a través de la dirección IP o instalar un certificado SSL de confianza en el lado del servidor.
- Pantalla táctil (recomendado para garantizar un cómodo manejo)
- Resolución de pantalla para smartphones: mín. 240 x 320 píxeles (recomendado: 320 x 480 píxeles o más)
- Resolución de pantalla para tabletas: mín. 800 x 480 píxeles (recomendado: 1024 x 600 píxeles o más)
- Acceso a Internet
- Compatibilidad para la transferencia simultánea de voz y datos mediante teléfonos móviles y red móvil
- Una conexión de datos 3G/4G/5G estable. Tenga en cuenta que las conexiones lentas, en particular 2G/EDGE/GPRS, pueden provocar una mala experiencia de usuario y limitaciones funcionales (VoIP).

  Alternativa: conexión WLAN simple con un cliente SIP para la telefonía.
- Se recomienda encarecidamente un plan de datos con tarifa plana.

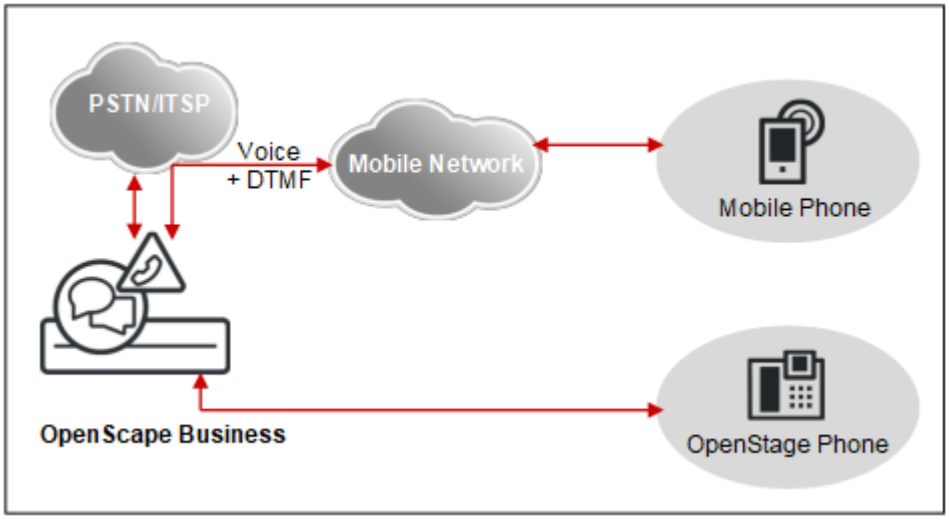
La app Mobile UC se puede descargar gratuitamente en el Google Play Store o en el App Store de Apple.

En función del equipo y del sistema operativo utilizados se pueden ver afectados la comodidad de manejo y el funcionamiento. Solo se garantiza la asistencia si se puede determinar un problema con el dispositivo de referencia. Para consultar información sobre dispositivos de referencia, navegadores y sistemas operativos, consulte las notas de la versión y el wiki de expertos: `https://wiki.unify.com/wiki/myPortal_to_go`.

19.2.2 Mobility Entry

Mobility Entry permite integrar teléfonos móviles. De esta forma, el usuario puede acceder a determinadas prestaciones del sistema a través del teléfono móvil.

Mobility Entry permite el control de conexiones de voz mediante MF después del acceso telefónico.



Procedimiento de marcación de Mobility Entry

Para realizar llamadas salientes, las extensiones de teléfono móvil pueden elegir diferentes procedimientos de marcación.

Mobility Entry ofrece los siguientes procedimientos de marcación:

- Enlace de devol. llam.
- Call through (Llamada directa)

Si en el enlace de devolución de llamada de la extensión de teléfono móvil se llama a un número de marcación directa especial, la llamada se interrumpe antes de establecer la conexión y se realiza inmediatamente una devolución de llamada (enlace de devolución de llamada). Después de la devolución de llamada no son necesarias más autorizaciones. La extensión de teléfono móvil puede realizar llamadas internas y externas a través del sistema de comunicación y usar todas las prestaciones de Mobility.

Estos son los requisitos para el enlace de devolución de llamada:

- El número externo del teléfono llamante está registrado y configurado en el sistema de comunicación. Si no es así, la llamada se interrumpe y no se realiza la devolución de llamada.
- El número de marcación directa DISA está configurado.
- El número de teléfono externo de la extensión de telefonía móvil se transmite al sistema de comunicación (información CLIP).

Prestaciones en estado de reposo

- Marcar número
- Programar o borrar el desvío de llamadas
- Activar o desactivar No molestar

- Enviar info
- Restablecer todos los servicios
- Activar o desactivar la Supresión de la indicación del número de llamada (CLIR)

Prestaciones en estado de comunicación

- Consulta
- Alternar
- Conferencia
- Desconectar y volver a usuario en espera
- Activar devolución de llamada
- Habilitar la marcación posterior MF

Para señalizar las prestaciones, se utilizan códigos de sistema (por ejemplo, *1 para programar desvío de llamadas).

Nota: Para las extensiones Mobility Entry debe estar activado el flag de extensión **Autorización Disa**.

Con OpenScape Business X hay disponibles como máximo 16 recursos DTMF-Code Receiver, es decir, solo 16 extensiones (analógicas, Mobility, etc.) como máximo pueden reservar al mismo tiempo DTMF -Code-Receiver. Las extensiones que tienen activado este flag **Activación de función basada en DTMF** se reservan durante la llamada un Code-Receiver cada una.

En OpenScape Business S, el control de las funciones mediante códigos MF se admite si las cifras MF se pueden transferir por RFC 2833. Si en la red se utiliza un Session Border Controller (SBC) externo, no es posible el reconocimiento MF.

Nota: Solo es necesario configurar Mobility Entry en los nos con acceso directo de línea urbana.

Conceptos relacionados

One Number Service (Servicio de número único) en la página 979
Comparación entre extensiones móviles y Mobility Entry en la página 975
Interdependencias para extensiones móviles y Mobility Entry en la página 977

19.2.3 Comparación entre extensiones móviles y Mobility Entry

Las extensiones móviles myPortal for Mobile y myPortal to go y Mobility Entry son compatibles con distintas prestaciones.

Prestación	**myPortal to go**	Mobility Entry
Funciones generales		
Contrato de telefonía móvil con opción de datos	sí (tarifa plana recomendada)	no

Prestación	**myPortal to go**	Mobility Entry
En este tipo de asignación, todos los campos del esquema de datos de Open Directory Service están asignados de forma fija a la salida LDAP.	sí	sí
Transferencia del número de teléfono de llamante al teléfono móvil (si la red transfiere los números de teléfono externos como CLIP, CLIP no screening)	sí	sí
One Number Service (si la red transmite los números de teléfono externos como CLIP, CLIP no screening)	sí	sí
No molestar/Encaminamiento de llamadas conmutable	no	sí
Supresión de la indicación del número de llamada activable/ desactivable	no	sí
Identificación automática de extensiones registradas	sí	sí
Servicio sin número de teléfono (como extensión virtual)	sí	sí
Utilizable con OpenScape Business S	sí	sí
Presencia, Diario, Buzón de voz		
Modificar el estado de presencia propio	sí	no
Consultar el estado de presencia de otras extensiones	sí	no
Diario	Nuevas, Todas, Perdidas, Contestadas, Entrantes, Mensajes de voz	no
Buzón de voz común, también se puede consultar fuera de la oficina	sí	sí
Indicación de los mensajes de voz entrantes	Indicación de mensajes de voz nuevos, escuchados y guardados	no
Marcar		
Acceso a los contactos del teléfono móvil	sí	sí
Acceso a los contactos del sistema de comunicación	Directorio externo (UC Suite), directorio interno, contactos personales y listín del sistema	no
Favoritos	sí	no
Marcación manual	sí	sí
Rellamada	sí	no

Prestación	myPortal to go	Mobility Entry
Procedimiento de marcación	Enlace de devolución de llamada, Call Through (Llamada directa), Marcación asociada	Enlace de devolución de llamada, Call through (Llamada directa)
Durante la llamada		
Consulta	sí (no con teléfonos SIP)	sí
Alternar	sí (no con teléfonos SIP)	sí
Conmutación	sí (no con teléfonos SIP)	sí
Conferencia	sí (no con teléfonos SIP)	sí
Devolución de llamada en caso de libre y ocupado	no	sí
Captura de llamadas del teléfono móvil en el teléfono de sistema	sí	sí
Indicación de ocupado también en conversaciones con el teléfono móvil (con Servicio de número único)	sí	sí

Conceptos relacionados

Mobility Entry en la página 974

19.2.4 Interdependencias para extensiones móviles y Mobility Entry

myPortal to go y Mobility Entry tienen interdependencias con otras prestaciones (por ejemplo, con DISA).

Interdependencia	myPortal to go	Mobility Entry
N.° llam. marc. directa de Mobility Callback	En el modo de marcación Mobile Callback es necesario configurar el número de marcación directa Mobility Callback.	
Número de destino externo	La marcación de números de destino externos por parte de la extensión móvil se controla en el sistema en virtud de la configuración LCR. De esta forma, la marcación se puede realizar a través de la red fija RDSI, de la red fija analógica o del ITSP.	
Activar CLIP no screening	Para poder visualizar en la extensión móvil el número de un llamante, el proveedor de red debe suministrar el número sin verificación.	
CLIP de la extensión móvil	El CLIP de la extensión móvil debe transferirse al sistema de comunicación. El proveedor de red es el encargado de suministrar el CLIP.	

Interdependencia	myPortal to go	Mobility Entry
Administración LCR	Algunos proveedores de red (red fija o ITSP) no aceptan números de destinos con prefijo internacional. Por esta razón, el sistema debe eliminar el prefijo de los números de destino. Puede administrarse a través de la función LCR.	
Canales B/Conexiones externas	El número de canales B depende de la duración de la conexión o del número de extensiones móviles. Todas las conexiones entrantes externas para una extensión móvil necesitan dos canales de voz en el sistema. Si hay disponibles muy pocos canales de voz, la accesibilidad de la extensión móvil no queda garantizada y es posible que ésta no pueda establecer tampoco ninguna llamada con el servicio de número único.	
Números de llamada de emergencias	Si una extensión móvil marca un número de llamada de emergencias a través del sistema de comunicación, no se puede determinar la ubicación de su teléfono móvil. Se recomienda marcar directamente los números de llamada de emergencia.	
Marcación de números de teléfono internos	Cuando el usuario móvil marca números internos en formato internacional (por ejemplo, 0004989100), el número de ubicación del sistema de comunicación tiene que estar configurado. De lo contrario, los destinos internos se marcan a través de la línea urbana y, con ello, derivan costes.	
Mantenimiento de los directorios	Para garantizar la capacidad de contacto con los interlocutores en la marcación desde directorios con todos los tipos de marcación, es conveniente registrar los números de teléfono externos en formato canónico (por ejemplo, +49 89 100).	-
Firewall	A datos channel is configurar a the integrated web servidor of the sistema de comunicación. Por este motivo, en el firewall debe configurarse un desvío de puertos al puerto 8801 (para http) o al puerto 8802 (para https). Sin embargo, no se recomienda configurar un desvío de puertos para el puerto 8803 (https) para acceder al UC Smart Assistant.	-
Conexión de datos	Se recomienda firmar un contrato de telefonía móvil con tarifa plana de datos. Los usuarios que dispongan de tarifas por volumen, en la configuración de myPortal to go deberían desactivar la opción "Actualización automática".	-
Conexiones en paralelo	Algunas prestaciones requieren una conexión de datos y voz simultánea. Este tipo de conexión debe estar admitida tanto por el proveedor de red de telefonía móvil como por el terminal móvil.	-

Interdependencia	myPortal to go	Mobility Entry
Establecimiento de conexión entre el sistema de comunicación y una extensión móvil a través de	Todos los tipos de línea	Todos los tipos de línea compatibles con la transmisión MF.

Conceptos relacionados

Mobility Entry en la página 974

19.2.5 One Number Service (Servicio de número único)

El One Number Service (ONS) convierte el teléfono móvil en una extensión de red fija. Se puede acceder a la extensión desde todo el mundo con un número de teléfono. La identificación se realiza exclusivamente con su número de teléfono de red fija.

Definiendo una configuración de equipo (Team) se puede utilizar el servicio de número único (One Number Service) con un número de teléfono común para el puesto de trabajo de oficina (teléfono del sistema) y el teléfono móvil. El llamante marca el número de teléfono del teléfono del sistema (red fija). Las llamadas salientes del teléfono móvil se señalizan en la extensión del agente llamado con el número de teléfono de red fija. Otra ventaja del One Number Service es la indicación de ocupado para la extensión móvil.

Conceptos relacionados

Mobility Entry en la página 974

19.2.6 Telefonía Dual-Mode

Los teléfonos móviles Dual-Mode son compatibles con redes GSM/UMTS y con redes WLAN. Es posible registrarse en el sistema de comunicación a través de una red WLAN, en calidad de extensión SIP o de cliente del sistema (por ejemplo, con una extensión HFA).

Si el teléfono móvil Dual-Mode se encuentra en el ámbito de una red WLAN, llama automáticamente como cliente de sistema (extensión HFA) o como extensión SIP. Fuera del ámbito de una red WLAN, el teléfono móvil Dual-Mode recibe llamadas a través de GSM/UMTS (disponible el abanico de funciones de integración de teléfono móvil).

Nota: La telefonía Dual-Mode para HFA solo se admite cuando se utiliza el cliente myPortal to go y no con otros dispositivos o clientes.

El reenvío automático al número de teléfono GSM solo funciona cuando la extensión HFA o SIP correspondiente está registrada en el sistema como extensión de teléfono móvil (integración de teléfono móvil). Es decir, si la extensión HFA o SIP está registrada, recibe llamadas como extensión HFA o SIP. Si no lo está, recibe llamadas a través del número de teléfono GSM asignado en la configuración de integración de teléfono móvil. No hay disponibles funciones de llamada CTI para clientes SIP en

myPortal to go. En lugar de ello el control se realiza en su caso dentro del cliente HFA o SIP (véanse también las notas de la versión y la página `http://wiki.unify.com`).

Las llamadas transcurren dentro de la empresa a través de la LAN. Mientras la comunicación telefónica se realiza mediante WLAN, no recae ninguna tasa de llamadas sobre el teléfono móvil. Handover y Roaming se admiten dentro del alcance de la WLAN (si la infraestructura WLAN se ha diseñado para ello), pero no de WLAN a GSM, o a la inversa.

19.2.7 Configuración de myPortal to go y Mobility Entry

myPortal to go (Web Edition) y Mobility Entry se configuran con el asistente **Integración de teléfono móvil**.

El asistente **Integración de teléfono móvil** permite al administrador:

- Configuración del One Number Service
- Configurar myPortal to go (Web Edition)
- Configuración de Mobility Entry
- Configuración de teléfonos Dual-Mode

La integración de teléfono móvil de teléfonos GSM se realiza mediante extensiones virtuales. De esta forma, las prestación se transmiten a la extensión móvil. A cada extensión con una licencia correspondiente (Mobility User) se puede asignar como máximo una extensión móvil

Modos de servicio de teléfonos móviles

Se han implementado los siguientes modos de servicio para teléfonos móviles:

- **Modo GSM**

  Las llamadas del número móvil interno solo se señalizan en el teléfono móvil GSM.
- **Modo WLAN**

  Si se puede acceder al teléfono móvil WLAN a través de WLAN, la llamada se realiza a través de WLAN. Si no se puede acceder a la WLAN, la llamada se realiza mediante GSM.

Twinning

Las llamadas se señalizan en paralelo en el teléfono de sistema y en el teléfono móvil (Twinning). Para implementar el twinning, después de configurar la Integración de teléfono móvil hay que definir una **Configuración de equipo**. Para ello utilice el asistente **Configuración de equipo** y como primer teléfono seleccione el número de teléfono con el que desea realizar la señalización en paralelo (p.ej., el teléfono del sistema). Para utilizar myPortal to go (Web Edition), el último paso es cambiar la configuración del nombre de usuario con el del grupo Team. Este es el último paso del asistente **Integración de teléfono móvil**. En el teléfono de sistema, para la telecaptura sin interrupciones de llamadas de telefonía móvil se puede programar una tecla de llamada directa para la extensión Mobility. Con los teléfonos del sistema (HFA) se tiene todo el abanico de funciones. Se puede usar también teléfonos SIP pero con restricciones. Por ejemplo, no admiten las teclas MULAP.

Conceptos relacionados

Configuración de configuraciones de equipo / grupos Team y funciones Jefe/ Secretaria / grupos Top mediante asistentes en la página 728
Requisitos para Application Launcher en la página 1216

19.2.7.1 Cómo integrar un teléfono móvil GSM

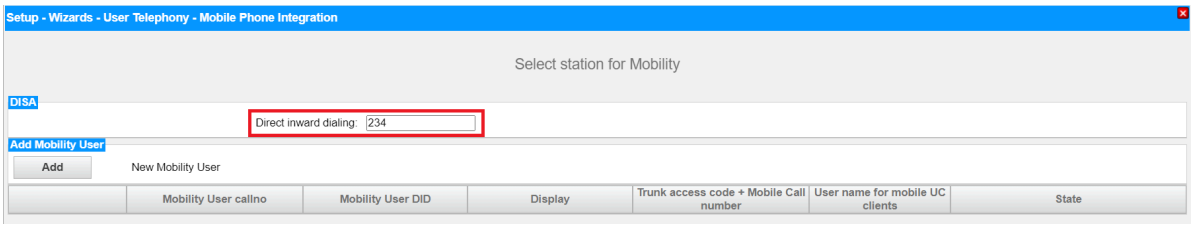
El asistente **Integración de teléfono móvil** permite integrar teléfonos móviles en el sistema de comunicación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Activado Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Integración de teléfono móvil**. Se abre la ventana **Seleccionar extensión para Mobility**.
4) En **Acceso DISA**, seleccione el número de **Marcación directa** (o indique uno) con el que las extensiones móviles pueden acceder al sistema de comunicación.



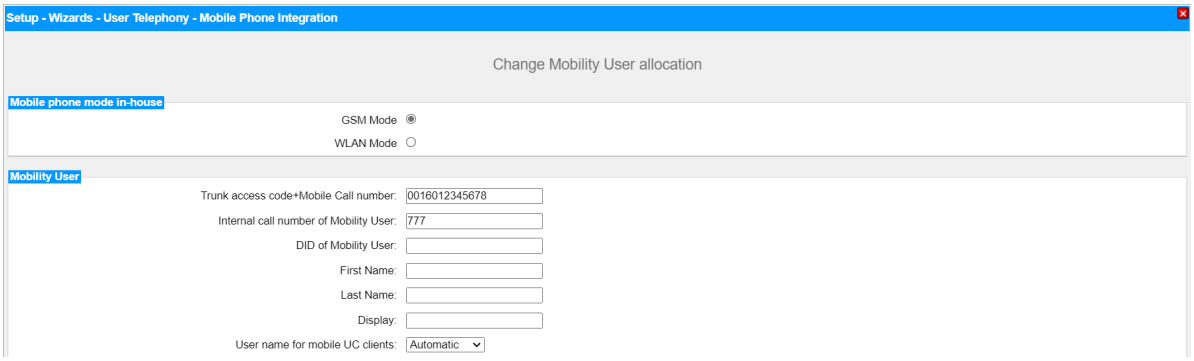
Nota: DISA es requerido para Mobilty Entry (control del sistema mediante MF) y para myPortal for Mobile (solo si se utiliza Call through).

5) Haga clic en la opción **Añadir** o **Editar** del usuario cuyo teléfono móvil GSM desea integrar en el sistema de comunicación. Se muestra la ventana **Asignar usuario Mobility**.
6) Seleccione **Modo GSM** como modo de servicio del teléfono móvil.
7) En **Código para ocupación de línea urbana+Número de teléfono móvil** indique el número del teléfono móvil (por ejemplo, 0016012345678).
8) Indique el **Número interno del usuario Mobility** (por ejemplo, 777), un **nombre interno** de su elección y el **Número de marcación directa**. Recuerde que el número de teléfono interno todavía no puede estar asignado.

: Si desea utilizar DID 879, 890 o 891, debe hacer la configuración a través de ManagerE y no a través de WBM.

9) En la lista desplegable **Nombre de usuario para myPortal to go (Web Edition)**, seleccione la opción **Automático** (al seleccionar esta opción,

se asigna como nombre de usuario el número de teléfono interno de la extensión).



10) Solo con UC Smart: en caso necesario, asigne un buzón a la extensión:

a) En la lista desplegable **Tipo de buzón UC Smart**, seleccione si la Ext. telef. tendrá un buzón estándar o un buzón de puesto de operadora (AutoAttendant).

b) Solo con buzón predefinido: Si desea que los llamantes puedan dejar mensajes en el buzón de voz, active la casilla de verificación **Grabación**.

c) En la lista desplegable **Saludo** introduzca un saludo.

d) Si desea restablecer la contraseña del buzón de voz, active la casilla de verificación **Reponer contraseña**.

Nota: La casilla de verificación **Reponer contraseña** no debe estar marcada al cambiar la configuración de un buzón de voz. Hace que se restablezca la contraseña del buzón de voz. Al cambiar la configuración, el usuario ya debe modificar la contraseña inicial al acceder por primera vez al buzón de voz.

---

11) Haga clic en **OK & Continuar**.

12) Haga clic en **OK y Continuar** y, a continuación, en **Salir**.

19.2.7.2 Cómo integrar un teléfono Dual-Mode (GSM/WLAN) con cliente HFA o SIP

El asistente **Integración de teléfono móvil** permite configurar un teléfono móvil como teléfono Dual-Mode con cliente de sistema (cliente HFA) o SIP (modo WLAN).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

El dispositivo HFA o la extensión SIP se deben configurar mediante la administración basada en web (WBM).

Se ha asignado a la extensión una licencia de usuario Mobility.

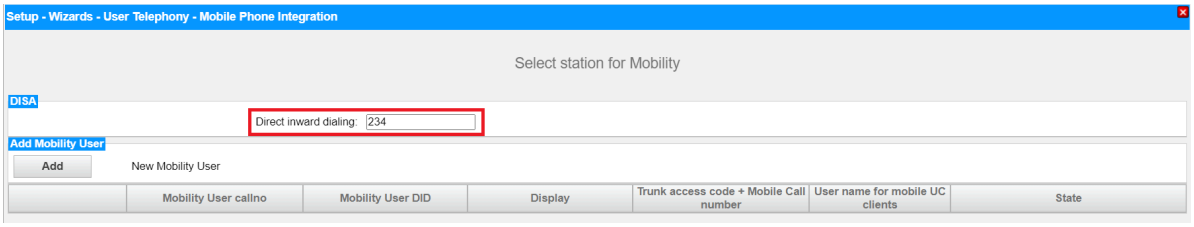
Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.

3) Haga clic en **Editar** para iniciar el asistente **Integración de teléfono móvil**. Se abre la ventana **Seleccionar extensión para Mobility Entry**.

4) En **Puerto DISA**, seleccione el número de **Marcación directa** (o indique uno) con el que las extensiones móviles pueden acceder al sistema de comunicación.



Nota: DISA es requerido para Mobilty Entry (control del sistema mediante MF) y para myPortal for Mobile (solo si se utiliza Call through).

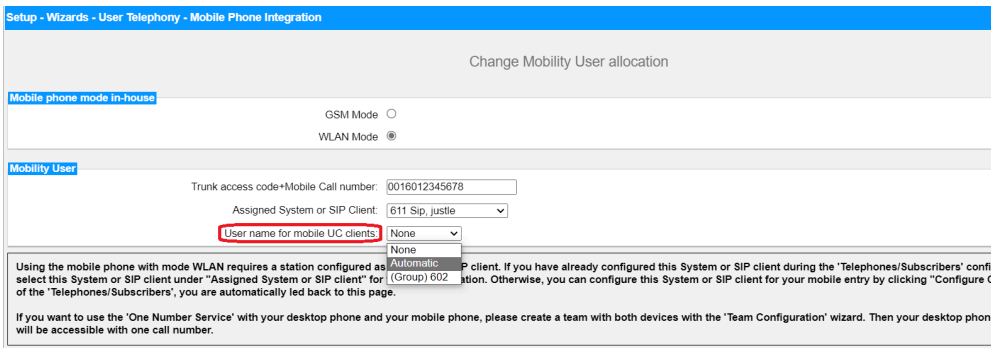
5) Haga clic en la opción **Añadir** o **Editar** del usuario cuyo teléfono móvil GSM desea integrar en el sistema de comunicación. Se muestra la ventana **Asignar usuario Mobility**.

6) Seleccione **Modo WLAN** como modo de servicio del teléfono móvil.

7) En **Código para ocupación de línea urbana+Número de teléfono móvil** indique el número del teléfono móvil (por ejemplo, 0016012345678).

8) En la lista desplegable seleccione el **cliente de sistema o cliente SIP asignado**.

Si el sistema asignado (cliente HFA) o el cliente SIP todavía no está configurado, haga clic en **Configurar cliente** y configure un sistema o un cliente SIP. Una vez concluida la configuración de la extensión de sistema o de SIP, regresará automáticamente a esta página.



9) En la lista desplegable **Nombre de usuario para myPortal to go (Web Edition)**, seleccione el dispositivo HFA o SIP correspondiente. Si selecciona **Automático**, se usará como nombre de usuario el número interno del usuario.

10) Haga clic en **OK & Continuar**.

11) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

19.2.7.3 Cómo activar la interfaz Web para teléfonos móviles y clientes Web

Requisitos previos

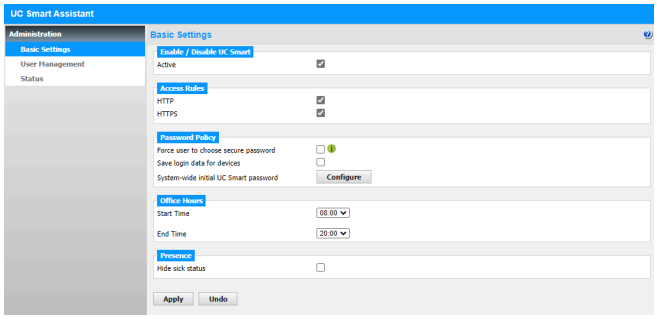
Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Hay que activar Web Services como requisito previo para las siguientes prestaciones:

- Integración de teléfono móvil
- Application Launcher

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) Si utiliza UC Smart, en el árbol de navegación, haga clic en **Aplicaciones** > **UC Smart** > **Ajustes básicos**.
3) Compruebe si UC Smart está **Activo**.
4) Si desea activar Web Services para teléfonos móviles, seleccione al menos una de estas opciones:
   - Si desea permitir conexiones cifradas, active la casilla de verificación **HTTPS**.
   - Si desea permitir conexiones sin cifrar, active la casilla de verificación **HTTP**.



Nota: Por motivos de seguridad se recomienda encarecidamente utilizar exclusivamente una conexión cifrada (HTTPS) se se utiliza myPortal to go (Web Edition) por Internet.

---

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

19.2.7.4 Cómo borrar la integración de teléfono móvil

El asistente **Integración de teléfono móvil** permite borrar la integración del teléfono móvil.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía de usuario**.
3) Haga clic en **Editar** para iniciar el asistente **Integración de teléfono móvil**. Se abre la ventana **Seleccionar extensión para Mobility Entry**.
4) Haga clic en **Editar** de la extensión que desea borrar. Se muestra la ventana **Asignar usuario Mobility**.
5) En la ventana, haga clic en **Borrar datos**.
6) Haga clic en **OK & Continuar**.
7) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

19.3 Movilidad en la oficina

La movilidad en la oficina se consigue a través de DeskSharing, teléfonos Cordless y teléfonos WLAN. Para DeskSharing, IP-Mobility (Mobile Logon y Flex Call) ofrece prestaciones para extensiones móviles que deseen utilizar el teléfono de un puesto de trabajo ajeno como el suyo propio.

19.3.1 Escritorio compartido

Con Escritorio compartido, varios suscriptores pueden compartir un teléfono del sistema y, por lo tanto, un teléfono IP (HFA).

Con Escritorio compartido, los suscriptores no tienen un lugar de trabajo fijo ni un teléfono fijo de oficina. Escritorio compartido permite que varios suscriptores móviles del sistema de comunicación compartan un lugar de trabajo en la oficina y/o el teléfono. El suscriptor simplemente inicia sesión en el teléfono del lugar de trabajo donde trabaja en ese momento.

Tras el inicio de sesión, el número de extensión del abonado que ha iniciado sesión se transfiere al teléfono del sistema utilizado. Ya no se puede contactar con el teléfono del sistema usado con su número de extensión original. Si el suscriptor inicia sesión en otro teléfono del sistema, su número de extensión se transfiere a ese nuevo teléfono del sistema. Cuando el usuario cierra sesión, el teléfono del sistema vuelve a iniciar sesión automáticamente con su propio número no móvil.

Se debe realizar uno de los siguientes pasos en el teléfono del sistema para activar la función:

- Introducir el código para «inicio de sesión móvil» + el número de la estación móvil + la contraseña/PIN opcional

Al utilizar teléfonos con diferentes números de teclas de función, la transferencia de la disposición de las teclas puede tener restricciones.

Si se va a implementar el uso de Escritorio compartido para los teléfonos IP (HFA) en los nodos de la red, se debe instalar un DLS (servicio de implementación) externo. Para este propósito se asume que el usuario tiene la experiencia requerida.

Se pueden usar las siguientes funciones para Escritorio compartido:

- Llamada de altavoz (búsqueda de usuarios)
- Conferencia
- Anular
- Alternar
- Estacionamiento
- Consulta
- Transferir
- Telecaptura de llamadas
- No molestar
- Desvío de llamadas
- Enviar mensaje (mensaje en espera)
- Devolución de llamada
- Supresión del número de extensión
- Timbre adicional en

Nota: Para cada número de teléfono móvil, se requiere una licencia adicional de Escritorio compartido. El suscriptor debe tener la licencia de Escritorio compartido activada y debe estar configurado como **móvil**. Además, la función Reubicar debe estar habilitada.

Un teléfono del sistema que se usa como Escritorio compartido no requiere necesariamente una licencia. Sin embargo, si no hay ninguna licencia activada y ningún suscriptor de Escritorio compartido ha iniciado sesión, ni siquiera será posible realizar llamadas de emergencia desde este teléfono. **El teléfono o suscriptor del sistema debe configurarse como no móvil.**

Si no se va a usar un teléfono del sistema para Escritorio compartido, debe configurarse como **no móvil y bloqueado**.

Nota: La función Escritorio compartido no debe usarse con las dos primeras estaciones del sistema activas.

19.3.2 Solución Cordless integrada

OpenScape Business Cordless es una solución Cordless (inalámbrica) integrada para el funcionamiento de teléfonos Cordless (teléfonos DECT) mediante el sistema de comunicación. Con los teléfonos DECT conectados se pueden utilizar las prestaciones HFA de OpenScape Business.

Con esta solución integrada, los teléfonos DECT son extensiones internas y específicas del sistema, a diferencia de los sistemas DECT independientes, que se conectan mediante interfaces estándar.

La conexión de las extensiones base OpenScape Business para el servicio de los teléfonos DECT se puede implementar mediante:

- Para OpenScape Business X1/X3/X5: conexión directa con las interfaces $U_{P0/E}$ de la placa base de los sistemas de comunicación (DECT Light)
- Para OpenScape Business X3/X5: conexión con las interfaces $U_{P0/E}$ de un módulo SLU8N/SLU8NR (DECT Light)

- Para OpenScape Business X8: conexión con las interfaces $U_{P0/E}$ de un SLMUC (SLMU + CMAe)

La tecnología inalámbrica Cordless se corresponde con el estándar DECT (Digital Enhanced Cordless Telecommunications). Todo el área de cobertura gestionada por el sistema consta de extensiones base que forman una red continua de células de red solapadas o islas independientes. El tamaño de una célula de red depende de las condiciones locales/del edificio.

Modo ECO

En modo ECO, la potencia de envío de los teléfonos DECT se reduce en un valor definido (estático) o cada teléfono DECT adapta automáticamente su potencia de envío a la potencia de la señal recibida (adaptativo). El modo ECO se puede activar en el sistema de comunicación a nivel de sistema para todos los teléfonos DECT (**modo Experto** > **Telefonía** > **Cordless** > **Para todo el sistema**). No hay que hacer ningún ajuste de configuración en los teléfonos DECT. En OpenScape Business X1, X3, X5 hay que reiniciar el sistema de forma manual para activar esta prestación.

- Ajuste estático de la potencia de transmisión

  Los teléfonos DECT y la extensión base reducen la potencia de transmisión a un valor fijo definido.
- Ajuste adaptativo de la potencia de transmisión

  Los teléfonos DECT transmiten con potencia de transmisión normal o reducida, en función de la fuerza del campo de recepción. Con el handover, primero se conecta con la potencia de envío completa y, a continuación, se reduce en función de la recepción.

Teléfonos DECT

La solución Cordless integrada admite la conexión de teléfonos con capacidad GAP de otros fabricantes. El abanico de prestaciones HFA completo solo se puede utilizar con los teléfonos DECT autorizados.

Configuración

En Configuración de la solución Cordless integrada puede consultar una descripción de la configuración.

Módulos y extensiones base

Puede encontrar las descripciones de los módulos y extensiones base en la *documentación de servicios de OpenScape Business, en los capítulos Módulos y Extensión base*.

19.3.2.1 Visión general del sistema

Con OpenScape Business X3/X5, la conexión de las extensiones base OpenScape Business se realiza directamente con las interfaces $U_{P0/E}$ de la placa base o con las interfaces $U_{P0/E}$ de un módulo SLU8N/SLU8NR instalado (DECT Light). Con OpenScape Business X8, las extensiones base se pueden conectar con los módulos *cordless* SLMUC.

Conexión directa (DECT Light)

Las extensiones base se pueden conectar directamente con las interfaces $U_{P0/E}$ de las placas base OCCM, OCCMB, OCCMA y OCCMR, OCCMBR, OCCMAR de los sistemas de comunicación OpenScape Business X3R/X3W y OpenScape Business X5R/X5W o con las interfaces $U_{P0/E}$ de un módulo SLU8N/SLU8NR.

Al utilizar el submódulo CMAe en las placas base, están disponibles las funciones de conversión ADPCM y de cancelación de eco (48 canales para CMAe). Se pueden realizar hasta cuatro llamadas por cada extensión base. En las interfaces $U_{P0/E}$ de las placas base OCCM, OCCMB, OCCMA y OCCMR, OCCMBR, OCCMAR se pueden conectar hasta siete extensiones base.

Si no hay instalado ningún CMAe, se pueden realizar dos llamadas por cada extensión base como máximo. En este caso, la conversión ADPCM se ejecuta directamente desde la extensión base.

Nota: Si no hay instalado ningún CMAe, no hay disponibles funciones de tratamiento de eco.

Para la conexión de extensiones base con un módulo SLU8N/SLU8NR se aplican las siguientes condiciones de conexión:

- En total se pueden operar 15 extensiones base como máximo (7 en la placa base y otras 8 en un módulo SLU8N/SLU8NR). El número máximo de teléfonos DECT que se pueden conectar sigue siendo 64 con un CMAe.
- Solo se puede utilizar un módulo SLU8N/SLU8NR para conectar extensiones base.
- Para la conexión de la extensión base con una interfaz $U_{P0/E}$ del módulo SLU8N/SLU8NR, solamente se puede utilizar el primer puerto de la extensión base. Los puertos 2 y 3 de la extensión base no son compatibles para establecer una conexión con otra interfaz $U_{P0/E}$.
- Las interfaces $U_{P0/E}$ del módulo SLU8N/SLU8NR se pueden proveer de forma mixta, con extensiones base o teléfonos.

Conexión de módulos *cordless*

En las interfaces $U_{P0/E}$ de los siguientes módulos *cordless* se puede conectar la extensión base BS5:

- SLMUC (SLMU + CMAe) con OpenScape Business X8 (consulte *el capítulo SLMUC de la documentación de servicio*).

  Las extensiones base se pueden conectar a través de una, dos o tres interfaces $U_{P0/E}$. Las últimas 8 interfaces de un módulo SLMUC solo pueden utilizarse como 2.ª o 3.ª interfaz UP0 de la extensión base. La conexión adicional de interfaces $U_{P0/E}$ aumenta el valor de tráfico de la extensión base conectada y, con ello, aumenta también el número de canales de llamada disponibles simultáneamente.

19.3.2.2 Conexión de módulos Cordless

En la conexión de módulos Cordless, las extensiones base de conectan a las interfaces $U_{P0/E}$ de los módulos Cordless (módulos SLC).

Pueden conectarse los siguientes módulos Cordless a las interfaces $U_{P0/E}$:

- SLC16N con OpenScape Business X5W (solo sistema mural)
- SLCN con OpenScape Business X8

En OpenScape Business X8 se pueden utilizar hasta cuatro módulos Cordless (SLC). A través de los cuatro módulos Cordless se pone a disposición la funcionalidad completa Cordless (itinerancia y Seamless Connection Handover), ya que los campos radioeléctricos de los módulos Cordless se sincronizan mediante líneas de interconexión SLC (Multi-SLC). Por el momento, no se admite el handover a nivel de red.

Si no hay módulos SLCN ni SLC16N, y la extensión base (BS) está conectada en $U_{P0/E}$, se requerirá un módulo CMA o CMAe en el módulo de control si se cuenta con una red OpenScape Business con itinerancia CMI entre nodos.

19.3.2.3 Configuración del sistema

En función del sistema de comunicación, se pueden conectar hasta 64 extensiones base y se pueden usar hasta 250 teléfonos DECT.

La siguiente tabla muestra la ampliación máxima del sistema de la solución Cordless integrada e informa en qué casos se puede hacer un acceso a línea urbana analógico del sistema de comunicación.

Nota: Las extensiones base BS4 (S30807-U5491-X), BS3/1 (S30807-H5482-X), BS3/3 (S30807-H5485-X) y BS3/S (X30807-X5482-X100) se encuentran en la salida del producto y ya no se pueden hacer pedidos. No obstante, se puede establecer conexión con los sistemas de comunicación OpenScape Business X.

Si hay un defecto, deben utilizarse las extensiones base actuales.

Consejo: Si no hay instalado ningún CMA/CMAe, se pueden realizar dos llamadas por cada extensión base como máximo. En este caso, la conversión ADPCM se ejecuta directamente desde la extensión base DECT, pero la cancelación de eco no se admite directamente. Si es necesario realizar cancelación de eco, se requiere un submódulo CMA/CMAe.

Nota: En la tabla siguiente, la combinación de la tarjeta SLMU con el módulo CMAe se denomina SLMUC.

OpenScape Business	Número máximo de módulos				Módulo de reloj	**Número máximo de extensiones base (BS), si se establece la conexión mediante 1xU_{P0}**	Puertos/ Comunica simultáne por extensión base	**Número máx. de dispositivos registrados**	Número máximo de comunicaciones simultáneas
	SLC16N	**SLCN**	**SLUN**	**SLMUC**					
X1	–	–	–	–	–	7	1/2	16	14
	–	–	–	–	CMA	7	1/4	16	16
	–	–	–	–	CMAe	7	1/4	16	16
X3	–	–	–	–	–	7	1/2	32	16
Onboard $U_{P0/E}$ (SLUC)	–	–	–	–	CMA	7	1/4	32	16
	–	–	1	–	CMA	15	1/4	32	16
	–	–	–	–	CMAe	7	1/4	64	28
	–	–	1	–	CMAe	15	1/4	64	48
X5	–	–	–	–	–	7	1/2	32	16
Onboard $U_{P0/E}$ (SLUC)	–	–	–	–	CMA	7	1/4	32	16
	–	–	1	–	CMA	15	1/4	32	16
	–	–	–	–	CMAe	7	1/4	64	28
	–	–	1	–	CMAe	15	1/4	64	48
X5W	1	–	–	–	–	16	3/12	64	32*
X8	–	4	–	–	–	64	3/12	250 (128 por SLCN)	128**
	–	–	–	4	CMAe	64	3/12	250 (128 por SLCN)	192***

* El valor máx. por SLCN16 es 32. En el caso de la itinerancia, la conversión ADPCM siempre se ejecuta en el módulo SLC16N donde se encuentra actualmente el auricular. Por tanto, el número de llamadas simultáneas por sistema podría ser superior a 32 si el auricular se encuentra en el SLC16N que se visita

** El valor máx. por SLCN es 32. En función de la ubicación de los auriculares en el caso de la itinerancia, todos los dispositivos que están registrados (250) podrían estar teóricamente activos si hay disponibles 4 tarjetas SLCN.

*** SLCN y SLMUC pueden combinarse en un único sistema. El valor máx. es 32 por SLCN y 48 por SLMUC. En función de la ubicación de los auriculares en el caso de la itinerancia, todos los dispositivos que están registrados (250) podrían estar teóricamente activos si hay disponibles 4 tarjetas SLCN/SLMUC en total.

19.3.2.4 Teléfonos DECT/Cordless

Al insertar módulos SLC e introducir la identificación de sistema DECT, se configuran 16 componentes móviles. Se asignan los códigos de componente móvil (PIN) y los componentes móviles pueden iniciar sesión. Primero hay que autorizar los componentes móviles adicionales que se vayan a utilizar.

Si en un servicio técnico se sustituye un componente móvil, hay que modificar el PIN antes de registrar el dispositivo de sustitución. Por norma general, al hacer una sustitución hay que asignar un nuevo PIN en el sistema de comunicación para la extensión correspondiente. Con ello, termina automáticamente la sesión del componente móvil. Además, por motivos de seguridad esto impide que, aunque alguien conozca el PIN antiguo, pueda ser utilizado más para dar de alta un teléfono inalámbrico sin autorización.

19.3.2.5 Significado de los resultados de la prueba de área de cobertura

Importante:

Los valores registrados con un teléfono móvil no son muy precisos y solo intentan brindar una evaluación aproximada. Además, se pueden tomar valores diferentes en cada teléfono móvil aunque las condiciones ambientales sean idénticas. Si requiere resultados más precisos, le recomendamos que utilice la herramienta Hicom Cordless Service (HCS-DECT).

La siguiente figura muestra un ejemplo de los resultados de la medición de un teléfono móvil Gigaset cuando una llamada está en curso:

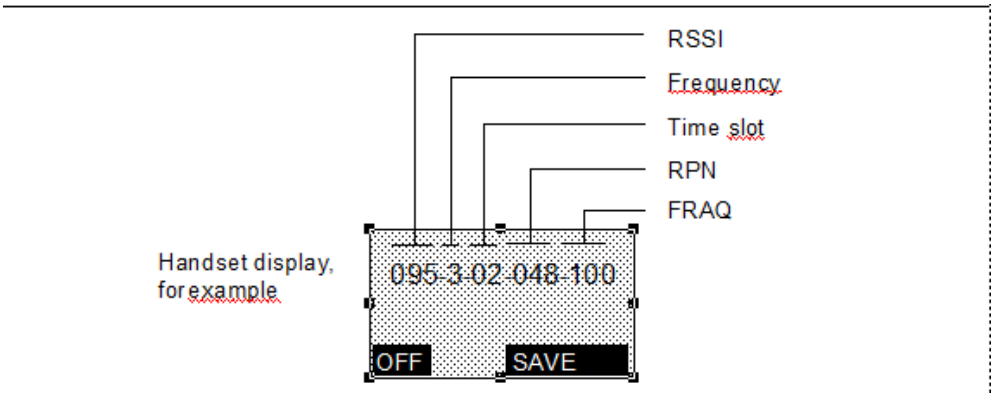


Figura 8: Resultado de la medición

Capítulo	Descripción
RSSI (señal de radio)	Intensidad del campo de la señal recibida por la extensión base, normalizado a máx. 100. Con un valor <50, la conexión inalámbrica con la extensión base deja de estar garantizada. Una intensidad de campo aceptable es >50 (> -60 dBm).

Capítulo	Descripción
Frecuencia	Frequencia (0 – 9)
Tramo temporal (Slot)	Tramo temporal (0 – 11) de recepción del canal en el que se realiza la medición.
RPN (número de puerto)	**OpenScape Business X1/X3/X5/X8** Id. de extensión base, por ejemplo, 048, número de puerto en los módulos SLC. Si el auricular cambia a una célula de red/extensión base superpuestas, el número de puerto actual (donde el canal D de la extensión base está configurado) aparece en el visor del auricular. Fórmula: A x 16 + B A = número of módulo SLC (1 - 127); 16 = factor B = puerto de módulo SLC asociado (donde el canal D de la extensión base está configurado) Ejemplos: RPN = 1 x 16 + puerto 0 = 016 RPN = 2 x 16 + puerto 8 = 040. El número de puerto (PRN) se muestra para auriculares Gigaset S3 profesional y Gigaset SL3 profesional en formato hexadecimal con una H anexada. El valor hexadecimal se muestra sin H anexada; p.ej. "-028-" en el caso de auriculares Gigaset S4 profesional y OpenStage SL4 profesional. Ejemplo: Si el valor 040 apareció anteriormente, el valor 028H ahora aparece para Gigaset S3/SL3 profesional. El formato hexadecimal se diferencia únicamente sobre la base del sufijo "H". Esto también es válido para dispositivos OpenScape DECT Phone S5/SL5/S6/SL6/R6 (sin prefijo H).
FRAQ (frame quality)	Calidad de la transmisión en %. 95 % a 100 % satisfactorio (para cortos períodos 90 % a 94 % no crítico), < 95 % averiado.

Para más información acerca del menú de medición, véase: *OpenScape Cordless Enterprise, Documentación de asistencia técnica, Capítulo: Prueba de área de cobertura* y *OpenScape Business X3/X5/X8, Documentación de asistencia técnica, Capítulo: Comprobar la cobertura móvil.*

19.3.3 Configuración de la solución Cordless integrada

La configuración de la solución Cordless integrada incluye la configuración de las extensiones base y el registro de los teléfonos DECT/componentes móviles en el sistema de comunicación.

La configuración se realiza mediante el modo Experto.

Se han cumplido todos los requisitos previos, como definición de proyecto, iluminación, instalación y cableado, montaje físico del sistema e inserción de módulos SLC o CMA (consulte también la documentación de servicio). Los teléfonos DECT están cargados. Se conoce la identificación del sistema DECT. Hay información sobre extensiones, números de teléfono, nombres y, en su caso, sobre la asignación a los módulos SLC.

Procedimiento general para configurar la solución Cordless integrada

1) Introducir la identificación del sistema DECT y configurar otros parámetros Cordless
2) Configurar extensiones base Cordless
3) Registrar teléfonos DECT en Cordless
4) En caso necesario, añadir más teléfonos DECT

Después de la puesta en marcha de los teléfonos DECT se puede modificar el número de teléfono, el nombre y otros ajustes de los teléfonos DECT mediante la Gestión basada en Web (WBM), con el asistente **Terminales/Extensiones**.

Identificación del sistema DECT

La identificación del sistema DECT permite distinguir entre los distintos sistemas DECT, lo que a su vez permite identificar las señales de radio. Solo así se pueden sincronizar los componentes móviles registrados con el sistema.

La identificación del sistema DECT es una secuencia de números hexadecimal de 8 posiciones y se proporciona al adquirir el sistema DECT. Es válida en todo el sistema (también en operaciones de servicio).

La identificación del sistema DECT consta de:

Dígito	Significado
1.er dígito	E/ARC (Access Right Code)
2.° 5.° dígito	EIC (Equipment Installers Code)
6.° 7.° dígito	FPN (Fixed Part Number)
8.º dígito	FPS (Fixed Part Subscriber)

19.3.3.1 Cómo indicar la identificación de sistema DECT y configurar otros parámetros Cordless (datos a nivel del sistema)

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto** o Hipath 3000 Manager.
Los pasos siguientes hacen referencia solo a WBM, pero se pueden realizar acciones similares utilizando Hipath 3000 Manager.

Hay conectada una extensión base OpenScape Business con el sistema de comunicación.

La identificación del sistema DECT de 8 dígitos proporcionada en el pedido del sistema DECT está disponible.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Cordless**.
3) En el grupo de menús, haga clic en **Cordless** > **Para todo el sistema**.
4) En **EIC**, introduzca la identificación del sistema DECT de 8 dígitos.
5) Modifique los ajustes a nivel de sistema de **Tratamiento de eco** y **Modo ECO** solo en caso necesario. Puede consultar una explicación sobre estos ajustes en Cordless>Para todo el sistema
6) Haga clic en **Aplicar**, seguido de **Aceptar**.

19.3.3.2 Cómo configurar extensiones base Cordless

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto** o Hipath 3000 Manager. Los pasos siguientes hacen referencia solo a WBM, pero se pueden realizar acciones similares utilizando Hipath 3000 Manager.

Hay conectada una extensión base OpenScape Business con el sistema de comunicación.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Cordless**.
3) En el grupo de menús, haga clic en **Cordless**. Se muestran todas las extensiones base conectadas.
4) Si hay una o varias extensiones base conectadas directamente (sin módulo SLC) con el sistema (SLUC), las extensiones base se pueden activar o desactivar mediante la lista desplegable **Tipo**:
   a) **Extensión base**: la extensión base se activa y se preconfiguran automáticamente 16 teléfonos DECT y una línea de interconexión SLC.
   b) **Puerto sin terminal** la extensión base se desactiva con todos los teléfonos DECT correspondientes y la línea de interconexión SLC.
5) Si es necesario, en **Nombre** modifique el nombre preconfigurado de la extensión base (p.ej. `Base 1`).
6) En **Nivel** defina el nivel para la extensión base (50 % o 100 %).
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

19.3.3.3 Cómo configurar por primera vez teléfonos DECT

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto** o está utilizando Hipath 3000 Manager.

Hay conectada una extensión base OpenScape Business con el sistema de comunicación.

Se deben realizar los siguientes pasos de configuración antes de registrar dispositivos DECT en el sistema.

Paso a paso

1) Haga lo siguiente, si está utilizando WBM:
   a) En la barra de navegación, haga clic en **Modo Experto**.
   b) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Cordless**.
   c) En el grupo de menús, haga clic en **Cordless** > **SLC**. Se muestran todos los teléfonos DECT que haya configurados. Al conectar una extensión base, se configuran automáticamente 16 teléfonos DECT.
   d) Si es necesario, en **N° llam.** modifique el número de teléfono interno preconfigurado del teléfono DECT.
   e) Si es necesario, en **Marc. dir.** modifique el número de marcación directa preconfigurado del teléfono DECT.
   f) Si es necesario, en **Nombre** modifique el nombre preconfigurado del teléfono DECT.
   g) Si es necesario, en **Código móvil** modifique el código móvil (PIN) preconfigurado del teléfono DECT. Este código hay que introducirlo en el teléfono DECT la primera vez que se inicia sesión en la extensión base.
   h) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

2) Haga lo siguiente, si está utilizando Hipath 3000 Manager:
   a) Cargue la comprobación de la base de datos de KDS **Leer/escribir KDS** y **Sistema> PC**
   b) En el árbol del menú, continúe **Configuración> Cordless** en el árbol de navegación.
   c) En el árbol del menú, haga clic en **Cordless> SLC** luego en el parámetro **Terminales móviles** comprobar todo. Se muestran todos los teléfonos DECT que haya configurados. Al conectar una extensión base, se configuran automáticamente 16 teléfonos DECT.
   d) Si es necesario, en **N° llam.** modifique el número de teléfono interno preconfigurado del teléfono DECT.
   e) Si es necesario, en **Nombre** modifique el nombre preconfigurado del teléfono DECT.
   f) Si es necesario, en **Código móvil** modifique el código móvil (PIN) preconfigurado del teléfono DECT. Este código hay que introducirlo en el teléfono DECT la primera vez que se inicia sesión en la extensión base.
   g) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
   h) Transfiera el KDS al sistema, si se han realizado cambios.

Tareas relacionadas

Cómo configurar extensiones DECT en la página 470

19.3.3.4 Cómo iniciar sesión con un teléfono DECT (OpenStage/Gigaset-Mobilteil) en Cordless

Antes de registrar un teléfono DECT, debe usar un teléfono del sistema y abrir la ventana de registro con el código de registro DECT. A continuación, introduzca los números de extensión de los teléfonos DECT que desea

registrar. Puede registrar un máximo de 10 números de extensión en la misma ventana de registro. La ventana de registro se abre durante 10 minutos.

Si no hay ningún teléfono del sistema disponible, puede utilizar la función Hipath 3000 Manager **Online** y realizar las acciones desde allí en lugar de usar un teléfono físico. Los pasos que se describen a continuación se refieren al teléfono físico.

Los pasos que se describen a continuación se refieren al teléfono físico.

Paso a paso

1) Abra la ventana de registro en el sistema de comunicación:
   a) En el teléfono físico, introduzca el código *94 2 y luego 19970707.
   b) Introduzca los números de extensión de los teléfonos DECT que desea registrar.

2) Registro del teléfono DECT:
   a) Desde la pantalla de inicio del teléfono DECT, pulse la **tecla de menú**.
   b) Vaya a **Configuración > Registro > Registrar teléfono** y seleccione **Base**.
   c) Se le pedirá que introduzca el PIN del sistema de la extensión. Introduzca el código móvil de ocho dígitos y confirme la entrada.

      Debe esperar una o dos llamadas silenciosas, es decir, llamadas automáticas cortas (en algunos dispositivos, esto equivale a 2 timbres).

      Si está registrando un número de llamada inactivo (que no se haya utilizado antes; negro en WBM y gris en KDS) entonces el registro se completa con una llamada silenciosa. Si está registrando un número de llamada activo que se haya utilizado anteriormente (verde en WBM y KDS), el registro se completa con dos llamadas silenciosas.

      No realice ninguna otra acción (por ejemplo, iniciar llamadas telefónicas DECT) hasta que el proceso haya finalizado.

Una vez que haya registrado el teléfono con éxito, verá el número de extensión en la pantalla de inicio y podrá utilizar el dispositivo.

Ejemplo: Registrar el teléfono móvil (número de extensión 125) en el sistema utilizando el código móvil (PIN) 11112345, configurado como código móvil mediante Manager E o utilizando WBM, tal como se indica en el capítulo: Cómo configurar por primera vez teléfonos DECT en la página 994.

1) Active la ventana de registro desde un teléfono físico conectado al sistema introduciendo *942.
2) En la pantalla del teléfono, verá: **Código**.
3) Introduzca 19970707 y verá en la pantalla del teléfono: **N.º tel.**: introduzca 125.
4) Si es necesario, encienda el teléfono móvil pulsando la tecla de colgar durante más de un segundo. A continuación se emite el tono de confirmación.
5) Realice las siguientes entradas antes de que transcurran diez minutos. Pulse la tecla de menú.
6) Vaya a la **Configuración** del menú del teléfono y confirme.
7) Vaya a **Registro** y confirme la primera opción: **Registrar teléfono** (no seleccione la segunda opción: Seleccionar base)

8) Seleccione una extensión (en este ejemplo, **Base 2**) y confirme. En el centro de la pantalla, verá **Registro** y **Por favor, introduzca el PIN del sistema**.
9) Introduzca el PIN de ocho dígitos (código de móvil; en este caso **11112345**) y confirme la entrada. Si el registro se realiza con éxito, espere una "llamada silenciosa"; es decir, una llamada automática corta (en algunos dispositivos, esto equivale a 2 timbres). Si está registrando un número de llamada inactivo (que no se haya utilizado antes; negro en WBM y gris en KDS) entonces el registro se completa con una llamada silenciosa. Si está registrando un número de llamada activo que se haya utilizado anteriormente (verde en WBM y KDS), el registro se completa con dos llamadas silenciosas. No realice ninguna otra acción (por ejemplo, iniciar llamadas telefónicas DECT) hasta que el proceso haya finalizado. A continuación, en la parte izquierda de la pantalla, verá Base 2 (en este caso). Después verá el número de extensión (125) en su pantalla de inicio.
10) Puede cambiar el nombre Base 2 si es necesario. Para ello, vaya a Configuración y confirme, vaya a Registro y confirme, y luego elija la segunda opción Seleccionar base. Seleccione el nombre de la base que desea cambiar pulsando **Nombre**, y luego indique el nuevo nombre de la base (por ejemplo, 125).

19.3.3.5 Cómo añadir otros teléfonos DECT

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto** o Hipath 3000 Manager. Los pasos siguientes hacen referencia solo a WBM, pero se pueden realizar acciones similares utilizando Hipath 3000 Manager.

Hay conectada una extensión base OpenScape Business con el sistema de comunicación.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Cordless**.
3) En el grupo de menús, haga clic en **Cordless** > **SLC**.
4) En el grupo de menús, haga clic en el módulo deseado.
5) Haga clic en la pestaña **Añadir teléfonos DECT**.
6) En **Número de teléfonos** indique el número de los teléfonos DECT que desea añadir. Los teléfonos DECT añadidos se muestran en la pestaña **Editar teléfonos DECT**.
7) Haga clic en **Aplicar**, seguido de **Aceptar**.

19.3.3.6 Cómo borrar teléfonos DECT

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto** o Hipath 3000 Manager. Los pasos siguientes hacen referencia solo a WBM, pero se pueden realizar acciones similares utilizando Hipath 3000 Manager.

Hay conectada una extensión base OpenScape Business con el sistema de comunicación.

Hay configurados teléfonos DECT.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Cordless**.
3) En el grupo de menús, haga clic en **Cordless** > **SLC**. Se muestran todos los teléfonos DECT que haya configurados.
4) En la columna **Eliminar**, seleccione los teléfono DECT que desea borrar.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

19.3.3.7 Cómo configurar el parámetro Multi-SLC

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto** o Hipath 3000 Manager. Los pasos siguientes hacen referencia solo a WBM, pero se pueden realizar acciones similares utilizando Hipath 3000 Manager.

En el OpenScape Business X8 hay insertados varios módulos SLMUC.

Hay conectada una extensión base OpenScape Business con el sistema de comunicación.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Cordless**.
3) En el grupo de menús, haga clic en **Cordless** > **Multi-SLC**.
4) Editar parámetros del módulo SLMUC:
   a) Si es necesario, edite el ID exclusivo preconfigurado en todo el sistema del módulo SLMUC en **Nº SLC**

      Rango de valores: 1-15,17-31,33-47,...,127. No se pueden utilizar múltiplos de 16.
   b) Si es necesario, edite el número de teléfono exclusivo preconfigurado en todo el sistema de la línea de interconexión SLC del módulo SLMUC en **Número SLC**.

      Nota: Por cada línea de interconexión SLC se configura una extensión S0 interna. El número de teléfono SLC se corresponde con el número de teléfono de la extensión S0 interna.
   c) Compruebe que en la extensión S0 interna esté desactivado el flag de extensión **Bloqueo de aviso de llamada en espera act**.
5) Si es necesario, repita el paso 4 para los demás módulos SLMUC.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

19.3.3.8 Cómo consultar los datos de las extensiones base

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto** o Hipath 3000 Manager. Los pasos siguientes hacen referencia solo a WBM, pero se pueden realizar acciones similares utilizando Hipath 3000 Manager.

Hay conectada una extensión base OpenScape Business con el sistema de comunicación.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Cordless**.
3) En el grupo de menús, haga clic en **Cordless**.
4) En el grupo de menús, haga clic en la extensión base deseada. Se muestran los datos sobre la extensión base. Puede consultar una explicación de los datos en Cordless>Extensiones base.
5) Puede seleccionar hasta 10 canales de frecuencia diferentes al mismo tiempo para una extensión base. Puede consultar una explicación de los canales de frecuencia en la tabla en Cordless>Extensiones base.
6) Haga clic en **Aplicar**, seguido de **Aceptar**.

19.3.3.9 Cómo activar el tono de aviso de MWI (Message Waiting Indication) para los teléfonos DECT

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto** o Hipath 3000 Manager. Los pasos siguientes hacen referencia solo a WBM, pero se pueden realizar acciones similares utilizando Hipath 3000 Manager.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **Flags del sistema**.
4) En el área **Flags del sistema** active la casilla de verificación **Timbre CMI MWI**.
5) Haga clic en **Aplicar**, seguido de **Aceptar**.

19.3.3.10 Cómo consultar el estado de registro de los teléfonos DECT

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto** o Hipath 3000 Manager. Los pasos siguientes hacen referencia solo a WBM, pero se pueden realizar acciones similares utilizando Hipath 3000 Manager.

Hay conectada una extensión base OpenScape Business con el sistema de comunicación.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Cordless**.
3) En el grupo de menús, haga clic en **Cordless** > **SLC**. Se muestran todos los teléfonos DECT que haya configurados.
4) En la columna **Activo** aparece el estado de registro de cada teléfono DECT:
   - Verde: el teléfono móvil está activo.
   - Rojo: interruptor de bloqueo de módulos con teléfono móvil registrado establecido.
   - Amarillo: el teléfono móvil se ha desconectado (cerrado sesión) de nuevo automáticamente porque se ha modificado el PIN.
   - Gris: en este puerto todavía no se ha dado de alta un teléfono móvil.
5) Haga clic en **Aplicar**, seguido de **Aceptar**.

19.3.4 Cordless IP

Cordless IP (DECT IP) es una solución Cordless opcional, como alternativa a la solución Cordless integrada o al uso con OpenScape Business S.

Los teléfonos Cordless de Cordless IP se comunicación con el sistema de comunicación mediante la extensión base BSIP, como teléfonos SIP. Por ello, con Cordless IP solo se pueden utilizar prestaciones SIP. Más información sobre Cordless IP en la documentación de HiPath Cordless IP.

Para todas las extensiones SIP registradas en un Cordless IP, el parámetro de extensión **Acept. llamada autom., CSTA** debe estar desactivado. Si no es así, es posible que no se lleven a cabo llamadas entre extensiones SIP mediante DECT IP.

19.3.5 Teléfonos WLAN y puntos de acceso

Los teléfonos WLAN y los teléfonos Dual-Mode permiten la comunicación móvil. Estos teléfonos pueden integrarse en infraestructuras WLAN ya existentes. Los puntos de acceso WLAN permiten establecer redes inalámbricas y utilizar servicios de datos y voz a través de la misma infraestructura. Se recomienda utilizar únicamente puntos de acceso WLAN de alto rendimiento (por ejemplo, de Enterasys).

19.3.5.1 Requisitos de la WLAN

Si se utiliza WLAN hay que comprobar si se cumplen los requisitos básicos para el uso de Voice-over-WLAN. Para implementar la parte inalámbrica de la red se debe realizar un estudio previo in situ de la cobertura de la señal inalámbrica (Site Survey).

Ayuda para la toma de decisiones:

- Las instalaciones pequeñas con hasta 3 AP, se pueden evaluar eficazmente con una visita in situ o con la evaluación de un plano del edificio. Por norma general, estas instalaciones no necesitan ningún estudio de cobertura in situ.
- En instalaciones con más de 4 puntos de acceso hay que realizar siempre un estudio de cobertura. Esto se aplica especialmente a las instalaciones que se extienden a varios edificios o a varias plantas dentro de un edificio.
- También se necesita un estudio de cobertura, sea cual sea el número de puntos de acceso, en los entornos con una alta presencia de radiofrecuencias, o cuando la solución debe coexistir con otros sistemas WLAN ya existentes.

19.4 Movilidad en el hogar

La movilidad en el hogar se logra mediante el teletrabajo. Esto se consigue integrando teléfonos no locales (como un teléfono fijo o un teléfono móvil) en la red de comunicación de OpenScape Business.

Están disponibles los siguientes tipos de puestos de teletrabajo:

- Estaciones VPN

  OpenScape Business tiene una funcionalidad VPN integrada. Un total de 10 teletrabajadores pueden estar activos simultáneamente a través de VPN. Esto puede implicar un ordenador personal o un teléfono móvil con sistema operativo Android o iOS. La conexión VPN se establece entre el cliente VPN nativo del PC o del teléfono móvil y el servidor OpenVPN de OpenScape Business.

  Los usuarios de UC Suite pueden especificar su número de teléfono particular desde casa a través de su cliente UC y luego usar su teléfono privado como teléfono de oficina (CallMe).
- Dispositivo en casa: Estaciones SIP@Home o estaciones System Device@Home

  Los teléfonos SIP compatibles con STUN (por ejemplo, Yealink T19) (estaciones SIP Device@Home) o los teléfonos HFA (estaciones System Device@Home) pueden registrarse en el sistema de comunicación a través de Internet utilizando la función SBC interna de OpenScape Business. Para ello, la función debe habilitarse en los datos de la estación para cada teléfono SIP o HFA a través del WBM.

  Un servidor STUN debe especificarse adicionalmente en el WBM solo si no se utiliza ningún ITSP o si el ITSP utilizado no ofrece ningún servidor STUN.

  SIP Device@Home no admite la transmisión de señales de vídeo.

  Nota: Cuando se utilizan varios dispositivos SIP/HFA @Home detrás del mismo enrutador, las limitaciones de NAT pueden causar problemas con la carga útil de las llamadas debido a conflictos por reutilización de puertos; para evitar esto, configure cada dispositivo con un puerto de origen (RTP) único.

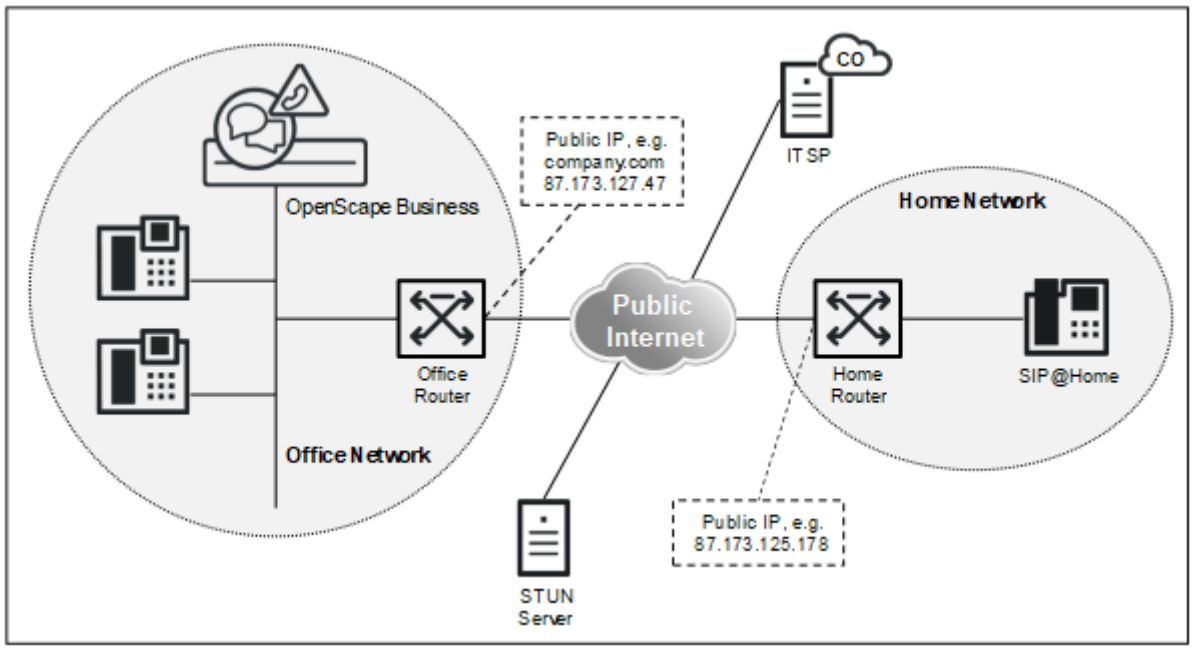


Figura 9: Componentes de Device@Home (SIP Device@Home o System Device@Home)

19.4.1 Configuración de VPN

Para conectar extensiones con el sistema de comunicación a través de la funcionalidad VPN integrada, hay que realizar ajustes de configuración en OpenScape Business y en las extensiones VPN.

Configuración de OpenScape Business

Para obtener información sobre la configuración VPN del sistema de comunicación, véase Cómo configurar conexión de teletrabajadores a través de VPN .

Configuración de extensiones VPN (cliente VPN)

Para obtener información sobre la configuración de los clientes VPN, véase Clientes VPN .

19.4.2 Configuración de Equipo SIP@Home

Para establecer conexiones a través de Internet entre un teléfono SIP compatible con STUN y OpenScape Business, hay que realizar ajustes de configuración.

Configuración de OpenScape Business

Para que las extensiones SIP se puedan registrar en el sistema de comunicación a través de Internet, hay que activar en ellas la función SBC integrada (véase Cómo activar Equipo@Home).

Mediante el protocolo STUN, la función SBC integrada detecta la dirección IP pública del sistema de comunicación y el puerto utilizado. Si el sistema

de comunicación está conectado con un proveedor de servicios de telefonía por Internet (ITSP) que ofrezca un servidor STUN, no hay que realizar más ajustes de configuración en el sistema de comunicación. Sin embargo, si no se utiliza ningún ITSP o el ITSP utilizado no se vale de un servidor STUN, hay que configurar un servidor STUN en el sistema (véase Cómo indicar un servidor STUN para Equipo@Home).

Configuración del router de Internet de la oficina

Para que el teléfono SIP pueda acceder al sistema de comunicación a través de Internet, en el router Internet de oficina hay que configurar un desvío de puertos para el puerto SIP externo. Para evitar ataques SIP procedentes de Internet, hay que utilizar como puerto SIP externo un puerto SIP que no sea el estándar.

En el teléfono SIP hay que configurar el protocolo de transporte.

Tabla 9: Configuración de desvío de puertos en el router de la oficina.

Protocolo de transporte	Puerto SIP interno	Puerto SIP externo	Comentario
UDP	5070	Entrada de, p.ej., 5090	Para el desvío de puertos, el puerto SIP interno y el externo no deben ser idénticos. Como puerto SIP externo se puede introducir un valor diferente del puerto SIP estándar interno 5070. Por ello se recomienda utilizar UDP.
TCP	5070 Cambio a, p.ej., 5080	Entrada de, p.ej., 5080 (= puerto SIP interno)	Para el desvío de puertos, el puerto SIP interno y el externo deben ser idénticos. Para utilizar un puerto SIP externo diferente del puerto SIP estándar 5070, hay que modificar el puerto SIP interno. Para ello hay que modificar la configuración de todos los componentes IP que utilizan SIP. Por ello **no** se recomienda utilizar TCP.
TLS	5071	Entrada de 5071 (= puerto TLS SIP interno)	Para el desvío de puertos, el puerto TLS SIP interno y el externo no deben ser idénticos. Dado que el puerto TLS SIP interno es diferente del puerto TLS SIP estándar, también se puede introducir 5071 como puerto TLS SIP externo. Por ello se recomienda utilizar TLS.

Nota: En un sistema actualizado, no se realiza automáticamente ningún cambio respecto a los puertos SIP. Después de la actualización, los puertos son:

SIP_EXT = 5060

SIP_TLS_SUB_EXT = 5062

El administrador debe modificar estos valores manualmente si se utiliza el Equipo@Home en un sistema migrado.

Para TLS, en el sistema de comunicación deben activarse certificados válidos. En la interfaz LAN del sistema de comunicación se admiten conexiones TLS para extensiones SIP, pero no así en la interfaz WAN. No se admite la carga útil SRTP con señalización SDES.

Si el router Internet de oficina se conecta con Internet sin dirección IP fija, en el router Internet de oficina debe configurarse DynDNS para que la extensión SIP pueda acceder al sistema de comunicación a través de Internet. Mediante la cuenta DynDNS, la dirección IP actual se registra a intervalos regulares. En las cuentas DynDNS gratuitas que vencen a intervalos regulares esto puede ser causar problemas.

Configuración del teléfono SIP

Como ejemplo para la configuración, puede encontrar algunos teléfonos SIP probados compatibles con STUN en la wiki de expertos de Unify, disponible en Internet. Encontrará los valores que hay que introducir en el teléfono SIP.

Configuración del router de Internet doméstico

En el router de Internet doméstico no se requiere ninguna configuración especial.

El router de Internet doméstico debe cumplir los requisitos siguientes:

- El router debe proporcionar funcionalidad VoIP con NAT activado (no NAT simétrico).
- La función ALG debe estar desactivada en el router.

La conexión con Internet debe tener ancho de banda suficiente para la transmisión de voz. Especialmente en las conexiones ADSL asimétricas hay que prestar atención al ancho de banda de carga.

Configuración de myPortal @work

Para que myPortal @work pueda acceder al sistema de comunicación a través de Internet, debe realizar lo siguiente:

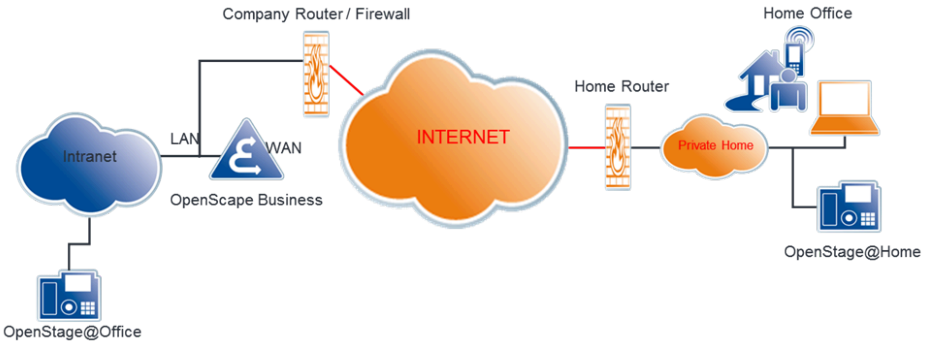
- Configure el servidor STUN según el sistema/cliente.
- Abra y desvíe al puerto 8802 (otros desvíos no son válidos).
- El flag SBC no es necesario. No es necesaria ninguna autenticación.

19.4.3 Configuración de Dispositivo de sistema@Casa

Para establecer conexiones a través de Internet entre un teléfono Dispositivo del Sistema y OpenScape Business, hay que realizar ajustes de configuración

en OpenScape Business, en el router de Internet de la oficina y en el teléfono Dispositivo del Sistema.

- **Figura 10: Ejemplo de caso práctico de Dispositivo de sistema@Casa**



Configuración de OpenScape Business

Para que las extensiones System Device@Home se puedan registrar en el sistema de comunicación a través de Internet, hay que activar en ellas la función SBC integrada (véase Cómo activar Equipo@Home en la página 1006).

Mediante el protocolo STUN, la función SBC integrada detecta la dirección IP pública del sistema de comunicación y el puerto utilizado. Si el sistema de comunicación está conectado con un proveedor de servicios de telefonía por Internet (ITSP) que ofrezca un servidor STUN, no hay que realizar más ajustes de configuración en el sistema de comunicación. Sin embargo, si no se utiliza ningún ITSP o el ITSP utilizado no ofrece ningún servidor STUN, hay que registrar un servidor STUN en el sistema de comunicación (véase Cómo indicar un servidor STUN para Dispositivo de sistema@Casa).

Configuración del router de Internet de la oficina

Para que las extensiones Dispositivo de sistema@Casa puedan acceder al sistema de comunicación a través de Internet, en el router de Internet de la oficina hay que configurar un desvío de puertos para el puerto Dispositivo del Sistema. Para poder registrarse desde Internet, hay que configurar el firewall/ router de la oficina con una regla de desvío de puertos:

- Puerto externo TCP/4060 a puerto interno TCP/4062(HFA), para no TLS

  Puerto externo TCP/4061 a puerto interno TCP/4063(HFA), para TLS

  Nota: Durante la migración de V2R1 a una versión superior, también se debe cambiar la configuración del router de Internet de la oficina según esta regla.

  Los puertos mencionados arriba solo se necesitan para dispositivos del sistema (Teléfono HFA).

- Rango de puertos RTP en el rango de puertos X:30274-30529RTP de OpenScape Business en OpenScape Business S: 30528-30887 (valores estándar)

  Los clientes de UC con VoIP activado como myPortal to go, myPortal @work también necesitan estos puertos.

- TCP/8802 (HTTPS) (requerido para clientes de comunicaciones unificadas o UC, como my Portal to go, myPortal to go Web, my Portal @work o VoIP for myPortal, configurado como sistema Device@Home)

Nota: La zona de firewall interna debe estar cerrada.

El protocolo de transporte se define en la extensión del Dispositivo de sistema@Casa.

Si el router de Internet de la oficina se conecta con Internet sin dirección IP fija, en el router de Internet de la oficina debe configurarse DynDNS para que las extensiones Dispositivo de sistema@Casa puedan acceder al sistema de comunicación a través de Internet. Mediante la cuenta DynDNS, la dirección IP actual se registra a intervalos regulares. En las cuentas DynDNS gratuitas que vencen a intervalos regulares esto puede ser causar problemas.

Configuración del router de Internet doméstico

En el router de Internet doméstico no se requiere ninguna configuración especial.

El router de Internet doméstico debe cumplir los requisitos siguientes:

- El router debe proporcionar funcionalidad VoIP con NAT activado (no NAT simétrico).
- La función ALG debe estar desactivada en el router.

La conexión con Internet debe tener ancho de banda suficiente para la transmisión de voz. Especialmente en las conexiones ADSL asimétricas hay que prestar atención al ancho de banda de carga.

Configuración del teléfono HFA

El gateway se debe configurar con el nombre DNS (por ejemplo, mycompany.net), para que el teléfono pueda acceder al sistema a través de Internet. La IP de DLI también se debe configurar. Se debe añadir un número de teléfono interno para el suscriptor. También hay que definir la contraseña del dispositivo.

Restricciones

- No es posible configurar aplicaciones XML en OpenStage

19.4.4 Cómo activar Equipo@Home

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el árbol de navegación, haga clic en **Extensiones** > **Clientes IP** > **Clientes SIP** o **Clientes sist.**
4) En el grupo de menús, haga clic en la extensión SIP o HFA deseada.

5) Haga clic en la pestaña **Editar datos cliente workpoint**.
6) No olvide indicar una contraseña. Los valores indicados aquí también se deben registrar en el teléfono SIP o en el dispositivo del sistema.

Nota:

En una conexión por Internet, hay que utilizar una contraseña segura (mín. 8 caracteres, con mayúsculas, números y caracteres especiales).

Nota: La contraseña de los clientes de Deskshare que sean declarados como @Home solamente debe contener caracteres numéricos. Esta contraseña en realidad es el código PIN para la activación de la función de movilidad (código de servicio de la función: *9419). Los dispositivos solamente admiten caracteres numéricos para el PIN.

Cuando haya definido la contraseña, el ajuste **Registro de Internet con un SBC interno** estará disponible para que lo habilite.

Nota: Después de un Speed Upgrade o de reiniciar el sistema, la casilla de verificación Autenticación activa se activará en todos los puntos de terminal SIP y estará en gris, para que el usuario no pueda desactivarla, si hay al menos una extensión SIP con el flag **Registro de Internet con un SBC interno** activado.

19.4.5 Cómo actualizar software para dispositivos de sistema (HFA) @Casa

El procedimiento normal de actualización de software de del DLI para un dispositivo conectado internamente no es válido para dispositivos de sistema (HFA) @Casa, ya que este requiere acceso directo a la dirección IP del dispositivo para la transferencia de archivos. El DLI no puede determinar la dirección IP de dispositivos de sistema (HFA) @Casa debido a los motivos siguientes:

- El dispositivo @Casa reside en una red doméstica que utiliza direcciones IP privadas. El acceso a Internet se efectúa mediante un router doméstico con traducción de direcciones de red o NAT .
- El DLI en OpenScape Business se encuentra en una red de la empresa o la oficina que utiliza redes IP privadas. La red de la compañía está conectada a Internet mediante el router de la empresa o la oficina.

Así pues, el procedimiento de actualización de software del DLI utiliza una conexión HTTPS adicional a través del puerto 8804 (configuración estándar) junto con el puerto DLI 18443 (configuración estándar), para determinar la versión de software del dispositivo @Casa y efectuar la actualización de software.

La comprobación de la versión de software del dispositivo @Casa se efectúa únicamente si se cumple una de las condiciones siguientes:

- Reinicio del dispositivo
- Cambio de la configuración efectuado de manera local o remota
- Cambios de inventario del dispositivo
- Inicio de sesión o cierre de sesión de un usuario móvil en un dispositivo

En estos casos, el DLI comprueba la versión de software del dispositivo y efectúa una actualización de software si en OpenScape Business está disponible una versión más reciente.

La actualización automática de software de un dispositivo @Casa por parte del DLI debe configurarse en OpenScape Business. De forma predeterminada está desactivada. Debe activarse expresamente.

Deben realizarse los pasos siguientes.

Paso a paso

1) Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil Experto.

2) En la barra de navegación, haga clic en **Modo Experto**.

3) En el árbol de navegación, haga clic en **Servidor de telefonía > Ajustes básicos**.

4) En el árbol de navegación, haga clic en **Configuración básica > Despliegue de parámetros de teléfono**.

- Al hacer clic en **Distribuir SW en dispositivos @Casa**, se otorgan permisos para la actualización de software a través de DLI para dispositivos de sistema (HFA) @Casa. De modo predeterminado, la opción no está seleccionada.
- Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

5) Configuración del firewall

En OpenScape Business, no se requiere la configuración manual del firewall. El puerto 8804 se abre durante el inicio del sistema. Las solicitudes que llegan al sistema las responde el sistema solo si está activado el flag **Distribuir SW en dispositivos @Casa**.

6) Abra los puertos DLI 18443 y 8804 utilizados con la configuración adecuada (enrutamiento de puerto) en el enrutador de la empresa o la oficina.

Limitaciones

El dispositivo HFA@Casa reside detrás de un firewall (enrutador doméstico). El enrutador o firewall induce una traducción de direcciones de red (NAT) y esto hace que la dirección IP sea invisible desde el mundo exterior. Como resultado, los teléfonos IP no pueden verse remotamente para ser administrados por DLI.

El efecto secundario de la restricción de red anterior es que no se pueden realizar eventos DLI, ya que estos se envían a la dirección IP local (no accesible) del dispositivo.

El impacto es que no será posible ninguna actualización de software bajo demanda. Por otra parte, la actualización del software será posible cuando el dispositivo inicie un intercambio de mensajes abriendo una sesión HTTPS a DLI. Las sesiones se abren al producirse eventos específicos basados en dispositivos, tales como:

- el reinicio del dispositivo.
- un cambio de configuración en el dispositivo (a través de la pantalla local o de administración basada en Web).

- cambios de inventario del dispositivo.
- inicio de sesión o cierre de sesión de un usuario móvil en un dispositivo.

En todos estos casos, DLI verificará el software del dispositivo y, si es necesario, el dispositivo se actualizará con el software oficial compatible con OSBiz.

Nota: La implementación del software se lleva a cabo al iniciarse el teléfono (cuando se registra en OSBiz o cuando el sistema OSBiz entra en servicio).

19.4.6 Cómo indicar un servidor STUN para Equipo@Home

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

No se utiliza ningún ITSP o el ITSP utilizado no ofrece ningún servidor STUN.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **Gateway de voz**.

3) En el grupo de menús, haga clic en **Proveedor de servicios de telefonía por Internet**.

4) Haga clic en la pestaña **Editar configuración STUN**.

5) En el área **Servidor STUN predeterminado**, en **Dirección IP / Nombre de host**, introduzca la dirección IP o el nombre de host del servidor STUN (p.ej., `stun.serviceprovider.com`).

6) En el área **Servidor STUN predeterminado**, en **Puerto**, introduzca el puerto del servidor STUN (p.ej. `3478`).

7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

20 Seguridad

Security incluye la protección del sistema de comunicación y de los datos guardados y transferidos mediante el acceso no autorizado. Esta protección se puede realizar, entre otras formas, a través de la protección de acceso de la red IP (firewall) y con formas de transmisión cifradas (SSL, VPN).

Security Checklist

En los ajustes previos, el sistema de comunicación contempla la seguridad de la comunicación. Al realizar la puesta en servicio hay que adaptar las funciones a la situación específica del cliente; también hay que tomar medidas de seguridad adicionales en el entorno del cliente. Para concienciar sobre los riesgos de seguridad e implementar las medidas adecuadas, la documentación del producto incluye una lista de comprobación sobre seguridad. Se recomienda encarecidamente hablar de ello con el cliente al realizar la puesta en servicio y documentar las medidas tomadas.

20.1 Firewall

Un firewall es un sistema de componentes de software y hardware que restringe el acceso entre distintas redes para aplicar un concepto de seguridad.

Los firewalls están instalados en las interfaces entre las distintas redes y controlan el tráfico de datos entre los distintos segmentos para impedir el intercambio no deseado y para permitir únicamente el tráfico deseado. La aplicación más habitual de un firewall es controlar el tráfico entre una red local (LAN) e Internet.

En cada red empresarial, un firewall aisla la LAN interna de Internet.

El sistema de comunicación ofrece funciones de seguridad integradas; las funciones de OpenScape Business X y OpenScape Business S son diferentes.

OpenScape Business V1 ofrece las siguientes prestaciones:

- Firewall de puertos / NAT (firewall entre el puerto WAN y la LAN)
- Firewall de aplicación (firewall para acceder al sistema de comunicación)

OpenScape Business S usa el firewall de Linux.

20.1.1 Porthandling

Porthandling permite liberar los puertos (Port Mapping, desvío de puertos) en el firewall del router integrado de OpenScape Business X.

Números de puerto

Nota: ¡Abra solamente los puertos si es absolutamente necesario para una aplicación determinada!

Los puertos (servicios) son necesarios para la comunicación a través de los protocolos TCP y UDP, ya que permiten a varias aplicaciones intercambiar datos simultáneamente a través de una única conexión.

Con el término “firewall” se hace referencia, por norma general, a un firewall de puertos (también denominado cortafuegos o bloqueo de servicios/puertos). El firewall de puertos solo actúa en la conexión WAN de OpenScape Business.

Con OpenScape Business S, se puede activar un firewall de puertos en la conexión LAN con Linux. Con OpenScape Business X, el firewall está activo en la conexión WAN para proteger la red interna (en la conexión LAN) de accesos malintencionados procedentes de Internet. No obstante, si se debe poder acceder a determinados puertos/servicios desde Internet, deberá liberarlos (véase Liberación de puerto). Todos los puertos/servicios para las funciones de OpenScape Business X se liberan en la conexión LAN (hacia la red de clientes interna) de forma automática.

OpenScape Business S solo posee una conexión LAN (a la red de clientes interna) y está protegido hacia a Internet con otros componentes/routers de la red de clientes. Además, el firewall Linux interno del servidor está activado. Para las funciones de OpenScape Business es necesario liberar todos los puertos/servicios (por ejemplo, para que los teléfonos puedan comunicarse con OpenScape Business S). Esto se realiza de forma automática. No obstante, el administrador puede bloquear determinados servicios.

Los números de puerto pueden adoptar valores entre 0 y 65535, que serán asignados a las distintas aplicaciones. Entre el 0 y el 1023 están los denominados "Well Known Ports" (o "Puertos bien conocidos") que son asignados de forma permanente por el IANA (Internet Assigned Numbers Authority) y que son conocidos de forma general. Encontrará una lista de estos puertos en la dirección http://www.iana.org/assignments/port-numbers.

20.1.1.1 Liberación de puerto

Si el sistema establece acceso a Internet (a través del puerto WAN), de forma predeterminada solo se permiten la comunicación que va desde el interior (desde la red empresarial o desde el propio sistema de comunicación) hacia Internet, y los paquetes de respuesta correspondientes. Las solicitudes procedentes de Internet se bloquean. Esta configuración de seguridad puede pasarse por alto liberando el puerto de forma selectiva para, por ejemplo, operar un servidor Web en la red.

Nota: Si desea utilizar el sistema de comunicación como router Internet, debe cerrar el puerto 5060 (ajuste estándar). Con telefonía Internet mediante ITSP, el sistema de comunicación abre los puertos correspondientes y los mantiene abiertos.

Si desea utilizar un router externo o firewall, el puerto 5060 debe estar cerrado. Corresponde al sistema de comunicación abrir este puerto (si es necesario).

20.1.1.2 Cómo configurar Liberación de puerto

El asistente **Firewall** permite activar la liberación de puertos para que se pueda acceder al sistema de comunicación o PC de la LAN mediante el puerto WAN. La liberación de puertos supone un riesgo de acceso por personas no autorizadas. Por ello solo hay que liberar los puertos que sea estrictamente necesario.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Seguridad**.
3) Haga clic en **Editar** para iniciar el asistente **Firewall**. Aparece la ventana **Liberación de puerto**.
4) En la línea de la aplicación o del servicio deseados, active la casilla de verificación **Regla NAT activa**, para la que quiere liberar puertos.
5) En los campos **Puerto global**, **Dirección IP local** y **Puerto local** indique los datos de la liberación.
6) Para la liberación de puerto de un servicio no registrado, haga clic en **Añadir** y rellene los campos **Descripción**, **Regla NAT activa**, **Puerto global**, **Dirección IP local** y **Puerto local**.
7) Haga clic en **OK & Continuar**.
8) Haga clic en **Salir**.

20.1.1.3 Administración de puertos

La administración de puertos permite modificar algunos de los puertos que utiliza el propio sistema de comunicación. Esto permite, por ejemplo, personalizar la comunicación de red para cada red de clientes, aunque los puertos ya se estén utilizando en otro lugar.

Si se han hecho cambios en la administración de puertos, por norma general, estas modificaciones deben hacerse en todos los componentes (teléfonos, sistemas, etc.), para garantizar las funciones.

20.1.1.4 Cómo editar ajustes globales del Administrador de puertos

Aquí puede introducir los números de puerto de las distintas funciones.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Administración de puertos**. Se abrirá la pestaña **Editar ajustes globales del Administrador de puertos**.
4) En **Número puerto**, indique el puerto para la función correspondiente, o bien, mantenga la configuración predeterminada.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

20.1.2 NAT

NAT (Network Address Translation) es un procedimiento de traducción de direcciones para sustituir una dirección IP de un paquete de datos por otra. En una red interna, los clientes utilizar direcciones IP privadas. Como las direcciones IP privadas de una red pública no se transfieren, NAT permite mapear las direcciones IP privadas en una dirección IP pública. De esta forma, los clientes internos tienen acceso a la red pública. Al mismo tiempo la estructura de la red interna con las direcciones IP privadas se "enmascara", no es visible en la red pública (por ejemplo, Internet). Para la liberación de puerto no se requiere NAT ni reglas NAT.

La traducción de direcciones se realiza en el paso entre una red interna y una pública. NAT puede ejecutarse en un router Internet, en un servidor o en otro dispositivo especializado. De esta forma, por ejemplo, un router Internet puede conectar la red interna con Internet con ayuda de NAT.

La red interna solo aparece en Internet con una única dirección IP pública asignada por el ISP al router Internet. Todos los accesos realizados a Internet desde la red interna se encaminan a través de esa dirección IP oficial con distintos números de puerto. El router Internet sustituye las direcciones IP privadas con la dirección IP oficial asignada por el ISP. En los paquetes de datos entrantes, la dirección IP oficial vuelve a ser sustituida con las direcciones IP privadas. Para esta asignación son decisivos los números de puerto. Solo se puede acceder directamente desde Internet a aquellas direcciones IP privadas liberadas de forma expresa.

Reglas NAT

Las reglas NAT permiten establecer si se puede acceder directamente desde Internet a direcciones IP privadas (locales). Para hacerlo, se pueden definir reglas NAT propias o utilizar las reglas NAT estándar predefinidas para los servicios de servidor FTP, servidor HTTP, etc. En total se pueden definir 20 reglas NAT. Para utilizar una regla NAT, deben indicarse los datos de dirección locales de los PC clientes que dispondrán de esos servicios para Internet. También se debe activar la regla NAT. Con ayuda de un editor de tablas se pueden configurar varias reglas NAT. Se pueden borrar las reglas NAT que han dejado de ser necesarias.

Puertos

En el inicio, los servidores suelen necesitar que el sistema operativo proporcione puertos específicos para poder aceptar conexiones. Un servidor HTTP con el puerto 80, un servidor FTP con el puerto 21, etc. Normalmente, los clientes necesitan que el sistema operativo proporcione un puerto aleatorio para poder establecer conexiones.

20.1.2.1 Cómo configurar regla NAT

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **Encaminamiento**.
3) Configure la regla NAT:
   - Si desea definir una nueva regla NAT, en el grupo de menús haga clic en **NAT** y a continuación en la pestaña **Añadir NAT**.
   - Si desea modificar una regla NAT existente, en el grupo de menús **NAT** desplácese hasta la regla NAT deseada.
4) En el campo **Descripción**, indique un nombre para la regla NAT. En el caso de las reglas NAT estándar no se puede modificar el nombre.
5) En el campo **Dirección IP local**, indique la dirección IP en la red interna del cliente que desea liberar.
6) En el campo **Puerto local**, indique el número de puerto que utiliza la aplicación del cliente interno.
7) En el campo **Puerto global**, indique el número de puerto que utiliza la aplicación del interlocutor externo.
8) En la lista desplegable **Protocolo** seleccione el protocolo de transporte utilizado por la aplicación (**TCP** o **UDP**). Si se trata de una regla NAT estándar el protocolo no se puede modificar.
9) Si desea utilizar la regla NAT, active el campo de opción **Regla NAT activa**.
10) Haga clic en **Aplicar** y, a continuación, en **Aceptar**. Las reglas NAT activadas se identifican con un símbolo de color verde en la opción de menú **NAT**.

20.1.2.2 Cómo configurar varias reglas NAT con el editor de tablas NAT

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En la barra de navegación, haga clic en **Telefonía** > **Encaminamiento**.
3) En el grupo de menús, haga clic en **Encaminamiento**.
4) En el grupo de menús, haga clic en **NAT** y a continuación en la pestaña **Editor tablas NAT**.
5) Configure la regla NAT:
   - Si desea definir una nueva regla NAT, rellene los campos de la primer línea tal y como se describe a continuación.
   - Si desea modificar una regla NAT existente, haga clic en los campos deseados de la regla NAT y rellénelos tal y como se describe a continuación.
6) En la columna **Dirección IP local** indique la dirección IP en la red interna del cliente que desea liberar.
7) En la columna **Puerto local**, indique el número de puerto que utiliza la aplicación del cliente interno.
8) En la columna **Puerto global**, indique el número de puerto que utiliza la aplicación del interlocutor externo.

9) En la lista desplegable **Protocolo** seleccione el protocolo de transporte utilizado por la aplicación (**TCP** o **UDP**). Si se trata de una regla NAT estándar el protocolo no se puede modificar.
10) Para aplicar la regla NAT, marque la columna **Activo** con un signo de verificación.
11) En la columna **Descripción**, introduzca un nombre para la regla NAT. En el caso de las reglas NAT estándar no se puede modificar el nombre.
12) Guarde la regla NAT:
    - Si ha configurado una nueva regla NAT, haga clic en **Agregar** y a continuación en **Aceptar**. La nueva regla NAT se añade al final de la tabla.
    - Si ha modificado una regla NAT existente, pase al punto 5.
13) Haga clic en **Aplicar**. Una regla NAT activada se identifica con un símbolo de color verde en la opción de menú **NAT**.

20.1.2.3 Cómo borrar regla NAT

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Telefonía** > **Encaminamiento**.
2) En el árbol de navegación, haga clic en **Encaminamiento**.
3) En el grupo de menús, haga clic en **NAT**.
4) En el grupo de menús, haga clic sobre la regla NAT que desea borrar, y haga clic en la pestaña **Borrar NAT**. Las reglas NAT estándar predefinidas no se pueden borrar.
5) Confirme la advertencia pulsando **Borrar** y, a continuación, haga clic en **Aceptar**. La regla NAT es borrada de la lista de reglas NAT de la opción de menú **NAT**.

20.1.3 Cortafuegos de aplicaciones

El cortafuegos de aplicaciones se utiliza para restringir el acceso a servicios específicos como FTP o LDAP. Por defecto está deshabilitado y se puede habilitar definiendo las reglas adecuadas.

El cortafuegos de aplicaciones de OpenScape Business X puede bloquear o restringir los siguientes servicios a direcciones IP o rangos de direcciones IP específicos:

Servicio	Puertos
FTP	21, 40000 - 40040
ssh (bloqueado por defecto)	22
LDAP	389
HTTPS	443
Postgres	5432

Servicio	Puertos
Manager E	7000
CSTA	7001 (FP), 7004 (FP), 8800 (CSP)
OBSERVER	Este servicio permitía el acceso desde una aplicación OpenScape Observer, que ya no es compatible.

Solo los servicios enumerados se pueden bloquear a través de un menú de selección en el modo Experto.

Las funciones telefónicas como SIP, HFA, etc., no se pueden bloquear mediante el cortafuegos de aplicaciones.

Un servicio puede ser seleccionado varias veces; cada vez, pueden especificarse diferentes restricciones de IP.

Nota: La activación/desactivación o modificación de los parámetros del cortafuegos puede restringir gravemente la funcionalidad de la placa (por ejemplo, puede no ser compatible con la administración basada en LAN).

Nota: El cortafuegos de aplicaciones, cuando está habilitado, no bloquea los servicios de forma predeterminada hasta que se añade una regla para ello, momento en el que solo las direcciones IP incluidas en la regla pueden acceder a ese servicio específico.

El cortafuegos de aplicaciones puede restringir el acceso a las funciones entre nodos cuando el sistema está conectado en red a otros sistemas OpenScape Business. Por ejemplo, la función de supervivencia requiere que el servicio POSTGRES funcione correctamente. Si se añade manualmente una regla para el servicio POSTGRES, añada las direcciones IP de los otros nodos de red de OpenScape Business a la regla POSTGRES para garantizar el funcionamiento correcto de la característica de supervivencia.

20.1.3.1 Cómo mostrar la configuración del Firewall de aplicación

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **Firewall de aplicación**.
4) Haga clic en la pestaña **Display Services** (Mostrar servicios) para mostrar los servicios bloqueados.
5) En el campo **Nombre de regla** aparece el nombre de la regla.

6) En **Regla activada**, una marca de verificación indica si una regla está activa o no.
7) En el campo **Lím. inferior de área dir. IP origen** puede ver el límite inferior de las direcciones IP bloqueadas.
8) En el campo **Lím. superior de área dir. IP origen** puede ver el límite superior de las direcciones IP bloqueadas.

20.1.3.2 Cómo restringir servicios mediante el firewall de aplicación

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **Firewall de aplicación**.
4) Haga clic en la pestaña **Agregar servicio** para bloquear un rango de direcciones IP o un servicio.
5) En **Nombre de regla** asigne un nombre para el servicio (esta regla).
6) En **Área direcciones**, establezca el **Lím. inferior** y el **Lím. superior** de las direcciones IP de origen permitidas.

   Para bloquear el acceso completamente, introduzca 127.0.0.1.

   Consejo: Solo debe activar una regla después de comprobar que ha configurado correctamente las direcciones IP autorizadas.
7) Haga clic en **Guardar**.

20.1.3.3 Cómo borrar la configuración del Firewall de aplicación

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **Firewall de aplicación**.
4) Haga clic en la pestaña **Delete all Services** (Borrar todos los servicios) para borrar todos los servicios.

20.1.4 Administración de servicios (OpenScape Business S)

El firewall interno de Linux está activado de forma predeterminada, de esta forma se bloquean el acceso a OpenScape Business S. El sistema de comunicación también ofrece servicios (como, por ejemplo, el servicio de

telefonía) en los que son necesarios puertos abiertos (servicios). Después de instalar OpenScape Business S, es necesario abrir estos puertos/servicios en el firewall. Si no desea utilizar servicios (como SNMP) puede bloquearlos en el firewall de Linux.

Nota: Tenga en cuenta que el bloqueo de servicios utilizados por OpenScape Business S puede influir negativamente en las funciones del sistema de comunicación, e incluso provocar su caída.

20.1.4.1 Cómo agregar o bloquear servicios

Paso a paso

1) En la barra de tareas, haga clic en **Computer** (Equipo).
2) En el grupo de menús, haga clic en **System** > **YaST** (Sistema > YaST).
3) Introduzca la contraseña del usuario "root" y haga clic en **Continue** (Continuar).
4) En el grupo de menús, haga clic en **Security and Users** (Seguridad y usuarios).
5) En el área **Security and Users** (Seguridad y usuarios), haga clic en **Firewall**.
6) En el grupo de menús de la ventana **Firewall Configuration: Start-UP** (Configuración de firewall: inicio), haga clic en **Allowed Services** (Servicios autorizados).
7) En el campo **Allowed Services for Selected Zone** (Servicios autorizados para la zona seleccionada), seleccione la zona para la que desea modificar los servicios (**External Zone** (Zona externa), **Demilitarized Zone** (Zona desmilitarizada) o **Internal Zone** (Zona interna)).
8) En el campo **Service to allow** (Servicio que se va a autorizar), seleccione los servicios que desea liberar (agregar) de forma selectiva y haga clic en **Add** (Agregar). En el menú desplegable aparecen todos los servicios autorizados en ese momento.
9) En el campo **Allowed Service** (Servicio autorizado), seleccione los servicios que desea bloquear y haga clic en **Delete** (Eliminar).
10) Si es necesario, active la casilla de verificación **Protect Firewall from Internal Zone** (Proteger firewall de zona interna).
11) Haga clic en **Advanced** (Avanzado) para agregar puertos o protocolos numéricos al firewall si es necesario (**TCP Ports** (Puertos TCP), **UDP Ports** (Puertos UDP), **RPC Ports** (Puertos RPC) y **IP Protocols** (Protocolos IP)). A continuación, haga clic en OK (Aceptar).
12) Haga clic en **Next** (Siguiente). Se muestran los ajustes de configuración realizados para el firewall. Si es necesario, con la opción **Show Details** (Mostrar detalles) puede consultar más información.
13) Haga clic en **Salir**.

20.2 Cifrado de datos de señalización y carga útil (SPE)

SPE ofrece seguridad en la transmisión de datos se señalización y de uso entre los teléfonos de sistema IP y el sistema de comunicación. La base de esta prestación es un procedimiento de cifrado asimétrico con el que se utilizan claves públicas y privadas.

Cifrado de los datos de señalización y uso:

- Cifrado de señalización: la transmisión de señal entre el gateway los clientes se cifra con una clave de 128 bits. Para la transferencia se utiliza el protocolo TLS con cifrado AES.
- Cifrado de carga útil: los datos de uso (también denominados "datos de voz" o "carga útil") se transmiten mediante el protocolo de transporte seguro en tiempo real (SRTP, Secure Real-time Transport Protocol). Se cifran con una clave de 128 bits (AES). SRTP también se utiliza para las redes IP. El procedimiento de intercambio de claves para SRTP se denomina Multimedia Internet Keying o "MIKEY" en su forma abreviada.

Para SPE hay que garantizar una identificación unívoca de los distintos teléfonos del sistema y de los sistemas de comunicación implicados. Esto se consigue mediante certificados, que también proporcionan las claves públicas.

Las claves o los certificados se distribuyen mediante el servidor DLS (aunque también se pueden distribuir manualmente).

Consejo: La función SPE no se ofrece a los usuarios de SIP y WL2.

Solo se establecen conexiones cifradas en conexión directa entre dos teléfonos del sistema o para conferencias.

Cifrado SRTCP

SRTCP (Secure Real-Time Transport Control Protocol o "Protocolo de control de transporte seguro en tiempo real") es una ampliación del protocolo SRTP e implementa la seguridad de los datos de control. La ampliación consta de tres campos adicionales: un índice SRTCP, un flag de cifrado y una etiqueta de autenticación.

Conformidad SPE

Family / Protocol / Interface		Signalling Encryption								Payload Encryption				
	Column1	HFA Subscriber	SIP Subscriber	TDM Subscriber	Analog Subscriber	SIP-Q Trunking	ISDN CO	FAX (T38, G711)	Column2	HFA Subscriber2	SIP Subscriber2	TDM Subscriber2	Analog Subscriber2	IP-Q Trunking (GW)
OpenScape Office MX/LX														
HFA		s	nv	t	t	s	t	t		y	n	y	y	y
SIP-UA		t*	t*	nv	nv	t*	nv	nv		n	n	n	n	n
SIP-Trunking/ITSP		t*	nv	nv	nv	t*	nv	nv		n	n	n	n	n
SIP-Q Homogenous		s	t*	t	t	s	t	t*		y	n	y	y	y
Media Server / Conference		t	nv	nv	nv	t	nv	nv		n	n	n	n	n
Openscape Business X3/X5/X8														
HFA		s	nv	t	t	s	t	t		y	n	y	y	y
SIP-UA		t*	t*	nv	nv	t*	nv	nv		n	n	n	n	n
SIP-Trunking/ITSP		t*	nv	nv	nv	t*	nv	nv		n	n	n	n	n
SIP-Q Homogenous		s	t*	t	t	s	t	t*		y	n	y	y	y
SIP-Q Heterogenous - H4k		s	t*	t	t	s	t	t*		y	n	y	y	y
SIP-Q Heterogenous - OSV		s	t*	t	t	s	t	t*		y	n	y	y	y
Media Server / Conference		t	nv	nv	nv	t	nv	nv		n	n	n	n	n
MEB / VSL		t	nv	nv	nv	t	nv	nv		n	n	n	n	n

Leyenda:

Cifrado de señalización	
nv	Sin seguridad VoIP
t	Estándar: TLS en el lado de VoIP; sin carga útil (payload) segura de extremo a extremo
s	Cifrado de datos de señalización y carga útil (SPE)
*	Sin End-to-end Signaling Encryption (TLS)
Cifrado de carga útil	
y	Secure Payload (SRTP)
n	Non-Secure Payload (RTP)

20.2.1 Cómo activar o desactivar el soporte SPE

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema** > **Flags del sistema**.
4) Elija una de estas opciones:
   - Si desea activar SPE (Signaling and Payload Encryption), active la casilla de verificación **Soporte SPE**.
   - Si desea desactivar SPE (Signaling and Payload Encryption), desactive la casilla de verificación **Soporte SPE**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

20.2.2 Cómo modificar los ajustes de seguridad SPE

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Seguridad** > **Signaling and Payload Encryption (SPE)**.
3) En la pestaña **Editar ajustes de seguridad** y en **Extensión mínima de las claves RSA** seleccione la longitud mínima de clave del protocolo de seguridad (512, 1024 o 2048).
4) Marque la entrada **Con la verificación CRL se necesita validación de certificados**, si desea hacer una comparación con las listas CRL (listas de revocación de certificados).
5) En **Intervalo máximo de remarcado [horas]** introduzca el tiempo (en horas) tras el cual se asignarán los nuevos pares de claves.
6) Haga clic en **Aplicar**.

20.2.3 Cómo importar el certificado SPE y la clave privada (PKCS#12)

Si no hay disponible ningún certificado específico del usuario, con SSL > Generación de certif. se puede generar un certificado de entidad emisora con firma automática para generar y guardar un certificado de servidor con firma de entidad emisora (PKCS#12). A continuación, se importa para SPE.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Seguridad** > **Signaling and Payload Encryption (SPE)**.
3) En el grupo de menús, desplácese hasta **Certificado SPE**.
4) En **Importar certificado SPE y clave privada (archivo PKCS#12)**, en el campo **Clave de descifrado**, introduzca la clave de descifrado creada al generar el archivo.
5) En **Archivo con certificado y clave privada (PEM o Formato PKCS#12)**, indique el archivo de certificado o selecciónelo con la opción **Examinar** de los directorios.

Consejo: Cuando instale por primera vez un certificado con SPE activado, el sistema se reiniciará automáticamente.

6) Haga clic en **Mostrar huella dactilar de certif.** si desea comprobar la integridad.

20.2.4 Cómo importar un certificado de entidad emisora SPE

No es necesario hacer este paso si se usan certificados generados automáticamente en **SSL Generación de certif.**.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Seguridad** > **Signaling and Payload Encryption (SPE)**.
3) En el grupo de menús, desplácese hasta **Certificados de entidad emisora SPE**.
4) En la ventana **Importar certificado de entidad emisora seguro (archivo X.509) para SPE** y en **Archivo con certificado (PEM o binario)**, introduzca el nombre de archivo del certificado o seleccione el archivo con **Examinar**.
5) En **Protocolo de punto de distribución CRL (CDP)**, seleccione el protocolo para las listas CRL (listas de revocación de certificados) (**LDAP** o **HTTP**).
6) En **CDP (sin, por ejemplo, ldap://)** introduzca el servidor deseado.
7) Haga clic en **Mostrar huella dactilar de certif.**

20.2.5 Cómo activar o desactivar SPE para una extensión

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el grupo de menús de **Extensiones** > **Extensiones** > **Clientes IP**, desplácese hasta la extensión deseada (cliente de sistema)

3) En la ventana **Extensiones** y en la pestaña **Editar parámetros exten.**, desplácese hasta la entrada **Seguridad de Payload**.
4) Elija una de estas opciones:
   - Si desea activar la función, en **Seguridad de Payload**, seleccione la entrada **Activado**.
   - Si desea desactivar la función, en **Seguridad de Payload**, seleccione la entrada **Desactivado**.
5) Haga clic en **Aplicar**.

20.3 Red privada virtual VPN

Una red privada virtual (VPN o "Virtual Private Network") es una red informática que utiliza una red pública (p. ej. Internet) para transportar datos privados. De esta forma, permite una transmisión segura a través de una red desprotegida. Para ello, los datos se transmiten codificados.

Resumen de VPN

VPN le ofrece:

- Conexión segura a través de un medio desprotegido (Internet)
- Protección frente a la manipulación de datos confidenciales
- Integración segura de socios externos en la red empresarial
- Acceso a informaciones de empresa para el servicio externo

Para garantizar la seguridad de la comunicación, la VPN funciona de la siguiente forma: se establece un túnel entre los interlocutores. Al establecer el túnel se realiza una autenticación y una autorización. Una vez establecido el túnel se transfieren los datos en sí de forma cifrada.

Una VPN puede establecerse entre (al menos) dos equipos o redes (extremos del túnel).

Existen dos tipos de interconexión en red:

- Site-to-Site-VPN

  Este tipo de interconexión realiza el cifrado entre dos gateways VPN. Los datos se transfieren cifrados dentro de las LAN.

- End-to-Site-VPN

  Remote Access VPN (acceso remoto de teletrabajadores)

Información específica de sistema

Los parámetros VPN se administran, fundamentalmente, a través del asistente VPN.

Recuerde que la conexión con el sistema de comunicación debe transcurrir a través de una conexión protegida con SSL. Esta conexión se implementa a través de OpenSwan y OpenSSL.

Dependencias

Tema	Dependencia
DynDNS	Se debe poder acceder a los puntos terminales de VPN mediante un nombre de dominio o una dirección IP fija. Si no es así, se puede utilizar DynDNS.
DynDNS	Si modifica una dirección IP en la VPN, el sistema de comunicación actualiza los datos referidos al nombre host (dirección IP) en el DynDNS.
DNS	Cada colateral VPN puede resolver el nombre host/la dirección IP a través del protocolo DNS estándar. Todos los nombres DNS (p. ej. Nombre host) deben ser nombres de dominio totalmente cualificados (FQDN). Durante la actualización de la dirección IP a través de DNS no se pueden establecer conexiones a través de túneles IPSec.

20.3.1 Requisitos para VPN

Para garantizar la calidad de la transmisión de voz y datos, las redes en uso deben cumplir ciertos requisitos. especialmente en lo referente al cifrado hay que planificar más nacho de banda que con otra interconexión.

En los siguientes ejemplos de las tablas se ha utilizado como base el modo de cifrado "Modo de túnel ESP con autenticación". Este modo ofrece la mayor seguridad en las VPN de sitio a sitio.

Estructura de un paquete de voz cifrado:

Longitud del encabezado ESP

Padding

Cálculo de ancho de banda para el algoritmo de cifrado AES:

Cálculo de anchos de banda para el algoritmo de cifrado DES / 3DES:

Ancho de banda para fax T.38

Protocolo	Bytes	
ESP Trailer	12	
ESP Padding	vario (y)	cifrado
ESP Padding Header	2	cifrado
Carga útil de voz	vario (x)	cifrado
RTP	12	cifrado
UDP	8	cifrado
IP (original)	20	cifrado
ESP-Header	8 + iv	

Protocolo	Bytes	
IP (Túnel)	20	
802.1Q VLAN Tagging	4	
MAC (con preámbulo, FCS)	26	
Suma	**112 + iv + x + y**	

La longitud del encabezado ESP depende del algoritmo de cifrado utilizado.

Requerido para el Cipher Block Chaining (encadenamiento de bloques de cifrado, CBC). El encabezado ESP incluye un vector de inicialización (IV). La longitud del IV es idéntica a la longitud del bloque de cifrado.

Se requiere el Padding ya que los algoritmos de cifrado se basan en el cifrado de bloques. Esto significa que la parte cifrada del paquete (encabezado RTP/UDP/IP original + carga útil de voz + padding de encabezado ESP) debe corresponderse a un múltiplo entero de la longitud del bloque de cifrado.

Longitud de bloque del algoritmo de cifrado:

Algoritmo de cifrado	Longitud de bloque	Longitud iv del vector de inicialización
AES	16 bytes (128 bits)	16 bytes (128 bits)
3DES	8 bytes (64 bits)	8 bytes (64 bits)

Cálculo de los bytes de padding necesarios para los paquetes de voz:

(42 + x + y) (bytes) = N x (0 o 16 (bytes)) (N entero)

Codec	Parámetro de empaquetad	Tamaño de marco (ms)	Carga útil (bytes)	Padding (bytes)	Longitud de paquete Ethernet (bytes)	Relación de carga general del paquete/ carga útil	Carga Ethernet (con) encabezado (kbps)
G.711	20	20	160	6	294	75%	117,6
G.711	30	30	240	6	372	50%	99,2
G.711	40	40	320	6	454	38%	90,8
G.711	60	60	480	6	614	25%	81,9
G.729A	1	20	20	2	150	600%	60,0
G.729A	2	40	40	6	182	300%	36,4
G.729A	3	60	60	2	198	200%	26,4

Codec	Parámetro de empaquetad	Tamaño de marco (ms)	Carga útil (bytes)	Padding (bytes)	Longitud de paquete Ethernet (bytes)	Relación de carga general del paquete/ carga útil	Carga Ethernet (con) encabezado (kbps)
G.711	20	20	160	6	286	75%	114,4
G.711	30	30	240	6	366	50%	97,6
G.711	40	40	320	6	446	38%	89,2
G.711	60	60	480	6	606	25%	80,8

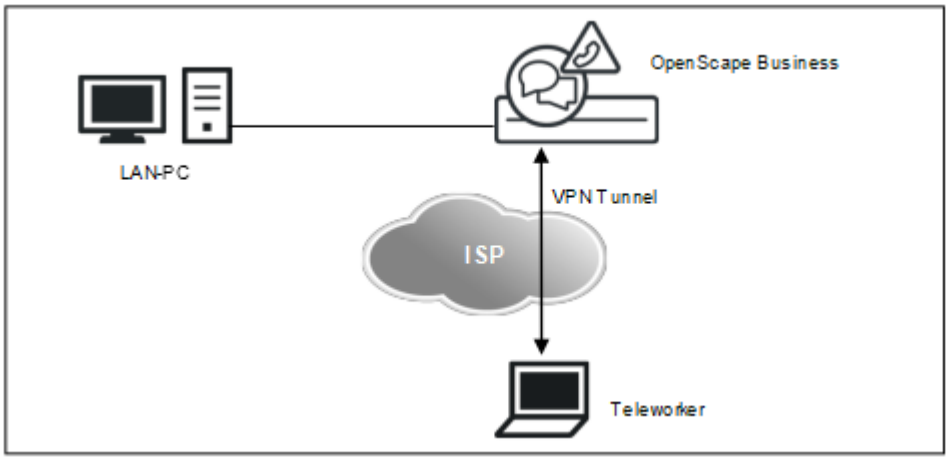
Codec	Parámetro de empaquetad	Tamaño de marco (ms)	Carga útil (bytes)	Padding (bytes)	Longitud de paquete Ethernet (bytes)	Relación de carga general del paquete/ carga útil	Carga Ethernet (con) encabezado (kbps)
G.729A	1	20	20	2	142	600%	56,8
G.729A	2	40	40	14	166	300%	33,2
G.729A	3	60	60	10	182	200%	24,3

Algoritmo de cifrado	Tamaño de marco (ms)	Carga útil y (bytes)	Padding x (bytes)	Longitud de paquete Ethernet (bytes)	Carga útil de paquete (carga general en porcentaje)	Carga Ethernet (con) encabezado (kbps)
DES / 3DES	30	169	1	278	64%	74,1
AES	30	169	9	294	74%	78.3

20.3.2 Conexión de teletrabajadores a través de VPN

Una conexión protegida a través de VPN permite conectar teletrabajadores al sistema de comunicación.

Sistema independiente con conexión de teletrabajadores mediante VPN



El sistema de comunicación tiene funciones VPN integradas (configuración mediante asistente). En cada sistema de comunicación puede haber activos al mismo tiempo hasta 10 teletrabajadores mediante VPN.

Para OpenScape Business están habilitados los siguientes clientes VPN:

- Cliente VPN NCP
- Cliente Shrew Soft VPN
- Cliente VPN Android
- Cliente VPN iOS
- Cliente VPN Mac OSX

Exportar datos de teletrabajadores

Los archivos de teletrabajador se pueden exportar como archivo ZIP (sin cifrar). En el archivo ZIP, por cada cliente VPN compatible hay un archivo de texto propio con los datos de teletrabajador: para el cliente VPN NCP en forma de archivo `.ini`, para el cliente VPN Shrew Soft en forma de archivo `.vpn` y para el cliente VPN OSX en forma de archivo `.networkConnect`. Estos archivos de texto también se pueden importar en el cliente VPN.

Consejo: Si hay acentos o diéresis no se consideran en los archivos de texto con los datos de teletrabajador. Los espacios en blanco se sustituyen con guiones bajos.

Indicación de estado de las conexiones VPN

En el asistente **VPN** encontrará una indicación de estado de todas las conexiones VPN. En el **Centro de servicios** (**Diagnostico** > **Estado** > **Estado VPN**), encontrará una vista general detallada de todas las conexiones VPN.

VPN con OpenScape Business S

Con OpenScape Business S, la VPN se implementa a través de un router externo. Esta introducción no incluye una descripción de aplicaciones externas.

20.3.2.1 Cómo configurar conexión de teletrabajadores a través de VPN

Con el asistente **VPN** puede permitir el acceso de teletrabajadores (colaterales VPN) a la LAN interna a través de VPN (red privada virtual) y conectar sistemas de comunicación por VPN. Si el sistema de comunicación no tiene una dirección IP fija (dirección IP pública, dirección IP global), hay que configurar un servicio DynDNS, por ejemplo, www.dyndns.org.

Requisitos previos

El acceso a Internet está configurado mediante la interfaz WAN.

Si la interfaz WAN no tiene una dirección IP fija (pública), hay que configurar DynDNS. Para realizar correctamente una prueba DynDNS se requiere una conexión con Internet.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Red / Internet**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración VPN**. La configuración estándar es **VPN desactivado**.
4) Haga clic en **Configuración de VPN**.
5) Si desea editar una conexión de VPN configurada, en la conexión de VPN deseada haga clic en **Editar**.
6) Si desea establecer una conexión de VPN, haga clic en **Agregar**.
7) En el campo **Nombre del gateway:** introduzca un nombre para la conexión de VPN (p.ej. `node2mch.dyndns.org`).

8) Si es necesario, introduzca un **Comentario** en el campo destinado a ello.
9) Active la casilla de verificación **activo** (preasignada de forma predeterminada).
10) Seleccione la casilla de verificación **Utilizar datos del propio sistema**.
11) Si es necesario, seleccione el **Tipo de dirección**:
    - Si la interfaz WAN tiene una dirección IP fija (pública), en la lista desplegable **Tipo dirección** seleccione la entrada **Dirección IP** y en **Dirección IP global/Nombre DNS (WAN)** introduzca la dirección IP fija (pública).
    - Si la interfaz WAN no tiene una dirección IP fija (pública), en la lista desplegable **Tipo dirección** seleccione la entrada **Nombre DNS**. En **Dirección IP global/Nombre DNS (WAN)** aparece el nombre DNS del sistema de comunicación configurado para DynDNS.
12) Modifique la **Dirección IP local (LAN)** solamente si es necesario.
13) Modifique la **máscara de subred local** solamente si es necesario.
14) Si desea editar un teletrabajador que ya esté configurado, en el área **Teletrabajador** y en el teletrabajador deseado, haga clic en **Editar**.
15) Si desea configurar un teletrabajador nuevo, en el área **Teletrabajador**, haga clic en **Añadir**.
16) Introduzca un nombre de configuración de teletrabajador en el campo **Nombre**.
17) Configure el tipo del cliente VPN utilizado:
    - Para un teletrabador VPN IPSec (clientes VPN NCP y Shrew Soft):

      Desactive la casilla de verificación **L2TP/IPSec**, como **Tipo dirección** seleccione la entrada **Dirección IP** y en el campo **Dirección IP virtual / Nombre DynDNS** seleccione una dirección IP virtual / un nombre DynDNS para el teletrabajador si el cliente VPN en uso es compatible con direcciones IP virtuales (sin importar la conexión del teletrabajador con Internet, si por router o por módem DSL).
    - Para teletrabajadores VPN L2TP/IPSec (clientes VPN iOS, Android y Mac OSX):

      Active la casilla de verificación **L2TP/IPSec** y asigne un **nombre de usuario** y una **contraseña** para el teletrabajador.
18) Active la casilla de verificación **activo** (preasignada de forma predeterminada).
19) Haga clic en **Aceptar**. Se abre la ventana con la visión general de los teletrabajadores. Puede indicar nuevos teletrabajadores.
20) Cuando haya configurado todos los teletrabajadores, haga clic en **OK & Continuar**. Aparece la ventana **Seleccionar sistema**.
21) Haga clic en **OK & Continuar**. Se abre la ventana **Ajustes de seguridad para conexiones**.
22) Para la conexión de VPN que acaba de configurar, asigne una clave para la conexión de VPN segura en **PreShared Secret** y repita la clave en **Repetir PreShared Secret**. La clave debe tener como mínimo 20 caracteres.
23) Si es necesario, agregue un **Comentario**.
24) Haga clic en **Aceptar**. Se abre la ventana **Información de estado VPN**.
25) Haga clic en **Activar VPN**.

26) Solo si se ha seleccionado Nombre DNS como Tipo dirección: compruebe los datos ya configurados de la cuenta DynDNS y haga clic en **Prueba de conexión**. Los datos de acceso DynDNS se transmiten al proveedor de servicios. Este proceso dura, aproximadamente, 10 segundos. Si la comprobación no termina correctamente, compruebe sus datos de acceso. Si la comprobación termina con éxito, haga clic en **Aceptar**.

27) Haga clic en **OK & Continuar**. Los teletrabajadores acceden a la interfaz WAN del sistema de comunicación.

28) Haga clic en **Salir**.

20.3.2.2 Cómo exportar los datos de teletrabajador

Con el asistente **VPN** puede exportar los datos de teletrabajador.

Requisitos previos

Hay configurada una conexión de VPN.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Red / Internet**.

3) Haga clic en **Editar** para iniciar el asistente **Configuración VPN**. La configuración estándar es **VPN desactivado**.

4) Haga clic en **Exportar/Importar**.

5) En el área **Exportar datos de teletrabajador desde sistema**, haga clic en **Exportar**. Guarde el archivo ZIP en el lugar que usted elija.

Consejo: En el archivo ZIP, por cada cliente VPN admitido hay un archivo propio con los datos de teletrabajador. Los datos de teletrabajador no se cifran. Maneje estos datos con responsabilidad.

---

6) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

20.3.3 Interconexión de sistemas de comunicación mediante VPN

Varios sistemas de comunicación OpenScape Business se pueden interconectar entre sí de forma segura mediante una red VPN site-to-site.

Interconexión mediante VPN

Tiene la posibilidad de configurar en un sistema de comunicación todos los datos para una interred de varios sistemas, exportar los datos de topología de forma cifrada e importarlos en todos los demás sistemas de la interred. Esto permite una configuración rápida y homogénea de todos los sistemas de la interred.

La distinción entre el sistema propio y los sistemas extranjeros tiene lugar a través de la identificación del nombre DynDNS propio o (si se utilizan direcciones IP fijas) a través de la dirección de Internet propia.

- Exportar datos de topología desde sistema
  - Todos los datos sobre la estructura de la red VPN se reunen en un archivo XML cifrado y se proporcionan para la exportación a otro sistema en formato ZIP.
- Importación de datos de topología al sistema
  - Todos los datos sobre la estructura de la red VPN se importan como archivo ZIP (que incluye el archivo XML cifrado) y se aplican para ese sistema.

La clave (contraseña) para la exportación se puede elegir y se debe comunicar al administrador que vaya a importar los ajustes.

Indicación de estado de las conexiones VPN

En el asistente **VPN** encontrará una indicación de estado de todas las conexiones VPN. En el **Centro de servicios** (**Diagnostico** > **Estado** > **Estado VPN**), encontrará una vista general detallada de todas las conexiones VPN.

20.3.3.1 Cómo configurar la red mediante VPN

El asistente **VPN** permite configurar todos los sistemas de la red VPN con un sistema. Puede exportar los datos de topología e importarlos en todos los sistemas de la interred VPN.

Requisitos previos

El acceso a Internet está configurado mediante la interfaz WAN.

Si la interfaz WAN no tiene una dirección IP fija (pública), hay que configurar DynDNS. Para realizar correctamente una prueba DynDNS se requiere una conexión con Internet.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Red / Internet**.

3) Haga clic en **Editar** para iniciar el asistente **Configuración VPN**. La configuración estándar es **VPN desactivado**.

4) Haga clic en **Configuración de VPN**.

5) Haga clic en **Agregar**.

6) En el campo **Nombre del gateway:** asigne un nombre para el primer sistema de la interred VPN (p.ej. `node1mch.dyndns.org`).

7) Si es necesario, introduzca un **Comentario** en el campo destinado a ello.

8) Active la casilla de verificación **activo** (preasignada de forma predeterminada).

9) Seleccione la casilla de verificación **Utilizar datos del propio sistema**. Los campos contiguos se predefinen con los datos del sistema.

10) Seleccione el **Tipo dirección** predefinido solamente si es necesario:
    - Si la interfaz WAN tiene una dirección IP fija (pública), en la lista desplegable **Tipo dirección** seleccione la entrada **Dirección IP** y en **Dirección IP global/Nombre DNS (WAN)** introduzca la dirección IP fija (pública).
    - Si la interfaz WAN no tiene una dirección IP fija (pública), en la lista desplegable **Tipo dirección** seleccione la entrada **Nombre DNS**. En **Dirección IP global/Nombre DNS (WAN)** aparece el nombre DNS del sistema de comunicación configurado para DynDNS.
11) Modifique la **Dirección IP local (LAN)** solamente si es necesario.
12) Modifique la **máscara de subred local (LAN)** solamente si es necesario.
13) Haga clic en **OK & Continuar**. Aparece la ventana **Seleccionar sistema**.
14) Haga clic de nuevo en **Añadir**.
15) En el campo **Nombre del gateway:** asigne un nombre para el segundo sistema de la interred VPN (p.ej. `node2mch.dyndns.org`).
16) Si es necesario, introduzca un **Comentario** en el campo destinado a ello.
17) Active la casilla de verificación **activo** (preasignada de forma predeterminada).
18) Seleccione el **Tipo dirección** del segundo sistema:
    - Si la interfaz WAN tiene una dirección IP fija (pública), en la lista desplegable **Tipo dirección** seleccione la entrada **Dirección IP** y en **Dirección IP global/Nombre DNS (WAN)** introduzca la dirección IP fija (pública).
    - Si la interfaz WAN no tiene una dirección IP fija (pública), en la lista desplegable **Tipo dirección** seleccione la entrada **Nombre DNS**. En **Dirección IP global/Nombre DNS (WAN)** aparece el nombre DNS del sistema de comunicación configurado para DynDNS.
19) Indique la **Dirección IP local (LAN)** del segundo sistema.
20) Indique la **máscara de subred local (LAN)** del segundo sistema.
21) Haga clic en **OK & Continuar**. Aparece la ventana **Seleccionar sistema**.
22) Repita los pasos 14 a 21 en todos los demás sistemas de la interred VPN.
23) A continuación, haga clic en **OK y Continuar**. Se abre la ventana **Ajustes de seguridad para conexiones**.
24) Por cada conexión de VPN entre sistemas, asigne una clave propia en **PreShared Secret** y repita la misma clave en **Repetir PreShared Secret**. La clave debe tener como mínimo 20 caracteres.
25) Si es necesario, añada un **Comentario** para cada conexión de VPN.
26) Haga clic en **Aceptar**. Se abre la ventana **Información de estado VPN**.
27) Haga clic en **Exportar/Importar** para exportar los datos de topología. Se abre la ventana **Exportar e importar datos de configuración VPN**.
28) En el área **Exportar datos de topología desde sistema**, en **Clave** y **Repetir clave**, introduzca una clave (mín. 7 caracteres) para proteger los datos. A continuación, haga clic en **Exportar**. Guarde el archivo ZIP en el lugar que usted elija.
29) Haga clic en **OK & Continuar**.
30) Haga clic en **Activar VPN**.
31) Solo si se ha seleccionado **Nombre DNS** como Tipo dirección: compruebe los datos ya configurados de la cuenta DynDNS y haga clic en **Prueba de conexión**. Los datos de acceso DynDNS se transmiten al proveedor

de servicios. Este proceso dura, aproximadamente, 10 segundos. Si la comprobación no termina correctamente, compruebe sus datos de acceso. Si la comprobación termina con éxito, haga clic en **Aceptar**.

32) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.
33) En la administración basada en web (WBM) del segundo sistema, en la barra de navegación, haga clic en **Configuración** y en el árbol de navegación, haga clic en **Asistentes** > **Red / Internet**.
34) Haga clic en **Editar** para iniciar el asistente **Configuración VPN**. La configuración estándar es **VPN desactivado**.
35) Haga clic en **Exportar/Importar** para importar los datos de topología. Se abre la ventana **Exportar e importar datos de configuración VPN**.
36) Haga clic en **Importar datos de topología al sistema** para importar los datos de topología.
37) Indique la **Clave** (contraseña) que ha indicado al exportar los datos en el primer sistema.
38) Desplácese hasta el lugar de almacenamiento del archivo ZIP. A continuación, haga clic en **Importar**.
39) Haga clic en **OK & Continuar**. Puede ver los sistemas configurados.
40) Haga clic en **Activar VPN**.
41) Solo si se ha seleccionado **Nombre DNS** como Tipo dirección: compruebe los datos ya configurados de la cuenta DynDNS y haga clic en **Prueba de conexión**. Los datos de acceso DynDNS se transmiten al proveedor de servicios. Este proceso dura, aproximadamente, 10 segundos. Si la comprobación no termina correctamente, compruebe sus datos de acceso. Si la comprobación termina con éxito, haga clic en **Aceptar**.
42) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.
43) Repita los pasos 33 a 42 para los demás sistemas de la interred VPN.

20.3.3.2 Cómo exportar e importar datos de topología de una red VPN

Con el asistente **VPN** puede exportar e importar los datos de topología de la red mediante VPN.

Requisitos previos

Hay configurada una conexión de VPN.

Para importar los datos de topología, debe conocer la clave asignada en la exportación.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Red / Internet**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración VPN**. La configuración estándar es **VPN desactivado**.
4) Haga clic en **Exportar/Importar**.
5) Si desea exportar los datos de topología, en el área **Exportar datos de topología desde sistema** en **Clave** y **Repetir clave** introduzca una clave

(mín. 7 caracteres) para proteger los datos. A continuación, haga clic en **Exportar**. Guarde el archivo ZIP en el lugar que usted elija.

6) Si desea importar los datos de topología, en el área **Importar datos de topología al sistema** en **Clave** introduzca la clave para cifrar los datos y desplácese al lugar de almacenamiento del archivo ZIP. Por último, haga clic en **Importar**.
7) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

20.3.4 Mecanismos de seguridad VPN

En VPN, los datos se codifican a través de distintos mecanismos de seguridad como Túnel IPSec, Security Associations y métodos de autenticación (Peer-to-Peer, firmas digitales).

Túnel IPSec

IPSec sirve para codificar datos y, normalmente, se puede aplicar sin tunelado. IPSec es una de las formas de implementar VPN. Puede codificar todo el paquete IP, incluyendo el encabezado IP: sucede en el modo túnel.

Los túneles deben estar siempre configurados en los dos colaterales VPN.

IPSec permite aplicar la administración automática de claves IKE (Internet Key Exchange). Es un estándar integrado en IPSec.

Security Associations SA

SA-IKE

SA Payload

Autenticación

Una SA (Security Association) es una asociación entre dos unidades en comunicación de redes informáticas. Describe la forma en la que las dos partes aplican servicios de seguridad para poder comunicarse entre sí.

Las conexiones VPN necesitan siempre tres SA que se negocian en dos fases:

- Fase 1: Creación de la SA de IKE

  una para la autenticación mutua inicial y para el intercambio de las claves de sesión (SA-IKE)

- Fase 2: Negociación de las SA de carga útil (Payload)

  una por cada dirección de la conexión establecida para el tráfico de carga útil (SA-Payload)

El protocolo IKE tiene, en esencia, dos tareas distintas. En primer lugar hay que establecer una SA utilizada exclusivamente por el protocolo IKE (SA-IKE). A continuación se utiliza la SA-IKE disponible para la negociación segura de todas las demás SA necesarias para la transmisión de datos de carga útil (SA-Payload). Por tanto, IKE opera en dos fases consecutivas:

Durante el establecimiento de conexión entre los colaterales VPN, deben negociarse distintos parámetros (p. ej. con qué frecuencia ha de volver a generarse una clave o qué procedimiento de codificación se va a utilizar). Estos parámetros se depositan y administran en SA-IKE.

La fase 2 de IKE sirve para la negociación de todos los parámetros de seguridad para los SA-Payload entre los colaterales VPN.

Siempre se tienen que configurar dos SA, una para la transmisión y otra para la recepción.

Esencialmente se ejecutan los siguientes pasos:

- Negociación de los algoritmos de codificación y autenticación
- Negociación de los protocolos de seguridad utilizados (ESP y AH)
- Negociación del modo de servicio de los protocolos de seguridad
- Negociación de la vigencia de las SA
- Definición del material de cifrado

En VPN se realiza una comunicación Peer-to-Peer. La autenticación de las partes VPN se puede realizar de dos formas:

- Pre-Shared Keys

  En VPN se utilizan fundamentalmente claves previamente distribuidas (Preshared Key). Para hacerlo, cada una de las partes VPN tiene que configurar un par de claves. A partir de estas claves se crea, para la autenticación, un valor hash que comprueba cada parte.
- Firmas digitales

  Cada parte VPN tiene asignado un certificado. Para que la autenticación tenga éxito, los colaterales VPN tienen que comprobar, en ambos extremos del túnel, la firma digital de su colateral respecto a una entidad emisora de confianza.

Información específica de sistema

Los parámetros de VPN se administran, fundamentalmente, a través del asistente.

Recuerde que la conexión de administrador debe transcurrir a través de una conexión protegida con SSL.

- Security Associations SA

  El sistema de comunicación admite los grupos Oakley 1, 2 y 5
- IPSec

  El sistema de comunicación utiliza el modo Túnel IPSec con ESP (Encapsulating Security Payload). ESP es un protocolo IPSec que garantiza la codificación de paquetes y su integridad y autenticidad
- SA Payload

  El sistema de comunicación admite los algoritmos de cifrado DES, 3DES y AES

  De todos los grupos de algoritmos MAC conocidos (MAC=Message Authentication Code) para la autenticación del origen y de la integridad de los datos, se admiten SHA1, HMAC-SHA2 y HMAC-MD5.

- Modos de servicio recomendados
  - IKE en "Main Mode" (Modo principal) con Perfect Forward Secrecy
  - Función hash con SHA-2
  - Autenticación con certificados (RSA)
  - Codificación con AES (hasta 256 bits)
  - Compatibilidad de direcciones IP públicas y dinámicas a través de direcciones IP virtuales o a través de mecanismos de actualización DynDNS para PC de teletrabajador

20.3.5 Certificados VPN

Un certificado vincula una determinada clave pública a un determinado cliente VPN. El cliente puede ser un cliente del sistema de comunicación o un teletrabajador. La combinación única de una clave pública y un cliente VPN es la base del proceso de autenticación.

Certificados y autoridades de certificación

Entidad emisora Lightweight

CRL (Certificate Revocation Lists o Listas de Revocación de Certificados)

Los certificados se firman de forma digital y son emitidos por las denominadas autoridades de certificación (Certification Authority, CA). IPSec acepta un certificado si ha sido emitido por una autoridad de certificación de confianza.

En un entorno VPN sencillo, la definición de una autoridad de certificación única puede ser suficiente. Esta central de certificación opera como una autoridad de certificación maestra en toda la VPN y se identifica frente a todos los clientes VPN a través de su certificado de entidad emisora auto-firmado.

Todos los clientes VPN necesitan un certificado emitido por dicha autoridad de certificación.

Los certificados del estándar X.509 (el más frecuente hoy en día) incluyen estos elementos principales:

- información sobre la identidad del propietario del certificado
- la clave pública del propietario del certificado
- información relativa a la autoridad de certificación que ha firmado el certificado (un número de serie, validez, información sobre la identidad de la autoridad y la firma digital de la autoridad de certificación).

En entornos en los que el cliente no siempre utiliza una PKI, la función Entidad emisora Lightweight ayuda a la certificación. Una entidad emisora Lightweight ofrece estas opciones:

- Crear pares de claves pública/privada
- Firmar y emitir certificados correspondientes
- Guardar pares de claves con sus correspondientes certificados en archivos

En la criptografía, con PKI (Public-Key-Infrastructure) se hace referencia a un sistema que permite emitir, distribuir y comprobar certificados digitales.

Se da una situación crítica cuando un certificado ha pasado a ser conocido (o existe la sospecha) y ya no es de confianza para la autenticación de peers. En este caso, la central de certificación debe revocar el certificado e informar a

todos los peers sobre la revocación de forma inmediata. Se rechaza cualquier intento de un peer remoto de autenticar su identidad a través de un certificado revocado.

Una CRL es, básicamente, una lista de todos los certificados revocados. Las CRL deben ser creadas por la autoridad de certificación que emitió los certificados.

Una CRL incluye estos elementos principales:

- Listado de los certificados revocados. Los certificados se identifican por los números de serie
- Momento de la publicación de la siguiente CRL actualizada (indicación de la validez de la CRL)
- Informaciones relativas a la autoridad de certificación que ha creado el certificado (información sobre la identidad de la CA y firma digital de la misma)

El administrador debe actualizar y distribuir regularmente y de forma manual las CRL.

Información específica de sistema

La autenticación se realiza en base a algoritmos criptográficos con claves públicas. El sistema de comunicación admite el RSA como algoritmo criptográfico con claves públicas. El sistema de comunicación solo es compatible con certificados que cumplan con el estándar X.509.

El sistema de comunicación actúa siempre como cliente VPN en la autenticación.

- Entidad emisora Lightweight

  El sistema de comunicación ofrece funciones de entidad emisora limitadas (entidad emisora Lightweight). El administrador proporciona el material de cifrado para un sistema importando manualmente pares de claves privada/pública y certificados a través de la conexión de administración protegida por SSL para todos los interlocutores envueltos en la comunicación.

- CRL

  Las CRL (Certificate Revocation Lists o Listas de Revocación de Certificados) se utilizan para revocar certificados. El administrador importa las CRL en el sistema de comunicación a través de una conexión protegida por SSL.

20.3.5.1 VPN - Cómo generar certificados de entidad emisora Lightweight

Lightweiht CA es una función que requiere licencia para la generación y administración de certificados de entidad emisora y de par.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.

3) En el grupo de menús, desplácese hasta **VPN** > **Entidad emisora Lightweight**. En la ventana **Generación de certif.** puede generar un certificado de entidad emisora propio.
4) En el campo **Nombre del certif.** asigne un nombre al certificado.
5) En **N.º de serie del certificado** asigne un número de serie al certificado.

Consejo: Un número de serie que haya sido concedido no se puede volver a utilizar con ningún otro certificado. Esto es así porque los números de serie de todos los certificados creados (en cualquier momento) deben ser únicos y exclusivos.

---

6) En **Tipo algoritmo firma**, introduzca el algoritmo deseado para el certificado (sha256RSA o sha512RSA).
7) En **Longitud de la clave pública**, indique la longitud de la clave pública (por ejemplo, 2048).
8) Indique la fecha y hora del comienzo del periodo de validez en **Inicio de la vigencia del certif. (GMT)**. La fecha se interpreta como GMT (Greenwich Mean Time).
9) En **Fin de la vigencia del certif. (GMT)**, indique la fecha y hora para el fin de la vigencia.
10) En **Solicitante**, indique el **País (C)**, la **Organización (O)**, la **Unidad organizativa (OU)** y el **Nombre común (CN)**.
11) De forma opcional, en **Nombre alternativo solicitante**, puede introducir otro solicitante. Si lo ha hecho, también debe indicar el formato (p. ej., dirección IP o nombre DNS). La ventana de entrada de datos depende del formato elegido.
12) En el campo **Punto distribución CRL**, indique el punto de distribución de las listas CRL (se muestran en un menú desplegable).
13) Haga clic en **Generar certificado**.

20.3.5.2 VPN - Administración de certificados - Cómo mostrar certificado

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Admin. certificados**. Se abre la ventana **Mostrar certif. de archivo**.
4) Si es necesario, active la casilla de verificación **Formato PKCS#12**.
5) Indique la **Clave de descifrado**.
6) En **Archivo con certificado**, indique el archivo de certificado o selecciónelo a través del campo **Examinar**.
7) Haga clic en **Cargar**.

20.3.5.3 VPN - Cómo importar certif. de entidad emisora de confianza (X.509)

X.509 es un estándar para certificados. Permite guardar también en el certificado el nombre y la firma digital del emisor del certificado. X.509 es parte del servicio de directorios X.500 para sistemas mundiales, distribuidos y abiertos.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Admin. certificados** > **Certif. de entidad emisora de confianza** > **Certificados configurados**.
4) En el campo **Nombre del certif.** asigne un nombre al certificado.
5) En el campo **Archivo con certificado**, indique el archivo de certificado o selecciónelo a través del campo **Examinar**.
6) Confirme y haga clic en **Activar tablas VPN configuradas.**

20.3.5.4 VPN - Certificados de par - Cómo generar Solicitud de certificado (CSR)

Puede crear un certificado de par firmado por entidad emisora basado en un certificado de entidad emisora. El requisito es que se haya generado, como mínimo, un certificado de entidad emisora. El certificado creado se guarda en un archivo PKCS#12. Los archivos PKCS#12 (PKCS#12 Estándar de sintaxis de intercambio de información personal) guardan certificados con una clave privada. De esta forma, un archivo PKCS#12 contiene los datos esenciales para el cifrado y descifrado personal.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Certificados de par**.
4) En la pestaña **Generar solicitud de certificado (CSR)**, genere los datos necesarios.
5) Introduzca el **Nombre de la solicitud de certif.**
6) En **Tipo algoritmo firma** introduzca el algoritmo deseado (sha256RSA o sha512RSA).
7) Introduzca la longitud de la clave (2048) en **Longitud de la clave**.
8) En **Solicitante** introduzca todos los datos para **País (C)**, **Organización (O)**, **Unidad organizativa (OU)** y el **Nombre común (CN)**.
9) En **Nombre alternativo solicitante** indique el **Formato del nombre DN** y, si es necesario, **Otro formato** o un **Nombre alternativo solicitante**.
10) Guarde el archivo *.csr que debe firmar una CA.

20.3.5.5 Cómo generar un certificado de par de VPN (PKCS#12)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Entidad emisora Lightweight**.
4) Haga clic en el certificado de entidad emisora y, a continuación, en **Generar certificado de par firmado por entidad emisora (PKCS#12)**.
5) Indique la **Clave de cifrado**.
6) Introduzca un número de serie a su elección en **N.º de serie del certificado**.
7) En **Longitud de la clave**, introduzca la longitud de la clave (1024, 1536 o 2048).
8) Indique la fecha y hora del comienzo del periodo de validez en **Inicio de la vigencia del certif. (GMT)**. La fecha especificada se indica en el tiempo del meridiano de Greenwich (GMT).

   Nota: El periodo de validez del certificado de par debe ajustarse a las directrices de seguridad válidas en la empresa. Poco antes del final del periodo de validez, hay que ampliar el certificado o generar uno nuevo.

9) Introduzca la fecha y hora para el final del periodo de validez en **Fin de la vigencia del certif. (GMT)**.
10) En **Solicitante** introduzca todos los datos para **País (C)**, **Organización (O)**, **Unidad organizativa (OU)** y el **Nombre común (CN)**.
11) De forma opcional, en **Nombre alternativo solicitante**, puede introducir otro solicitante. Si lo ha hecho, también debe indicar el formato (p. ej., dirección IP o nombre DNS). La ventana de entrada de datos depende del formato elegido.
12) Introduzca el **Punto distribución CRL** (opcional).
13) Haga clic en **Generar certificado**.

20.3.5.6 VPN - Cómo importar certificado de par (PKCS#12)

Los archivos PKCS#12 (Estándar de sintaxis de intercambio de información personal) guardan certificados con una clave privada. De esta forma, un archivo PKCS#12 contiene los datos esenciales para el cifrado y descifrado personal.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Certificados de par**.
4) Haga clic en la pestaña **Importar certificado de par (PKCS#12)**.
5) Introduzca un nombre para el certificado solicitado en **Nombre del certif.**.
6) En **Clave de descifrado**, indique su contraseña personal para el descifrado del certificado.
7) En **Archivo con certificado**, indique un nombre de archivo o busque el archivo mediante el botón **Examinar**.
8) Haga clic en **Mostrar huella dactilar de certif.**
9) Haga clic en **Importar certif. de archivo**.

20.3.6 Clientes VPN

Mediante un túnel VPN, los teletrabajadores pueden establecer una conexión de VPN segura con la red de empresa. Para ello, requiere un cliente VPN en su dispositivo (PC, PC tableta o smartphone). Todos los datos transmitidos entre el cliente VPN, el firewall de la empresa y el servidor VPN del sistema de comunicación están cifrados.

Son compatibles los siguientes clientes VPN:

- **Cliente VPN NCP**

  Los clientes NCP se pueden utilizar en cualquier entorno VPN con IPSec. Esto es importante si se necesita acceder desde un PC remoto a gateways VPN de distintos fabricantes o si ya hay instalado en la red empresarial un gateway VPN central de un tercero. En caso de red de sucursales el gateway NCP Secure Enterprise se puede conectar con otros gateways VPN sobre conexiones IPSec.

  El cliente NCP es de pago, pero ofrece una interfaz de usuario gráfico y una indicación de estado de la conexión.
- **Cliente Shrew Soft VPN**

  El cliente Shrew Soft VPN es un cliente de VPN gratuito con interfaz gráfica. A partir de la versión 2.1.5 también es compatible con la autenticación híbrida.

  El cliente Shrew Soft VPN incluye, entre otras prestaciones, ISAKMP, compatibilidad con Xauth y RSA, protocolos de cifrado 3DES, AES, Blowfish y otras prestaciones que habitualmente solo se encuentran en soluciones profesionales.
- **Cliente VPN iOS y Android**

  El sistema operativo iOS y Android tiene integrado el cliente VPN L2TP/IPSec.

  Los clientes L2TP/IPSec VPN utilizan el intervalo de direcciones IP `10.254.253.x`. Si ya se utilizan direcciones IP de este intervalo en la red de clientes, hay que modificar el intervalo de direcciones IP en la Gestión basada en Web (WBM), mediante **Modo experto** > **Mantenimiento** > **Diagnóstico aplicación** > **Prueba IPSec Test: rutinas de prueba IPSec** > **Definir dirección IP para L2TP** (por ejemplo, de `10.254.253.1` a `10.254.252.1`).

- **Cliente VPN Mac OSX**

  El sistema operativo Mac OSX tiene integrado el cliente VPN Mac OSX.

Información específica de sistema

- Los datos de teletrabajador de un cliente VPN se pueden exportar como archivo ZIP (sin cifrar). En el archivo ZIP, por cada cliente VPN compatible hay un archivo de texto propio con los datos de teletrabajador: para el cliente VPN NCP en forma de archivo `.ini`, para el cliente VPN Shrew Soft en forma de archivo `.vpn` y para el cliente VPN OSX en forma de archivo `.networkConnect`. Estos archivos de texto también se pueden importar en el cliente VPN.
- Infraestructura LAN con varias redes secundarias

  Si desea utilizar una infraestructura LAN con varias redes secundarias VPN, es necesario crear reglas para dichas redes. Las reglas no se pueden configurar mediante el asistente. La configuración debe realizarse mediante el modo Experto.
- Túnel en túnel

  No se puede integrar un segundo túnel VPN mediante uno ya existente.

20.3.6.1 Configuración de cliente VPN NCP

Para una conexión de VPN mediante el cliente VPN NCP hay que tener en cuenta los ajustes de configuración indicados a continuación, si la configuración se va a realizar de forma manual. Mediante el sistema de comunicación es posible exportar un archivo de texto `ncp_vpn.ini` con los datos de cliente VPN configurados e importarlo en el cliente VPN. De esta forma, los ajustes de configuración están preestablecidos.

Ajustes básicos

- Nombre de perfil

  elegible de forma libre, se recomienda el uso de un nombre inequívoco
- Tipo de conexión

  VPN a colateral IPSec
- Medio de conexión

  Según el tipo de conexión utilizado

  p. ej. LAN (por IP) o xDSL (PPPoE)

Acceso telefónico a la red

No se necesitan ajustes de configuración.

Inicio de sesión HTTP

No se necesitan ajustes de configuración.

Módem

No se necesitan ajustes de configuración.

Gestión de línea

- Establecimiento de conexión

  automático o manual

  Timeout = 0

  Nota: ¡De esta forma la conexión ya no se interrumpe en caso de inactividad!

- Asignación de prioridad a VoIP (Voice over IP)

  marcar con marca de verificación
- Autenticación EAP

  no se necesitan ajustes de configuración
- Autenticación HTTP

  no se necesitan ajustes de configuración

Configuración IPSec

- Gateway = Dirección IP o nombre DNS del sistema de comunicación

  A través de esta dirección IP o nombre DNS se puede acceder al sistema de comunicación desde Internet

  Designación en el asistente VPN: **Direcc. IP/Nombre DynDNS:**
- Directriz IKE = Modo automático
- Directriz IPSec = Modo automático
- Modo Exchange = Modo principal
- Grupo PFS = Grupo DH 2 (1024 bits)
- Validez / Duración
  - Directriz IKE: 000:00:07:00 (7 minutos)
  - Directriz IPSec: 000:00:08:00 (8 minutos)
- Editor

  no se necesitan ajustes de configuración

Opciones avanzadas IPSec

no se necesitan ajustes de configuración

Identidad

- Tipo = Dirección IP

  ID = Dirección IP del PC de teletrabajador (véase también Asignación de direcciones IP)

  Utilizar Pre-shared Key

  marcar con marca de verificación

  Shared Secret = Esta es la contraseña para la conexión VPN

  Designación en el asistente VPN: **PreShared Secret**
- Autenticación ampliada (XAUTH)

  no en uso, no es necesaria la configuración

Asignación de direcciones IP

- Asignación manual de dirección IP

  Dirección IP = Dirección IP del PC de teletrabajador

  Designación en el asistente VPN: **Direcc. IP virtual/Nombre DNS**
- DNS / WINS

  marcar con marca de verificación
- Servidor DNS = Dirección IP del sistema de comunicación

  Designación en el asistente VPN: **Dirección de subred IP local (LAN)**

Redes IP VPN

No se necesitan ajustes de configuración

Comprobación de certificado

no se necesitan ajustes de configuración

Link (enlace) Firewall

- Activar Stateful Inspection (inspección dinámica):

  en caso de conexión existente
- Solo permitir comunicación en el túnel:

  marcar con marca de verificación

20.3.6.2 Cómo configurar un cliente VPN NCP

Para la conexión segura de VPN con el sistema de comunicación, en el dispositivo de teletrabajador debe haber instalado y configurado un cliente VPN NCP.

Requisitos previos

El administrador de su sistema de comunicación lo ha configurado en la administración basada en web (WBM) de OpenScape Business como teletrabajador y le ha proporcionado el archivo ZIP de exportación con los datos de teletrabajador.

El administrador de su sistema de comunicación le ha proporcionado la clave PreShared Secret para la conexión de VPN.

En el dispositivo de teletrabajador está instalado el cliente VPN NCP (cliente VPN LANCOM Advanced). Podrá encontrar la información necesaria al respecto en la documentación del cliente NCP VPN.

El dispositivo de teletrabajador tiene una conexión activa con Internet.

Paso a paso

1) Extraiga los archivos `ncp_readme.txt` y `ncp_VPN.ini` y almacénelos en un directorio local. Las entradas del archivo `ncp_VPN.ini` se refieren al perfil `HOOME`.

2) Importe el perfil `HOOME` en el cliente NCP VPN.

3) Amplíe el perfil `HOOME` con un servidor DNS más. La dirección del servidor DNS es la dirección IP privada (LAN) de su sistema de comunicación.

4) Inicie el cliente NCP VPN
5) Marque el perfil `HOOME` y haga clic en **Conectar**.

20.3.6.3 Cómo configurar un cliente VPN Shrew Soft

Para la conexión segura de VPN con el sistema de comunicación, en el dispositivo de teletrabajador debe haber instalado y configurado un cliente VPN Shrew Soft.

Requisitos previos

El administrador de su sistema de comunicación lo ha configurado en la administración basada en web (WBM) de OpenScape Business como teletrabajador y le ha proporcionado el archivo ZIP de exportación con los datos de teletrabajador.

El administrador de su sistema de comunicación le ha proporcionado la clave PreShared Secret para la conexión de VPN.

En el dispositivo de teletrabajador está instalado el cliente VPN Shrew Soft. Puede descargar el cliente Shrew Soft VPN en `http://www.shrew.net`.

El dispositivo de teletrabajador tiene una conexión con Internet activa.

Paso a paso

1) Extraiga los archivos `shrewsoft_readme.txt` y `shrewsoft_openswan.vpn` y almacénelos en un directorio local.
2) Inicie el **Shrew Soft VPN Client Access Manager** y configúrelo. Guarde los datos.
3) Importe el archivo `shrewsoft_openswan.vpn` en el cliente Shrew Soft.
4) A continuación, en **Shrew Soft Client VPN Access Manager** (**Connect**), puede ver la conexión.

20.3.6.4 Cómo configurar un cliente VPN iOS o Android

Para la conexión segura de VPN con el sistema de comunicación, en el dispositivo de teletrabajador hay que configurar una conexión de VPN L2TP.

Requisitos previos

El administrador de su sistema de comunicación lo ha configurado en la administración basada en web (WBM) de OpenScape Business como teletrabajador y le ha proporcionado su nombre de usuario, su contraseña y la clave PreShared Secret de la conexión de VPN.

El dispositivo de teletrabajador tiene una conexión activa con Internet.

Paso a paso

1) En el dispositivo de teletrabajador iOS o Android, abra el menú **Ajustes** > **General** > **VPN**.
2) Con **Añadir VPN**, añada una conexión de VPN nueva.
3) Haga clic en la pestaña **L2TP**.
4) En el campo **Descripción**, asigne un nombre para la conexión de VPN.

5) En el campo **Servidor**, indique la dirección IP pública o el nombre DNS del sistema de comunicación.
6) En el campo **Cuenta**, introduzca el nombre de usuario del teletrabajador.
7) En el campo **Contraseña**, introduzca la contraseña del teletrabajador.
8) En el campo **Shared Secret**, indique la clave (Preshared Secret) del túnel VPN.
9) Active el conmutador **Para todos los Daten**.
10) En el menú **Ajustes**, active el conmutador **VPN**.

20.3.6.5 Cómo configurar un cliente VPN Mac OSX

Para la conexión segura de VPN con el sistema de comunicación, en el dispositivo de teletrabajador hay que configurar una conexión de VPN L2TP.

Requisitos previos

El administrador de su sistema de comunicación lo ha configurado en la administración basada en web (WBM) de OpenScape Business como teletrabajador y le ha proporcionado el archivo ZIP de exportación con los datos de teletrabajador.

El administrador de su sistema de comunicación le ha proporcionado su nombre de usuario, la contraseña y la clave PreShared Secret para la conexión de VPN.

El dispositivo de teletrabajador tiene una conexión activa con Internet.

Paso a paso

1) Descomprima el archivo `.networkConnect` y guárdelo en un directorio local.
2) Haga doble clic en el archivo `.networkConnect`.
3) Haga clic en **VPN (L2TP)**.
4) En el campo **Configuración**, seleccione la conexión de VPN.
5) En el campo **Dirección del servidor**, indique la dirección IP pública o el nombre DNS del sistema de comunicación.
6) En el campo **Nombre de usuario**, introduzca el nombre de usuario del teletrabajador.
7) Defina los ajustes de seguridad:
   a) Haga clic en **Ajustes de autenticación**.
   b) En el campo **Contraseña**, introduzca la contraseña del teletrabajador.
   c) En el campo **Clave ("Shared Secret")**, introduzca la clave (Preshared Secret) del túnel VPN.
   d) Haga clic en **Aceptar**.
8) Haga clic en **Más opciones** y active la casilla de verificación **Enviar todo el tráfico a través de la conexión VPN**. Haga clic en **Aceptar**.
9) Haga clic en **Aplicar** y, a continuación, en **Conectar**. Si la conexión con OpenScape Business es correcta, se muestra el estado **Conectado**.

20.3.7 VPN - Servicios

A través de la función de servicios configurados puede administrar servicios. Los servicios configurados solo se convierten en servicios activos previa activación.

20.3.7.1 VPN - Servicios activos - Cómo mostrar servicios IPSec

Puede ver una lista de todos los servicios IPSec activos, con datos detallados, en forma de tabla.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Servicios** > **Servicios activos**.
4) En la pestaña **Mostrar servicios IPsec** puede ver los datos detallados de los servicios IPsec activos.

20.3.7.2 VPN - Servicios activos - Cómo mostrar servicio IPSec especial

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Servicios** > **Servicios activos**.
4) En el grupo de menús, haga clic en el servicio especial cuya información desea consultar (**Nombre servicio**, **Puerto origen**, **Puerto destino**, **Protocolo IP**, **Regla "pass" correspond.**, **Regla "deny" correspond.**).

20.3.7.3 VPN - Servicios configurados - Cómo mostrar servicios IPSec

Puede ver una lista de todos los servicios IPSec configurados, con datos detallados, en forma de tabla.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Servicios** > **Servicios configurados**.
4) En la pestaña **Mostrar servicios IPsec** puede ver los datos detallados para los servicios IPsec configurados.

20.3.7.4 VPN - Servicios configurados - Cómo editar servicio IPSec

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Nota: Antes de modificar o activar el servicio IPsec, conviene realizar una copia de seguridad. Las reglas IPsec se comportan como registros de firewall y pueden restringir el acceso al sistema. Si activa IPsec y deja de tener acceso al sistema, puede restablecer el sistema de comunicación con **Volver a cargar**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Servicios** > **Servicios configurados**.
4) En el grupo de menús, haga clic en el servicio especial que desea modificar.
5) En **Nombre servicio** cambie el nombre del servicio.
6) En **Puerto origen** cambie el puerto de origen.
7) En **Puerto destino**, cambie el puerto de destino.
8) En **Protocolo IP**, cambie el servicio (por ejemplo, UDP).
9) Una vez finalizada la configuración VPN, los cambios se aplican con **Activar tablas VPN configuradas**

20.3.7.5 VPN - Servicios configurados - Cómo cambiar nombre a servicio IPSec

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Servicios** > **Servicios configurados**.
4) En el grupo de menús, haga clic en el servicio especial cuyo nombre desea cambiar.
5) En **Nombre servicio** cambie el nombre del servicio.

6) Una vez finalizada la configuración VPN, los cambios se aplican con **Activar tablas VPN configuradas**

20.3.7.6 VPN - Servicios configurados - Cómo borrar servicio IPSec

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Servicios** > **Servicios configurados**.
4) En el grupo de menús, haga clic en el servicio especial que desea borrar.
5) Una vez finalizada la configuración VPN, los cambios se aplican con **Activar tablas VPN configuradas**

20.3.8 VPN - Túnel

Un túnel designa un transporte de paquetes de datos cifrados hasta un punto terminal definido de forma fija. Los túneles activos son túneles configurados tras una activación de la configuración. En total, se pueden configurar hasta 256 túneles por gateway.

20.3.8.1 VPN - Túneles act. - Cómo mostrar datos generales de túnel

Puede ver todos los datos de túnel activos en forma de tabla con información detallada.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Túnel** > **Túneles act.**.

4) En la pestaña **Mostrar datos generales de túnel** puede ver información detallada sobre los túneles activos. Entre ellos:

- **Nombre del túnel**
- **Estado en pila IP**
- **Tipo punto terminal túnel local**
- **Dir. punto terminal túnel local**
- **Tipo punto terminal túnel remoto**
- **Dir. punto terminal túnel remoto**
- **Vigencia propuesta de las claves de sesión**
- **Vigencia propuesta de la sesión de intercamb. claves**
- **Reglas correspond. Regla envío correspond**
- **Reglas correspond. Regla recepción correspond**

20.3.8.2 VPN - Túneles act. - Cómo mostrar reglas de todos túneles

Puede visualizar las reglas de todos los túneles activos en una ventana.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Túnel** > **Túneles act.**.
4) En la pestaña **Mostrar reglas de todos túneles** puede ver información detallada sobre los túneles activos, como

- **Datos túnel**
- **Datos regla**
- **Dirección orig**
- **Dir. destino**
- **Datos servicio**

20.3.8.3 VPN - Túneles config. - Cómo mostrar datos generales de túnel

Puede ver todos los datos para túneles configurados en forma de tabla con información detallada

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Túnel** > **Túneles config**.

4) En la pestaña **Mostrar datos generales de túnel** puede ver información detallada sobre los túneles configurados. Entre ellos:

- **Nombre del túnel**
- **Tipo punto terminal túnel local**
- **Dir. punto terminal túnel local**
- **Tipo punto terminal túnel remoto**
- **Dir. punto terminal túnel remoto**
- **Vigencia propuesta de las claves de sesión**
- **Vigencia propuesta de la sesión de intercamb. claves**
- **Reglas correspond. Regla envío correspond**
- **Reglas correspond. Regla recepción correspond**

20.3.8.4 VPN - Túneles config. - Cómo mostrar reglas de todos túneles

Puede visualizar las reglas de todos los túneles configurados en una ventana.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Túnel** > **Túneles config**.
4) En la pestaña **Mostrar reglas de todos túneles** puede ver información detallada sobre los túneles configurados, como

- **Datos túnel**
- **Datos regla**
- **Datos fuente**
- **Datos destino**
- **Datos servicio**

20.3.8.5 VPN - Cómo añadir túnel configurado

Puede configurar un nuevo túnel IPSec. En total, se pueden configurar hasta 256 túneles por gateway.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Túnel** > **Túneles config**.
4) En la pestaña **Añadir túnel** se encuentra el campo de entrada para el nuevo túnel.
5) Marque **Datos túnel**.

6) En **Nombre del túnel**, introduzca el nombre deseado para el nuevo túnel.
7) En la lista desplegable **Tipo punto terminal túnel local**, seleccione el tipo de la dirección de punto terminal en el lado de envío del túnel (se puede introducir un nombre de host o DNS).
8) En **Dir. punto terminal túnel local**, indique la dirección del remitente en el formato adecuado para el tipo de punto terminal.
9) En la lista desplegable **Tipo punto terminal túnel remoto**, seleccione el tipo de la dirección de punto terminal en el lado de recepción del túnel (se admite la entrada de la dirección IP).
10) En **Dir. punto terminal túnel remoto**, indique la dirección del destinatario en el formato adecuado para el tipo de punto terminal. Si se establece la dirección 0.0.0.0, el punto terminal de túnel es desconocido. En tal caso, será siempre el colateral (p. ej., teletrabajador) el encargado de establecer el túnel.
11) En **Manejo de clave de sesión**, indique el procedimiento para el intercambio de claves (valores posibles: automático, con el protocolo IKE).
12) En **Algoritmos de cifrado propuestos**, seleccione cuántos algoritmos se pueden utilizar (AES o 3DES).
13) En **Algoritmos hash propuestos**, seleccione cuántos algoritmos de comprobación se pueden utilizar (MD5, SHA1 o SHA2). Los algoritmos seleccionados son ofrecidos por el iniciador del intercambio IKE.
14) En **Vigencia propuesta de las claves de sesión**, introduzca un periodo de validez para las Session Keys (claves de sesión) utilizadas. Terminado ese tiempo, no se intercambiarán más datos dentro de esa sesión. Para sustituir las claves de sesión invalidadas, se negocian automáticamente nuevas claves de sesión.
15) En **Vigencia propuesta de la sesión de intercamb. claves**, indique un tiempo de vigencia. Terminada la sesión de intercambio de claves, se negociarán automáticamente nuevas claves mediante IKE.
16) En **Volumen de datos propuesto de las claves de sesión**, introduzca el volumen de datos máximo para las claves de sesión. Si se supera ese volumen máximo, se negociará automáticamente una nueva clave de sesión mediante IKE. Al seleccionar **Ilimitado**, la validez de las claves de sesión no se limita por el volumen de datos.
17) En la parte superior de la ventana, active la casilla de verificación **Datos intercambio clave**.
18) Introduzca todos los datos de intercambio de clave (**active "Perfect Forward Secrecy" y seleccione el procedimiento de autenticación de pares VPN, Pre-Shared-Key** o **Firmas digitales**).

Consejo: Si ha seleccionado **Pre-Shared Keys** como procedimiento de autenticación, debe introducir una Pre-Shared Key de 20 dígitos (y repetir la entrada).

Consejo: Si desea utilizar como procedimiento de autenticación **Firmas digitales** (de una Entidad emisora

Lightweight) en una red VPN con varios nodos, debe configurar pasos adicionales.

a) Cree un certificado LWCA en un nodo.
b) Exporte el certificado (.crt) en un archivo.
c) Cree y exporte una lista de revocación de certificados (.crl) en un archivo.
d) Cree y exporte un certificado de par (.p12) firmado por el certificado de entidad emisora para cada nodo.
e) El certificado de entidad emisora (.crt), la lista de revocación de certificados (.crl) y los certificados de par correspondientes se deben importar en cada nodo.

19) Indique los **Grupos Diffie-Hellman propuestos** (Grupo DH 2, 5 o 14).

20) Una vez finalizada la configuración VPN, los cambios se aplican con **Activar tablas VPN configuradas**

20.3.9 VPN - Reglas

Las reglas establecen qué ha de suceder con un paquete IP. La acción de regla *PASS* significa que el paquete IP continúa siendo transportado (pasado). La acción de regla *DENY* significa que el paquete IP no continúa siendo transportado (ignorado). Asimismo, se puede seleccionar si el paquete IP (cifrado) utilizará o no un túnel VPN.

El sistema de comunicación puede administrar 640 reglas. 6 de ellas están preasignadas (reglas predeterminadas) y 634 se pueden asignar libremente.

20.3.9.1 VPN - Reglas activas - Cómo mostrar reglas

Puede visualizar todas las reglas activas.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.

3) En el grupo de menús, desplácese hasta **VPN** > **Reglas** > **Reglas activas**.

4) Haga clic en la pestaña **Mostrar reglas**. Podrá ver información detallada sobre las reglas activas. Esta información incluye

- **Prioridad**
- **Servicio**
- **Acción para la regla**
- **Cifrado obligatorio**
- **Estado de regla**
- **Estado en pila IP**
- **Dirección orig**
- **Dir. destino**
- **Túnel para cifrado**

20.3.9.2 VPN - Reglas activas - Cómo mostrar regla especial

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Reglas** > **Reglas activas**.
4) En el grupo de menús, haga clic en la Regla deseada. Se abrirá la ventana **Mostrar regla** con los datos detallados de esa regla (**Prioridad**, **Servicio**, **Acción para la regla**, **Cifrado obligatorio**, **Estado de regla**, **Dirección orig.**, **Dir. destino**)

20.3.9.3 VPN - Reglas configuradas - Cómo mostrar todas las reglas

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Reglas** > **Reglas configuradas**.
4) Haga clic en la pestaña **Mostrar reglas**. Podrá ver información detallada sobre las reglas activas. Esta información incluye
   - **Prioridad**
   - **Servicio**
   - **Acción para la regla**
   - **Cifrado obligatorio**
   - **Activar regla**
   - **Dirección orig. (tipo y dirección IP)**
   - **Dir. destino (tipo y dirección IP)**

20.3.9.4 VPN - Reglas configuradas - Cómo añadir regla

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Reglas** > **Reglas configuradas** > **Añadir regla**.

4) Realice la configuración de los siguientes parámetros:
   - **Prioridad**
   - **Servicio**
   - **Acción para la regla (PASS, PASS_INCOMING, PASS_OUTGOING, DENY)**
   - **Cifrado obligatorio**
   - **Estado de regla**
   - **Dirección de origen - Tipo**
   - **Dirección orig - Dirección (dirección inferior del área)**
   - **Dirección orig - Máscara de subred (dirección superior del área)**
   - **Dirección de destino - Tipo**
   - **Dir. destino - Dirección (dirección inferior del área)**
   - **Dir. destino - Máscara de subred (dirección superior del área)**
   - **Túnel lado recepción**
   - **Túnel lado envío**
5) Haga clic en **Aplicar**.

20.3.9.5 VPN - Cómo editar regla

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Reglas** > **Reglas configuradas**.
4) En el grupo de menús, marque la regla que desea modificar.
5) En **Prioridad**, indique la prioridad.
6) En **Servicio**, introduzca el servicio (por ejemplo, DNS).
7) En **Acción para la regla** introduzca la regla (**PASS**, **PASS_INCOMING**, **PASS_OUTGOING**, **DENY**).
8) Si es necesario, active la casilla de verificación **Cifrado obligatorio**.
9) Active la casilla de verificación **Activar regla**.
10) En **Dirección orig.**, indique el **tipo** y la **dirección IP** de la regla modificada.
11) En **Dir. destino**, indique el **tipo** y la **dirección IP** de la regla modificada.
12) Una vez finalizada la configuración VPN, los cambios se aplican con **Activar tablas VPN configuradas**

20.3.9.6 VPN - Cómo añadir regla para dirección opuesta

Si se ha creado una regla IPSec para la ruta de transmisión, debería agregarse inmediatamente después de la regla para la dirección opuesta. Con la función "Añadir regla para dirección opuesta" se aplican las entradas de las reglas seleccionadas. Al hacerlo, se intercambian entre sí las direcciones de origen y de destino y se cambia pertinentemente la asignación de túnel.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Reglas** > **Reglas configuradas**.
4) En el grupo de menús, marque la regla que desea editar.
5) Haga clic en la pestaña **Añadir regla para dirección opuesta**.
6) Haga clic en **Aplicar**.
7) Una vez finalizada la configuración VPN, los cambios se aplican con **Activar tablas VPN configuradas**

20.3.9.7 VPN - Cómo borrar regla

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Reglas** > **Reglas configuradas**.
4) En el grupo de menús, marque la regla que desea borrar.
5) Haga clic en la pestaña **Borrar regla**. La regla seleccionada aparece con todos los datos.
6) Haga clic en **Borrar**. Aparece un mensaje de aviso, indicando que se dispone a borrar esta regla.
7) Una vez finalizada la configuración VPN, los cambios se aplican con **Activar tablas VPN configuradas**

20.3.10 Servidor PKI

Con servidor PKI designa un servidor que puede emitir, distribuir y comprobar certificados digitales. Los certificados emitidos dentro de una PKI (Infraestructura de clave pública) se utilizan para asegurar la comunicación.

Al utilizar certificados (firmas digitales), se intenta utilizar la URL de PKI configurada por el servidor de PKI para descargar el CRL.

20.3.10.1 VPN - Cómo mostrar servidor PKI

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Public Key Infrastructure (PKI)**.
4) Haga clic en la pestaña **Mostrar servidor PKI**. Podrá ver el **Nombre servidor PKI**, el **Tipo servidor PKI** y la **URL de servidor PKI**.

20.3.10.2 VPN - Cómo añadir servidor PKI

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **VPN** > **Public Key Infrastructure (PKI)**.
4) Haga clic en la pestaña **Añadir servidor PKI**.
5) Indique el **Nombre servidor PKI**.
6) Indique el **Tipo servidor PKI** (p. ej. LDAP).
7) Indique la **URL de servidor PKI**.
8) Confirme y haga clic en **Aplicar**.

20.4 Gestión de certificados

SSL (Secure Sockets Layer) permite la administración protegida del sistema de comunicación. Los datos no se pueden leer ni manipular desde puestos no autorizados. La autorización se hace mediante certificados. Usted puede generar y administrar certificados.

El acceso de administración se realiza de forma cifrada por HTTPS y usando el protocolo TLS 1.2. Los certificados sirven para la autenticación del sistema de comunicación. De forma predeterminada se usa un certificado con firma automática. Para aumentar la seguridad se puede utilizar un certificado específico de usuario.

SSL ofrece los siguientes servicios de seguridad:

- Autenticidad (el interlocutor es quien pretende ser)
- Confidencialidad (los datos no pueden ser leídos por un tercero)
- Integridad (los datos se reciben en el mismo estado en el que fueron enviados)

Estos servicios de seguridad exigen un acuerdo previo sobre el mecanismo de seguridad y el intercambio de claves criptográficas. Ambas tareas se realizan al establecer la conexión.

SSL utiliza certificados y claves para garantizar una transferencia de datos segura.

CRL (Certificate Revocation Lists, listas de revocaciones de certificados)

Las CRL (Certificate Revocation Lists o listas de revocaciones de certificados) son archivos que incluyen una lista de certificados bloqueados, sus números de serie y sus datos de bloqueo. Además, una lista CRL incluye el nombre del emisor de la lista de bloqueo de certificado y de la siguiente hora de actualización.

CDP (CRL Distribution Point)

El punto de distribución CRL (CDP) es el directorio (la ubicación) de la versión actual de las CRL (p. ej. http://sectestcal.microsoft.com/ErtEnvoll/SecTestCAL.crl).

Información específica de sistema

En la administración basada en SSL tiene lugar una comunicación cliente-servidor.

El servidor se autentica con el cliente con ayuda de los certificados generados o importados en la Gestión basada en Web (WBM). En el navegador se puede importar uno de estos certificados como certificado confidencial para evitar la emisión de mensajes de advertencia del navegador al establecer conexión con el servidor SSL.

Consejo: La generación de certificados SSL también se puede utilizar para SPE.

20.4.1 Introducción

¿Qué son los certificados SSL?

Los certificados TLS/SSL se utilizan para proteger los datos durante la comunicación entre servidores como OpenScape Business y clientes basados en web mediante cifrado y para verificar la identidad de la empresa perteneciente al sitio web, de forma que el usuario pueda estar seguro de que realmente se está comunicando con el servidor real.

OpenScape Business emite un certificado SSL temporal ("autofirmado") durante la instalación inicial del sistema o al cambiar la dirección IP de la LAN, pero este certificado no contiene datos suficientes para verificar la identidad, aparte de la propia dirección IP de la LAN del usuario.

Dicho certificado no cumple los estándares de seguridad actuales y debe sustituirse por un certificado SSL individual de confianza emitido por una Autoridad de Certificación (CA) oficial lo antes posible tras la instalación inicial de OpenScape Business. Es la única forma de cumplir las normas mínimas de los actuales sistemas operativos cliente y navegadores web para una comunicación segura por Internet.

Las CA suelen ofrecer certificados SSL con distintos niveles de confianza: Validación de Dominio (DV), Validación de Organización (OV) y Validación Extendida (EV). Para OpenScape Business, los certificados validados por dominio son suficientes. Suele ser la opción más barata, y algunas CA son incluso gratuitas.

¿Para qué servicios web utiliza OpenScape Business el certificado SSL?

El certificado SSL activo se utiliza para el acceso del administrador a través del Portal de Administración, así como para otras aplicaciones basadas en web (por ejemplo, programación de claves) y clientes UC basados en WSI como myPortal @work, myPortal to go, Application Launcher, myContacts y myPortal for Teams.

¿Dónde puedo obtener un certificado SSL de confianza?

Para obtener un certificado SSL, debe ponerse en contacto con una autoridad de certificación. Debe verificar el nombre de dominio utilizado para acceder a OpenScape Business con el fin de crear una solicitud de firma de certificado (CSR), que se envía a la CA para su validación.

Hay que tener en cuenta que los certificados SSL de confianza emitidos por una CA únicamente tienen un periodo de validez limitado de unos meses a unos años para garantizar que cumplen las normas de seguridad actuales. Es importante vigilar la fecha de caducidad y renovar los certificados SSL antes de que llegue la fecha de caducidad.

Si no se renuevan los certificados SSL, el entorno cliente puede clasificar el sitio web como "inseguro" e impedir la comunicación con el servidor.

Tenga en cuenta que algunos entornos de cliente tienen requisitos especiales para los certificados SSL, que puede que no cumplan todas las CA.
Estos requisitos especiales se relacionan más adelante en la sección "consideraciones relativas al cliente". Cuando seleccione su CA, siga las instrucciones correspondientes.

¿Por qué ha cobrado tanta importancia la cuestión de los certificados?

El uso de certificados SSL fiables, específicos del cliente o del servidor, es extremadamente importante y los principales fabricantes de sistemas operativos y navegadores lo imponen cada vez más. Seguridad, profesionalidad, integridad y confidencialidad en el tratamiento de datos personales son los argumentos clave para ello.

Debido al uso creciente de servicios y clientes basados en la web, incluyendo a través de Internet, el uso permanente del certificado SSL temporal, autofirmado (y por lo tanto inseguro) por defecto de OpenScape Business está fuera de discusión.

Además, el certificado temporal autofirmado de OSBiz tiene una validez de varios años, mientras que algunos entornos cliente han empezado a restringir la validez del certificado, a veces a no más de un año.

Además, en muchas instalaciones de clientes que se configuraron originalmente con versiones de software anteriores a la V3R2.1, la validez de estos certificados temporales autofirmados expira el 1 de enero de 2024.

El portal de administración de OpenScape Business ofrece una serie de herramientas para generar y gestionar certificados SSL y también ayuda al administrador del sistema a crear solicitudes de firma de certificados. A continuación se explican las funciones más importantes a este respecto.

20.4.2 Cómo generar certificado de entidad emisora

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **SSL** > **Generación de certif**.
4) Haga clic en la pestaña **Generar certificado de entidad emisora**.
5) Asigne el **Nombre del certif.**.
6) En el campo **N.° de serie del certificado** indique también un número consecutivo.
7) En **Tipo algoritmo firma** (**sha256RSA**, **sha512RSA**), seleccione el algoritmo.
8) En **Longitud de la clave** seleccione la clave pública.
9) En los campos correspondientes, indique el comienzo y el final de la vigencia del certificado.
10) A continuación, rellene los campos para **Nombre Solicitante** o **Nombre alternativo solicitante**.
11) Introduzca el **Punto distribución CRL**.
12) Haga clic en **Aplicar** y, a continuación, en **OK**.

20.4.3 Cómo generar certificado con firma automática

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **SSL** > **Generación de certif.**.
4) Haga clic en la pestaña **Generar certif. con firma automática** de la ventana **Generación de certif.**.
5) En el campo **Nombre del certif.** asigne un nombre al certificado generado.
6) En el campo **N.° de serie del certificado** indique también un número consecutivo.
7) En **Tipo algoritmo firma**, seleccione el algoritmo.
8) En **Longitud de la clave pública**, seleccione la clave pública.
9) En los campos correspondientes, indique el comienzo y el final de la vigencia del certificado.
10) A continuación, rellene los campos para **Solicitante** o **Nombre alternativo solicitante**.
11) Introduzca el **Punto distribución CRL**.
12) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

20.4.4 Cómo generar una solicitud de certificado (CSR)

Dependiendo de la autoridad de certificación que elija, existen diferentes opciones para crear solicitudes de firma de certificados en línea (por ejemplo, a través del portal web de una CA) o fuera de línea. El portal de administración

de OpenScape Business ofrece una opción para crear una CSR para su descarga y transmisión a la CA.

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

En la página Generar solicitud de firma de certificado (CSR), deben rellenarse los siguientes campos para generar los archivos de clave y csr.

General:

Nombre de la solicitud de certif: Un nombre para el CSR que se utilizará en el nombre del archivo que se descargará.

Tipo algoritmo firma: Seleccione entre sha256RSA y sha512RSA.

Longitud de la clave pública: La única opción es 2048.

País (C): Utilice un código de país de dos letras, por ejemplo DE.

Organización (O): denota el nombre formal de la entidad o compañía a la que se asigna el certificado.

Unidad organizativa (UO): designa una subunidad o departamento específico dentro de una organización, ofreciendo una granularidad adicional para identificar la estructura organizativa.

Nombre común (CN): identificador vital, que suele representar el nombre de dominio para el que se emite el certificado, y que constituye un elemento clave para verificar la identidad del titular del certificado.

Nombre alternativo solicitante (opcional):

La extensión Nombre alternativo solicitante (SAN) es una característica de los certificados X.509 utilizada en el campo de la criptografía. X.509 es una norma que define el formato de los certificados de clave pública. La extensión SAN permite asociar identidades adicionales, como nombres de host, direcciones IP o direcciones de correo electrónico, a un único certificado X.509. Esto es especialmente útil en situaciones en las que se puede acceder a un servidor con diferentes nombres o direcciones.

Formato del nombre DN: Se debe rellenar información similar al nombre del asunto, como el país (C), la organización (O), la unidad de organización (OU) o el nombre común (CN).

Otro formato:

Nombre alternativo solicitante, extensión: Las opciones son Nombre DNS, Dirección IP, Dirección de correo electrónico, Indicador Uniforme de Recursos, Otros

Nombre alternativo solicitante: La extensión SAN ayuda a solventar las limitaciones en los casos en que un único nombre común es insuficiente o cuando es necesario incluir varias identidades en un mismo certificado. Esto es importante para los servicios web modernos, en los que un servidor puede ser accesible a través de varios nombres de dominio o direcciones IP.

Este es un ejemplo del aspecto que puede tener la extensión SAN en un certificado:

Nombre alternativo solicitante:

DNS:www.ejemplo.com

DNS:correo.ejemplo.com

Dirección IP:192.168.1.1

Email:admin@example.com

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **SSL** > **Gestión de certificados** > **Certificados de servidor**.
4) En la pestaña **Generar solicitud de firma de certificado (CSR)**:
5) Introduzca el nombre del certificado en el campo **Nombre de la solicitud de certif.**.
6) Haga clic para seleccionar **sha256RSA** o **sha512RSA** en la lista desplegable **Tipo de algoritmo de firma** .
7) La **Longitud de la clave pública** se fija en **2048** caracteres.
8) Introduzca el país **País C**.
9) Introduzca la organización **Organización O**.
10) Introduzca la **Unidad Organizativa (OU)**.
11) Introduzca el **Nombre común (CN)**.
12) Haga clic en **Formato de nombre DN** u **Otro formato** para seleccionar el formato del certificado.
13) Opcionalmente, elija uno de los valores de **Nombre alternativo solicitante, extensión**.
14) Opcionalmente, haga clic en el botón **Agregar** para añadir un **Nombre alternativo solicitante** en el CSR.
15) Haga clic en **Aplicar** y, a continuación, en **OK**.

20.4.5 Cómo importar un certificado de servidor (PKCS#12)

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **SSL** > **Gestión de certificados** > **Certificados de servidor**.
4) Haga clic en la pestaña **Importar certif. servidor (PKCS#12)** en la ventana **Certificados de servidor**.

Nota: Si selecciona otro formato, se pueden configurar varias entradas SAN.

---

5) Introduzca el **Nombre del certificado**.
6) Introduzca la **Clave de cifrado**.

7) En **Archivo con certificado** indique el archivo de certificado deseado mediante el botón **Seleccionar archivo**.
8) Haga clic en **Importar certif. de archivo** y después en **OK**.

20.4.6 Cómo importar certificados de servidor (PEM)

Como alternativa, se admiten certificados en formato PEM. Puede hacerlo importando el certificado y el archivo de claves como dos archivos separados.

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **SSL** > **Gestión de certificados** > **Certificados de servidor**.
4) Haga clic en la pestaña **Importar certif. servidor (PKCS#12)** en la ventana **Certificados de servidor**.

Nota: Si selecciona otro formato, se pueden configurar varias entradas SAN.

---

5) En la sección **Importar archivos de certificados y claves**:
6) Introduzca el **Nombre del certificado**. (Puede introducir un nombre de su elección)
7) Introduzca la **Clave de cifrado**. (Puede introducir una frase de contraseña de su elección)
8) En **Archivo de certificado**, elija el archivo de certificado mediante el botón **Elegir archivo**.
9) En **Archivo de claves**, elija el archivo de claves mediante el botón **Elegir archivo**.
10) Haga clic en **Importar certificado y clave** y, a continuación, en **OK**.

20.4.7 Cómo mostrar certificados

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **SSL** > **Admin. certificados** > **Certificados de servidor**.
4) Haga clic en el certificado deseado. Se abre la ventana **Certificados de servidor**.
5) Haga clic en la pestaña **Mostrar certificado**. Podrá ver el certificado actual.

20.4.8 Cómo borrar un certificado

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **SSL** > **Admin. certificados** > **Certificados de servidor**.
4) Haga clic en el certificado deseado. Se abre la ventana **Certificados de servidor**.
5) Haga clic en la pestaña **Borrar certificado**. Aparece el nombre del certificado en vigor con la advertencia de que se dispone a borrarlo.
6) Si de verdad quiere borrar el certificado, haga clic en **Borrar**.

20.4.9 Cómo exportar un certificado (X.509)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **SSL** > **Admin. certificados** > **Certificados de servidor**.
4) Haga clic en el certificado deseado. Se abre la ventana **Certificados de servidor**.
5) Haga clic en la pestaña **Exportar certificado (X.509)**. Puede abrir o guardar el certificado.

20.4.10 Cómo importar certificado renovado (X.509)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **SSL** > **Admin. certificados** > **Certificados de servidor**.
4) Haga clic en el certificado deseado. Se abre la ventana **Certificados de servidor**.
5) Haga clic en la pestaña **Importar certificado renovado (X.509)**. Aparece el nombre del certificado en vigor.

6) En el campo **Archivo con certificado** indique el archivo de certificado o selecciónelo a través del campo **Examinar**.
7) Termine su entrada con **Huella dactilar de**.

20.4.11 Cómo activar un certificado

Esta función permite definir el certificado que se va a usar para la administración basada en Web.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **SSL** > **Admin. certificados** > **Certificados de servidor**.
4) Haga clic en el certificado deseado.
5) Haga clic en la pestaña **Activar certificado**. Aparece una advertencia indicando que la acción interrumpe todas las conexiones HTTP existentes.
6) En la lista desplegable **Sistema** seleccione el sistema (OpenScape Business, UC Booster Server, UC Booster Card) para el que desea activar el certificado.

   Nota: Para que todo funcione correctamente, en cada certificado hay que registrar la dirección IP del sistema en el campo **Nombre común**. Asegúrese de activar el certificado correcto para el sistema seleccionado.

7) Haga clic en **Act. inmediat.**.

   Nota: El Certificado del servidor importado se debe emitir directamente desde una autoridad de certificación (CA) de raíz. No se deben utilizar CA intermedias.

20.4.12 Gestión de certificados para Booster Server

Al instalar inicialmente un Booster Server, se crea un certificado con la dirección IP del Booster como nombre común. El certificado tiene un periodo de validez de 10 años y se expide para la organización "Unify Software and Solutions GmbH & Co. KG", con la unidad organizativa especificada como "Unify".

Es posible sustituir el certificado por defecto en el Booster Server transfiriendo un certificado diferente a través de la interfaz Web-Based Management (WBM) del sistema. Una vez transferido, el nuevo certificado puede ser activado, proporcionando una configuración de seguridad alternativa para el Booster Server.

Nota: Del mismo modo, si su sistema utiliza UC Booster Card (OCAB) en su lugar, puede elegir **UC Booster Card** en el menú desplegable del **paso 6**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Seguridad**.
3) En el grupo de menús, desplácese hasta **SSL** > **Admin. certficados** > **Certificado de servidor**.
4) Elija uno de los certificados importados.
5) Haga clic en la pestaña **Activar certificado**.
6) En el menú desplegable del sistema, seleccione **OpenScape Business UC Booster Server**.
7) Haga clic en el botón **Activar ahora** para aplicar el certificado seleccionado al Booster Server.

20.5 Seguridad Web

En Seguridad Web encontrará el filtro de acceso Web con el que puede controlar las clases de servicio para clientes y el Protocolo admin, con el que puede hacer un seguimiento de los accesos y cambios en el sistema de comunicación.

20.5.1 Conexiones con el servidor Web

Las conexiones de los clientes (p.ej. myPortal to go) con el servidor Web interno del sistema de comunicación se pueden hacer de forma cifrada (HTTPS) o sin cifrar (HTTP).

Nota: Las conexiones sin cifrar con el servidor Web pueden hacer que se produzcan accesos no autorizados a datos confidenciales. Por motivos de seguridad se recomienda encarecidamente utilizar exclusivamente una conexión cifrada (HTTPS) se se utiliza myPortal to go (Web Edition) por Internet.

Para myPortal to go (App Edition) solo hay disponible una conexión cifrada con el servidor Web.

20.5.1.1 Cómo configurar las conexiones con el servidor Web (UC Suite)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Seguridad**.

3) En el grupo de menús, desplácese hasta **Web-Acceso**.
4) Configure las conexiones con el servidor Web:
   - Si desea permitir conexiones cifradas, active la casilla de verificación **HTTPS**.
   - Si desea permitir conexiones sin cifrar, active la casilla de verificación **HTTP**.
5) Si corresponde, active **Guardar datos de inicio de sesión en el terminal** para habilitar esta función. De esta forma, los datos de inicio de sesión se guardan en el navegador Web del teléfono móvil mediante las denominadas cookies.
6) Haga clic en **Guardar**.

20.5.1.2 Cómo configurar las conexiones con el servidor Web (UC Smart)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **UC Smart** > **Ajustes básicos**.
3) Compruebe si UC Smart está **Activo**.
4) Configure las conexiones con el servidor Web:
   - Si desea permitir conexiones cifradas, active la casilla de verificación **HTTPS**.
   - Si desea permitir conexiones sin cifrar, active la casilla de verificación **HTTP**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

20.5.2 Protocolo admin.

El Protocolo admin. permite saber qué cambios se han hecho en el sistema de comunicación y quién hizo tales cambios.

20.5.2.1 Cómo cargar protocolo admin.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento**.
3) En el árbol de navegación, desplácese hasta **Protocolo admin.** > **Datos protocolo admin**.

4) En la ventana **Datos protocolo admin** aparece el mensaje "El Protocolo admin. se transferirá desde el sistema. Confirme".
5) Haga clic en **Cargar**.

20.5.2.2 Cómo modificar el idioma del protocolo de administración

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Mantenimiento**.
3) En el árbol de navegación, desplácese hasta **Protocolo admin.** > **Configuración**.
4) En la ventana **Editar config.**, **Idioma protocolo admin.**, establezca el idioma deseado.
5) Haga clic en **Aplicar**.

20.6 Seguridad SQL

OpenScape Business guarda datos de configuración del sistema, registros de datos de llamada, credenciales de cuenta de usuario, datos de UC y demás en una base de datos SQL interna. El acceso a la base de datos está protegido mediante credenciales de inicio de sesión.

Hasta la versión de software V2R2, los credenciales de inicio de sesión utilizados se protegen con una contraseña, que no pueden modificar los administradores de OpenScape Business. A partir de V2R2, la contraseña se puede modificar. La contraseña se genera automáticamente y no se muestra al administrador. Para la compatibilidad en escenarios con varios nodos que ejecuten versiones de software antiguas, es posible restablecer el valor "antiguo" de una contraseña que se haya modificado. La configuración de contraseñas de acceso SQL se encuentra en Seguridad SQL. La configuración de contraseñas de acceso SQL se puede utilizar en entornos de red y de nodo único. En los capítulos siguientes se detalla la gestión de escenarios multinodo o de nodo único concretos.

20.6.1 Nodo único

Actualización de software desde V2R1 o anterior

Después de una actualización de versión (upgrade) de software a V2R1, la contraseña de la base de datos SQL antigua está activa. El administrador del sistema debe modificar la contraseña SQL en la versión nueva de software con el Portal de administración (WBM).

Configuración del nuevo sistema

Al configurar la fecha en el sistema por primera vez, se generará una nueva contraseña SQL. La contraseña SQL solo cambia automáticamente al definir por primera vez la fecha y la hora.

Configuración de un sistema de "nodo único" recargado

Cada vez que se recarga el sistema, la contraseña de base de datos SQL antigua está activa en el sistema. El administrador del sistema debe modificar la contraseña SQL en la versión V2R2 con el Portal de administración (WBM).

20.6.2 Varios nodos

El sistema de nodo único se ha configurado e integrado en la red de la forma ya conocida. Después de la configuración del sistema, el nuevo nodo esclavo sincroniza su contraseña SQL con el nodo maestro. No es necesario llevar a cabo ninguna acción para adaptar la contraseña SQL en el nodo esclavo.

Recarga de un nodo V2R2 o superior en una red V2R2 o superior

Después de recargar un nodo de red en la red, hay que configurar e integrar el nodo de nuevo en la red.

Recarga de un nodo maestro

En el caso de los nodos maestros, el administrador del sistema debe modificar la contraseña SQL con el Portal de administración (WBM). Todos los nodos esclavos sincronizan su contraseña SQL con la nueva del nodo maestro. No es necesario llevar a cabo ninguna acción para cambiar la contraseña SQL en los nodos esclavos.

Recarga del nodo esclavo

En el caso de los nodos esclavos, no es necesario llevar a cabo ninguna acción, ya que el nodo esclavo sincroniza su contraseña SQL con el nodo maestro.

Nuevo nodo esclavo V2R2 en una red V2R1 (escenario no recomendado)

El sistema de nodo único se ha configurado e integrado en la red de la forma ya conocida. Después de configurar el sistema, el nodo esclavo nuevo detecta que el nodo maestro utiliza la contraseña SQL antigua y la utiliza también. No es necesario llevar a cabo ninguna acción adicional para adaptar la contraseña SQL en el nodo esclavo.

Nota: Se recomienda estrictamente actualizar toda la red con la versión de software más reciente.

Nuevo nodo maestro V2R2 en una red V2R1 (escenario no recomendado)

El sistema de nodo maestro se ha configurado e integrado en la red de la forma ya conocida. Después de configurar el sistema, el nuevo nodo maestro utiliza la contraseña SQL antigua. El administrador del sistema no puede cambiar la contraseña antigua, porque los esclavos V2R1 no pueden sincronizarse con una nueva contraseña SQL en el nodo maestro. En este caso, el nodo no funcionará en la red. Si el administrador del sistema ha modificado la contraseña SQL de forma accidental, debe restablecerla al valor predeterminado en la configuración del nodo maestro.

Nota: Se recomienda estrictamente actualizar toda la red con la versión de software más reciente.

20.6.3 Cómo configurar contraseñas para la base de datos SQL

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía** > **Seguridad**.
3) En el árbol de navegación, desplácese hasta **Seguridad SQL**.
4) Configure las contraseñas para la base de datos SQL:
   - Si desea generar una contraseña nueva que no conozca el usuario, seleccione la casilla **Generar nuevo**.
   - Si quiere activar la contraseña predeterminada, seleccione la casilla **Activar predeterminado**.

Nota: En el área de notificaciones de la página de aterrizaje, aparecerá el mensaje siguiente si se utiliza la contraseña SQL estándar (o una contraseña generada con el algoritmo de generación de contraseñas antiguo):

'`Contraseña SQL estándar en uso. Puede cambiarla en el modo Experto`'

El mensaje es un enlace URL que lleva a la página de seguridad SQL para hacer los cambios.

20.7 Protección frente a ataques SIP (SIP Attack Protection)

Los denominados "ataques SIP" son una nueva forma de ataques dirigidos contra sistemas de comunicación a través de la telefonía IP. Los ataques se pueden realizar tanto desde la LAN como a través de Internet (a través de routers mal configurados). La protección frente a ataques SIP ofrece un acceso SIP protegido por contraseña.

Para un acceso de extensiones SIP se aplican las siguientes reglas:

- Autenticación activa
- Una contraseña cualificada que
- – tenga entre 8 y 20 caracteres,
  – incluya una o varias mayúsculas (de A a Z),
  – incluya una o varias minúsculas (de a a z),
  – incluya uno o varios números (de 0 a 9),
  – incluya uno o varios caracteres especiales (p. ej.: %),
  – no tenga más de 3 caracteres repetidos.
- Definición de un ID de extensión SIP diferente del número de teléfono.

Al configurar una nueva extensión SIP, la autenticación está activada de forma predeterminada y se genera una contraseña aleatoria. Esta contraseña aleatoria no es conocida, por lo que la debe modificar el administrador.

En el sistema de comunicación, los ajustes correspondientes se realizan mediante el asistente "Telefonía central" o a través del Manager E.

Cuando se inicia el sistema, se comprueba la lista de contraseñas y se realiza una entrada en el registro de eventos si se ha configurado una extensión SIP sin contraseña.

Consejo: Si desea utilizar el sistema de comunicación como router Internet, debe cerrar el puerto 5060 (ajuste estándar). Con telefonía Internet mediante ITSP, el sistema de comunicación abre los puertos correspondientes y los mantiene abiertos.

Si desea utilizar un router externo o firewall, el puerto 5060 debe estar cerrado. Corresponde al sistema de comunicación abrir este puerto (si es necesario).

---

21 Interconexión de OpenScape Business

Los sistemas de comunicación OpenScape Business se pueden interconectar entre sí y con los sistemas de comunicación OpenScape 4000 (HiPath 4000) y OpenScape Voice. En una interconexión OpenScape Business homogénea, las extensiones pueden utilizar prestaciones como Presencia, Buzón de voz, Conferencias, y un largo etcétera que hasta ahora solo se podían utilizar en un único sistema de comunicación OpenScape Business.

Interconexiones posibles:

- Interconexión de voz pura de OpenScape Business X
- Interconexión OpenScape Business X y OpenScape Business S (opcional con UC Suite o UC Smart).
- OpenScape Business X con OpenScape 4000 (funcionalidad UC en OpenScape Business solo si se cumplen ciertos requisitos)
- OpenScape Business X con OpenScape Voice (sin funcionalidad UC en OpenScape Business)
- Conectar equipo auxiliar externo con OpenScape Business mediante la interconexión SIP.
- Interconexión mediante RDSI
- Interred OpenScape Business con conexión central de línea urbana ITSP

Los sistemas de comunicación se preparan para la interconexión con el asistente **Configuración de red**. En este asistente se indica si se trata de un nodo maestro o esclavo. Además, a la ruta 16 (redes) se le asignan automáticamente 16 líneas.

Todas las interconexiones que utilizan prestaciones de Unified Communications (como por ejemplo UC Smart o UC Suite), deben definirse con un plan de numeración cerrado. Las interconexiones sin las prestaciones de Comunicaciones Unificadas pueden basarse en planes de numeración abiertos o cerrados. Para poder responder con flexibilidad a los deseos de ampliación de los clientes, se recomienda utilizar siempre la numeración cerrada en las interredes de nueva creación.

Consejo: La configuración de una red IP es una tarea compleja que solo deberían realizar técnicos de servicio con experiencia.

No se puede crear una interred OpenScape Business X1 pura, ya que un sistema X1 no puede ser un sistema maestro y en la interred siempre debe haber un sistema maestro.

No se admite una interconexión de OpenScape Business con estos sistemas:

- HiPath 3000 SIP-Q, solo se admite interconexión TDM sobre base S_0/S_{2M} con CorNet NQ, véase Interconexión mediante RDSI.
- HiPath 5000 RSM
- OpenScape Office MX
- OpenScape Office LX

La migración de un HiPath 3000 (incl. HiPath 5000 RSM) a OpenScape Business se describe en el capítulo Migración.

Nota: Para obtener información sobre licencias y actualización o migración de sistemas en una red, consulte la sección **Red - Licencias** en el capítulo Actualizaciones.

21.1 Plan de interconexión

Antes de configurar una interred debería crearse, previa consulta con los clientes, un plan de interconexión.

El plan de interconexión debería incluir estos datos:

- ID de nodo (Node-ID) y direcciones IP correspondientes
- Plan de numeración

21.1.1 Redes homogéneas y no homogéneas

En términos generales, con la interconexión se distingue entre redes homogéneas (en las que todos los componentes pertenecen a una única familia de sistemas) y redes no homogéneas (diferentes sistemas).

Red homogénea (red nativa)

Red no homogénea (red híbrida)

Una red homogénea (nativa) consta de componentes de la familia de sistemas OpenScape Business.

Una red no homogénea (híbrida) consta de componentes de la familia de sistemas OpenScape Business y, por ejemplo, un OpenScape 4000 o un OpenScape Voice.

Vista general de todos los nodos de OpenScape Business de una interred

La entrada **Redes** de la barra de navegación de la administración basada en web (WBM) permite ver todos los nodos OpenScape Business de una interred. Además, también se pueden ordenar todas las extensiones de OpenScape Business de la interred por nodos.

Se muestra la siguiente información:

- **ID de nodo**: ID de nodo
- **M** / **S**: indica si el nodo es maestro o esclavo
- **Nombre de red**: nombre del nodo
- **Tipo**: tipo nodo (**OSBiz X**: modelo de hardware, **OSBiz S**: softswitch)
- **OSBiz X / OSBiz S**: dirección IP del nodo, se puede hacer clic sobre ella (abre Gestión basada Web [WBM])
- **Servidor de aplicaciones**: dirección IP del servidor UC (UC Booster Card o UC Booster Server)
- **Estado de registro**: estado del registro
- **Alive**: esta opción indica si el nodo está activo o no

21.1.1.1 Cómo mostrar la vista general de todos los nodos OpenScape Business

Requisitos previos

Hay varios sistemas de comunicación OpenScape Business interconectados.

Paso a paso

1) En la barra de navegación, haga clic en **Redes**.
2) En el árbol de navegación, haga clic en **Vista de dominios**. Aparece un listado de todos los nodos OpenScape Business de la interred.

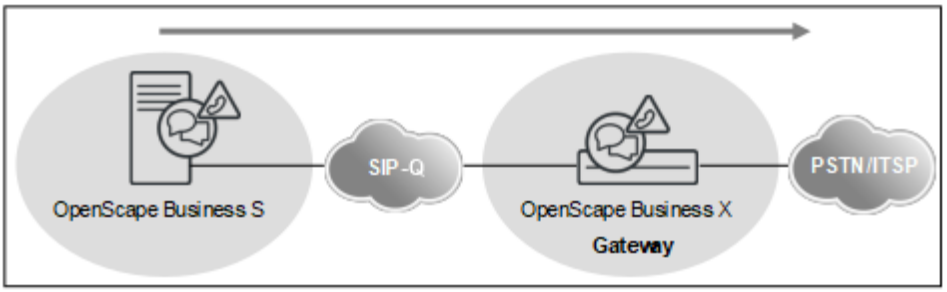
21.1.2 Gateway único y multigateway

En una interconexión homogénea de OpenScape Business, se distingue entre "de gateway único" y "de varios gateways", que también reciben la denominación de interconexiones de gateway único (o "single gateway") o multigateway, respectivamente.

Gateway único

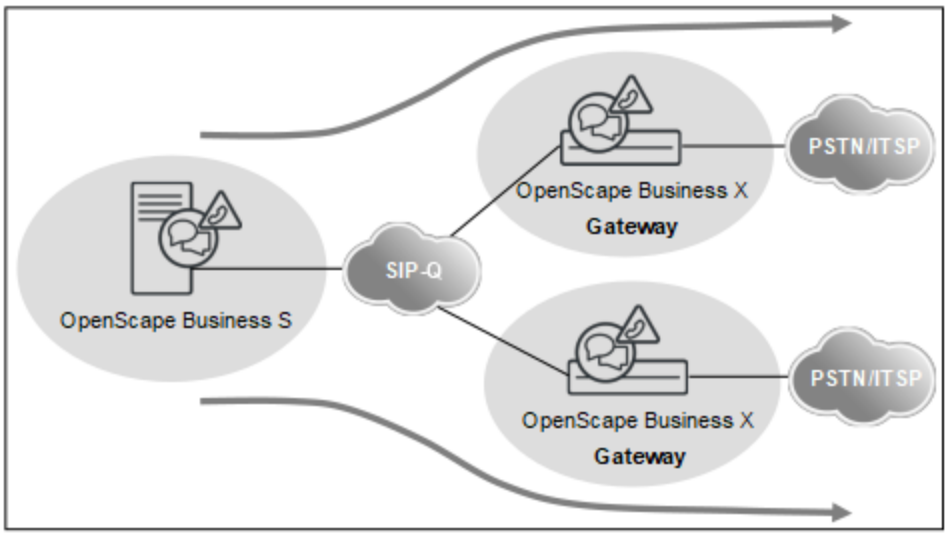
Multigateway

En las interconexiones de gateway único las llamadas desde el servidor y hacia él se encaminan a través de un solo gateway. Todas las extensiones IP registradas en el servidor usan este mismo gateway.



- Este tipo de interconexión se admite cuando hay uno o varios OpenScape Business S en la red.
- Las extensiones IP están conectadas con distintos sistemas de comunicación.
- OpenScape Business X se utiliza como gateway.

En las interconexiones multigateway, las llamadas se encaminan a través de varios gateways de OpenScape Business.



- Solo 1 proveedor de PSTN o un número de llamada de línea urbana por gateway
- Las extensiones de varias ubicaciones se registran en un sistema central (OpenScape Business S).
- Cada una de las extensiones de OpenScape Business S está asignada a un determinado gateway (OpenScape Business X).
- En la red solo puede haber un único OpenScape Business S.
- OpenScape Business y OpenScape Business S se encuentran en la misma zona horaria y en el mismo país (con el mismo código de país).
- Solo hay un código de acceso a línea urbana a nivel de red.
- En los gateways puede haber configuradas, por ejemplo, extensiones RDSI y analógicas de forma local.

21.2 Prestaciones a nivel de red

Fundamentalmente, las prestaciones de voz a nivel de red se determinan mediante el protocolo de interconexión SIP-Q. Las prestaciones de Comunicaciones Unificadas (UC) a nivel de red se determinan mediante la interconexión de la solución de UC (UC Suite o UC Smart) y sus clientes UC.

21.2.1 Prestaciones a nivel de red de las soluciones de UC

La tabla siguiente ofrece una vista general de las prestaciones a nivel de red de las soluciones de Comunicaciones Unificadas UC Smart y UC Suite.

No es posible la interconectividad UC con OpenScape 4000 y OpenScape Voice. En una interred OpenScape Business, hay que utilizar UC Smart o UC Suite. No se admiten soluciones mixtas de UC.

Funciones de UC a nivel de red	UC Smart		UC Suite		
	myPortal @	myPortal to	myPortal for Desktop / Outlook	myPortal @w	myPortal to go
Visibilidad a nivel de red del estado de presencia (gestión de presencia)	x	x	x	x	x
Modificación del estado de presencia proprio mediante cliente	x	x	x	x	x
Modificación del estado de presencia proprio mediante TUI	x	x	x	x	x
Desvío de llamadas basado en el estado	x	x	x	A través de destinos definidos en otros clientes de UC Suite	destinos definidos con myPortal
Indicación de estado a nivel de red en Favoritos	x	x	x	x	x
Indicación de estado a nivel de red en directorios	x	x	x	x	x
Indicación de estado a nivel de red en el Diario	-	-	x	-	-
Activar servicio CallMe	-	-	x	x	x
Integración de calendario (Outlook)	-	-	x	-	-
Integración de calendario, iCal (solo myPortal for Desktop)	-	-	x	-	-
Indicación a nivel de red del estado de llamada (libre, ocupado, estado de llamada)	x	x	x	x	x
Creación de grupos a nivel de red	x	x	x	-	-
Indicación compacta de los favoritos	-	-	x	-	-
Conversaciones	x	-	-	x	-
Directorio personal	Local	Local	Local	Local	Local
Directorio interno	Local	Local	Local	Local	Local
Directorio externo	-	-	x	x	x

Funciones de UC a nivel de red	UC Smart		UC Suite		
	myPortal @	myPortal to	myPortal for Desktop / Outlook	myPortal @w	myPortal to go
Búsqueda en directorios a nivel de red	x	x	x	x	x
Acceso a destinos marcación abrev. (KWZ) definidos en sistema	Local	Local	-	Local	Local
Importar/Administrar contactos personales (CSV/XML)	x	-	x	-	-
Acceso a contactos de Outlook	x	-	x	-	-
Importación de contactos personales (Mac OS) (myPortal for Desktop)	-	-	x	-	-
Integración del servidor de directorios externos por LDAP	-	-	x	-	-
Todas las llamadas	x	x	x	x	x
Llamadas abiertas	-	x	x	-	-
Llamadas perdidas	x	x	x	x	x
Llamadas contestadas	x	x	x	x	x
Llamadas programadas	-	-	x	-	-
Llamadas a través de VOIP	x	-	x	x	-
Diario de fax	-	-	x	-	-
Marcación manual	x	x	x	x	x
Marcación de escritorio (Click to Call)	-	-	x	-	-
Desvío	x	x	x	x	x
Retener	x	x	x	x	x
Grabación de llamadas (Voice Recording)	-	-	x	-	-
Enviar correo electrónico	x	x	x	x	x
Enviar SMS	-	x	-	-	x
Popups	x	-	x	x	-
Conferencia AdHoc	x	x	x	x	x
Conferencias programadas	-	-	x	-	-

Funciones de UC a nivel de red	UC Smart		UC Suite		
	myPortal @	myPortal to	myPortal for Desktop / Outlook	myPortal @w	myPortal to go
Conferencias permanentes y abiertas (conferencia Drag&Drop)	x	-	x	-	-
Integración de Web Collaboration	x	-	x	x	-
Buzón de voz (buzón de voz visual)	x	x	x	x	x
Escucha de mensajes de voz con el teléfono	x	x	x	x	x
Escucha de mensajes de voz con tarjeta de sonido PC	-	-	x	-	-
Cómo enviar un mensaje de voz como correo electrónico	x	x	x	-	-
Fax (para sistemas operativos Windows)	-	-	x	-	-
Mensajería instantánea (chat) a nivel de red	x	-	x	-	-

21.2.2 Prestaciones de voz a nivel de red

En una interconexión mediante el protocolo SIP-Q, se admiten las siguientes prestaciones de voz para OpenScape business y otros sistemas de comunicación.

Prestación	SIP-Q (red IP)
Basic Call	Sí
Devolución de llamada en caso de ocupado	Sí
Devolución de llamada en caso de libre	Sí
Intercalar	Sí
Aviso llam. en espera	Sí
Segunda llamada	Sí
Calling Line Identification Presentation (CLIP, Indicación del número llamante en la extensión llamada)	Sí
Calling Line Identification Restriction (CLIR, Supresión de la indicación del número llamante en la extensión llamada)	Sí
Connected Line Identification Presentation (COLP, Indicación del número de llamada en la extensión llamante)	Sí

Prestación	SIP-Q (red IP)
Connected Line Identification Restriction (COLR, Supresión del número de llamada en la extensión llamante)	Sí
Calling / Connected Name Identification Presentation (CNIP, Indicación del nombre del llamante en la extensión llamada)	Sí
Calling / Connected Name Identification Restriction (CNIR, Supresión del nombre del llamante en la extensión llamada)	Sí
No molestar	Sí
Desvío de llamadas	Sí
Transferencia automática de llamadas en caso de ocupado	Sí
Transferencia automática diferida en caso de libre	Sí
Call Deflection (Desvío de llamadas)	Sí
Advice of Charge at Call Setup (Aviso de cargos al configurar llamada)	No
Advice of Charge during Call (Aviso de cargos durante la llamada)	Sí
Advice of Charge at the end of the call (Aviso de cargos al finalizar llamada)	Sí
Optimación de rutas	no
Reencaminamiento	no
Message Waiting Indication (Indicación de mensaje en espera) / Info	Sí
Identif.	Sí
Retener	Sí
Alternar	Sí
Transferencia	Sí
Conferencia	Sí
Llamada recordatoria	Sí
Llamada de emergencia	Sí
Interceptación	Sí
Private Numbering Plan (PNP, Plan de numeración privado)	no
Telecaptura de llamadas	no
Línea colectiva	Sí
SPE (Excepto con Conferencia y Aplicaciones)	sí

21.3 Registro de licencia de una interconexión

En los sistemas de comunicación interconectados se puede seleccionar un registro de licencia central.

En el servidor de licencias, todas las licencias de los sistemas individuales se reunen en una licencia a nivel de red. En la interred se pueden asignar las licencias a los distintos nodos a través de la Gestión basada en Web (WBM).

Para obtener más información, véase Registro de licencia de varios sistemas de comunicación (interred).

21.4 Requisitos de la interconexión

Para garantizar la calidad de la transmisión de voz, las redes IP utilizadas y el sistema de comunicación deben cumplir determinados requisitos. La calidad de voz y la fiabilidad de la comunicación de voz dependen de la técnica de redes utilizada.

Parámetros de red, requisito para LAN y WAN

Parámetros	Requisito mínimo	Observación
Delay (one way)	50 ms	Unos valores más altos empeoran la calidad de la voz.
Round Trip Delay	100 ms	Unos valores más altos empeoran la calidad de la voz.
Jitter	20 ms	Unos valores más altos empeoran la calidad de la voz.
Packet Loss	3%	En las transmisiones de fax o módem con G.711, la pérdida de paquete no debe superar el 0,05 % (si no es posible T.38).
Consecutive Packet Loss	3 with G.711	Unos valores más altos empeoran la calidad de la voz.

Recomendación para el cálculo de anchos de banda

- En la interred se requiere un ancho de banda de al menos 256 bits/s (en dirección de recepción y envío).
- El cálculo de anchos de banda debería partir de un 50% máximo para la parte de voz respecto al ancho de banda total. Por ejemplo, en una WAN de 1 MBit, se deben calcular 500 kbps como máximo para la voz. En el códec G.711 son, por ejemplo, 5 tronqueos de IP como máximo.
- Con independencia de ello, hay que tener en cuenta las propiedades de red relativas a QoS, Delay, Packet Loss etc.

21.4.1 Requisitos a la interconexión LAN

Para garantizar la calidad de la transmisión de voz y datos, las redes IP utilizadas y el sistema de comunicación deben cumplir ciertos requisitos de la LAN.

Requisitos LAN

La red de datos debe ser del tipo Ethernet:

- Se recomiendan como mínimo cables Cat.5 (cables de varios hilos blindados y sin blindar de hasta 100 MHz para la sección horizontal y vertical conforme a la especificación EN 50288).
- Compatibilidad para QoS: IEEE 802.1p, DiffServ (RFC 2474).
- Todos los puertos LAN activos deben admitir 100/1000 MBit/s y comunicación de dúplex completo.

Todos los sistemas de comunicación deben estar conectados mediante un conmutador o un puerto dedicado de un router. No se admite el uso de concentradores ni repetidores.

Conexiones de Payload con RTP (Realtime Transport Protocol) en un entorno LAN

El ancho de banda necesario para la transmisión de voz en una red IP se puede calcular con ayuda de la siguiente tabla:

Tipo de códec	Parámetro de empaquetado	Tasa de muestreo de sonido (ms)	Carga útil (bytes)	Longitud de paquete Ethernet (bytes)	Carga útil de paquete (carga general en porcentaje)	Carga Ethernet (con encabezado) (kbps)
G.711	20	20	160	230	44%	92
G.711	30	30	240	310	29%	82,7
G.711	40	40	320	390	22%	78
G.711	60	60	480	550	15%	73,3
G.729A	1	20	20	90	350%	36
G.729A	2	40	40	110	175%	22
G.729A	3	60	60	130	117%	17,3
RTCP		5000		280		0,4

La carga de la LAN es válida para la dirección de envío y recepción.

El cálculo incluye el etiquetado VLAN según IEEE 802 1q. Sin etiquetado VLAN, la longitud de un paquete es 4 bytes más corta.

La carga general se calcula de esta forma:

Protocolo	Bytes
Encabezado RTP	12
Encabezado UDP	8
Encabezado IP	20

Protocolo	Bytes
802.1Q VLAN Tagging	4
MAC (con preámbulo, FCS)	26
Suma	70

Transporte de carga útil en el entorno LAN T.38:

	Tasa de muestreo de sonido (ms)	Carga útil (bytes)	Longitud de paquete Ethernet (bytes)	Carga útil de paquete (carga general en porcentaje)	Carga Ethernet (con encabezado) (kbps)
T.38	30	169	227	34%	60,5

Conexiones de Payload con SRTP (Secure Realtime Transport Protocol) en un entorno LAN:

Tipo de códec	Tasa de muestreo de sonido (ms)	Carga útil (bytes)	Longitud de paquete Ethernet (bytes)	Longitud del paquete Ethernet SRTP (kbps)	Longitud del paquete Ethernet RTP (kbps	Ancho de banda adicional con SRTP (%)
G.711	20	160	244	97,6	92	6,1
G.711	30	240	324	86,4	82,4	4,5
G.711	40	320	404	80,8	78	3,6
G.711	60	480	564	75,2	73,3	2,5
G.729A	20	20	104	41,6	36	15,6
G.729A	40	40	124	24,8	22	12,7
G.729A	60	60	144	19,2	17,3	10,8

21.4.2 Plan de numeración en la red

El plan de numeración es un requisito previo importante para la interconexión. En función del plan de numeración la configuración de la interred puede ser más o menos costosa. Por norma general, Open Scape Business admite en la interred la numeración abierta y cerrada, aunque solo se pueden utilizar todas las funciones UC con la numeración cerrada.

Numeración cerrada

En la numeración cubierta (cerrada) los usuarios se identifican en la interred de forma inequívoca a través del número de teléfono de extensión. Todos los usuarios de la interred pueden acceder a cualquier otra extensión marcando directamente su número de teléfono.

La numeración cubierta ofrece la ventaja de no tener que marcar ningún número de teléfono de nodo para acceder a una extensión de otro sistema de comunicación en red.

Tabla 10: Ejemplo de numeración cubierta

	Nodo 1	Nodo 2	Nodo 3	Nodo 4
Números de teléfono	100	200	300	400
	101	201	301	401
	102	202	302	402
	103	203	303	403
	104	204	304	404

Numeración abierta

En la numeración abierta una extensión se identifica de forma inequívoca con el número de teléfono de nodo y el número de teléfono de extensión. De esta forma, las extensiones de distintos sistemas de comunicación (nodos) de la interred pueden tener el mismo número de teléfono de extensión.

En la numeración descubierta siempre hay que marcar, junto con el número de teléfono de la extensión, el número de teléfono de nodo. Para ello, las áreas de número de teléfono se pueden utilizar varias veces, y se pueden utilizar más números de teléfono.

Si se utiliza numeración abierta, no se admiten las siguientes prestaciones de UC:

- UC Smart
- UC Suite
- CSP a nivel de red (CSTA Service Provider)
- Servidor DSS
- CMD (CSTA Message Dispatcher)

Tabla 11: Ejemplo de numeración abierta:

	Nodo 1	Nodo 2	Nodo 3	Nodo 4
Número de teléfono de nodo (número de teléfono del sistema)	15	96	97	98
Números de teléfono	100	100	100	100
	101	101	101	101
	102	102	102	102
	103	103	103	103
	104	104	104	104

21.4.2.1 Marcación de números de teléfono públicos en la red

Sea cual sea el tipo de numeración que se utilice (abierta o cerrada) es recomendable marcar destinos internos del nodo y destinos internos de red a

través de números de teléfono públicos (por ejemplo, cuando un cliente marca contactos en formato totalmente cualificado desde directorios).

21.5 Optimización de rutas (Path Replacement)

La optimización de rutas (Path Replacement) permite evitar la doble ocupación de líneas IP en los sistemas de red interconectados.

Si hay interconectados varios sistemas OpenScape Business, pueden surgir los siguientes problemas, por ejemplo: La extensión A llama a la extensión B, pero esta desvía sus llamadas a la extensión C. Las extensiones A y C están conectadas en el mismo nodo de red, pero la extensión B está conectada a otro nodo. De esta forma, la llamada con desvío ocupa dos líneas entre ambos nodos de red. Para evitar esta ocupación por duplicado se debería activar la optimización de rutas.

Consejo: El flag del sistema para la optimización de rutas se debe activar en todos los sistemas OpenScape Business interconectados.

: Se recomienda encarecidamente no utilizar la función Path Replacement en redes donde se utilicen extensiones de fax analógicas. Esta limitación se abordará en la próxima versión de software.

La optimización de rutas se realiza:

- En la sección de red de OpenScape Business
- Tras el establecimiento de conexión (no en la fase de llamada)
- Tras escenarios de transferencia
- Tras una transferencia automática diferida o desvío de llamadas

La optimización de rutas no se realiza:

- Con timbre adicional o llamada de grupo
- Con conferencias
- Si durante la ejecución de la optimización de rutas se activa otra prestación, se interrumpe la optimización.
- En una interconexión no homogénea, los sistemas externos se configuran mediante interconexión SIP. En este caso (sea cual sea la configuración del flag) no se puede proceder a la sustitución de ruta (Path Replacement, p. ej., OpenScape 4000, OpenScape Voice, servidor SIP externo).

21.5.1 Cómo activar o desactivar la optimización de rutas (Path Replacement)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Sistema** > **Flags del sistema**.
4) Elija una de estas opciones:
   - Si desea permitir la telecaptura de llamadas recordatorias, active la casilla de verificación **Optimización de rutas**.
   - Si no desea permitir la telecaptura de llamadas recordatorias, desactive la casilla de verificación **Optimización de rutas**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6 Escenarios de interconexión

Los sistemas OpenScape Business se pueden interconectar entre sí y con otros sistemas de comunicación de diferentes formas.

- Interconexión de varios OpenScape Business X
- Interconexión de OpenScape Business X y OpenScape Business S (Gateway único)
- Interconexión de OpenScape Business X y OpenScape Business S (multigateway)
- Interconexión de OpenScape Business S en un entorno de hosting
- Interconexión de OpenScape Business X y OpenScape 4000
- Interconexión de OpenScape Business X y OpenScape Voice
- Conectar equipo auxiliar externo con OpenScape Business mediante la interconexión SIP
- Numeración abierta en redes OpenScape Business X
- Interconexión mediante RDSI
- Interred OpenScape Business con conexión central de línea urbana ITSP

Los detalles de llamada solo se pueden consultar por nodo de red, no a nivel de varios nodos.

21.6.1 Interdependencias y restricciones

En los escenarios de interconexión posibles hay que tener en cuenta algunas interdependencias y restricciones.

Interdependencias y restricciones

- Cada sistema de la interred está asignado a una zona horaria propia. De esta forma, todas las extensiones de un sistema tienen la misma zona horaria.
- Solo se pueden utilizar interconexiones multigateway OpenScape Business S dentro de un país (misma zona horaria, mismo código de acceso a línea urbana).
- Por norma general, todas las interredes de OpenScape Business se configuran mediante asistentes. OpenScape Voice y OpenScape 4000 se configuran en la interconexión de cada nodo a través del Modo Experto.

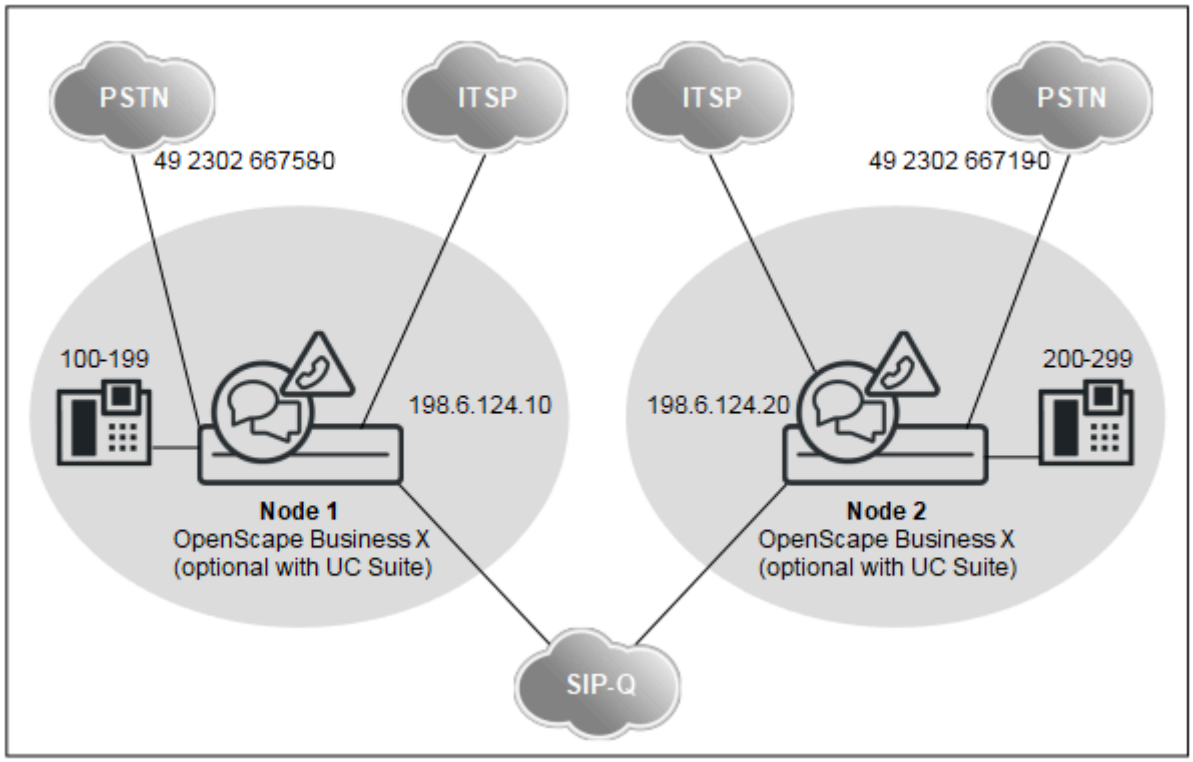
- El Gestor de presencia (funciones de servidor DSS = indicación a nivel de red de estados de ocupado en teclas DSS + telecaptura de llamadas) está disponible en redes OpenScape Business.
- Se utilizan líneas SIP-Q con la ruta 16 (última ruta) para configurar sistemas OpenScape Business homogéneos mediante el asistente **Configuración de red**. Para la interconexión de OpenScape 4000, OpenScape Voice u otros sistemas de comunicación se utilizan líneas SIP externas (SIP interconnection); la configuración se realiza en el Modo Experto.
- Si el sistema se configura como maestro o como esclavo mediante el asistente **Configuración de red**, se comprueba si hay asignadas líneas a la ruta "Redes". Si no es así, se asignan 16 líneas automáticamente a esa ruta. Si el sistema se retira de la interred, se mantienen las asignaciones.
- En cada no nodo solo se puede utilizar UN sistema de mensajería de voz. Por norma general, en una interred OpenScape Business se pueden utilizar distintos sistemas de buzón de voz:
  - Si se utiliza la UC Suite, el administrador debe desactivar otros sistemas de mensajería vocal que pudiera haber presentes en la interred.
  - Una interred HiPath 3000 con distintos sistemas de buzón de voz se puede migrar a OpenScape Business en forma 1:1.
- Por motivos técnicos, los sistemas OpenScape Business X1 no se pueden configurar como maestros. Como en cada red OpenScape Business se requiere un sistema maestro, al menos un sistema debe ser mayor que X1.

Consejo: El límite de ventas puede ser diferente a estos datos (y de los que se ofrecen en los distintos escenarios). Siga las indicaciones de la información de ventas.

21.6.2 Interconexión de varios OpenScape Business X

Se pueden interconectar entre sí hasta 32 sistemas de comunicación OpenScape Business X.

Datos de red



- Con solución de UC (UC Smart o UC Suite): solo numeración cerrada
- Sin solución de UC: numeración abierta o cerrada
- Configuración mediante la Gestión basada en Web (WBM) (asistentes) con numeración cerrada
- Las funciones de UC Suite se basan en el UC Booster Server o la UC Booster Card
- Hasta 32 sistemas interconectados y 1500 usuarios sin solución de UC
- Hasta 8 sistemas interconectados y 1500 usuarios con solución de UC

Prestaciones a nivel de red

Interconexión UC	Numeración cerrada	Numeración abierta
Número máximo de nodos	8 (solución de UC) y 32 (sin solución de UC)	
Número máximo de extensiones en un sistema de comunicación	En función de OpenScape Business X	
Número máximo de extensiones en la red	1500	

Interconexión UC	Numeración cerrada	Numeración abierta
UC Booster Card	UC Smart: 51 - 150 extensiones (0 - 50 extensiones sin UC Booster Card) UC Suite: 0 - 150 extensiones	No compatible
UC Booster Server	UC Smart: desde 15 extensiones UC Suite: desde 15 extensiones	No compatible

Administración	Numeración cerrada	Numeración abierta
WBM	Administración a nivel de red con asistentes	Administración a nivel de red, Modo Experto
Manager E	Administración a nivel de red para tareas especiales	Administración a nivel de red para tareas especiales
Administración de UC Suite (para UC Booster Server y UC Booster Card)	Administración a nivel de red con asistentes	No compatible
Importación masiva de datos mediante archivos csv (números de teléfono, números de marcación directa, nombres)	Independiente para cada nodo de la interred	

Registro de licencia	Numeración cerrada	Numeración abierta
Estructura de licencias	Se requiere una licencia de interconexión por cada nodo	

Configuración

Esta configuración (con numeración cerrada y UC Suite) muestra a través de un ejemplo qué pasos hay que seguir para configurar una interconexión.

Requisitos:

- Hay un plan de interconexión. A través del plan de interconexión se garantiza que todos los números de teléfono internos de la interred solo se asignen una vez en caso de numeración oculta. Se pueden utilizar distintas longitudes de números de teléfono. Solo los números de marcación directa pueden aparecer varias veces (por ejemplo, los números de línea urbana 49 2302 66758 100 y 49 2302 66719 100 tienen el mismo número de marcación directa 100).

  Consejo: Si es necesario, hay que adaptar los números de teléfono. No se ha implementado una numeración abierta.

- La red IP está configurada y todos los nodos pueden ponerse en comunicación entre sí por el ping
- Todos los nodos tienen la misma versión de software

Desvíos de llamada a nivel de nodo: si se producen llamadas entrantes mediante tronqueos de IP ya desviados, no se ejecutan otros desvíos al buzón de voz. El motivo es que, de lo contrario, no se puede realizar una asignación unívoca al buzón de voz

Si se desea utilizar reglas de representación a nivel de nodo, se deben configurar a través de los perfiles de las extensiones OpenScape Business o de conmutaciones de llamadas. En este caso, las llamadas a nivel de nodo no se señalizan como de desvío, sino como llamadas directas y, así, los desvíos de llamada del representante se desvían al buzón de voz.

Tabla 12: Configuración de los datos de ubicación para el nodo 1

Nodo 1	
G.-País de la ubicación	49
G.-Red local de la ubicación	2302

Nodo 1		
G.-Instalación de la ubicación		66758
Prefijo internacional		00
Prefijo nacional		0
Rutas		
RDSI	Código urbano	0
Redes	2° AKZ	0
Parámetros de ruta		
Ruta	Tipo de número de llamada, saliente	Tipo RNR
Redes	Desconocido	int/marcación directa
RDSI	(No se modifica la entrada)	N.° llam. marc. directa

En las tablas de encaminamiento se registran automáticamente los números de teléfono de todas las extensiones que están fuera del nodo 1 y los números de teléfono internos y los números de marcación directa que no coinciden con los números de teléfono internos correspondientes.

Tabla 13: Visión general de las entradas de LCR para el nodo 1

Plan de marcación		Tabla de rutas			Regla de marcación		
Nombre	**Cifras marcadas**	**Ruta**	**Gateway dedicado**	**ID de gateway**	**Regla de marcación**	**Procedimiento**	**Tipo**
Nodo 2 Internacional	0C0049230266719-Z	Redes	Obligatorio	2	D49230266719E3A	Corp. Red	Internacional
Nodo 2 NAT	0C0230266719-Z						
Nodo 2 Ext.	0C66719-Z						
Línea urbana	0CZ	RDSI	No		A	Ofertante de red principal	Desconocido
Diverso	-Z	Redes	No		A	Corp. Red	Desconocido

Tabla 14: Configuración de los datos de ubicación para el nodo 2

Nodo 2	
G.-País de la ubicación	49
G.-Red local de la ubicación	2302
G.-Instalación de la ubicación	66719
Prefijo internacional	00
Prefijo nacional	0
Rutas	

Nodo 2		
RDSI	Código urbano	0
Redes	2° AKZ	0
Parámetros de ruta		
Ruta	Tipo de número de llamada, saliente	Tipo RNR
Redes	Desconocido	int/marcación directa
RDSI	(No se modifica la entrada)	N.° llam. marc. directa

En las tablas de encaminamiento se registran automáticamente los números de teléfono de todas las extensiones que están fuera del nodo 2. y los números de teléfono internos y los números de marcación directa que no coinciden con los números de teléfono internos correspondientes.

Tabla 15: Visión general de las entradas de LCR para el nodo 2

Plan de marcación		**Tabla de rutas**			**Regla de marcación**		
Nombre	**Cifras marcadas**	**Ruta**	**Gateway dedicado**	**ID de gateway**	**Regla de marcación**	**Procedimiento**	**Tipo**
Nodo 1 Internacional	0C0049230266758-Z	Redes	Obligatorio	1	D49230266758E3A	Corp. Red	Internacional
Nodo 1 NAT	0C0230266758-Z						
Nodo 1 Ext.	0C66758-Z						
Línea urbana	0CZ	RDSI	No		A	Ofertante de red principal	Desconocido
Diverso	-Z	Redes	No		A	Corp. Red	Desconocido

Procedimiento de configuración de la interconexión:

1) Configuración de la instalación básica para el nodo 1 (maestro)
2) Configuración de interconexión para el nodo 1
3) Configuración de la instalación básica para el nodo 2 (esclavo)
4) Configuración de interconexión para el nodo 2
5) Control de la función de interconexión del maestro
6) Comprobación de direcciones y parámetros de ruta (maestro)
7) Comprobación de direcciones y parámetros de ruta (Ruta 16) (maestro)
8) Configuración de LCR para la interconexión (maestro)
9) Comprobación de direcciones y parámetros de ruta (esclavo)
10) Configuración de LCR para la interconexión (esclavo)

21.6.2.1 Cómo configurar la instalación básica para el nodo 1 (maestro)

Para la integración en una interred hay que asignar el prefijo de país y un ID de nodo. Los números de teléfono internos se deben configurar de forma unívoca.

Es importante indicar los números de teléfono nacionales y locales, ya que este número se configura en la ruta 1 de línea urbana RDSI y se utiliza para la normalización como número de teléfono de la ubicación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración básica**.
4) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo 49 para Alemania.
5) Introduzca el **Cód. local** y el **Número de teléfono del sistema**.
6) Active la casilla de verificación **Integración de red**.
7) En el campo **ID de nodo** para OpenScape Business, asigne un ID de nodo único en la interred (un "**1**" para el ejemplo de configuración).
8) Haga clic en **Ejecutar función**. Es conducido a la ventana **Funciones centrales para extensiones**.
9) En una red, todos los números de teléfono internos deben ser exclusivos. Por este motivo hay que borrar los números de teléfono estándar. Active el campo de opción **Borrar todos nos. llamada**.
10) Active la casilla de verificación **Borrar todos nos. llamada** y haga clic en **OK & Continuar**. Es conducido a la ventana **Cambiar números de función y de llamada preconfigurados**.

    Nota: Los códigos de función deben ser únicos en la interred. No puede haber números de teléfono duplicados.

11) Ajuste los números de teléfono preconfigurados a los números de teléfono de la red y haga clic en **OK & Continuar**. Los números de teléfono se pueden ajustar de forma manual a través del asistente. Como alternativa, también puede importar un archivo CSV con los números de teléfono correspondientes.
12) Ahora, configure los clientes IP.
13) Cambie los ajustes de configuración de las conferencias MeetMe. Debe indicar un código único en la interred.
14) A continuación, configure el envío de correo electrónico.
15) Haga clic en **Salir**.

21.6.2.2 Cómo configurar la interconexión para el nodo 1 (maestro)

En el siguiente paso se configura el asistente para la interconexión.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de red**.
4) Seleccione el ajuste **Red nativa con OSBiz X / OSBiz S**.
5) Defina el tipo de nodo (**Maestro**).
6) En **NodeId**, introduzca los números de nodo correspondientes de los sistemas OpenScape Business correspondientes (en el ejemplo de configuración, los del esclavo con el ID de nodo 2).
7) En **Dirección IP**, introduzca las direcciones IP de los sistemas OpenScape Business correspondientes (en el ejemplo de configuración, la del esclavo con el ID de nodo 2).
8) En **Nombre**, introduzca el tipo correspondiente del sistema secundario.
9) Si es necesario, active la casilla de verificación **Cifrado**.

Consejo: El cifrado se basa en SPE y no es válido para las aplicaciones.

Nota: Al activar la casilla de verificación no se configura el cifrado. Véase Cifrado de señalización y carga útil (SPE) .

10) Haga clic en **Salir**.

21.6.2.3 Cómo configurar la instalación básica para el nodo 2 (esclavo)

Para la integración en una interred hay que asignar el prefijo de país y un ID de nodo. Los números de teléfono internos se deben configurar de forma unívoca. Es importante indicar los números de teléfono nacionales y locales, ya que este número se configura en la ruta 1 de línea urbana RDSI y se utiliza para la normalización como número de teléfono de la ubicación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo 49 para Alemania.
4) Registre el **Cód. local** y el **Número de teléfono del sistema**.
5) Active la casilla de verificación **Integración de red**.
6) En el campo **ID de nodo** para OpenScape Business S, asigne un ID de nodo único en la interred (un "**2**" para el ejemplo de configuración).
7) Haga clic en **Ejecutar función**. Es conducido a la ventana **Funciones centrales para extensiones**.

8) En una red, todos los números de teléfono internos deben ser exclusivos. Por este motivo hay que borrar los números de teléfono estándar. Active el campo de opción **Borrar todos nos. llamada**.
9) Active la casilla de verificación **Borrar todos nos. llamada** y haga clic en **OK & Continuar**. Es conducido a la ventana **Cambiar números de función y de llamada preconfigurados**.

Nota: Los códigos de función deben ser únicos en la interred. No puede haber números de teléfono duplicados.

10) Ajuste los números de teléfono preconfigurados a los números de teléfono de la red y haga clic en **OK & Continuar**. Los números de teléfono se pueden ajustar de forma manual a través del asistente. Como alternativa, también puede importar un archivo CSV con los números de teléfono correspondientes.
11) Ahora, configure los clientes IP.
12) Cambie los ajustes de configuración de las conferencias MeetMe. Debe indicar un código único en la interred.
13) A continuación, configure el envío de correo electrónico.
14) Haga clic en **Salir**.

21.6.2.4 Cómo configurar la interconexión para el nodo 2 (esclavo)

En el siguiente paso se configura el asistente para la interconexión.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de red**.
4) Seleccione el ajuste **Red nativa con OSBiz X / OSBiz S**.
5) En **Tipo de nodo**, active la casilla **El sistema es un nodo ESCLAVO**.
6) En **Dirección IP** introduzca la dirección IP del maestro.

Consejo: Después de hacer clic en **OK&Continuar** la acción ya no se puede deshacer.

7) El **Estado de registro** se muestra con **Estado correcto** (o con el mensaje de error correspondiente). Con ello concluye el asistente.
8) Haga clic en **Salir**.

21.6.2.5 Cómo controlar la función de interconexión del maestro

Puede controlar el estado de la interconexión de forma general y para los distintos números de teléfono.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Red**.
2) En la línea de estado puede ver el **Estado de sincronización** de la red. Verde indica que la interconexión no tiene ningún problema, el color rojo indica problemas en la red.
3) En la ventana **Red**, marque la pestaña **Vista de dominios**. Se mostrarán todos los nodos disponibles con **ID de nodo**, **Nombre**, **Tipo de sistema**, **Dirección de servidor**, **Estado de registro** y **Disponibilidad**.
4) En la ventana **Red**, marque la pestaña **Números de teléfono**. Se abrirá una ventana con todos los datos sobre:
   - **Número de teléfono**
   - **N.° llam. marc. directa**
   - **Nombre**
   - **Tipo de puerto**
   - **Nodo**

21.6.2.6 Cómo configurar parámetros de ruta y rutas (línea urbana RDSI para el maestro)

Los siguientes pasos permiten configurar las rutas para la interconexión del maestro.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/ Interconexión**.
3) En el grupo de menús, haga clic en **Ruta**.
4) En la ventana **Cambiar ruta**, y en el campo **Nombre de ruta**, introduzca un nombre `Ruta 1` para la ruta de línea urbana.
5) En **Códigos de ruta**, introduzca el `0`.
6) En **Número de teléfono del sistema-entrante** y en el campo **Prefijo del país** introduzca el `49`.
7) En **Número de teléfono del sistema-entrante**, y en el campo **Código de red local**, introduzca el `2302`.
8) En **Número de teléfono del sistema-entrante**, y en el campo **Número de teléfono del sistema**, introduzca el `66758`.
9) Marque la casilla de verificación de **Número de teléfono del sistema-entrante** en el campo **Número emplazamiento**.
10) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.2.7 Cómo configurar direcciones y parámetros de ruta (Ruta 16) (maestro)

Para la dirección 16 (red) debe cumplimentarse la entrada para el segundo código urbano para maestro y esclavo. La ruta 16 es la ruta estándar para la interconexión en OpenScape Business.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en la última **Ruta** (**Ruta 16**).
4) En la ventana **Cambiar ruta**, y en el campo **Nombre de ruta**, introduzca un nombre `Red` para la ruta de interconexión.
5) En **Códigos de ruta** no introduzca nada.
6) En **Código urbano (2º AKZ)** , introduzca el 0.
7) Se pueden aplicar los ajustes de configuración estándar para los parámetros de ruta (tipo de número, saliente, tipo de número de llamada).
8) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.2.8 Cómo configurar LCR para la interconexión (maestro)

En el plan de marcación LCR hay que completar las entradas estándar de los índices 32, 33 y 34 con nuevas entradas para la marcación de números de teléfono en el formato "Internacional, Nacional y Extensiones" para el nodo 2. "Internacional" y "Nacional" siempre son necesarias. "Extensiones" es necesaria para los nodos de colateral que se encuentran en la misma red local. Estos datos se utilizan para la marcación desde aplicaciones (por ejemplo, myPortal for Desktop).

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.
3) En el grupo de menús, haga clic en **Plan de marcación**.
4) Introduzca los siguientes valores en puestos libres (aquí del 35 al 37) según los valores estándar:

Plan de marcación	Nombre	Cifras marcadas	Tabla de rutas
32	Estándar	88CZ	1
33	Red IP	-Z	13
34	COInternat	0C0049-Z	14
35	Nodo 2 Inter	0C0049230266719-Z	16

Plan de marcación	Nombre	Cifras marcadas	Tabla de rutas
36	Nodo 2 Nat	0C0230266719-Z	16
37	Nodo 2 Ext.	0C66719-Z	16

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
6) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 2.
   a) En **Nombre de regla**, introduzca la entrada **Nodo 2**.
   b) En **Formato de regla de marcación**, seleccione la entrada **D49230266719E3A**.
   c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
   d) En **Tipo**, seleccione la entrada **Prefijo del país**.
   e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
7) En el grupo de menús, haga clic en **Tabla rutas**.
8) Haga clic en la tabla de rutas 16.
   a) En **Dirección**, seleccione la opción **Networking**.
   b) En **Regla de marcación**, seleccione la opción **Nodo 2**.
   c) En **Clase mín.**, seleccione la opción **15**.
   d) En **Advertencia**, seleccione la opción **Ninguna**.
   e) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
   f) En **ID de nodo GW**, seleccione la opción **2**.
   g) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.2.9 Cómo configurar la dirección y parámetros de ruta (esclavo)

Los siguientes pasos permiten configurar la dirección y los parámetros de ruta para la interconexión del esclavo.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/ Interconexión**.
3) En el grupo de menús, haga clic en **Ruta**.
4) En la ventana **Cambiar ruta**, y en el campo **Nombre de ruta**, introduzca un nombre `Ruta 1` para la ruta de interconexión.
5) En **Códigos de ruta**, introduzca el `0`.
6) En **Número de teléfono del sistema-entrante** y en el campo **Prefijo del país** introduzca el `49`.
7) En **Número de teléfono del sistema-entrante**, y en el campo **Código de red local**, introduzca el `2302`.
8) En **Número de teléfono del sistema-entrante**, y en el campo **Número de teléfono del sistema**, introduzca el `66719`.

9) Marque la casilla de verificación de **Número de teléfono del sistema-entrante** en el campo **Número emplazamiento**.
10) Se pueden aplicar los ajustes predeterminados para los parámetros de ruta (tipo de número, saliente, tipo de número de llamada).
11) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.2.10 Cómo configurar LCR para la interconexión (esclavo)

En el plan de marcación LCR hay que completar las entradas estándar de los índices 32, 33, 34 y 35 con nuevas entradas para la marcación de números de teléfono en el formato "Internacional, Nacional y Extensiones" para el nodo 2. "Internacional" y "Nacional" siempre son necesarias. "Extensiones" es necesaria para los nodos de colateral que se encuentran en la misma red local. Estos datos se utilizan para la marcación desde aplicaciones (por ejemplo, myPortal for Desktop).

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.
3) En el grupo de menús, haga clic en **Plan de marcación**.
4) Introduzca los siguientes valores en puestos libres (aquí del 35 al 37) según los valores estándar:

Plan de marcación	Nombre	Cifras marcadas	Tabla de rutas
32	Estándar	88CZ	1
33	Red IP	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 1 Inter	0C0049230266758-Z	16
37	Nodo 1 Nat	0C00230266758-Z	16
38	Nodo 1 Ext.	0C66758-Z	16

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
6) En el grupo de menús, haga clic en **Regla de marcación** para el **Nodo 2**.
   a) En **Nombre de regla**, introduzca la entrada **Nodo 1**.
   b) En **Formato de regla de marcación**, seleccione la entrada **D49230266758E3A**.
   c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
   d) En **Tipo**, seleccione la entrada **Prefijo del país**.
   e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

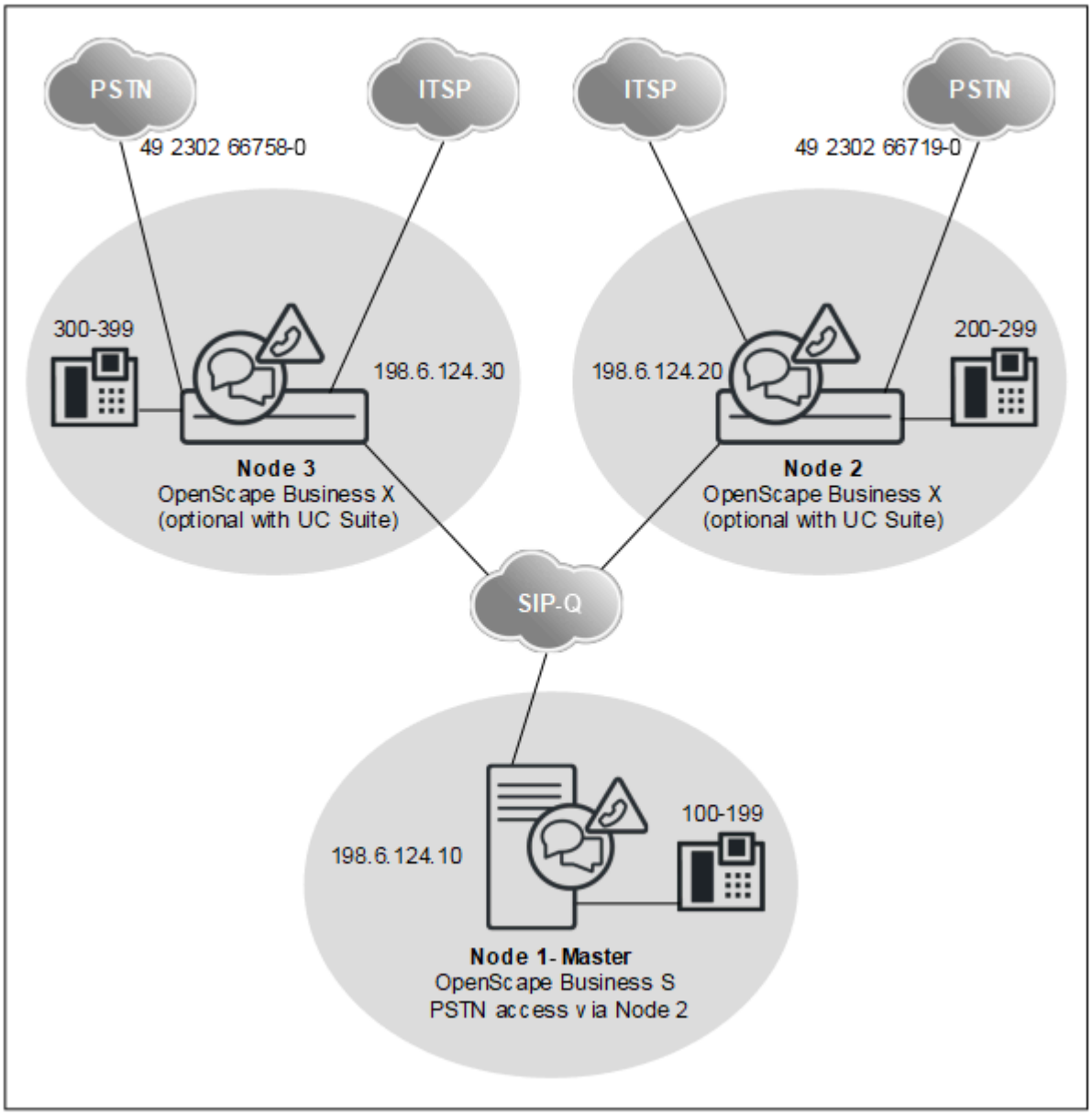
7) Haga clic en la tabla de rutas 16.
   a) En **Dirección**, seleccione la opción **Networking**.
   b) En **Regla de marcación**, seleccione la opción **Nodo 1**.
   c) En **Clase mín.**, seleccione la opción **15**.
   d) En **Advertencia**, seleccione la opción **Ninguna**.
   e) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
   f) En **ID de nodo GW**, seleccione la opción **2**.
   g) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

8) En el grupo de menús, haga clic en **Tabla rutas**.

21.6.3 Interconexión de OpenScape Business X con OpenScape Business S (Gateway único)

Se pueden interconectar entre sí hasta 32 sistemas de comunicación OpenScape Business X/S. En una interred puede haber varios OpenScape Business S. Con Gateway único, todas las extensiones IP registradas en OpenScape Business S utilizan solo UN gateway para el PSTN o ITSP.

Datos de red



- Numeración cerrada
- Funciones de UC y de voz a nivel de red con configuración de UC Suite mediante la Gestión basada en Web (WBM) (asistentes)
- Las funciones de UC se implementan mediante el UC Booster Server o la UC Booster Card
- En la interred puede haber varios OpenScape Business S.
- Hasta 32 sistemas interconectados y 1500 usuarios sin solución de UC
- Hasta 8 sistemas interconectados y 1500 usuarios con solución de UC

Prestaciones a nivel de red

Interconexión UC	Numeración cerrada	Numeración abierta
Número máximo de nodos	8 (solución de UC) y 32 (sin solución de UC)	

Interconexión UC	Numeración cerrada	Numeración abierta
Número máximo de extensiones en un sistema de comunicación	En función de OpenScape Business X	
Número máximo de extensiones en la red	1500	

Interconexión UC	Numeración cerrada	Numeración abierta
UC Booster Card	UC Smart: 51 - 150 extensiones (0 - 50 extensiones sin UC Booster Card) UC Suite: 0 - 150 extensiones	No compatible
UC Booster Server	UC Smart: desde 15 extensiones UC Suite: desde 15 extensiones	No compatible

Administración	Numeración cerrada	Numeración abierta
WBM	Administración a nivel de red con asistentes	No compatible
Manager E	Administración a nivel de red para tareas especiales (no para OpenScape Business S)	No compatible
Administración de UC Suite (para UC Booster Server y UC Booster Card)	Administración a nivel de red con asistentes	No compatible
Importación masiva de datos mediante archivos csv (números de teléfono, números de marcación directa, nombres)	Independiente para cada nodo de la interred	No compatible

Registro de licencia	Numeración cerrada	Numeración abierta
Estructura de licencias	Se requiere una licencia de interconexión por cada nodo	No compatible

Configuración

Esta configuración (con numeración cerrada y UC Suite) muestra a través de un ejemplo qué pasos hay que seguir para configurar una interconexión.

Requisitos:

- Hay un plan de interconexión. A través del plan de interconexión se garantiza que todos los números de teléfono internos de la interred solo se asignen una vez en caso de numeración oculta. Se pueden utilizar distintas longitudes de números de teléfono. Solo los números de marcación directa pueden aparecer varias veces (por ejemplo, los números de línea urbana 49 2302 66758 100 y 49 2302 66719 100 tienen el mismo número de marcación directa 100).
- La red IP está configurada y todos los nodos pueden ponerse en comunicación entre sí por el ping

Desvíos de llamada a nivel de nodo: si se producen llamadas entrantes mediante tronqueos de IP ya desviados, no se ejecutan otros desvíos al buzón

de voz. El motivo es que, de lo contrario, no se puede realizar una asignación unívoca al buzón de voz

Si se desea utilizar reglas de representación a nivel de nodo, se deben configurar a través de los perfiles de las extensiones OpenScape Business o de conmutaciones de llamadas. En este caso, las llamadas a nivel de nodo no se señalizan como de desvío, sino como llamadas directas y, así, los desvíos de llamada del representante se desvían al buzón de voz.

En una interred en que se utilice el periodo de gracia, siempre se debe utilizar el CLA de OpenScape Business S como CLA central.

Debido a los diferentes límites superiores se requieren dos archivos de periodo de activación diferentes para OpenScape Business y OpenScape Business S. El archivo de periodo de activación para OpenScape Business S incluye la base para OpenScape Business además de la base S para los escenarios de red.

Si en este escenario de OpenScape Business se emite una solicitud de licencia a un CLA de OpenScape Business S en el periodo de activación, se utilizan los límites de OpenScape Business S.

Si, por el contrario, se utiliza el CLA de OpenScape Business, un OpenScape Business S que emitiera una consulta no recibiría NINGÚN periodo de gracia, ya que este archivo no incluye ninguna base para OpenScape Business S.

Tabla 16: Configuración de los datos de ubicación para el nodo 1 OpenScape Business S

Nodo 1		
G.-País de la ubicación		49
G.-Red local de la ubicación		2302
G.-Instalación de la ubicación		66719
Prefijo internacional		00
Prefijo nacional		0
Rutas		
Ruta 1	Código urbano	0
Redes	2° AKZ	0
Parámetros de ruta		
Ruta	Tipo de número de llamada, saliente	Tipo RNR
Redes	Desconocido	int/marcación directa
RDSI	(No se modifica la entrada)	N.° llam. marc. directa

En las tablas de encaminamiento se registran automáticamente los números de teléfono de todas las extensiones que están fuera del nodo 1 y los números de teléfono internos y los números de marcación directa que no coinciden con los números de teléfono internos correspondientes.

Tabla 17: Visión general de las entradas de LCR para el nodo 1

Plan de marcación		Tabla de rutas			Regla de marcación		
Nombre	**Cifras marcadas**	**Ruta**	**Gateway dedicado**	**ID de gateway**	**Regla de marcación**	**Procedimiento**	**Tipo**
Nodo 2 Internacional	0C0049230266719-2Z	Redes	Obligatorio	2	D49230266719E3A	Corp. Red	Internacional
Nodo 2 NAT	0C0230266719-2Z						
Nodo 2 Ext.	0C66719-2Z						
Nodo 3 Internacional	0C0049230266758-3Z	Redes	Obligatorio	3	D49230266758E3A	Corp. Red	Internacional
Nodo 3 NAT	0C0230266758-3Z						
Nodo 3 Ext.	0C66758-3Z						
Línea urbana	0CZ	Redes	Obligatorio	2	E1A	Ofertante de red principal	Desconocido
Diverso	-Z	Redes	No		A	Corp. Red	Desconocido

Tabla 18: Configuración de los datos de ubicación para el nodo 2 OpenScape Business

Nodo 2		
G.-País de la ubicación		49
G.-Red local de la ubicación		2302
G.-Instalación de la ubicación		66719
Prefijo internacional		00
Prefijo nacional		0
Rutas		
RDSI	Código urbano	0
Redes	2° AKZ	0
Parámetros de ruta		
Ruta	Tipo de número de llamada, saliente	Tipo RNR
Redes	Desconocido	int/marcación directa
RDSI	(No se modifica la entrada)	N.° llam. marc. directa

En las tablas de encaminamiento se registran automáticamente los números de teléfono de todas las extensiones que están fuera del nodo 2. y los números de teléfono internos y los números de marcación directa que no coinciden con los números de teléfono internos correspondientes.

Tabla 19: Visión general de las entradas de LCR para el nodo 2

Plan de marcación		Tabla de rutas			Regla de marcación		
Nombre	**Cifras marcadas**	**Ruta**	**Gateway dedicado**	**ID de gateway**	**Regla de marcación**	**Procedimiento**	**Tipo**
Nodo 1 Internacional	0C0049230266719-1Z	Redes	Obligatorio	1	D49230266719E3A	Corp. Red	Internacional
Nodo 1 NAT	0C0230266719-1Z						
Nodo 1 Ext.	0C66719-1Z						
Nodo 3 Internacional	0C0049230266758-3Z	Redes	Obligatorio	3	D49230266758E3A	Corp. Red	Internacional
Nodo 3 NAT	0C0230266758-3Z						
Nodo 3 Ext.	0C66758-3Z						
Línea urbana	0CZ	RDSI	No		A	Ofertante de red principal	Desconocido
Diverso	-Z	Redes	No		A	Corp. Red	Desconocido

Tabla 20: Configuración de los datos de ubicación para el nodo 3 OpenScape Business

Nodo 3		
G.-País de la ubicación		49
G.-Red local de la ubicación		2302
G.-Instalación de la ubicación		66758
Prefijo internacional		00
Prefijo nacional		0
Rutas		
RDSI	Código urbano	0
Redes	2° AKZ	0
Parámetros de ruta		
Ruta	Tipo de número de llamada, saliente	Tipo RNR
Redes	Desconocido	int/marcación directa
RDSI	(No se modifica la entrada)	N.° llam. marc. directa

En las tablas de encaminamiento se registran automáticamente los números de teléfono de todas las extensiones que están fuera del nodo 3. y los números de teléfono internos y los números de marcación directa que no coinciden con los números de teléfono internos correspondientes.

Tabla 21: Visión general de las entradas de LCR para el nodo 3

Plan de marcación		Tabla de rutas			Regla de marcación		
Nombre	**Cifras marcadas**	**Ruta**	**Gateway dedicado**	**ID de gateway**	**Regla de marcación**	**Procedimiento**	**Tipo**
Nodo 1 Internacional	0C0049230266719-1Z	Redes	Obligatorio	1	D49230266719E3A	Corp. Red	Internacional
Nodo 1 NAT	0C0230266719-1Z						
Nodo 1 Ext.	0C66719-1Z						
Nodo 2 Internacional	0C0049230266719-2Z	Redes	Obligatorio	2	D49230266719E3A	Corp. Red	Internacional
Nodo 2 NAT	0C0230266719-2Z						
Nodo 2 Ext.	0C66719-2Z						
Línea urbana	0CZ	RDSI	No		A	Ofertante de red principal	Desconocido
Diverso	-Z	Redes	No		A	Corp. Red	Desconocido

Procedimiento de configuración de la interconexión:

1) Configuración de la instalación básica para el nodo 1 (maestro)
2) Configuración de interconexión para el nodo 1
3) Configuración de la instalación básica para el nodo 2 (esclavo)
4) Configuración de interconexión para el nodo 2
5) Configuración de la instalación básica para el nodo 3 (esclavo)
6) Configuración de la interconexión para el nodo 3 (esclavo)
7) Control de la función de interconexión del maestro
8) Configuración de LCR para la interconexión (nodo 1, maestro)
9) Cómo configurar LCR para la interconexión (nodo 2)
10) Configuración de direcciones y parámetros de ruta (nodo 3)
11) Configuración de direcciones y parámetros de ruta (Ruta 16) (nodo 3)
12) Configuración de LCR para la interconexión (nodo 3)

21.6.3.1 Cómo configurar la instalación básica para el nodo 1 (maestro)

Para la integración en una interred hay que asignar el prefijo de país y un ID de nodo. Los números de teléfono internos se deben configurar de forma unívoca. Es importante indicar los números de teléfono nacionales y locales, ya que este número se configura en la ruta 1 de línea urbana RDSI y se utiliza para la normalización como número de teléfono de la ubicación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo 49 para Alemania.
4) Introduzca el **Cód. local** y el **Número de teléfono del sistema**.
5) Active la casilla de verificación **Integración de red**.
6) En el campo **ID de nodo** para OpenScape Business S asigne un ID de nodo único en la interred. El ID de nodo debe estar entre "**1**" y "**100**" (seleccione "**1**" en el ejemplo de configuración).
7) Haga clic en **Ejecutar función**. Es conducido a la ventana **Funciones centrales para extensiones**.
8) En una red, todos los números de teléfono internos deben ser exclusivos. Por este motivo hay que borrar los números de teléfono estándar. Active el campo de opción **Borrar todos nos. llamada**.
9) Active la casilla de verificación **Borrar todos nos. llamada** y haga clic en **OK & Continuar**. Es conducido a la ventana **Cambiar números de función y de llamada preconfigurados**.

   Nota: Los códigos de función deben ser únicos en la interred. No puede haber números de teléfono duplicados.

10) Ajuste los números de teléfono preconfigurados a los números de teléfono de la red y haga clic en **OK & Continuar**. Los números de teléfono se pueden ajustar de forma manual a través del asistente. Como alternativa, también puede importar un archivo CSV con los números de teléfono correspondientes.
11) Importe los clientes IP.
12) A continuación, configure la telefonía Internet.
13) Cambie los ajustes de configuración de las conferencias MeetMe. Debe indicar un código único en la interred.
14) A continuación, configure el envío de correo electrónico.
15) Haga clic en **OK & Continuar**.
16) Haga clic en **Salir**.

21.6.3.2 Cómo configurar la interconexión para el nodo 1 (maestro)

En el siguiente paso se configura el asistente para la interconexión del nodo 1 (maestro).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.

3) Haga clic en **Editar** para iniciar el asistente **Configuración de red**.
4) Seleccione el ajuste **Red nativa con OSBiz X / OSBiz S**.
5) Defina el tipo de nodo (**Maestro**).
6) En **NodeId**, introduzca los números de nodo correspondientes de los sistemas OpenScape Business correspondientes (en el ejemplo de configuración, los del esclavo con el ID de nodo 2).
7) En **Dirección IP**, introduzca las direcciones IP de los sistemas OpenScape Business correspondientes (en el ejemplo de configuración las de los esclavos con el ID de nodo 2 y 3).
8) Active la casilla de verificación **Gateway**.
9) En **Nombre**, introduzca el tipo de sistema.
10) En **Tipo**, introduzca el tipo del sistema secundario.
11) Si es necesario, active la casilla de verificación **Cifrado**.

Consejo: El cifrado se basa en SPE y no es válido para las aplicaciones.

Nota: Al activar la casilla de verificación no se configura el cifrado. Véase Cifrado de señalización y carga útil (SPE) .

12) Haga clic en **Salir**.

21.6.3.3 Cómo configurar la instalación básica para el nodo 2 (esclavo)

Para la integración en una interred hay que asignar el prefijo de país y un ID de nodo. Los números de teléfono internos se deben configurar de forma unívoca. Es importante indicar los números de teléfono nacionales y locales, ya que este número se configura en la ruta 1 de línea urbana RDSI y se utiliza para la normalización como número de teléfono de la ubicación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo 49 para Alemania.
4) Registre el **Cód. local** y el **Número de teléfono del sistema**.
5) Active la casilla de verificación **Integración de red**.
6) En el campo **ID de nodo** para OpenScape Business asigne un ID de nodo único en la interred (un "**2**" y un "**3**" para el ejemplo de configuración).
7) Haga clic en **Ejecutar función**. Es conducido a la ventana **Funciones centrales para extensiones**.

8) En una red, todos los números de teléfono internos deben ser exclusivos. Por este motivo hay que borrar los números de teléfono estándar. Active el campo de opción **Borrar todos nos. llamada**.
9) Active la casilla de verificación **Borrar todos nos. llamada** y haga clic en **OK & Continuar**. Es conducido a la ventana **Cambiar números de función y de llamada preconfigurados**.

Nota: Los códigos de función deben ser únicos en la interred. No puede haber números de teléfono duplicados.

10) Ajuste los números de teléfono preconfigurados a los números de teléfono de la red y haga clic en **OK & Continuar**. Los números de teléfono se pueden ajustar de forma manual a través del asistente. Como alternativa, también puede importar un archivo CSV con los números de teléfono correspondientes.
11) Configure ahora las extensiones analógicas y RDSI.
12) Cambie los ajustes de configuración de las conferencias MeetMe. Debe indicar un código único en la interred.
13) A continuación, configure el envío de correo electrónico.
14) Haga clic en **OK & Continuar**.
15) Haga clic en **Salir**.

21.6.3.4 Cómo configurar la interconexión para el nodo 2 (esclavo)

En el siguiente paso se configura la interconexión del nodo 2 mediante el asistente.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de red**.
4) Seleccione el ajuste **Red nativa con OSBiz X / OSBiz S**.
5) En **Tipo de nodo**, active la casilla **El sistema es un nodo ESCLAVO**.
6) **Introduzca la dirección IP del nodo MAESTRO** (en el ejemplo de configuración, la dirección IP del nodo 1).

Consejo: Después de hacer clic en **OK&Continuar** la acción ya no se puede deshacer.

7) El **Estado de registro** se muestra con **Estado correcto** (o con el mensaje de error correspondiente). Con ello concluye el asistente.
8) Haga clic en **Salir**.

21.6.3.5 Cómo configurar la instalación básica para el nodo 3 (esclavo)

Para la integración en una interred hay que asignar el prefijo de país y un ID de nodo. Los números de teléfono internos se deben configurar de forma unívoca. Es importante indicar los números de teléfono nacionales y locales, ya que este número se configura en la ruta 1 de línea urbana RDSI y se utiliza para la normalización como número de teléfono de la ubicación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo 49 para Alemania.
4) Introduzca el **Cód. local** y el **Número de teléfono del sistema**. (idénticos al sistema de gateway asignado).
5) Active la casilla de verificación **Integración de red**.
6) En el campo **ID de nodo** para OpenScape Business, asigne un ID de nodo único en la interred (un "**3**" para el ejemplo de configuración).
7) Haga clic en **Ejecutar función**. Es conducido a la ventana **Funciones centrales para extensiones**.
8) En una red, todos los números de teléfono internos deben ser exclusivos. Por este motivo hay que borrar los números de teléfono estándar. Active el campo de opción **Borrar todos nos. llamada**.
9) Active la casilla de verificación **Borrar todos nos. llamada** y haga clic en **OK & Continuar**. Es conducido a la ventana **Cambiar números de función y de llamada preconfigurados**.

   Nota: Los códigos de función deben ser únicos en la interred. No puede haber números de teléfono duplicados.

10) Ajuste los números de teléfono preconfigurados a los números de teléfono de la red y haga clic en **OK & Continuar**. Los números de teléfono se pueden ajustar de forma manual a través del asistente. Como alternativa, también puede importar un archivo CSV con los números de teléfono correspondientes.
11) Configure ahora las extensiones analógicas y RDSI.
12) Cambie los ajustes de configuración de las conferencias MeetMe. Debe indicar un código único en la interred.
13) A continuación, configure el envío de correo electrónico.
14) Haga clic en **OK & Continuar**.
15) Haga clic en **Salir**.

21.6.3.6 Cómo controlar la función de interconexión del maestro

Puede controlar el estado de la interconexión de forma general y para los distintos números de teléfono.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Red**.
2) En la línea de estado puede ver el **Estado de sincronización** de la red. Verde indica que la interconexión no tiene ningún problema, el color rojo indica problemas en la red.
3) En la ventana **Red**, marque la pestaña **Vista de dominios**. Se mostrarán todos los nodos disponibles con **ID de nodo**, **Nombre**, **Tipo de sistema**, **Dirección de servidor**, **Estado de registro** y **Disponibilidad**.
4) En la ventana **Red**, marque la pestaña **Números de teléfono**. Se abrirá una ventana con todos los datos sobre:
   - **Número de teléfono**
   - **N.° llam. marc. directa**
   - **Nombre**
   - **Tipo de puerto**
   - **Nodo**

21.6.3.7 Configuración de la interconexión para el nodo 3 (esclavo)

En el siguiente paso, se configura la interconexión del nodo 3 mediante el asistente.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de red**.
4) Seleccione el ajuste **Red nativa con OSBiz X / OSBiz S**.
5) En **Tipo de nodo**, active la casilla **El sistema es un nodo ESCLAVO**.
6) **Introduzca la dirección IP del nodo MAESTRO** (en el ejemplo de configuración, la dirección IP del nodo 1).

   Consejo: Después de hacer clic en **OK&Continuar** la acción ya no se puede deshacer.

7) El **Estado de registro** se muestra con **Estado correcto** (o con el mensaje de error correspondiente). Con ello concluye el asistente.

8) Haga clic en **Salir**.

21.6.3.8 Cómo configurar LCR para la interconexión (nodo 3, esclavo)

En el plan de marcación LCR, las entradas predeterminadas de los índices 32, 33, 34 y 35 se deben completar con nuevas entradas para la marcación de números de teléfono con el formato "Internacional, Nacional y Extensiones" para los nodos 1 y 2. "Internacional" y "Nacional" siempre son necesarias. "Extensiones" es necesaria para los nodos de colateral que se encuentran en la misma red local. Deben completarse las entradas 36, 37 y 38 para la interconectividad con el nodo 1 (número de teléfono 100 > 199) y las entradas 39, 40 y 41 para la interconectividad con el nodo 2 (número de teléfono 200 > 299). Estos datos se utilizan para la marcación desde aplicaciones (por ejemplo, myPortal for Desktop).

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.

3) En el grupo de menús, haga clic en **Plan de marcación**.

4) Introduzca los siguientes valores en puestos libres (aquí del 35 al 40) según los valores estándar:

Plan de marcación	Nombre	Cifras marcadas	Tabla de rutas
31	Suite de aplicaciones	-371	12
32	Estándar	88CZ	1
33	Red IP	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 1 Inter	0C0049230266719-1Z	16
37	Nodo 1 Nat	0C0230266719-1Z	16
38	Nodo 1 Ext.	0C66719-1Z	16
39	Nodo 2 Inter	0C0049230266719-2Z	17
40	Nodo 2 Nat	0C0230266719-2Z	17
41	Nodo 2 Ext.	0C66719-2Z	17

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

6) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para los nodos 1 y 2.
   a) En **Nombre de regla**, introduzca la entrada **Nodo 1 + 2**.
   b) En **Formato de regla de marcación**, seleccione la entrada **D49230266719E3A**.
   c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
   d) En **Tipo**, seleccione la entrada **Prefijo del país**.
   e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
7) En el grupo de menús, haga clic en **Tabla rutas**, para configurar la tabla de rutas 16 para la conexión de red y asignarla al nodo 1 directo.
8) Haga clic en la tabla de rutas 16.
   a) En **Dirección**, seleccione la opción **Networking**.
   b) En **Regla de marcación**, seleccione la opción **Nodo 1 + 2**.
   c) En **Clase mín.**, seleccione la opción **15**.
   d) En **Advertencia**, seleccione la opción **Ninguna**.
   e) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
   f) En **ID de nodo GW**, seleccione la opción **1**.
   g) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
9) En el grupo de menús, haga clic en **Tabla rutas**, para configurar una tabla de rutas 17 para la conexión de red y asignarla al nodo 2 directo.
10) Haga clic en la tabla de rutas 17.
   a) En **Dirección**, seleccione la opción **Networking**.
   b) En **Regla de marcación**, seleccione la opción **Nodo 1 + 2**.
   c) En **Clase mín.**, seleccione la opción **15**.
   d) En **Advertencia**, seleccione la opción **Ninguna**.
   e) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
   f) En **ID de nodo GW**, seleccione la opción **2**.
   g) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.3.9 Cómo configurar LCR para la interconexión (nodo 2)

En el plan de marcación LCR, las entradas predeterminadas de los índices 32, 33, 34 y 35 se deben completar con nuevas entradas para la marcación de números de teléfono con el formato "Internacional, Nacional y Extensiones" para los nodos 1 y 3. "Internacional" y "Nacional" siempre son necesarias. "Extensiones" es necesaria para los nodos de colateral que se encuentran en la misma red local. Deben completarse las entradas 36, 37 y 39 para la interconectividad con el nodo 1 (número de teléfono 100 > 199) y las entradas 38, 40 y 41 para la interconectividad con el nodo 3 (número de teléfono 300 > 399). Estos datos se utilizan para la marcación desde aplicaciones (por ejemplo, myPortal for Desktop).

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.

3) En el grupo de menús, haga clic en **Plan de marcación**.

4) Introduzca los siguientes valores en puestos libres (aquí del 35 al 40) según los valores estándar:

Plan de marcación	Nombre	Cifras marcadas	Tabla de rutas
31	Suite de aplicaciones	-271	12
32	Estándar	88CZ	1
33	Red IP	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 1 Inter	0C0049230266719-1Z	16
37	Nodo 1 Nat	0C0230266719-1Z	16
38	Nodo 1 Ext.	0C66719-1Z	16
39	Nodo 3 Inter	0C0049230266758-3Z	17
40	Nodo 3 Nat	0C0230266758-3Z	17
41	Nodo 3 Ext.	0C66758-3Z	17

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

6) En el grupo de menús, haga clic en **Tabla rutas**.

7) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 1.

a) En **Nombre de regla**, introduzca la entrada **Nodo 1**.
b) En **Formato de regla de marcación**, seleccione la entrada **D49230266719E3A**.
c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
d) En **Tipo**, seleccione la entrada **Prefijo del país**.
e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

8) Haga clic en la tabla de rutas 16 para configurarla para la conexión de red con el nodo 1.

a) En **Dirección**, seleccione la opción **Networking**.
b) En **Regla de marcación**, seleccione la opción **Nodo 1**.
c) En **Clase mín.**, seleccione la opción **1**.
d) En **Advertencia**, seleccione la opción **Ninguna**.
e) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
f) En **ID de nodo GW**, seleccione la opción **1**.
g) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

9) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 3.

a) En **Nombre de regla**, introduzca la entrada **Nodo 3**.
b) En **Formato de regla de marcación**, seleccione la entrada **D49230266758E3A**.
c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
d) En **Tipo**, seleccione la entrada **Prefijo del país**.
e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10) En el grupo de menús, haga clic en **Tabla rutas**.

11) Haga clic en la tabla de rutas 17 para configurarla para la conexión de red con el nodo 3.

a) En **Dirección**, seleccione la opción **Networking**.
b) En **Regla de marcación**, seleccione la opción **Nodo 3**.
c) En **Clase mín.**, seleccione la opción **1**.
d) En **Advertencia**, seleccione la opción **Ninguna**.
e) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
f) En **ID de nodo GW**, seleccione la opción **3**.
g) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.3.10 Cómo configurar direcciones y parámetros de ruta (nodo 1, maestro)

En el nodo 1 es necesario configurar los ajustes para la dirección de línea urbana relativos a número emplazamiento, código de ruta y parámetros de ruta. Aquí se debe registrar el número de teléfono del sistema para la definición de la ubicación de gateway. Estos datos se utilizan para la marcación desde aplicaciones como, por ejemplo, myPortal.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/ Interconexión**.
3) En el grupo de menús, haga clic en **Ruta**.
4) En la ventana **Cambiar ruta**, y en el campo **Nombre de ruta**, introduzca un nombre `Ruta 1` para la ruta de línea urbana.
5) En **Códigos de ruta**, introduzca el `0`.
6) En **Número de teléfono del sistema-entrante** y en el campo **Prefijo del país** introduzca el `49`.
7) En **Número de teléfono del sistema-entrante**, y en el campo **Código de red local**, introduzca el `2302`.
8) En **Número de teléfono del sistema-entrante**, y en el campo **Número de teléfono del sistema**, introduzca el `66719`.
9) Marque la casilla de verificación de **Número de teléfono del sistema-entrante** en el campo **Número emplazamiento**.
10) Se pueden aplicar los ajustes predeterminados para los parámetros de ruta (tipo de número, saliente, tipo de número de llamada).
11) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.3.11 Cómo configurar direcciones y parámetros de ruta (Ruta 16) (Nodo 1)

Para la dirección 16 (red) debe cumplimentarse la entrada para el segundo código urbano para maestro y esclavo.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/Interconexión**.
3) En el grupo de menús, haga clic en la última **Ruta** (**Ruta 16**).
4) En la ventana **Cambiar ruta**, y en el campo **Nombre de ruta**, introduzca un nombre `Red` para la ruta de interconexión.
5) En **Códigos de ruta** no introduzca nada.
6) En **Código urbano (2º AKZ)** , introduzca el 0.
7) Se pueden aplicar los ajustes de configuración estándar para los parámetros de ruta (tipo de número, saliente, tipo de número de llamada).
8) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.3.12 Cómo configurar LCR para la interconexión (nodo 1)

En el plan de marcación LCR, las entradas predeterminadas de los índices 32, 33, 34 y 35 se deben completar con nuevas entradas para la marcación de números de teléfono con el formato "Internacional, Nacional y Extensiones" para los nodos 2 y 3. "Internacional" y "Nacional" siempre son necesarias. "Extensiones" es necesaria para los nodos de colateral que se encuentran en la misma red local. Estos datos se utilizan para la marcación desde aplicaciones (por ejemplo, myPortal for Desktop).

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.
3) En el grupo de menús, haga clic en **Plan de marcación**.
4) Introduzca los siguientes valores en puestos libres (aquí del 35 al 40) según los valores estándar:

Plan de marcación	Nombre	Cifras marcadas	Tabla de rutas
16	Estándar	0CZ	1
17	Estándar	0C1Z	1
18	Estándar	0CNZ	1
32	Estándar	88CZ	1
33	Red IP	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 2 Inter	0C0049230266719-2Z	16
37	Nodo 2 Nat	0C0230266719-2Z	16
38	Nodo 2 Ext.	0C66719-2Z	16
39	Nodo 3 Inter	0C0049230266758-3Z	17
40	Nodo 3 Nat	0C0230266758-3Z	17

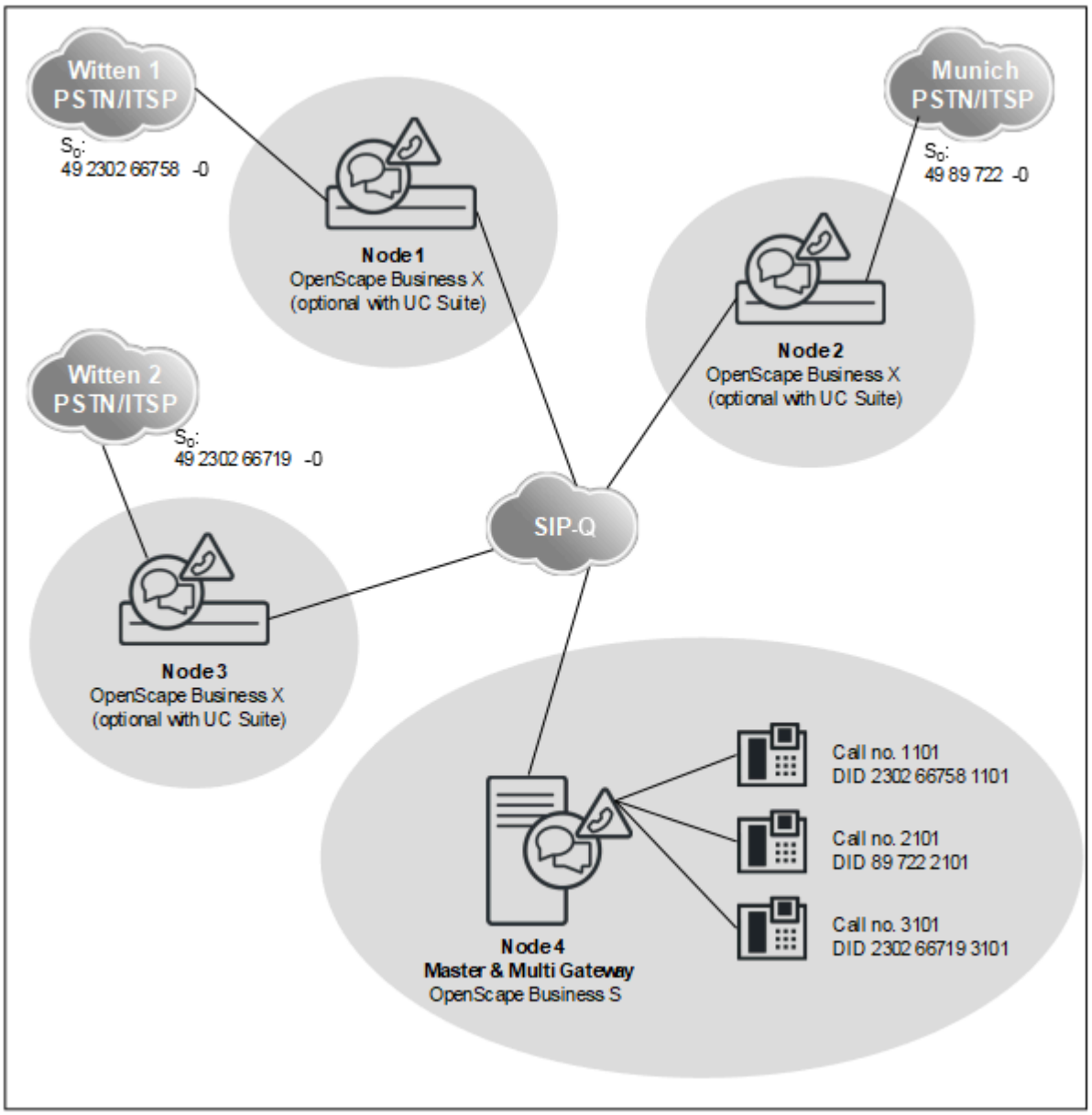
Plan de marcación	Nombre	Cifras marcadas	Tabla de rutas
41	Nodo 3 Ext.	0C66758-3Z	17

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
6) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 2.
   a) En **Nombre de regla**, introduzca la entrada **Nodo 2**.
   b) En **Formato de regla de marcación**, seleccione la entrada **D49230266719E3A**.
   c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
   d) En **Tipo**, seleccione la entrada **Prefijo del país**.
   e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
7) En el grupo de menús, haga clic en **Tabla rutas**.
8) Haga clic en la tabla de rutas 16 para configurarla para la conexión de red con el nodo 2.
   a) En **Dirección**, seleccione la opción **Networking**.
   b) En **Regla de marcación**, seleccione la opción **Nodo 2**.
   c) En **Clase mín.**, seleccione la opción **1**.
   d) En **Advertencia**, seleccione la opción **Ninguna**.
   e) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
   f) En **ID de nodo GW**, seleccione la opción **2**.
   g) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
9) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 3.
   a) En **Nombre de regla**, introduzca la entrada **Nodo 3**.
   b) En **Formato de regla de marcación**, introduzca la entrada **D49230266719E1A**.
   c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
   d) En **Tipo**, seleccione la entrada **Prefijo del país**.
   e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
10) En el grupo de menús, haga clic en **Tabla rutas**.
11) Haga clic en la tabla de rutas 17 para configurarla para la conexión de red con el nodo 3.
   a) En **Dirección**, seleccione la opción **Networking**.
   b) En **Regla de marcación**, seleccione la opción **Nodo 3**.
   c) En **Clase mín.**, seleccione la opción **1**.
   d) En **Advertencia**, seleccione la opción **Ninguna**.
   e) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
   f) En **ID de nodo GW**, seleccione la opción **3**.
   g) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
12) En el grupo de menús, haga clic en **Tabla rutas**.

21.6.4 Interconexión de OpenScape Business X y OpenScape Business S (multigateway)

Se pueden interconectar entre sí hasta 32 sistemas de comunicación OpenScape Business X y OpenScape Business S. Multigateway significa que todas las extensiones IP registradas en OpenScape Business S están asignadas a un gateway determinado.

Datos de red



- Numeración cerrada
- Funciones de UC y de voz a nivel de red con configuración de UC Suite mediante la Gestión basada en Web (WBM) (asistentes)
- Las funciones de UC se implementan mediante el UC Booster Server o la UC Booster Card
- En la interred solo puede haber un único sistema OpenScape Business S.

- Todos los sistemas tienen que usar el mismo código nacional
- Todos los sistemas tienen que estar en la misma zona horaria
- Solo puede haber un código de acceso a la línea urbana (p. ej. 0) en la red.
- Hasta 32 sistemas interconectados y 1500 usuarios sin solución de UC
- Hasta 8 sistemas interconectados y 1500 usuarios con solución de UC

Prestaciones a nivel de red

Interconexión UC	Numeración cerrada	Numeración abierta
Número máximo de nodos	8 (solución de UC) y 32 (sin solución de UC)	
Número máximo de extensiones en un sistema de comunicación	En función de OpenScape Business X	
Número máximo de extensiones en la red	1500	

Interconexión UC	Numeración cerrada	Numeración abierta
UC Booster Card	UC Smart: 51 - 150 extensiones (0 - 50 extensiones sin UC Booster Card) UC Suite: 0 - 150 extensiones	No compatible
UC Booster Server	UC Smart: desde 15 extensiones UC Suite: desde 15 extensiones	No compatible

Administración	Numeración cerrada	Numeración abierta
WBM	Administración a nivel de red con asistentes	No compatible
Manager E	Administración a nivel de red para tareas especiales (no para OpenScape Business S)	No compatible
Administración de UC Suite (para UC Booster Server y UC Booster Card)	Administración a nivel de red con asistentes	No compatible
Importación masiva de datos mediante archivos csv (números de teléfono, números de marcación directa, nombres)	Independiente para cada nodo de la interred	No compatible

Registro de licencia	Numeración cerrada	Numeración abierta
Estructura de licencias	Se requiere una licencia de interconexión por cada nodo	No compatible

Configuración

Esta configuración (con numeración cerrada y la UC Suite) muestra, a partir de un ejemplo, los pasos a realizar para configurar una interconexión multigateway.

Requisitos:

- Hay un plan de interconexión. A través del plan de interconexión se garantiza que todos los números de teléfono internos de la interred solo se asignen una vez en caso de numeración oculta. Se pueden utilizar distintas longitudes de números de teléfono. Solo los números de marcación directa pueden aparecer varias veces.
- La red IP está configurada y todos los nodos pueden ponerse en comunicación entre sí por el ping
- Todos los nodos tienen la misma versión de software

Desvíos de llamada a nivel de nodo: si se producen llamadas entrantes mediante tronqueos de IP ya desviados, no se ejecutan otros desvíos al buzón de voz. El motivo es que, de lo contrario, no se puede realizar una asignación unívoca al buzón de voz

Si se desea utilizar reglas de representación a nivel de nodo, se deben configurar a través de los perfiles de las extensiones OpenScape Business o de conmutaciones de llamadas. En este caso, las llamadas a nivel de nodo no se señalizan como de desvío, sino como llamadas directas y, así, los desvíos de llamada del representante se desvían al buzón de voz.

Tabla 22: Configuración de los datos de ubicación para el nodo 1

Nodo 1		
G.-País de la ubicación		49
G.-Red local de la ubicación		2302
G.-Instalación de la ubicación		66758
Prefijo internacional		00
Prefijo nacional		0
Rutas		
RDSI	Código urbano	0
Redes	2° AKZ	0
Parámetros de ruta		
Ruta	Tipo de número de llamada, saliente	Tipo RNR
Redes	Desconocido	int/marcación directa
RDSI	(No se modifica la entrada)	N.° llam. marc. directa

En las tablas de encaminamiento se registran automáticamente los números de teléfono de todas las extensiones que están fuera del nodo 1 y los números de teléfono internos y los números de marcación directa que no coinciden con los números de teléfono internos correspondientes.

Tabla 23: Visión general de las entradas de LCR para el nodo 1

Plan de marcación		Tabla de rutas			Regla de marcación		
Nombre	**Cifras marcadas**	**Ruta**	**Gateway dedicado**	**ID de gateway**	**Regla de marcación**	**Procedimiento**	**Tipo**
Nodo 2 Internacional	0C004989722-Z	Redes	Obligatorio	2	D4989722E3A	Corp. Red	Internacional
Nodo 2 NAT	0C089722-Z						
Nodo 2 Ext.	0C722-Z						
Nodo 3 Internacional	0C0049230266719-Z	Redes	Obligatorio	3	D49230266719E3A	Corp. Red	Internacional
Nodo 3 NAT	0C0230266719-Z						
Nodo 3 Ext.	0C66719-Z						
Nodo 4 Internacional	0C0049230266758-Z	Redes	NO		D230266758E3A	Corp. Red	Nacional
Nodo 4 NAT	0C0230266758-Z						
Nodo 4 Ext.	0C66758-Z						
Diverso	-Z	Redes	No		BA	Corp. Red	Desconocido
Línea urbana Internacional	0C0049-Z	RDSI	No		D0E3A	Ofertante de red principal	Desconocido
Línea urbana	0CZ	RDSI	No		A	Ofertante de red principal	Desconocido

Tabla 24: Configuración de los datos de ubicación para el nodo 2

Nodo 2		
G.-País de la ubicación		49
G.-Red local de la ubicación		89
G.-Instalación de la ubicación		722
Prefijo internacional		00
Prefijo nacional		0
Rutas		
RDSI	Código urbano	0
Redes	2° AKZ	0
Parámetros de ruta		
Ruta	Tipo de número de llamada, saliente	Tipo RNR

Nodo 2		
Redes	Desconocido	int/marcación directa
RDSI	(No se modifica la entrada)	N.° llam. marc. directa

En las tablas de encaminamiento se registran automáticamente los números de teléfono de todas las extensiones que están fuera del nodo 2. y los números de teléfono internos y los números de marcación directa que no coinciden con los números de teléfono internos correspondientes.

Tabla 25: Visión general de las entradas de LCR para el nodo 2

Plan de marcación		Tabla de rutas			Regla de marcación		
Nombre	**Cifras marcadas**	**Ruta**	**Gateway dedicado**	**ID de gateway**	**Regla de marcación**	**Procedimiento**	**Tipo**
Nodo 1 Internacional	0C0049230266758-Z	Redes	Obligatorio	1	D492302667E3A	Corp. Red	Internacional
Nodo 1 NAT	0C0230266758-Z						
Nodo 1 Ext.	0C66758-Z						
Nodo 3 Internacional	0C0049230266719-Z	Redes	Obligatorio	3	D49230266719E3A	Corp. Red	Internacional
Nodo 3 NAT	0C0230266719-Z						
Nodo 3 Ext.	0C66719-Z						
Nodo 4 Internacional	0C004989722-Z	Redes	NO		D89722E3A	Corp. Red	Nacional
Nodo 4 NAT	0C089722-Z						
Nodo 4 Ext.	0C722-Z						
Diverso	-Z	Redes	No		BA	Corp. Red	Desconocido
Línea urbana Internacional	0C0049-Z	RDSI	No		D0E3A	Ofertante de red principal	Desconocido
Línea urbana	0CZ	RDSI	No		A	Ofertante de red principal	Desconocido

Tabla 26: Configuración de los datos de ubicación para el nodo 3

Nodo 3	
G.-País de la ubicación	49
G.-Red local de la ubicación	2302
G.-Instalación de la ubicación	66719

Nodo 3		
Prefijo internacional		00
Prefijo nacional		0
Rutas		
RDSI	Código urbano	0
Redes	2° AKZ	0
Parámetros de ruta		
Ruta	Tipo de número de llamada, saliente	Tipo RNR
Redes	Desconocido	int/marcación directa
RDSI	(No se modifica la entrada)	N.° llam. marc. directa

En las tablas de encaminamiento se registran automáticamente los números de teléfono de todas las extensiones que están fuera del nodo 3. y los números de teléfono internos y los números de marcación directa que no coinciden con los números de teléfono internos correspondientes.

Tabla 27: Visión general de las entradas de LCR para el nodo 3

Plan de marcación		**Tabla de rutas**			**Regla de marcación**		
Nombre	**Cifras marcadas**	**Ruta**	**Gateway dedicado**	**ID de gateway**	**Regla de marcación**	**Procedimiento**	**Tipo**
Nodo 1 Internacional	0C0049230266758-Z	Redes	Obligatorio	1	D49230266758E3A	Corp. Red	Internacional
Nodo 1 NAT	0C0230266758-Z						
Nodo 1 Ext.	0C66758-Z						
Nodo 2 Internacional	0C004989722-Z	Redes	Obligatorio	2	D4989722E3A	Corp. Red	Internacional
Nodo 2 NAT	0C089722-Z						
Nodo 2 Ext.	0C722-Z						
Nodo 4 Internacional	0C004989230266719-Z	Redes	No		D230266719E3A	Corp. Red	Nacional
Nodo 4 NAT	0C0230266719-Z						
Nodo 4 Ext.	0C66719-Z						
Diverso	-Z	Redes	No		BA	Corp. Red	Desconocido
Línea urbana Internacional	0C0049-Z	RDSI	No		D0E3A	Ofertante de red principal	Desconocido

Plan de marcación		Tabla de rutas			Regla de marcación		
Nombre	**Cifras marcadas**	**Ruta**	**Gateway dedicado**	**ID de gateway**	**Regla de marcación**	**Procedimiento**	**Tipo**
Línea urbana	0CZ	RDSI	No		A	Ofertante de red principal	Desconocido

Configuración de los datos de ubicación para el nodo 4: vincule los datos de ubicación a una semi-ruta de línea urbana (Ruta 1) con Código de acceso a línea urbana = 0 y tipo = Línea urbana, ya que el nodo 4 no tiene conexión directa de línea urbana.

Tabla 28: Nodo 4, pseudo-ruta urbana

Nodo 4		
G.-País de la ubicación		49
G.-Red local de la ubicación		
G.-Instalación de la ubicación		
Prefijo internacional		00
Prefijo nacional		0
Rutas		
RDSI	Código urbano	0
Redes	2° AKZ	0
Parámetros de ruta		
Ruta	Tipo de número de llamada, saliente	Tipo RNR
Redes	Desconocido	int/marcación directa
RDSI	(No se modifica la entrada)	N.° llam. marc. directa

En las tablas de encaminamiento se registran automáticamente los números de teléfono de todas las extensiones que están fuera del nodo 1 y los números de teléfono internos y los números de marcación directa que no coinciden con los números de teléfono internos correspondientes.

Tabla 29: Nodo 4, Ruta (redes)

Nodo 4		
G.-País de la ubicación		
G.-Red local de la ubicación		
G.-Instalación de la ubicación		
Prefijo internacional		00
Prefijo nacional		0
Rutas		
RDSI	Código urbano	0

Nodo 4		
Redes	2° AKZ	0
Parámetros de ruta		
Ruta	Tipo de número de llamada, saliente	Tipo RNR
Redes	Nacional	int/marcación directa
RDSI	(No se modifica la entrada)	N.° llam. marc. directa

Tabla 30: Visión general de las entradas de LCR para el nodo 4

Plan de marcación		Tabla de rutas			Regla de marcación		
Nombre	**Cifras marcadas**	**Ruta**	**Gateway dedicado**	**ID de gateway**	**Regla de marcación**	**Procedimiento**	**Tipo**
Nodo 1 Internacional	0C0049230266758-Z	Redes	Obligatorio	1	D49230266758E3A	Corp. Red	Internacional
Nodo 1 NAT	0C0230266758-Z						
Nodo 2 Internacional	0C004989722-Z	Redes	Obligatorio	2	D4989722E3A	Corp. Red	Internacional
Nodo 2 NAT	0C089722-Z						
Nodo 3 Internacional	0C004989230266719-Z	Redes	Obligatorio	3	D49230266719E3A	Corp. Red	Internacional
Nodo 3 NAT	0C0230266719-Z						
Diverso	-Z	Redes	NO		A	Corp. Red	Desconocido
Línea urbana	0CZ	Redes	MULTI-GATEWAY	1	E1A	Ofertante de red principal	Desconocido

Procedimiento de configuración de la interconexión:

1) Configuración de la instalación básica para el nodo 4 (maestro)
2) Configuración de interconexión para el nodo 4 (maestro)
3) Configuración de la instalación básica para el nodo 1 (esclavo)
4) Configuración de la interconexión para el nodo 1 (esclavo)
5) Configuración de la instalación básica para el nodo 2 (esclavo)
6) Configuración de la interconexión para el nodo 2 (esclavo)
7) Configuración de la instalación básica para el nodo 3 (esclavo)
8) Configuración de la interconexión para el nodo 3 (esclavo)
9) Control de la función de interconexión del maestro
10) Configuración multigateway para el nodo 4 (maestro)
11) Configuración de direcciones y parámetros de ruta (nodo 1, esclavo)
12) Configuración de LCR para la interconexión (nodo 1, esclavo)
13) Configuración de direcciones y parámetros de ruta (nodo 2, esclavo)
14) Configuración de LCR para la interconexión (nodo 2, esclavo)
15) Configuración de direcciones y parámetros de ruta (nodo 3, esclavo)

16) Configuración de LCR para la interconexión (nodo 3, esclavo)
17) Configuración de direcciones y parámetros de ruta (nodo 4, maestro)
18) Configuración de LCR para la interconexión (nodo 4, maestro)

21.6.4.1 Cómo configurar la instalación básica para el nodo 4 (OpenScape Business S, maestro)

Para la integración en una interred hay que asignar el prefijo de país y un ID de nodo. Los números de teléfono internos se deben configurar de forma unívoca. Es importante indicar los números de teléfono nacionales y locales, ya que este número se configura en la ruta 1 de línea urbana RDSI y se utiliza para la normalización como número de teléfono de la ubicación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo 49 para Alemania.
4) No haga ninguna entrada para los campos **Cód. local** y **Número de teléfono del sistema**!.
5) Active la casilla de verificación **Integración de red**.
6) En el campo **ID de nodo** para OpenScape Business S asigne un ID de nodo único en la interred. El ID de nodo debe estar entre "**1**" y "**100**" (asigne "**4**" en el ejemplo de configuración).
7) Haga clic en **Ejecutar función**. Es conducido a la ventana **Funciones centrales para extensiones**.
8) En una red, todos los números de teléfono internos deben ser exclusivos. Por este motivo hay que borrar los números de teléfono estándar. Active el campo de opción **Borrar todos nos. llamada**.
9) Active la casilla de verificación **Borrar todos nos. llamada** y haga clic en **OK & Continuar**. Es conducido a la ventana **Cambiar números de función y de llamada preconfigurados**.

Nota: Los códigos de función deben ser únicos en la interred. No puede haber números de teléfono duplicados.

---

10) Ajuste los números de teléfono preconfigurados a los números de teléfono de la red y haga clic en **OK & Continuar**. Los números de teléfono se pueden ajustar de forma manual a través del asistente. Como alternativa, también puede importar un archivo CSV con los números de teléfono correspondientes.
11) Ahora, importe los clientes IP.
12) Configure los clientes IP.
13) Cambie los ajustes de configuración de las conferencias MeetMe. Debe indicar un código único en la interred.

14) A continuación, configure el envío de correo electrónico.
15) Haga clic en **Salir**.

21.6.4.2 Cómo configurar la interconexión para el nodo 4 (maestro)

En el siguiente paso, se configura la interconexión del nodo 3 mediante el asistente.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de red**.
4) Seleccione el ajuste **Red nativa con OSBiz X / OSBiz S**.
5) Active la casilla de verificación **El sistema es el nodo MAESTRO**.
6) En **ID de nodo**, introduzca el número de nodo correspondiente de los sistemas OpenScape Business pertinentes (en el ejemplo de configuración el de los esclavos con el ID de nodo 1, 2 y 3).
7) En **Dirección IP**, introduzca las direcciones IP de los sistemas OpenScape Business correspondientes (en el ejemplo de configuración las de los esclavos con el ID de nodo 1, 2 y 3).
8) Active la casilla de verificación **Gateway**.
9) En **Nombre**, introduzca el tipo de sistema (por ejemplo, esclavo 1).
10) En **Tipo**, introduzca el tipo del sistema secundario.
11) Si es necesario, active la casilla de verificación **Cifrado**.

Consejo: El cifrado se basa en SPE y no es válido para las aplicaciones.

Nota: Al activar la casilla de verificación no se configura el cifrado. Véase Cifrado de señalización y carga útil (SPE) .

---

12) Haga clic en **Salir**.

21.6.4.3 Cómo configurar la instalación básica para el nodo 1 (esclavo)

Para la integración en una interred hay que asignar el prefijo de país y un ID de nodo. Los números de teléfono internos se deben configurar de forma unívoca. Es importante indicar los números de teléfono nacionales y locales, ya que este número se configura en la ruta 1 de línea urbana RDSI y se utiliza para la normalización como número de teléfono de la ubicación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo 49 para Alemania.
4) Introduzca el **Cód. local** y el **Número de teléfono del sistema**.
5) Active la casilla de verificación **Integración de red**.
6) En el campo **ID de nodo** para OpenScape Business S, asigne un ID de nodo único en la interred (un "**1**" para el ejemplo de configuración).
7) Haga clic en **Ejecutar función**. Es conducido a la ventana **Funciones centrales para extensiones**.
8) En una red, todos los números de teléfono deben ser exclusivos. Por este motivo hay que borrar los números de teléfono estándar. Active el campo de opción **Borrar todos nos. llamada**.
9) Active la casilla de verificación **Borrar todos nos. llamada** y haga clic en **OK & Continuar**. Es conducido a la ventana **Cambiar números de función y de llamada preconfigurados**.

   Nota: Los códigos de función deben ser únicos en la interred. No puede haber números de teléfono duplicados.

10) Ajuste los números de teléfono preconfigurados a los números de teléfono de la red y haga clic en **OK & Continuar**. Los números de teléfono se pueden ajustar de forma manual a través del asistente. Como alternativa, también puede importar un archivo CSV con los números de teléfono correspondientes.
11) Configure ahora las extensiones analógicas y RDSI.
12) Cambie los ajustes de configuración de las conferencias MeetMe. Debe indicar un código único en la interred.
13) A continuación, configure el envío de correo electrónico.
14) Haga clic en **Salir**.

21.6.4.4 Cómo configurar la interconexión para el nodo 1 (esclavo)

En el siguiente paso se configura el asistente para la interconexión.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.

3) Haga clic en **Editar** para iniciar el asistente **Configuración de red**.
4) Seleccione el ajuste **Red nativa con OSBiz X / OSBiz S**.
5) **Introduzca la dirección IP del nodo MAESTRO** (OpenScape Business S se configura como nodo esclavo y se registra la dirección IP correspondiente del nodo maestro, OpenScape Business S. El maestro y el multigateway siempre se asignan al mismo sistema (en el ejemplo de configuración a OpenScape Business S).

Consejo: Después de hacer clic en **OK&Continuar** la acción ya no se puede deshacer.

---

6) El **Estado de registro** se muestra con **Estado correcto** (o con el mensaje de error correspondiente). Con ello concluye el asistente.
7) Haga clic en **Salir**.

21.6.4.5 Cómo configurar la instalación básica para el nodo 2 (esclavo)

Para la integración en una interred hay que asignar el prefijo de país y un ID de nodo. Los números de teléfono internos se deben configurar de forma unívoca. Es importante indicar los números de teléfono nacionales y locales, ya que este número se configura en la ruta 1 de línea urbana RDSI y se utiliza para la normalización como número de teléfono de la ubicación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo 49 para Alemania.
4) Registre el **Cód. local** y el **Número de teléfono del sistema**.
5) Active la casilla de verificación **Integración de red**.
6) En el campo **ID de nodo** para OpenScape Business S, asigne un ID de nodo único en la interred (un "**2**" para el ejemplo de configuración).
7) Haga clic en **Ejecutar función**. Es conducido a la ventana **Funciones centrales para extensiones**.
8) En una red, todos los números de teléfono internos deben ser exclusivos. Por este motivo hay que borrar los números de teléfono estándar. Active el campo de opción **Borrar todos nos. llamada**.
9) Active la casilla de verificación **Borrar todos nos. llamada** y haga clic en **OK & Continuar**. Es conducido a la ventana **Cambiar números de función y de llamada preconfigurados**.

Nota: Los códigos de función deben ser únicos en la interred. No puede haber números de teléfono duplicados.

---

10) Ajuste los números de teléfono preconfigurados a los números de teléfono de la red y haga clic en **OK & Continuar**. Los números de teléfono se pueden ajustar de forma manual a través del asistente. Como alternativa, también puede importar un archivo CSV con los números de teléfono correspondientes.
11) Configure ahora las extensiones analógicas y RDSI.
12) Cambie los ajustes de configuración de las conferencias MeetMe. Debe indicar un código único en la interred.
13) A continuación, configure el envío de correo electrónico.
14) Haga clic en **Salir**.

21.6.4.6 Cómo configurar la interconexión para el nodo 2 (esclavo)

En el siguiente paso se configura la interconexión del nodo 2 mediante el asistente.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de red**.
4) Seleccione el ajuste **Red nativa con OSBiz X / OSBiz S**.
5) En **Tipo de nodo**, active la casilla **El sistema es un nodo ESCLAVO**.
6) **Introduzca la dirección IP del nodo MAESTRO** (OpenScape Business S se configura como nodo esclavo y se registra la dirección IP correspondiente del nodo maestro, OpenScape Business S. El maestro y el multigateway siempre se asignan al mismo sistema (en el ejemplo de configuración a OpenScape Business S).

   Consejo: Después de hacer clic en **OK&Continuar** la acción ya no se puede deshacer.

7) El **Estado de registro** se muestra con **Estado correcto** (o con el mensaje de error correspondiente). Con ello concluye el asistente.
8) Haga clic en **Salir**.

21.6.4.7 Cómo configurar la instalación básica para el nodo 3 (esclavo)

Para la integración en una interred hay que asignar el prefijo de país y un ID de nodo. Los números de teléfono internos se deben configurar de forma unívoca. Es importante indicar los números de teléfono nacionales y locales, ya que este número se configura en la ruta 1 de línea urbana RDSI y se utiliza para la normalización como número de teléfono de la ubicación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) En el campo **Prefijo del país**, indique el prefijo del país, por ejemplo 49 para Alemania.
4) Registre el **Cód. local** y el **Número de teléfono del sistema**.
5) Active la casilla de verificación **Integración de red**.
6) En el campo **ID de nodo** para OpenScape Business, asigne un ID de nodo único en la interred (un "**3**" para el ejemplo de configuración).
7) Haga clic en **Ejecutar función**. Es conducido a la ventana **Funciones centrales para extensiones**.
8) En una red, todos los números de teléfono internos deben ser exclusivos. Por este motivo hay que borrar los números de teléfono estándar. Active el campo de opción **Borrar todos nos. llamada**.
9) Active la casilla de verificación **Borrar todos nos. llamada** y haga clic en **OK & Continuar**. Es conducido a la ventana **Cambiar números de función y de llamada preconfigurados**.

   Nota: Los códigos de función deben ser únicos en la interred. No puede haber números de teléfono duplicados.

10) Ajuste los números de teléfono preconfigurados a los números de teléfono de la red y haga clic en **OK & Continuar**. Los números de teléfono se pueden ajustar de forma manual a través del asistente. Como alternativa, también puede importar un archivo CSV con los números de teléfono correspondientes.
11) Configure ahora las extensiones analógicas y RDSI.
12) Cambie los ajustes de configuración de las conferencias MeetMe. Debe indicar un código único en la interred.
13) A continuación, configure el envío de correo electrónico.
14) Haga clic en **Salir**.

21.6.4.8 Cómo configurar la interconexión para el nodo 3 (esclavo)

En el siguiente paso, se configura la interconexión del nodo 3 mediante el asistente.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.
3) Haga clic en **Editar** para iniciar el asistente **Configuración de red**.
4) Seleccione el ajuste **Red nativa con OSBiz X / OSBiz S**.
5) En **Tipo de nodo**, active la casilla **El sistema es un nodo ESCLAVO**.
6) **Introduzca la dirección IP del nodo MAESTRO** (OpenScape Business S se configura como nodo esclavo y se registra la dirección IP correspondiente del nodo maestro, OpenScape Business S. El maestro y la ubicación múltiple siempre se asignan al mismo sistema (en el ejemplo de configuración a OpenScape Business S).

   Consejo: Después de hacer clic en **OK&Continuar** la acción ya no se puede deshacer.

7) El **Estado de registro** se muestra con **Estado correcto** (o con el mensaje de error correspondiente). Con ello concluye el asistente.
8) Haga clic en **Salir**.

21.6.4.9 Cómo controlar la función de interconexión del maestro

Puede controlar el estado de la interconexión de forma general y para los distintos números de teléfono.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Red**.
2) En la línea de estado puede ver el **Estado de sincronización** de la red. Verde indica que la interconexión no tiene ningún problema, el color rojo indica problemas en la red.
3) En la ventana **Red**, marque la pestaña **Vista de dominios**. Se mostrarán todos los nodos disponibles con **ID de nodo**, **Nombre**, **Tipo de sistema**, **Dirección de servidor**, **Estado de registro** y **Disponibilidad**.
4) En la ventana **Red**, marque la pestaña **Números de teléfono**. Se abrirá una ventana con todos los datos sobre:
   - **Número de teléfono**
   - **N.° llam. marc. directa**
   - **Nombre**
   - **Tipo de puerto**
   - **Nodo**

21.6.4.10 Cómo configurar multi-gateway para el nodo 4 (maestro)

La interred se configura como red multigateway se realiza en el nodo maestro.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración de red**.
3) En **Configuración de red**, seleccione el ajuste **Configuración de varias ubicaciones**. En la ventana **Configuración de varias ubicaciones** se establece la asignación de las extensiones a la ubicación. La asignación de los números de teléfono a los ID de nodo (NodeId) se utiliza, por ejemplo, para la ocupación de línea urbana saliente en el nodo de ubicación asignado.
4) En el ejemplo de configuración, introduzca las siguientes asignaciones en **Configuración de varias ubicaciones** (todos los teléfonos están registrados en OpenScape Business S):

Número de teléfono	Nombre	NodeId
1101	1101KN1	1-Esclavo Witten1
1102	1102KN1	1-Esclavo Witten1
1103	1103KN1	1-Esclavo Witten1
2101	2101KN2	2-esclavo Múnich
2102	2102KN2	2-esclavo Múnich
2103	2103KN2	2-esclavo Múnich
3101	3101KN3	3-esclavo Witten 2
3102	3102KN3	3-esclavo Witten 2
3103	3103KN3	3-esclavo Witten 2

5) Haga clic en **Salir**.

21.6.4.11 Cómo configurar la dirección y los parámetros de ruta (nodo 1, esclavo)

Los siguientes pasos permiten configurar la dirección y los parámetros de ruta para la interconexión del esclavo.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/ Interconexión**.
3) En el grupo de menús, haga clic en **Ruta**.
4) En la ventana **Cambiar ruta**, y en el campo **Nombre de ruta**, introduzca un nombre `Ruta 1` para la ruta de línea urbana.
5) En **Códigos de ruta**, introduzca el `0`.

6) En **Número de teléfono del sistema-entrante** y en el campo **Prefijo del país** introduzca el `49`.
7) En **Número de teléfono del sistema-entrante**, y en el campo **Código de red local**, introduzca el `2302`.
8) En **Número de teléfono del sistema-entrante**, y en el campo **Número de teléfono del sistema**, introduzca el `66758`.
9) Marque la casilla de verificación de **Número de teléfono del sistema-entrante** en el campo **Número emplazamiento**.
10) Se pueden aplicar los ajustes predeterminados para los parámetros de ruta (tipo de número, saliente, tipo de número de llamada).
11) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.4.12 Cómo configurar LCR para la interconexión (nodo 1, esclavo)

En el plan de marcación LCR, las entradas predeterminadas de los índices 32, 33, 34 y 35 se deben completar con nuevas entradas para la marcación de números de teléfono en el formato "Internacional, Nacional y Extensiones" para los nodos 2 y 3 así como para el nodo multigateway 4. "Internacional" y "Nacional" siempre son necesarias. "Extensiones" es necesaria para los nodos de colateral que se encuentran en la misma red local.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.
3) En el grupo de menús, haga clic en **Plan de marcación**.
4) Introduzca los siguientes valores en puestos libres (aquí del 36 al 43) según los valores estándar:

Plan de marcación	Nombre	Cifras marcadas	Tabla de rutas
31	Suite de aplicaciones	-171	12
32	Estándar	88CZ	1
33	Red IP	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 2 Inter	0C004989722-Z	16
37	Nodo 2 Nat	0C089722-Z	16
38	Nodo 3 Inter	0C0049230266719-Z	17
39	Nodo 3 Nat	0C0230266719-Z	17
40	Nodo 3 Ext.	0C66719-Z	17
41	Nodo 4 Inter	0C0049230266758-Z	18
42	Nodo 4 Nat	0C0230266758-Z	18
43	Nodo 4 Ext.	0C66758-Z	18

Plan de marcación	Nombre	Cifras marcadas	Tabla de rutas
44			-

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

6) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 2.

a) En **Nombre de regla**, introduzca la entrada **Nodo 2**.
b) En **Formato de regla de marcación**, seleccione la entrada **D4989722E3A**.
c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
d) En **Tipo**, seleccione la entrada **Prefijo del país**.
e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

7) En el grupo de menús, haga clic en **Tabla rutas**, para configurar la tabla de rutas 16 para la conexión de red y asignarla al nodo 2 directo.

a) Haga clic en la tabla de rutas 16.
b) En **Dirección**, seleccione la opción **Networking**.
c) En **Regla de marcación**, seleccione la opción **Nodo 2**.
d) En **Clase mín.**, seleccione la opción **15**.
e) En **Advertencia**, seleccione la opción **Ninguna**.
f) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
g) En **ID de nodo GW**, seleccione la opción **2**.
h) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

8) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 3.

a) En **Nombre de regla**, introduzca la entrada **Nodo 3**.
b) En **Formato de regla de marcación**, seleccione la entrada **D49230266719E3A**.
c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
d) En **Tipo**, seleccione la entrada **Prefijo del país**.
e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

9) En el grupo de menús, haga clic en **Tabla rutas**, para configurar una tabla de rutas 17 para la conexión de red y asignarla al nodo 3 directo.

a) Haga clic en la tabla de rutas 17.
b) En **Dirección**, seleccione la opción **Networking**.
c) En **Regla de marcación**, seleccione la opción **Nodo 3**.
d) En **Clase mín.**, seleccione la opción **15**.
e) En **Advertencia**, seleccione la opción **Ninguna**.
f) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
g) En **ID de nodo GW**, seleccione la opción **3**.
h) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 4.
    a) En **Nombre de regla**, introduzca la entrada **Nodo ML 4**.
    b) En **Formato de regla de marcación**, seleccione la entrada **D230266758E3A**.
    c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
    d) En **Tipo**, seleccione la entrada **Nacional**.
    e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
11) En el grupo de menús, haga clic en **Tabla rutas**, para configurar una tabla de rutas 18 para la conexión de red y asignarla al nodo 4 directo.
    a) Haga clic en la tabla de rutas 18.
    b) En **Dirección**, seleccione la opción **Networking**.
    c) En **Regla de marcación**, seleccione la opción **Nodo 4**.
    d) En **Clase mín.**, seleccione la opción **15**.
    e) En **Advertencia**, seleccione la opción **Ninguna**.
    f) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.4.13 Cómo configurar la dirección y los parámetros de ruta (nodo 2, esclavo)

Los siguientes pasos permiten configurar la dirección y los parámetros de ruta para la interconexión del esclavo.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/ Interconexión**.
3) En el grupo de menús, haga clic en **Ruta**.
4) En la ventana **Cambiar ruta**, y en el campo **Nombre de ruta**, introduzca un nombre `Ruta 1` para la ruta de línea urbana.
5) En **Códigos de ruta**, introduzca el `0`.
6) En **Número de teléfono del sistema-entrante** y en el campo **Prefijo del país** introduzca el `49`.
7) En **Número de teléfono del sistema** -entrante, y en el campo **Código de red local**, introduzca el 89.
8) En **Número de teléfono del sistema-entrante**, y en el campo **Número de teléfono del sistema**, introduzca el `722`.
9) Marque la casilla de verificación de **Número de teléfono del sistema-entrante** en el campo **Número emplazamiento**.
10) Se pueden aplicar los ajustes predeterminados para los parámetros de ruta (tipo de número, saliente, tipo de número de llamada).
11) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.4.14 Cómo configurar LCR para la interconexión (nodo 2, esclavo)

En el plan de marcación LCR, las entradas predeterminadas de los índices 32, 33, 34 y 35 se deben completar con nuevas entradas para la marcación de números de teléfono con el formato "Internacional, Nacional y Extensiones" para los nodos 1 y 2. "Internacional" y "Nacional" siempre son necesarias. "Extensiones" es necesaria para los nodos de colateral que se encuentran en la misma red local. Deben completarse las entradas 36, 37 y 39 para la interconectividad con el nodo 1 (número de teléfono 100 > 199) y las entradas 38, 40 y 41 para la interconectividad con el nodo 3 (número de teléfono 300 > 399). Estos datos se utilizan para la marcación desde aplicaciones (por ejemplo, myPortal for Desktop).

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.

3) En el grupo de menús, haga clic en **Plan de marcación**.

4) Introduzca los siguientes valores en puestos libres (aquí del 36 al 43) según los valores estándar:

Plan de marcación	Nombre	Cifras marcadas	Tabla de rutas
31	Suite de aplicaciones	-171	12
32	Estándar	88CZ	1
33	Red IP	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 1 Inter	0C0049230266758-Z	16
37	Nodo 1 Nat	0C0230266758-Z	16
38	Nodo 3 Inter	0C0049230266719-Z	17
39	Nodo 3 Nat	0C0230266719-Z	17
40	Nodo 3 Ext.	0C66719-Z	17
41	Nodo 4 Inter	0C004989722-Z	18
42	Nodo 4 Nat	0C089722-Z	18
43	Nodo 4 Ext.	0C722-Z	18
44			-

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

6) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 1.

a) En **Nombre de regla**, introduzca la entrada **Nodo 1**.
b) En **Formato de regla de marcación**, seleccione la entrada **D49230266758E3A**.
c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
d) En **Tipo**, seleccione la entrada **Prefijo del país**.
e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

7) En el grupo de menús, haga clic en **Tabla rutas**, para configurar la tabla de rutas 16 para la conexión de red y asignarla al nodo 1 directo.

a) Haga clic en la tabla de rutas 16.
b) En **Dirección**, seleccione la opción **Networking**.
c) En **Regla de marcación**, seleccione la opción **Nodo 1**.
d) En **Clase mín.**, seleccione la opción **15**.
e) En **Advertencia**, seleccione la opción **Ninguna**.
f) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
g) En **ID de nodo GW**, seleccione la opción **1**.
h) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

8) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 3.

a) En **Nombre de regla**, introduzca la entrada **Nodo 3**.
b) En **Formato de regla de marcación**, seleccione la entrada **D49230266719E3A**.
c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
d) En **Tipo**, seleccione la entrada **Prefijo del país**.
e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

9) En el grupo de menús, haga clic en **Tabla rutas**, para configurar una tabla de rutas 17 para la conexión de red y asignarla al nodo 3 directo.

a) Haga clic en la tabla de rutas 17.
b) En **Dirección**, seleccione la opción **Networking**.
c) En **Regla de marcación**, seleccione la opción **Nodo 3 directo**.
d) En **Clase mín.**, seleccione la opción **15**.
e) En **Advertencia**, seleccione la opción **Ninguna**.
f) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
g) En **ID de nodo GW**, seleccione la opción **3**.
h) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 4.

a) En **Nombre de regla**, introduzca la entrada **Nodo 4**.
b) En **Formato de regla de marcación**, seleccione la entrada **D89722E3A**.
c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
d) En **Tipo**, seleccione la entrada **Código de red local**.
e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

11) En el grupo de menús, haga clic en **Tabla rutas**, para configurar una tabla de rutas 18 para la conexión de red y asignarla al nodo 4 directo.

a) Haga clic en la tabla de rutas 18.
b) En **Dirección**, seleccione la opción **Networking**.
c) En **Regla de marcación**, seleccione la opción **Nodo 4**.
d) En **Clase mín.**, seleccione la opción **15**.
e) En **Advertencia**, seleccione la opción **Ninguna**.
f) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.4.15 Cómo configurar la dirección y los parámetros de ruta (nodo 3, esclavo)

Los siguientes pasos permiten configurar la dirección y los parámetros de ruta para la interconexión del esclavo.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/ Interconexión**.
3) En el grupo de menús, haga clic en **Ruta**.
4) En la ventana **Cambiar ruta**, y en el campo **Nombre de ruta**, introduzca un nombre `Ruta 1` para la ruta de línea urbana.
5) En **Códigos de ruta**, introduzca el `0`.
6) En **Número de teléfono del sistema-entrante** y en el campo **Prefijo del país** introduzca el `49`.
7) En **Número de teléfono del sistema-entrante**, y en el campo **Código de red local**, introduzca el `2302`.
8) En **Número de teléfono del sistema-entrante**, y en el campo **Número de teléfono del sistema**, introduzca el `66719`.
9) Marque la casilla de verificación de **Número de teléfono del sistema-entrante** en el campo **Número emplazamiento**.
10) Se pueden aplicar los ajustes predeterminados para los parámetros de ruta (tipo de número, saliente, tipo de número de llamada).
11) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.4.16 Cómo configurar LCR para la interconexión (nodo 3, esclavo)

En el plan de marcación LCR, las entradas predeterminadas de los índices 32, 33, 34 y 35 se deben completar con nuevas entradas para la marcación de números de teléfono con el formato "Internacional, Nacional y Extensiones" para los nodos 1 y 2. "Internacional" y "Nacional" siempre son necesarias. "Extensiones" es necesaria para los nodos de colateral que se encuentran en la misma red local. Estos datos se utilizan para la marcación desde aplicaciones (por ejemplo, myPortal for Desktop).

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.

3) En el grupo de menús, haga clic en **Plan de marcación**.

4) Introduzca los siguientes valores:

Plan de marcación	Nombre	Cifras marcadas	Tabla de rutas
31	Suite de aplicaciones	-171	12
32	Estándar	88CZ	1
33	Red IP	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 1 Inter	0C0049230266758-Z	16
37	Nodo 1 Nat	0C00230266758-Z	16
38	Nodo 1 Ext.	0C66758-Z	16
39	Nodo 2 Inter	0C004989722-Z	17
40	Nodo 2 Nat	0C0089722-Z	17
41	Nodo 4 Inter	0C0049230266719-Z	18
42	Nodo 4 Nat	0C0230266719-Z	18
43	Nodo 4 Ext.	0C66719-Z	18
44			-

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

6) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 1.

a) En **Nombre de regla**, introduzca la entrada **Nodo 1**.

b) En **Formato de regla de marcación**, seleccione la entrada **D49230266758E3A**.

c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.

d) En **Tipo**, seleccione la entrada **Prefijo del país**.

e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

7) En el grupo de menús, haga clic en **Tabla rutas**, para configurar la tabla de rutas 16 para la conexión de red y asignarla al nodo 1 directo.

a) Haga clic en la tabla de rutas 16.

b) En **Dirección**, seleccione la opción **Networking**.

c) En **Regla de marcación**, seleccione la opción **Nodo 1**.

d) En **Clase mín.**, seleccione la opción **15**.

e) En **Advertencia**, seleccione la opción **Ninguna**.

f) En **Gateway dedicado**, seleccione la opción **Obligatorio**.

g) En **ID de nodo GW**, seleccione la opción **1**.

h) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

8) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 2.
   a) En **Nombre de regla**, introduzca la entrada **Nodo 2**.
   b) En **Formato de regla de marcación**, seleccione la entrada **D4989722E3A**.
   c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
   d) En **Tipo**, seleccione la entrada **Prefijo del país**.
   e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

9) En el grupo de menús, haga clic en **Tabla rutas**, para configurar una tabla de rutas 17 para la conexión de red y asignarla al nodo 2 directo.
   a) Haga clic en la tabla de rutas 17.
   b) En **Dirección**, seleccione la opción **Networking**.
   c) En **Regla de marcación**, seleccione la opción **Nodo 2**.
   d) En **Clase mín.**, seleccione la opción **15**.
   e) En **Advertencia**, seleccione la opción **Ninguna**.
   f) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
   g) En **ID de nodo GW**, seleccione la opción **2**.
   h) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 4.
   a) En **Nombre de regla**, seleccione la entrada **ML Nodo 4**
   b) En **Formato de regla de marcación**, seleccione la entrada **D230266719E3A**
   c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**
   d) En **Tipo**, seleccione la entrada **Código de red local**
   e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

11) En el grupo de menús, haga clic en **Tabla rutas**, para configurar una tabla de rutas 18 para la conexión de red y asignarla al nodo 4 directo.
   a) Haga clic en la tabla de rutas 18.
   b) En **Dirección**, seleccione la opción **Networking**.
   c) En **Regla de marcación**, seleccione la opción **Nodo 4**.
   d) En **Clase mín.**, seleccione la opción **15**.
   e) En **Advertencia**, seleccione la opción **Ninguna**.
   f) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.4.17 Cómo configurar la dirección y parámetros de ruta (nodo 4, maestro)

Los siguientes pasos permiten configurar la dirección y los parámetros de ruta para la interconexión del esclavo.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **Líneas/ Interconexión**.

3) En el grupo de menús, haga clic en **Ruta**.
4) En la ventana **Cambiar ruta**, y en el campo **Nombre de ruta**, introduzca un nombre `Ruta 1` para la ruta de línea urbana.
5) En **Códigos de ruta**, introduzca el `0`.
6) En **Número de teléfono del sistema-entrante** y en el campo **Prefijo del país** introduzca el `49`.
7) No introduzca ningún valor en los campos **Código de red local** y Número de teléfono del sistema.
8) Marque la casilla de verificación de **Número de teléfono del sistema-entrante** en el campo **Número emplazamiento**.
9) Se pueden aplicar los ajustes predeterminados para los parámetros de ruta (tipo de número, saliente, tipo de número de llamada).
10) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.4.18 Cómo configurar LCR para la interconexión (nodo 4, maestro)

En el plan de marcación LCR, las entradas predeterminadas de los índices 32, 33, 34 y 35 se deben completar con nuevas entradas para la marcación de números de teléfono con el formato "Internacional, Nacional y Extensiones" para los nodos 1 y 2. "Internacional" y "Nacional" siempre son necesarias. "Extensiones" es necesaria para los nodos de colateral que se encuentran en la misma red local. Estos datos se utilizan para la marcación desde aplicaciones (por ejemplo, myPortal for Desktop).

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.
3) En el grupo de menús, haga clic en **Plan de marcación**.
4) Introduzca los siguientes valores en puestos libres (aquí del 36 al 43) según los valores estándar:

Plan de marcación	Nombre	Cifras marcadas	Tabla rutas
1	Llamada de emergencia	0C112	19
2	Llamada de emergencia	0C110	19
3	teletrabajo	0C0137Z	19
4	Televoto	0C0138Z	19
5	Servicios Premium	0C0900Z	19
6	Servicio de información	0C118Z	19
7	Número de teléfono especial	0C116116	19

Plan de marcación	Nombre	Cifras marcadas	Tabla rutas
16	Estándar	0CZ	19
17	Estándar	0C1Z	19
18	Estándar	0CNZ	19
31	Suite de aplicaciones	-471	12
32	Estándar	88CZ	1
33	Red IP	-Z	13
34	COInternat	0C0049-Z	15
36	Nodo 1 Inter	0C0049230266758-Z	16
37	Nodo 1 Nat	0C0230266758-Z	16
38	Nodo 1 Ext.	0C66758-Z	16
39	Nodo 2 Inter	0C004989722-Z	17
40	Nodo 2 Nat	0C089722-Z	17
41	Nodo 3 Inter	0C0049230266719-Z	18
42	Nodo 3 Nat	0C0230266719-Z	18
43	Nodo 3 Ext.	0C66719-Z	18
44			-

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

6) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 1.

a) En **Nombre de regla**, introduzca la entrada **Nodo 1**.
b) En **Formato de regla de marcación**, seleccione la entrada **D49230266758E3A**.
c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
d) En **Tipo**, seleccione la entrada **Prefijo del país**.
e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

7) En el grupo de menús, haga clic en **Tabla rutas**, para configurar la tabla de rutas 16 para la conexión de red y asignarla al nodo 1 directo.

a) Haga clic en la tabla de rutas 16.
b) En **Dirección**, seleccione la opción **Networking**.
c) En **Regla de marcación**, seleccione la opción **Nodo 1**.
d) En **Clase mín.**, seleccione la opción **15**.
e) En **Advertencia**, seleccione la opción **Ninguna**.
f) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
g) En **ID de nodo GW**, seleccione la opción **1**.
h) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

8) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 2.

a) En **Nombre de regla**, introduzca la entrada **Nodo 2**.
b) En **Formato de regla de marcación**, seleccione la entrada **D4989722E3A**.
c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
d) En **Tipo**, seleccione la entrada **Prefijo del país**.
e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

9) En el grupo de menús, haga clic en **Tabla rutas**, para configurar una tabla de rutas 17 para la conexión de red y asignarla al nodo 2 directo.

a) Haga clic en la tabla de rutas 17.
b) En **Dirección**, seleccione la opción **Networking**.
c) En **Regla de marcación**, seleccione la opción **Nodo 2**.
d) En **Clase mín.**, seleccione la opción **15**.
e) En **Advertencia**, seleccione la opción **Ninguna**.
f) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
g) En **ID de nodo GW**, seleccione la opción **2**.
h) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

10) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para el nodo 3.

a) En **Nombre de regla**, seleccione la entrada **ML Nodo 3**
b) En **Formato de regla de marcación**, seleccione la entrada **D230266719E3A**
c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**
d) En **Tipo**, seleccione la entrada **Prefijo del país**
e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

11) En el grupo de menús, haga clic en **Tabla rutas**, para configurar una tabla de rutas 18 para la conexión de red y asignarla al nodo 3 directo.

a) Haga clic en la tabla de rutas 18.
b) En **Dirección**, seleccione la opción **Networking**.
c) En **Regla de marcación**, seleccione la opción **Nodo 3**.
d) En **Clase mín.**, seleccione la opción **15**.
e) En **Advertencia**, seleccione la opción **Ninguna**.
f) En **Gateway dedicado**, seleccione la opción **Obligatorio**.
g) En **ID de nodo GW**, seleccione la opción **3**.
h) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

12) En el grupo de menús, haga clic en la **Regla de marcación** correspondiente para comunicaciones de línea urbana. Se trata de la regla de marcación predefinida "Gateway Call" (Llamada de gateway).

a) En **Nombre de regla** introduzca la entrada **Gateway Call**.
b) En **Formato de regla de marcación**, introduzca la entrada **E1A**.
c) En **Procedimiento de acceso del ofertante de red** seleccione la entrada **Red corporativa**.
d) En **Tipo**, seleccione la entrada **Desconocido**.
e) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

13) En el grupo de menús, haga clic en **Tabla rutas**, para configurar la tabla de rutas 19 para la transferencia a línea urbana de los esclavos. La

entrada de multigateway permite determinar la pertenencia de la extensión al nodo y realizar la transferencia a línea urbana en ese nodo.

14) Haga clic en la tabla de rutas 19.

a) En **Dirección**, seleccione la opción **Networking**.
b) En **Regla de marcación**, seleccione la opción **Gateway Call** (Llamada de gateway).
c) En **Clase mín.**, seleccione la opción **15**.
d) En **Advertencia**, seleccione la opción **Ninguna**.
e) En **Gateway dedicado**, seleccione la opción **Multi-Gateway**.
f) En **ID de nodo GW**, seleccione la opción **1**.
g) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.6.5 Interconexión de OpenScape Business en entornos de hosting

En un entorno con varias ubicaciones (entorno hosting), se puede asignar una ruta a cada dirección y a cada dirección, un registro de ITSP. Se pueden administrar 8 registros de ITSP como máximo. Es posible un registro por ITSP o varios registros en un solo ITSP. Se puede asignar un prefijo local a cada registro de ITSP y, a continuación, varias extensiones. La conexión de las extensiones de las diferentes ubicaciones con el sistema de comunicación se realiza mediante VPN o MPLS. Si las ubicaciones están en diferentes países, por cada país hay que utilizar un OpenScape Business S propio (escenario 1a). Si todas las ubicaciones están en el mismo país, se puede utilizar un mismo OpenScape Business S (escenario 1b).

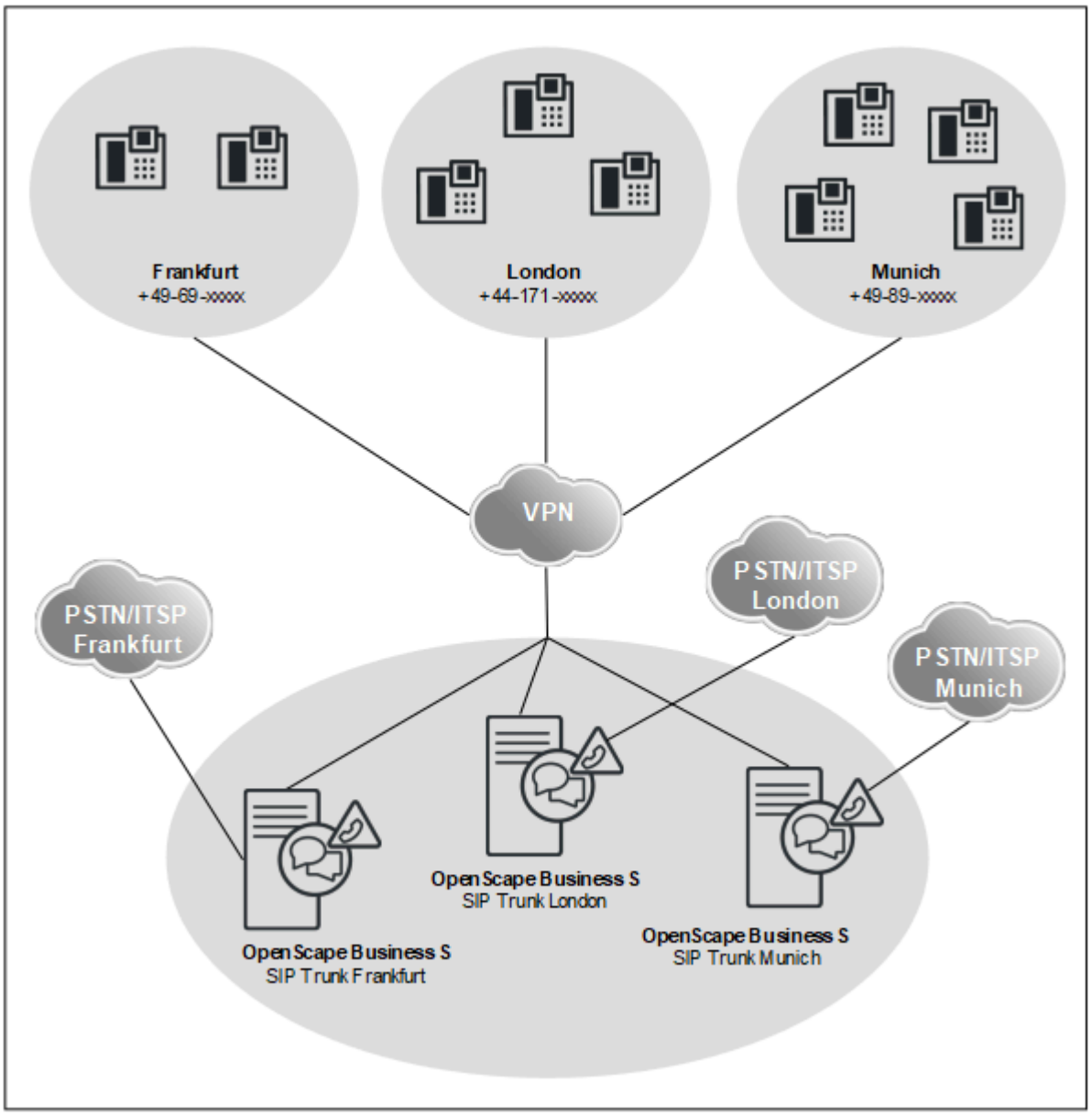
Los dos escenarios también se pueden implementar con los modelos de hardware de OpenScape Business X (por ejemplo, en pequeñas instalaciones). En una ubicación se pueden utilizar además los componentes TDM.

Los escenarios de hosting indicados a continuación se describen en términos generales. Se pueden implementar las variantes siguientes:

- Uso de OpenScape Business S y OpenScape Business X en el centro de datos del cliente o en el hoster
- OpenScape Business S en hardware de servidor dedicado o virtualizado
- Se requiere una infraestructura VPN o MPLS, especialmente con varias ubicaciones de clientes (sin router NAT específico de ubicación para acceder a Internet)
- Hasta 8 ITSP por sistema y país, proveedor MSN o de marcación directa
- Hasta 8 prefijos de ubicación (Area Codes - Códigos de área) por sistema y país, asignados hasta a 8 ubicaciones de cliente (Multisite)
- Escenarios Multisite combinables con interconexión clásica (voz y UC)
- Multisite con más de 8 ubicaciones implementable en interconexiones (interconexión multisitio n veces)
- Multisite entre países implementable en interconexiones (interconexión multisitio n veces)
- Escenario de interconexión con gateways RDSI completamente integrable
- Un requisito técnico es la posibilidad de utilizar números de marcación directa para proveedores RDSI y proveedores SIP por igual.

Escenario a: hosting con un OpenScape Business S por ubicación

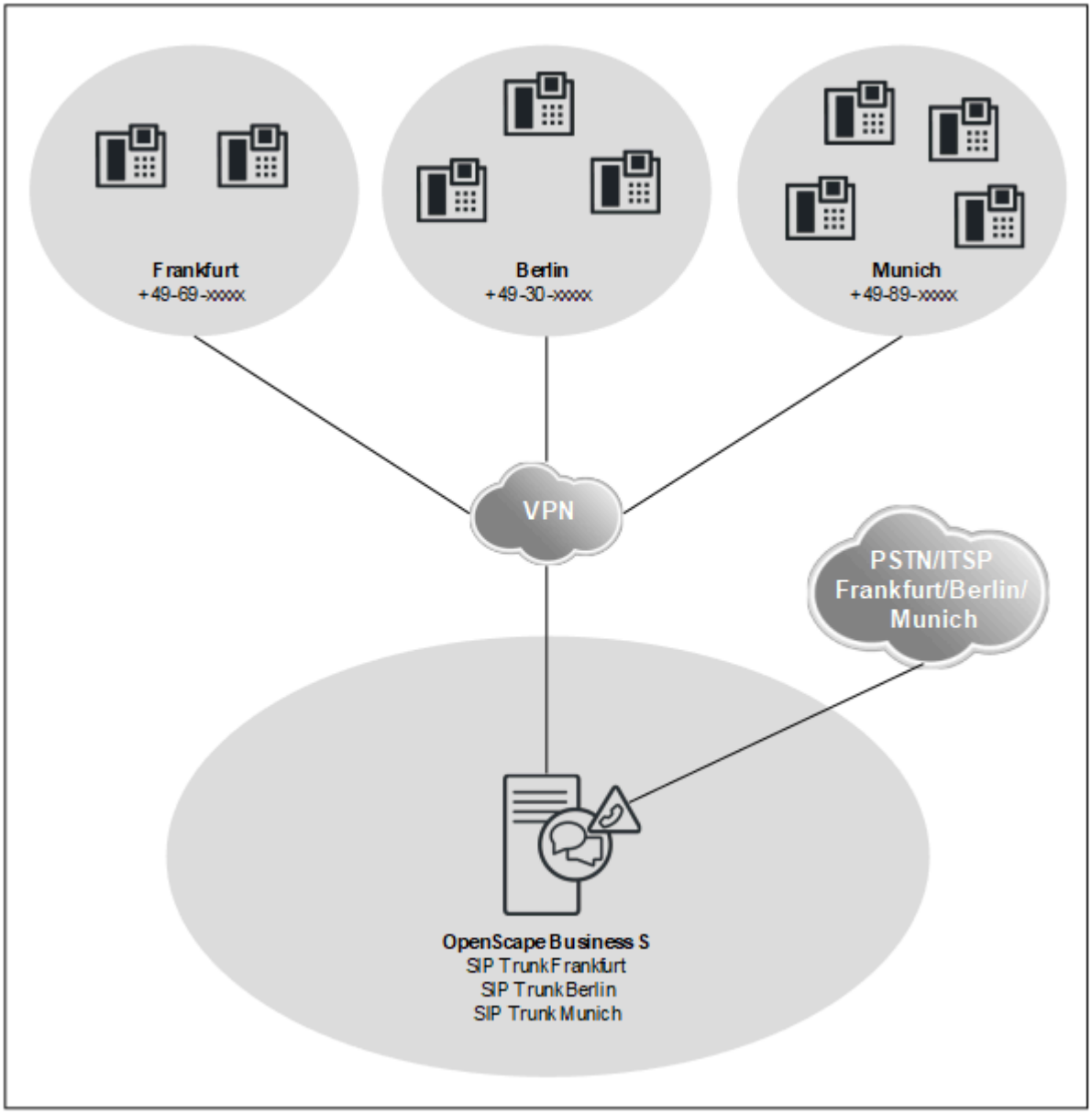
Datos de red



- Un cliente en una VPN o MPLS.
- Un OpenScape Business S por ubicación.
- Las ubicaciones pueden estar distribuidas en un país o entre varios países.
- Hasta 1000 usuarios y 180 troncos SIP por OpenScape Business S.
- Interconexión OpenScape Business opcional, hasta 1500 usuarios en total. Se pueden implementar instalaciones mayores en el marco de lanzamientos específicos de proyecto.

Escenario b: hosting con un OpenScape Business S para varias ubicaciones

Datos de red



- Un cliente en una VPN o MPLS.
- Un OpenScape Business S para todas las ubicaciones.
- Ubicaciones en un solo país.
- Hasta 8 ubicaciones con diferentes prefijos de ubicación.
- Hasta 8 proveedores SIP por OpenScape Business S.
- Un proveedor SIP por ubicación.
- Hasta 1000 usuarios y 180 tronqueos SIP.
- Interconexión OpenScape Business con varios OpenScape Business S en una VPN de manera opcional (OS Biz S 1 en país 1, OS Biz S 2 en país 2, etc.), hasta 1500 usuarios en total. Se pueden implementar instalaciones mayores en el marco de lanzamientos específicos de proyecto.

- Para ver un ejemplo de configuración, consulte la wiki para expertos en Internet, en *ITSP Configuration Guide* (Guía de configuración de ITSP).

21.6.6 Interconexión de OpenScape Business X y OpenScape 4000

Las interconexiones de OpenScape Business X con OpenScape 4000 pueden ser de dos tipos. Primero, con el direccionamiento directo entre los nodos OpenScape Business (escenario 4a) y, en segundo lugar, con el enrutamiento de todas las conexiones mediante OpenScape 4000 (escenario 4b).

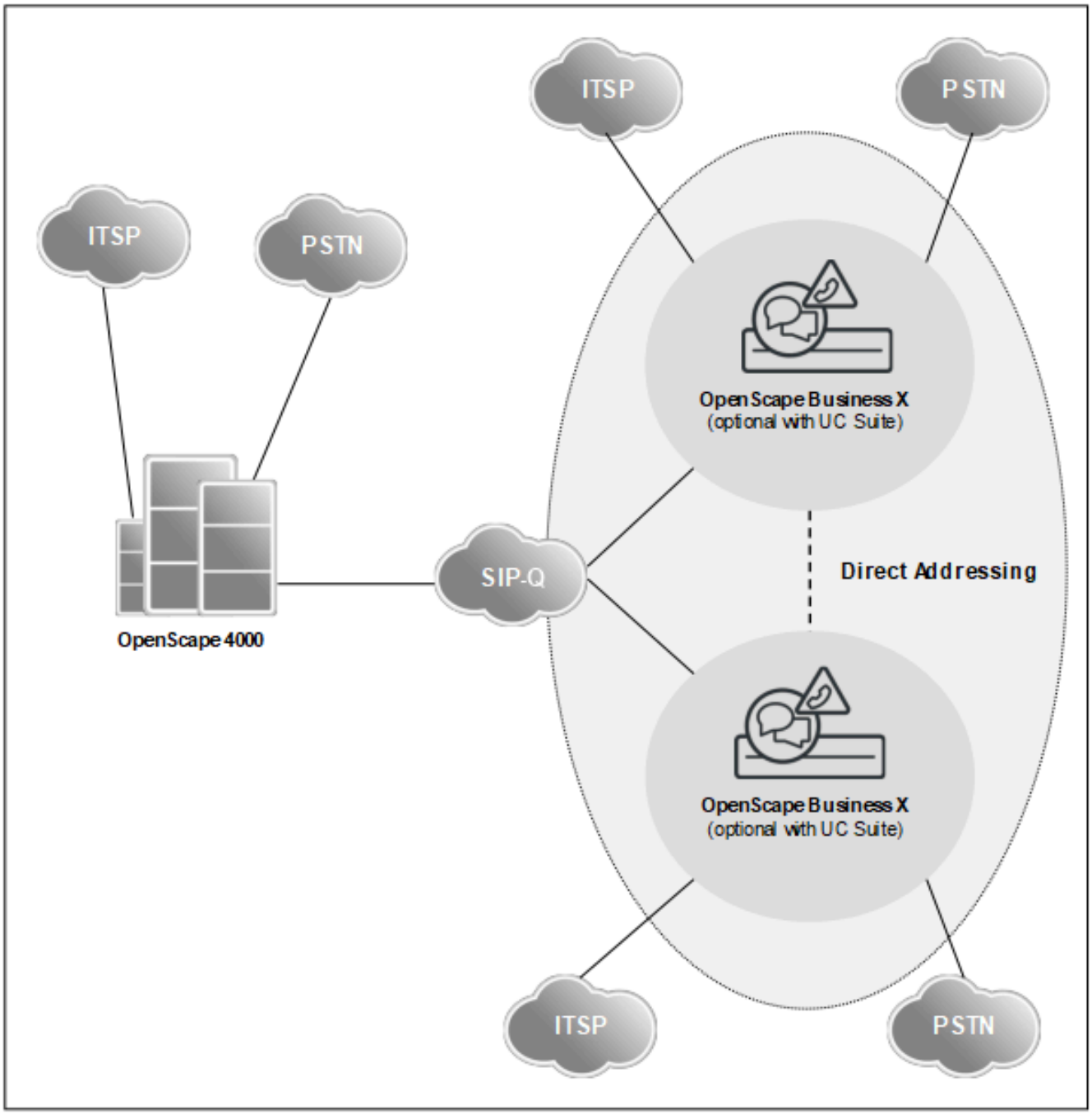
Nota: Puede encontrar un ejemplo de configuración para la interconexión con OpenScape Voice en la wiki de expertos de Unify, en la dirección `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`

Escenario a: Internet funciona con OpenScape 4000 y direccionamiento directo entre nodos OpenScape Business X

Datos de red:

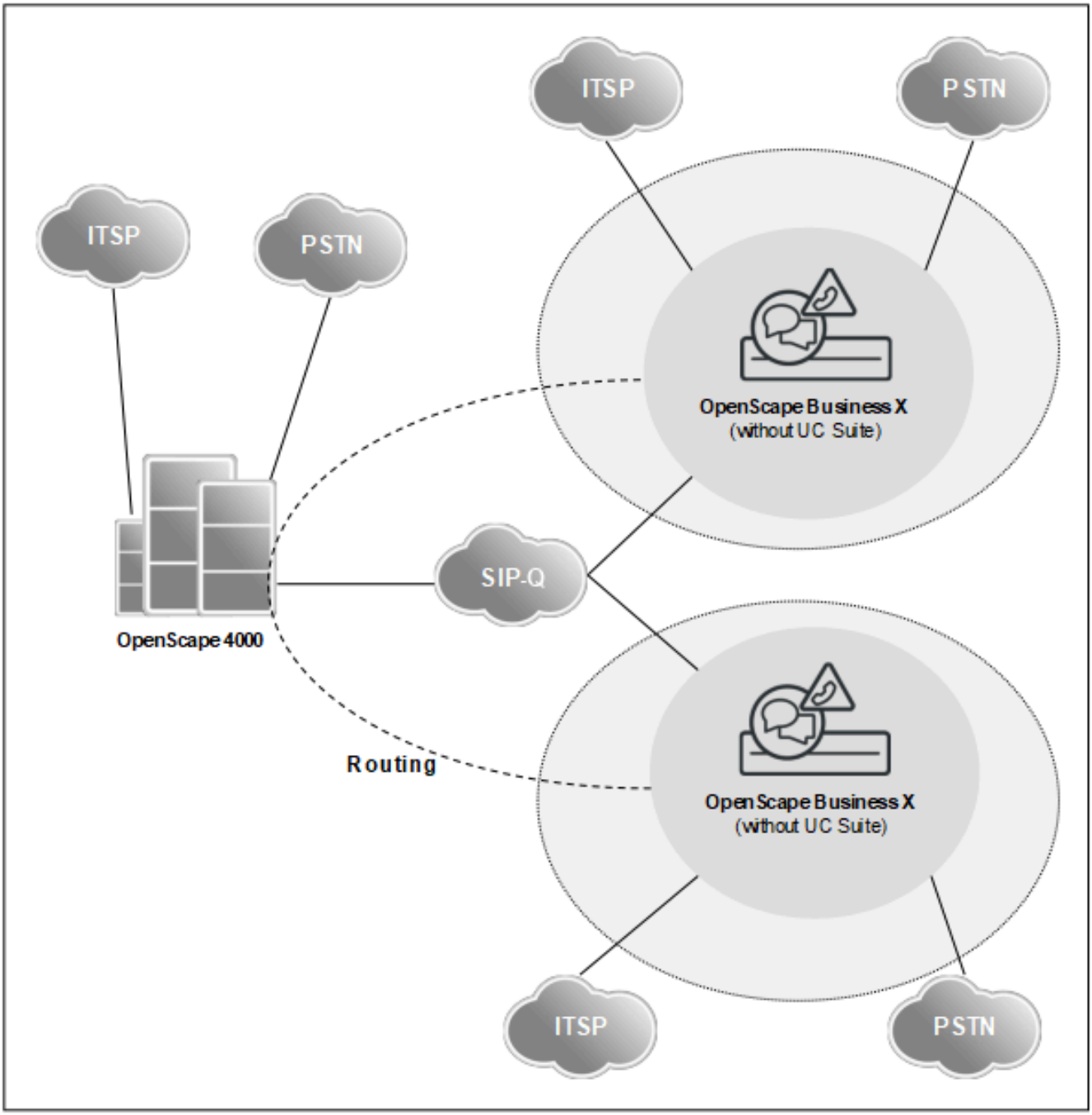
Escenario b: Internet funciona con OpenScape 4000 y enrutamiento de todas las conexiones mediante OpenScape 4000

Datos de red:



- Numeración cerrada en la interconexión OpenScape Business
- Funciones UC y de voz a nivel de red dentro de la interconexión OpenScape Business

- Configuración asistente Interconexión para intercon. OpenScape Business
- Configuración parte de red OpenScape 4000 en el Modo Experto
- El concepto SRS (Small Remote Site) no es compatible
- Las funciones de Unified Communications mediante UC Booster Server o UC Booster Card son opcionales.
- OpenScape Business S se puede integrar en modo gateway único o multigateway.



- Numeración abierta
- Funciones de voz a nivel de red
- Todas las llamadas a otro nodo se encaminan mediante OpenScape 4000

- Ninguna solución de UC con OpenScape Business por la numeración abierta de la interred
- El concepto SRS (Small Remote Site) no es compatible
- La configuración de cada nodo se debe hacer en el Modo Experto

Prestaciones a nivel de red

Extensión	Numeración cerrada en la interconexión de OpenScape Business (escenario 4a)	Numeración abierta (Escenario 4b)
Número máximo de nodos	100 (32 liberados, dependiente de OpenScape 4000	
Número máximo de extensiones por sistema	Según el modelo de OpenScape Business X	
Número máximo de extensiones en la red	1500 para la parte de red OpenScape Business	Depende de OpenScape 4000
Interconexión de voz	SIP-Q	

Interconexión UC	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
	Funciones a nivel de red de OpenScape Business	No compatible
UC Booster Card	UC Smart: 51 - 150 extensiones (0 - 50 extensiones sin UC Booster Card) UC Suite: 0 - 150 extensiones	No compatible
UC Booster Server	UC Smart: desde 150 extensiones UC Suite: desde 150 extensiones	No compatible
OpenScape Business S	Compatible	No compatible

Administración	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
	Gestión basada en Web (WBM) con asistentes para nodos OpenScape Business, OpenScape 4000 se administra a través del Modo Experto de OpenScape Business	Administración a nivel de red, Modo Experto
WBM	WBM con asistentes	WBM con Modo Experto
Manager E	No recomendado	No recomendado
UC-Suite-Administration	WBM con asistentes para nodos OpenScape Business	No compatible
Imp. masiva datos archivos csv (núm. tel., núm. marc. dir., nomb)	Independiente para cada nodo de la interred	

Registro de licencia	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
Estructura licenc.	Se requiere licencia intercon. por OpenScape Business	

myPortal for Desktop / myPortal for Outlook (UC Suite)	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
	A nivel de red con las funciones UC mediante UC Booster Server, UC Booster Card o OpenScape Business S	No compatible
Mensajería instantánea	A nivel de red, en la interconexión OpenScape Business	No compatible
Buzón de voz	Las extensiones usan su sistema de buzón de voz local; no hay ningún buzón de voz central para toda la interred.	No compatible
Estado de presencia	A nivel de red, en la interconexión OpenScape Business	No compatible
Indicación de ocupado	A nivel de red, en la interconexión OpenScape Business	No compatible
Directorio interno / Favoritos	A nivel de red, en la interconexión OpenScape Business	No compatible
Directorio externo	Local, importando archivos csv	No compatible
Búsqueda en directorios externos de otros nodos	No posible	No compatible
Directorio offline externo (LDAP)	LDAP	No compatible

myAttendant	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
	Con las funciones UC mediante UC Booster Server, UC Booster Card o OpenScape Business S	No compatible
Mensajería instantánea	A nivel de red, en la interconexión OpenScape Business	No compatible
Buzón de voz	Las extensiones usan su sistema de buzón de voz local; no hay ningún buzón de voz central para toda la interred.	No compatible
Estado de presencia	A nivel de red, en la interconexión OpenScape Business	No compatible

myAttendant	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
Indicación de ocupado	A nivel de red, en la interconexión OpenScape Business	No compatible
Directorio interno / Favoritos	A nivel de red, en la interconexión OpenScape Business	No compatible
Directorio externo	Local, importando archivos csv	No compatible
Búsqueda en directorios externos de otros nodos	No posible	No compatible
Directorio offline externo (LDAP)	LDAP	No compatible

OpenScape Business Attendant	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
	Interfaz limitada a números de teléfono de 8 dígitos	Interfaz limitada a números de teléfono de 8 dígitos
Estado de presencia	Network-wide	
Indicación de ocupado	Network-wide	
Directorio externo	LDAP	LDAP
Puesto de operadora central	A nivel de red, en la interconexión OpenScape Business	

Company AutoAttendant (UC suite)	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
Company AutoAttendant: después de que AutoAttendant responda a una llamada, el llamante debe marcar el número con el que quiere conectarse.	Los scripts ccv permiten marcar números de teléfono desde el directorio interno dentro de la interred.	No compatible
AutoAttendant personal: después de que AutoAttendant responda a una llamada, el llamante debe marcar un número de una cifra para conectarse con el destino.	Se puede usar cualquier número de teléfono preconfigurado por una extensión UC	No compatible

Company AutoAttendant (UC smart)	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
Company AutoAttendant (UC smart)	Local	Local

myAgent	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
	Con las funciones UC mediante UCBoosterServer, UC Booster Card u OpenScape Business S. Todos los agentes están registrados en UN nodo. Llamadas CC salientes mediante los circuitos de tronqueo SIP-Q, PSTN e ITSP.	No compatible

myAgent	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
Mensajería instantánea	A nivel de red	No compatible
Buzón de voz (Grabación, Message Waiting Indication, consulta)	Las extensiones usan su sistema de buzón de voz local; no hay ningún buzón de voz central para toda la interred.	No compatible
Estado de presencia	A nivel de red	No compatible
Indicación de ocupado	A nivel de red	No compatible
Estado agen.	Local	No compatible
Directorio interno	A nivel de red	No compatible
Directorio externo	Local, importando archivos csv	No compatible
Búsqueda en directorios externos de otros nodos	No posible	No compatible
Directorio offline externo (LDAP)	LDAP	No compatible
Contactos Outlook	Local	No compatible
Transferir una llamada	Local	No compatible
Información de cliente	Local	No compatible
Informes	Local	No compatible

Aplicaciones externas	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
Aplicación TAPI de OpenScape Business	Véase Application Connectivity	
Aplicaciones CSTA externas		
Application Launcher		
OpenScape Contact Center	Véase Multimedia Contact Center	

Telefonía	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
Proveedor SIP (ITSP)	Local	Local
Proveedor PSTN	Local; a los nodos de red sin proveedor PSTN propio se accede mediante SIP-Q o el gateway correspondiente.	
Survivability (Seguridad en caso de caída de la interred o de OpenScape Business S)	Se admite entre OpenScape Business X y OpenScape Business S	No compatible
Marcación núm. tel. púb. nodo propio	Compatible	
Marc. núm. tel. público en nodo interc.	A nivel de red, en la interconexión OpenScape Business	

Mobility	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
DeskSharing	En un nodo; a nivel de red en la interconexión OpenScape Business con DLS	No compatible
Mobility con control MF del sistema	Local (no es compatible con OpenScape Business S)	Local
myPortal to go (Web Edition), UC Suite	Estado de presencia y directorios a nivel de red (cada nodo necesita para ello UC Booster Server, UC Booster Card u OpenScape Business S)	No compatible
myPortal to go (Web Edition), UC Smart	Local, no para UC Booster Server, UC Booster Card y OpenScape Business S	No compatible

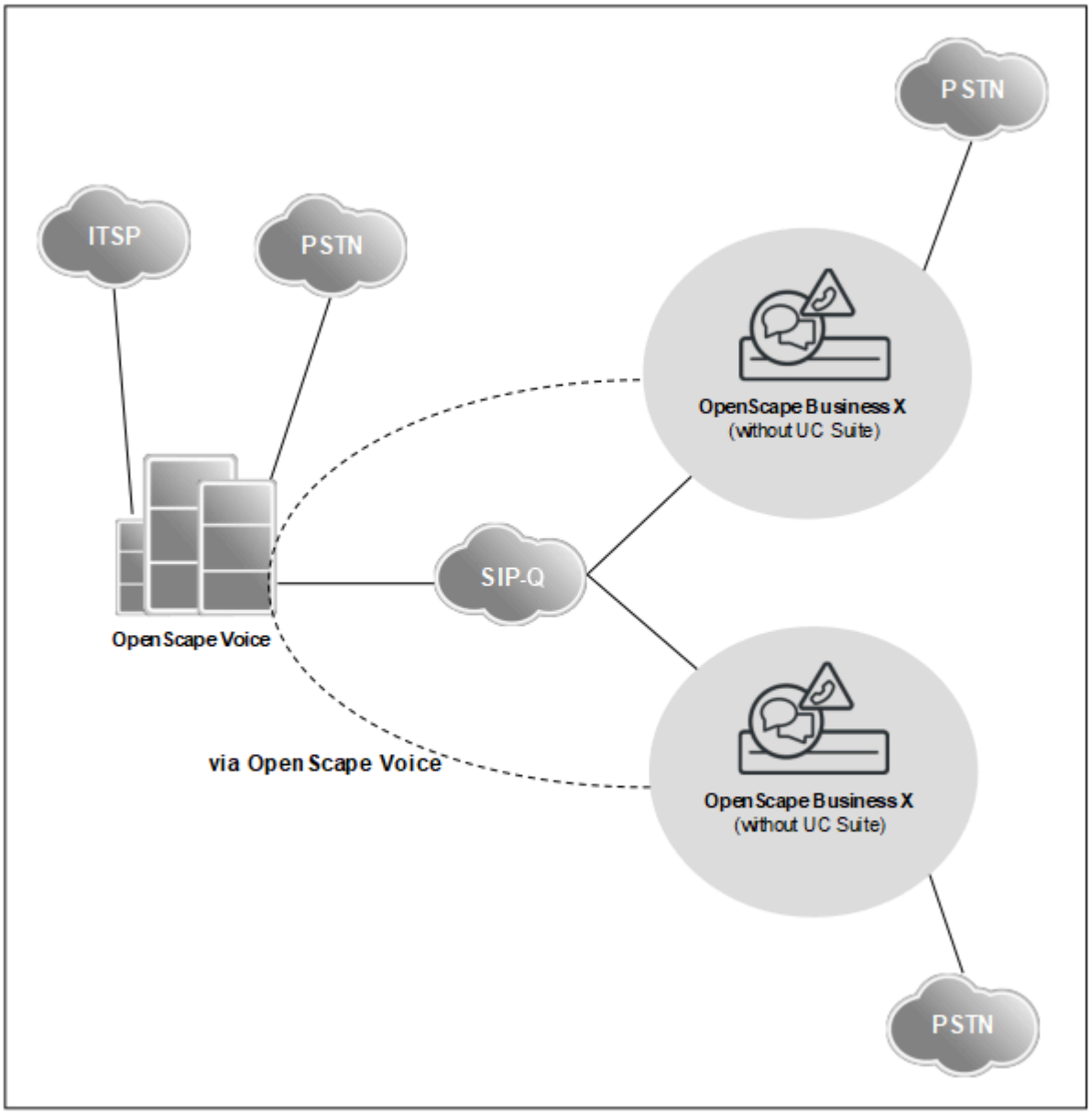
Otras funciones	Numeración cerrada (Escenario 4a)	Numeración abierta (Escenario 4b)
Cifrado de datos de señalización y carga útil (SPE)	Es compatible en interconexiones OpenScape 4000 / OpenScape Business. No compatible con conexiones UC y conferencias	Es compatible en interconexiones OpenScape 4000 / OpenScape Business. No compatible con conferencias
Servidor DSS	A nivel de red, en la interconexión OpenScape Business	No compatible
Telecaptura de llamadas	No compatible	No compatible

21.6.7 Interconexión de OpenScape Business X y OpenScape Voice

OpenScape Business X se puede interconectar con OpenScape Voice.

Nota: Puede encontrar un ejemplo de configuración para la interconexión con OpenScape Voice en la wiki de expertos de Unify, en la dirección `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`

Datos de red



- OpenScape Business X ofrece funciones de voz y de gateway a nivel de red para OpenScape Voice
- Se pueden utilizar uno o varios OpenScape Business X como gateway para líneas urbanas digitales (ISDN, T1, CAS)
- Con los gateways OpenScape Business X se pueden operar los siguientes terminales: digital, analógico, DECT, IP (HFA)
- Por norma general, UC no es compatible en esta interconexión por el lado de OpenScape Business X.
- Toda conversación de un nodo a otro se encamina a través de OpenScape Voice.
- Los nodos se configuran a través del Modo Experto.
- El plan de numeración de OpenScape Voice se basa en E.164, por lo que no hay numeración abierta ni cerrada.

Prestaciones a nivel de red

Ampliación máxima	
Número máximo de nodos	Depende de OpenScape Voice
Número máximo de extensiones en un sistema de comunicación	En función de OpenScape Business X
Número máximo de extensiones en la red	Depende de OpenScape Voice

Administración	
WBM	El asistente Interconexión no se puede utilizar. OpenScape Voice se administra por nodos a través del Modo Experto de OpenScape Business.
Manager E	No recomendado
Administración de UC	UC no es relevante en relación con OpenScape Voice
Importación masiva de datos mediante archivos csv (números de teléfono, números de marcación directa, nombres)	Por separado para cada nodo de OpenScape Business de la interred

Registro de licencia	
Estructura de licencias	Cada nodo por separado; por cada nodo OpenScape Business se requiere una licencia de red.

Restricciones e indicaciones sobre las prestaciones

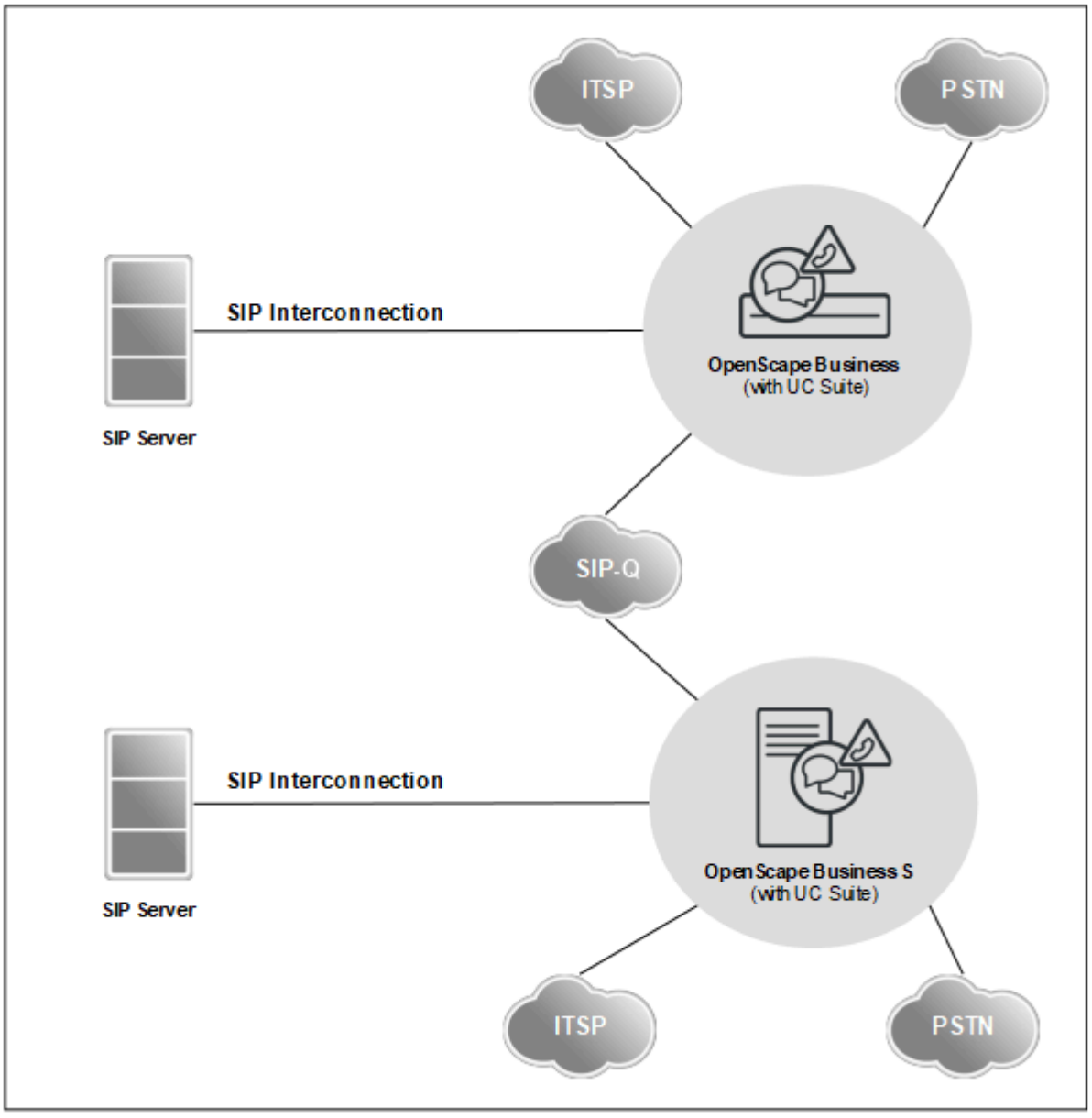
- La conexión de líneas urbanas analógicas con los gateways OpenScape Business **solo** está autorizada para Brasil (por la compatibilidad de Line Reversal y la liberación hacia atrás de líneas urbanas analógicas en las líneas urbanas de ese país).
- No se admite la interconexión en red de gateways OpenScape Business entre sí o con otros sistemas como OpenScape Voice. La interconexión en red de los gateways OpenScape Business con OpenScape Voice debe realizarse mediante una estructura de red en estrella.
- Path Replacement (optimización de rutas) a través de SIP-Q no Terminales se admite para los terminales conectados en un gateway OpenScape Business.
- Para evitar un empeoramiento de la calidad de voz con conexiones de líneas de tránsito, es conveniente utilizar el códec de voz G.711. No se recomienda utilizar el códec G.729, ya que prestaciones como Conferencia y Desvío llamadas podrían ocasionar el establecimiento de conexiones de líneas de tránsito, ya que no se admite Path Replacement (optimización de rutas).
- No se admiten prestaciones para todo el sistema como por ejemplo Grupos de telecaptura de llamadas, Llamadas de grupo y Líneas colectivas entre OpenScape Voice y gateways OpenScape Business. Los grupos pueden incluir solo OpenScape Voice o sólo extensiones OpenScape Business.
- Se admite el cifrado (SPE) entre gateways OpenScape Business y OpenScape Voice. La conexión entre OpenScape Voice y OpenScape Business debe realizarse mediante el protocolo de cifrado TLS. SRTP (SDES) no se admite en las interconexiones con OpenScape Voice V7R1.
- Solo se admite la interconexión en red con plan de numeración E.164.

- En el caso de los terminales IP (HFA) conectados con gateways OpenScape Business: para cada conexión activa OpenScape Business/OpenScape Voice se requieren 2 canales B por terminal HFA (1 canal B por terminal TDM). Hay que comprobar y tener en cuenta estos recursos DSP adicionales requeridos.

21.6.8 Conectar equipo auxiliar externo con OpenScape Business mediante la interconexión SIP

Se puede conectar equipo externo con OpenScape Business mediante la interconexión SIP, por ejemplo para poder usar aplicaciones como OpenScape Alarm Server, OpenScape 4000, OpenScape Voice u otros servidores SIP certificados.

Requisitos



- Solo se pueden conectar aplicaciones certificadas como OScAR.
- Un servidor SIP externo se puede conectar mediante el protocolo SIP o SIP-Q nativo.
- Hay disponibles dos rutas SIP-Q como máximo (una se requiere para la UC Suite, en su caso) y diez rutas SIP nativas como máximo (para ITSP se pueden utilizar hasta 8 rutas SIP nativas).

Encontrará información más detallada en la

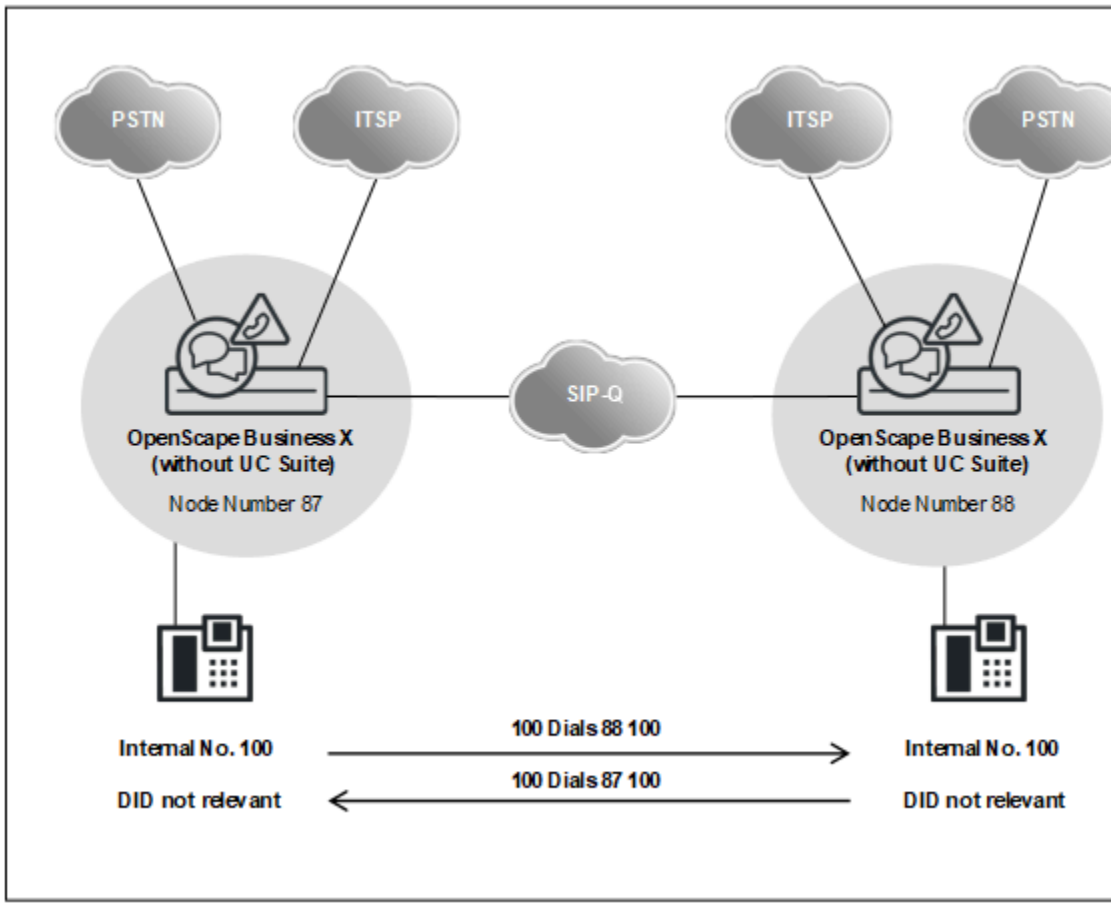
- Wiki para expertos sobre temas de telefonía, sistemas de comunicación y UC:

  `http://wiki.unify.com`

21.6.9 Numeración abierta en redes OpenScape Business X

Se puede configurar una interred con numeración abierta si se interconectan dos (o varios) sistemas de comunicación cuya numeración se solapa (es decir, la numeración no es única en la interred).

Datos de red



- Interconexión de voz a nivel de red con OpenScape Business.
- Las prestaciones de UC no son compatibles.
- Cada llamada en un nodo se realiza con número de teléfono interno.

- Cada llamada a otro nodos se realiza con número de nodo (más el número de teléfono interno).
- Configuración de cada nodo mediante el Modo Experto. El asistente Interconexión está bloqueado en cuanto hay configurado un número de nodo para numeración abierta.
- Línea urbana PSTN y ITSP son locales en cada nodo.

Nota: Si se hace una extensión a nivel de red con funcionalidad de UC, hay que cambiar de numeración abierta a cerrada para adaptar los números internos. Hay que desactivar la numeración abierta; además, hay que eliminar el número de nodo y añadirlo luego como prefijo (por ejemplo, el número interno extendido 87100 en lugar de 100 y 88100 en lugar de 100).

Diferencias:

- La selección de participantes en su propio nodo se realiza con el número interno extendido.

- El número interno y el número de marcación directa pueden ser diferentes en caso necesario, pero no hay que cambiar los números de marcación directa.

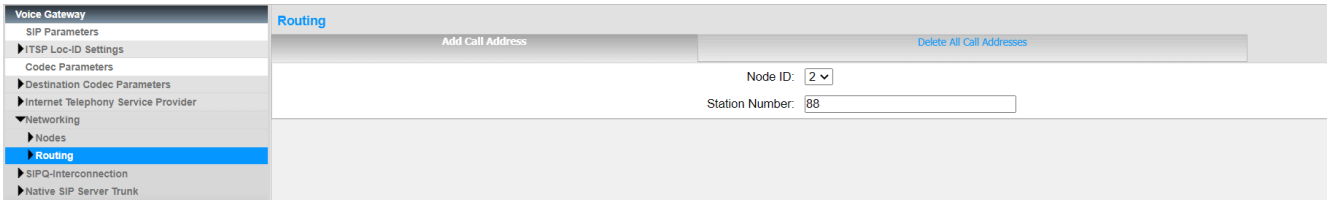
21.6.9.1 Cómo configurar la numeración abierta

Configurar la numeración abierta

1) Habilitar la numeración abierta para el sistema de comunicación a través del flag del sistema **Numeración abierta**
2) Introducir el número de nodo propio (en el ejemplo, "87")

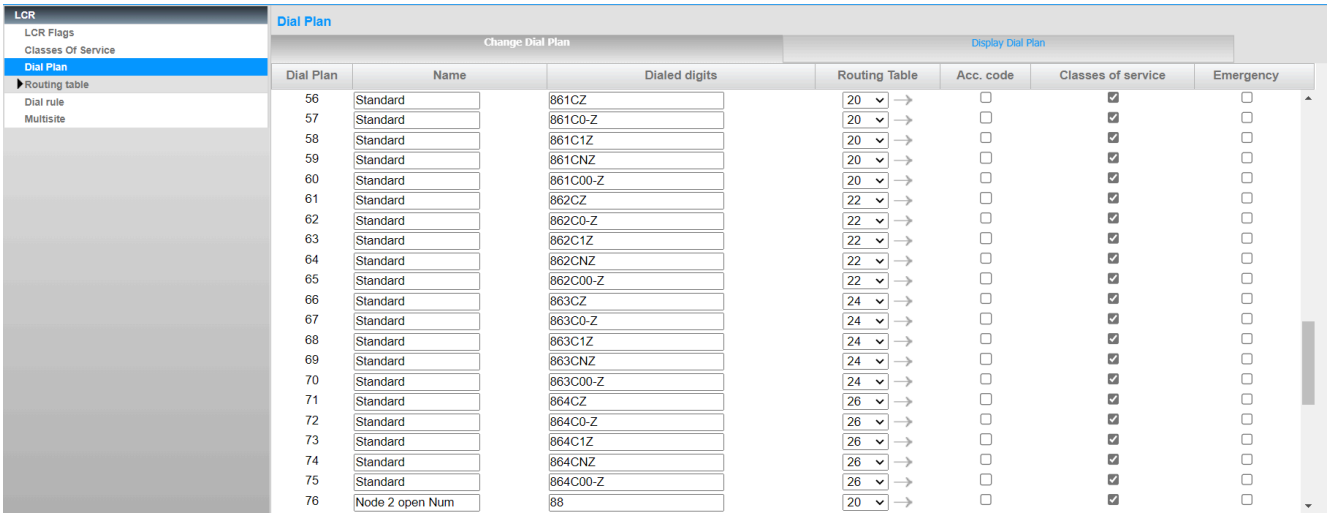
Configurar nodo (encaminamiento)

1) Los nodos de destino se direccionan mediante Gateway voz > Redes > Nodo > Encaminamiento (en el ejemplo, "88").
2) Si se utiliza una Numeración abierta, no se puede usar el asistente **Interconexión**; lo impide el flag del sistema **Numeración abierta**.



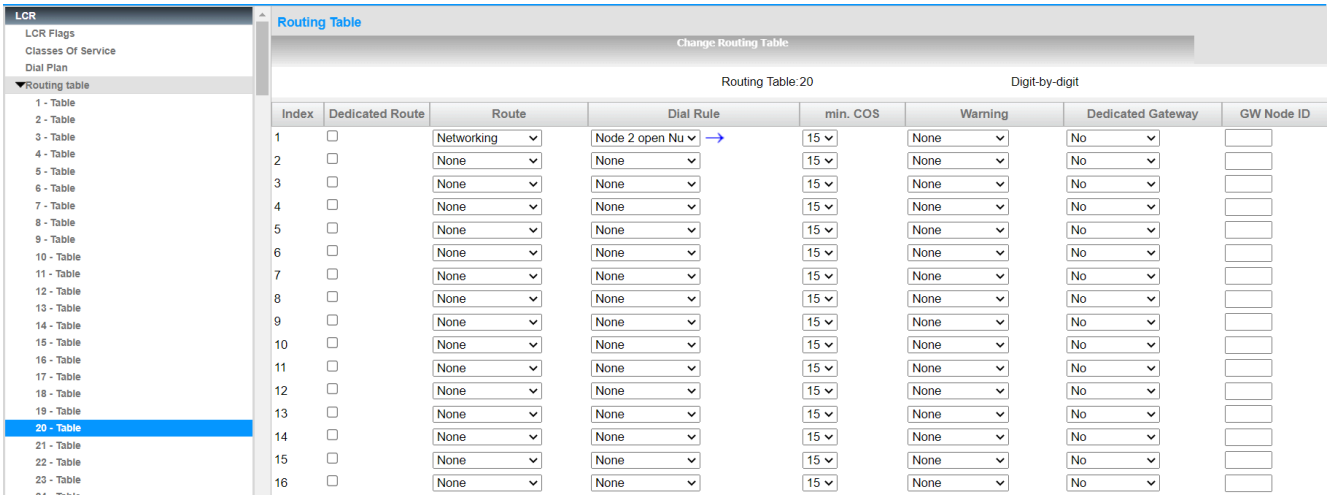
Configurar LCR

1) Definir la regla de marcación "Node 2 open Num" para el número de nodo y seleccionar la tabla de encaminamiento correspondiente.



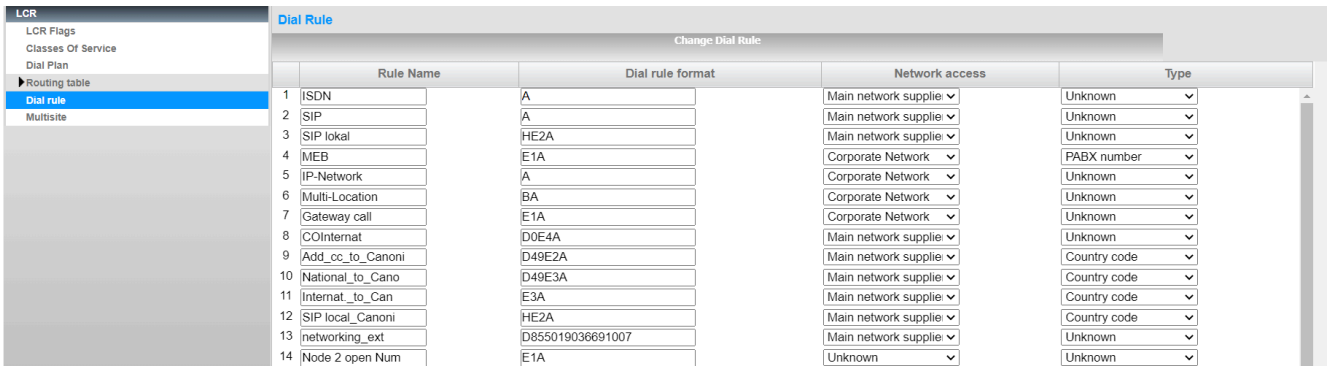
Dial Plan	Name	Dialed digits	Routing Table	Acc. code	Classes of service	Emergency
56	Standard	861CZ	20	☐	☑	☐
57	Standard	861C0-Z	20	☐	☑	☐
58	Standard	861C1Z	20	☐	☑	☐
59	Standard	861CNZ	20	☐	☑	☐
60	Standard	861C00-Z	20	☐	☑	☐
61	Standard	862CZ	22	☐	☑	☐
62	Standard	862C0-Z	22	☐	☑	☐
63	Standard	862C1Z	22	☐	☑	☐
64	Standard	862CNZ	22	☐	☑	☐
65	Standard	862C00-Z	22	☐	☑	☐
66	Standard	863CZ	24	☐	☑	☐
67	Standard	863C0-Z	24	☐	☑	☐
68	Standard	863C1Z	24	☐	☑	☐
69	Standard	863CNZ	24	☐	☑	☐
70	Standard	863C00-Z	24	☐	☑	☐
71	Standard	864CZ	26	☐	☑	☐
72	Standard	864C0-Z	26	☐	☑	☐
73	Standard	864C1Z	26	☐	☑	☐
74	Standard	864CNZ	26	☐	☑	☐
75	Standard	864C00-Z	26	☐	☑	☐
76	Node 2 open Num	88	20	☐	☑	☐

2) Indicación de la ruta configurada



Index	Dedicated Route	Route	Dial Rule	min. COS	Warning	Dedicated Gateway	GW Node ID
1	☐	Networking	Node 2 open Nu	15	None	No	
2	☐	None	None	15	None	No	
3	☐	None	None	15	None	No	
4	☐	None	None	15	None	No	
5	☐	None	None	15	None	No	
6	☐	None	None	15	None	No	
7	☐	None	None	15	None	No	
8	☐	None	None	15	None	No	
9	☐	None	None	15	None	No	
10	☐	None	None	15	None	No	
11	☐	None	None	15	None	No	
12	☐	None	None	15	None	No	
13	☐	None	None	15	None	No	
14	☐	None	None	15	None	No	
15	☐	None	None	15	None	No	
16	☐	None	None	15	None	No	

3) Introducir el nombre de la ruta "Redes" y la regla de marcación correspondiente "Node 2 open Num".

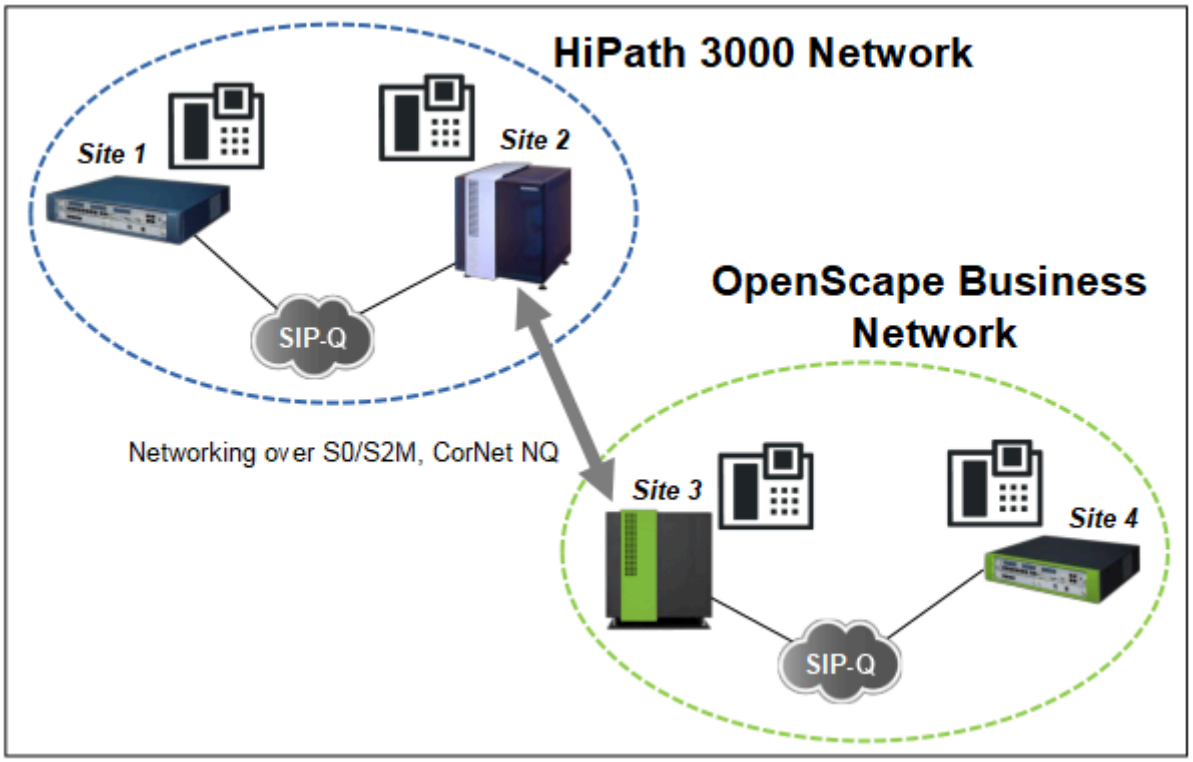


	Rule Name	Dial rule format	Network access	Type
1	ISDN	A	Main network supplie	Unknown
2	SIP	A	Main network supplie	Unknown
3	SIP lokal	HE2A	Main network supplie	Unknown
4	MEB	E1A	Corporate Network	PABX number
5	IP-Network	A	Corporate Network	Unknown
6	Multi-Location	BA	Corporate Network	Unknown
7	Gateway call	E1A	Corporate Network	Unknown
8	COInternat	D0E4A	Main network supplie	Unknown
9	Add_cc_to_Canoni	D49E2A	Main network supplie	Country code
10	National_to_Cano	D49E3A	Main network supplie	Country code
11	Internat_to_Can	E3A	Main network supplie	Country code
12	SIP local_Canoni	HE2A	Main network supplie	Country code
13	networking_ext	D85501903669100 7	Main network supplie	Unknown
14	Node 2 open Num	E1A	Unknown	Unknown

21.6.10 Interconexión mediante RDSI

Los sistemas OpenScape Business se pueden interconectar entre sí y con los sistemas de comunicación HiPath 3000 y OpenScape 4000 mediante líneas de conexión digitales. La conexión se puede realizar mediante líneas S_0 y S_{2M}.

Interconexión en red con HiPath 3000



La red HiPath 3000 existente permanece (en principio) intacta. La red se amplía con OpenScape Business. Si es necesario, los nodos HiPath 3000 se pueden migrar gradualmente a la red OpenScape Business.

Todas las llamadas HiPath 3000/OpenScape Business se conducen a través de gateways TDM correspondientes (S_0 o S_{2M} con protocolo CorNet NQ, en su caso con QSIG como protocolo independiente del fabricante).

Se aplican las siguientes condiciones generales:

- Registro de licencia independiente de HiPath 3000 / OpenScape Business
- Administración independiente de HiPath 3000 / OpenScape Business
- Recomendación: numeración cerrada en la red conjunta. Con numeración abierta pueden darse errores de comportamiento en CLIP y con entradas de diario/listas de llamantes.
- Recomendación: utilizar exclusivamente el códec G.711 para garantizar una buena calidad de voz en la red conjunta.
- El número de canales B debe corresponderse con el volumen de llamadas esperado.
- OpenScape Business requiere siempre una licencia de Networking..

Conexión de sistemas externos mediante QSIG

Al conectar sistemas externos con el protocolo QSIG hay que tener en cuenta los siguientes aspectos:

- Comprobar la compatibilidad de las variantes QSIG de los sistemas externos afectados (QSIG V1 o QSIG según el estándar ECMA, o QSIG V2 también denominado QSIG según el estándar ISO)
- Comparativa de los conjuntos de prestaciones de los sistemas afectados. Con ello se puede deducir en qué medida se corresponde con los deseos del cliente el abanico de funciones que cabe esperar en teoría, esto es, en qué medida los conjuntos de prestaciones de ambas variantes se corresponden con las necesidades del cliente.
- Para ampliar las garantías de las prestaciones esperadas se recomienda realizar una prueba de conexión in situ. Al hacerlo hay que tomar en consideración la interconectividad con otros protocolos de interconexión o de línea urbana.

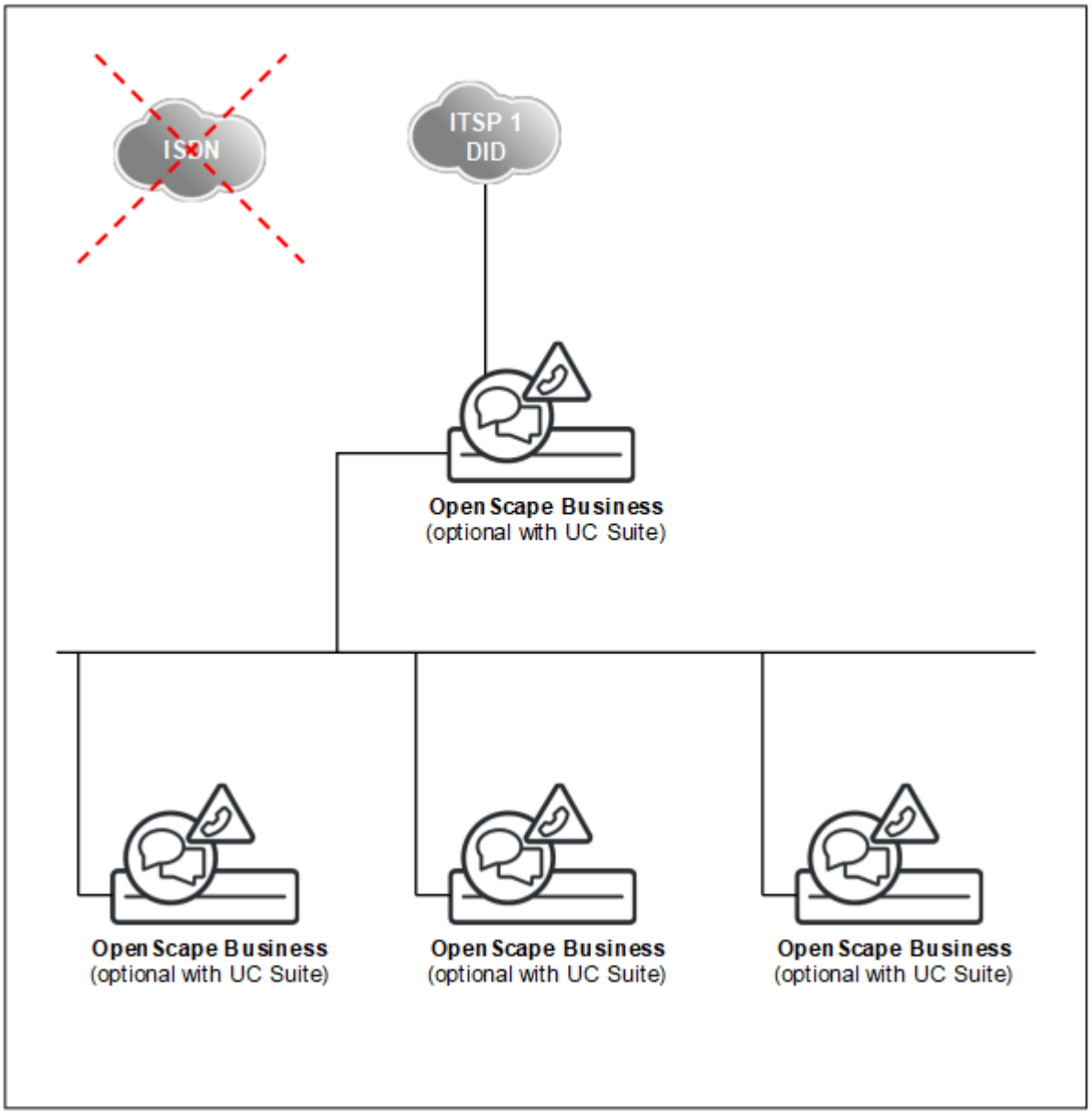
Nota:

El grupo troncal QSIG debe configurarse como ruta de tipo PABX en el sistema de OpenScape Business. Por lo tanto, las llamadas que procedan de la red QSIG se considerarán internas y seguirán CDL interno.

21.6.11 Interred OpenScape Business con conexión central de línea urbana ITSP

En lugar de con RDSI, las interconexiones puras de OpenScape Business se pueden implementar con una conexión central de línea urbana ITSP con capacidad de marcación directa.

Interconexión con conexión central de línea urbana ITSP con capacidad de marcación directa



Al planificar las redes de clientes hay que tener en cuenta los siguientes aspectos:

- **Una** conexión central de línea urbana ITSP con capacidad de marcación directa para toda la red OpenScape Business.
- Registro en una red local, es decir: todos los nodos de la red utilizan exactamente un número de teléfono de línea urbana, por ejemplo, 0049 89 7007-xxxxx.
- Los nodos interconectados se pueden utilizar para emergencias, es decir, en caso de caída del acceso central de ITSP se pueden utilizar conexiones propias de línea urbana para las conexiones salientes. Es posible que en este caso no se pueda hacer una identificación correcta del llamante hacia el exterior. Es posible que las llamadas de emergencia no se puedan entregar correctamente. La accesibilidad entrante mediante esta conexión local también está ligada con ciertas restricciones. Por los motivos

señalados, no se recomiendan las conexiones locales, pero no se impiden técnicamente.
- Por el mismo motivo, no se recomienda utilizar conexiones RDSI adicionales en el nodo local, pero tampoco se impide su implementación técnicamente.
- Se aplican todas las reglas para la evaluación de marcación y Call Routing (encaminamiento de llamadas) para redes y sistemas individuales de OpenScape Business. En este caso, la asignación de números de teléfono de los números de teléfono de línea urbana ITSP se realiza exclusivamente mediante la configuración de marcación directa de la extensión (no mediante la tabla de Mapping, véase Configuración de ITSP en el capítulo 9.2 y la wiki de expertos de Unify en Internet).

21.7 Puesto de interceptación central en la interred (no para EE. UU.)

OpenScape Business permite desviar llamadas entrantes que no están asignadas a ningún usuario o a las que no se responde a un puesto de interceptación definido de la interred para que no se pierda ninguna llamada.

Si el puesto de interceptación central de la interred está configurado mediante RDSI, el funcionamiento es idéntico al funcionamiento sin interconexión.

En combinación con una línea urbana ITSP resultan algunas restricciones para el puesto de interceptación central, ya que cada nodo tiene su propio ITSP:

- Los criterios de interceptación ITSP solo son válidos para el nodo correspondiente.
- Funcionan la interceptación en caso de libre, en caso de dispositivo ocupado, en caso de marcación incompleta, en caso de marcación errónea y en caso de llamada recordatoria sin contestar.
- Los tipos de interceptación "marcación errónea" e "incompleta" no funcionan con ITSP.
- Los números de teléfono incorrectos o incompletos se devuelven al ITSP con señal de ocupado.

Si desea utilizar un puesto de interceptación central en una interred, en cada nodo deben configurarse extensiones virtuales. Estas extensiones virtuales se desvían al usuario myAttendant a través de la interred.

Ejemplo de línea urbana ITSP: si el número de teléfono del sistema ITSP es 0211-23456789 + número de marcación directa ITSP, se publica el número de teléfono 0211-23456789-0 como número central del sistema de comunicación.

- La extensión 100 es myAttendant con número de marcación directa de ITSP propio 100 y una extensión virtual 199 con el número de marcación directa de ITSP "0".
- En la lista de asignación de ITSP de cada nodo el número de marcación directa de ITSP "0" se asigna a la extensión virtual propia.
- En **Llamadas entrantes/Transferencia automática diferida**, las extensiones virtuales se asignan a la extensión 100.

  Primer destino: extensión virtual propia

  Segundo destino: extensión 100 en el nodo de destino

  Tiempo de llamada 5 segundos

Para identificar mejor las llamadas es recomendable dotar a las extensiones virtuales de todos los nodos con su número de teléfono (DID) y un

nombre (por ejemplo, Empresa) a través de la aplicación myAttendant (en **Configuración**/**myAttendant**/**Números de llam. de marcación directa**). Con ello, en la ventana **Llamadas activas** de myAttendant se puede realizar una identificación detallada del llamante.

21.7.1 Cómo configurar un puesto de interceptación central en una interred multigateway

Ejemplo de configuración para un puesto de interceptación central en la interred multigateway a través de los gateways OpenScape Business preconectados. Todas las llamadas que entran en un nodo y que cumplan con los criterios de interceptación se deben encaminar a OpenScape Business S, donde se encuentra el AutoAttendant central.

Requisitos previos

OpenScape Business S es el maestro (todas las extensiones HFA y SIP están registradas en él).

Varios OpenScape Business X están configurados como nodos esclavos (con PSTN o ITSP como línea urbana). Los nodos pueden estar en el mismo lugar o en un ubicaciones diferentes (distintas marcaciones previas).

Paso a paso

1) Configuración de una extensión virtual en OpenScape Business.
   a) Configuración de una extensión virtual con el nombre "Interceptación 22 System2"

2) Configuración de un puesto de interceptación central con criterios de interceptación en OpenScape Business.
   a) **Modo experto**
   b) **Configuración básica** > **Sistema** > **Interceptación/PO/Hot-line**
   c) Seleccione la extensión virtual 22 en **Puesto de interceptación**, **Día y Noche**.
   d) Introduzca los siguientes parámetros para la extensión 22 en **Puesto de interceptación**, en **Interceptación**:

Nombre	Interceptación 22 System2
Marcación directa	xxxxxxx22
Tipo terminal	virtual

   e) Active los parámetros indicados en **Puesto de interceptación** en caso de **Interceptación**.
   f) Configuración de la extensión virtual en **Puesto de interceptación** con **Candado telefónico**.

3) Configuración de la transferencia automática diferida en OpenScape Business.

a) Configuración de la transferencia automática diferida de la extensión virtual 22 a través de la interred con OpenScape Business S.
b) **Modo Experto**
c) **Llamadas entrantes** > **Transferencia automática diferida**
d) Seleccione la extensión virtual 22
e) Pase a **Modificar transferencia autom. diferida**
f) A continuación: **Destino ext.** (introduzca los números de teléfono de las colas de AutoAttendant, por ejemplo, 7410)
g) Seleccione **Dirección =** Red (el número de teléfono de cola de AutoAttendant 7410 debe estar encaminado de forma selectiva en el LCR, con omisión de la regla predeterminada -Z 33).

4) Configuración del encaminamiento para OpenScape Business.

El número de teléfono de cola de espera de AutoAttendant 7410 debe estar encaminado de forma selectiva en el LCR (con omisión de la regla predeterminada -Z 33).

En **Plan marcación**:	Configure el **Nombre** (VSL Queue Pilot)
	Introduzca el número de teléfono en **Cifras marcadas** (7410)
	Seleccione **Tabla de rutas** (XX)
En **Tabla de rutas** XX:	Seleccione **Dirección =** Red
	Asigne la Regla de marcación
	En **Gateway dedicado**, seleccione la entrada **Obligatorio**
	Introduzca el **GW ID de nodo** de OpenScape Business S
En **Regla de marcación**:	Introduzca el **Nombre de regla**
	Introduzca **Formato de regla de marcación** D7410 (número de Queue Pilot)
	Seleccione **Procedimiento de acceso del ofertante de red**: Red corporativa
	Seleccione Tipo: Desconocido

5) Configuración de una cola en OpenScape Business S.

a) Configuración de una cola (Queue Pilot) con un CCV, por ejemplo, **Marcar por extensión**, **Marcar por nombre**, **Iniciar proceso después de marcar los dígitos**.

6) Configuración de una transferencia automática diferida en OpenScape Business S.

a) Configuración de una transferencia automática diferida de Queue Pilot 7410 en OpenScape Business S.
b) **Modo Experto**
c) **Llamadas entrantes** > **Transferencia automática diferida**
d) Seleccione Queue Pilot 7410
e) Pase a **Modificar transferencia autom. diferida**
f) en primer lugar: **Destino externo** (introduzca los números de teléfono de colas de AutoAttendant, por ejemplo, 7410)
g) A continuación: seleccione **Buzón de voz**

21.8 Gestor de presencia

El Gestor de presencia permite señalizar a nivel de red los estados de extensión “Libre", “Ocupado" y “Llamada" en los LED de los teléfonos HFA. Se requiere para ello una numeración cerrada y al menos un UC Booster Server en el nodo maestro de la interred o un OpenScape Business S como nodo maestro. Por cada nodo se necesita una licencia de red.

Con el estado Libre, el LED correspondiente está pagado; con el estado Ocupado, está encendido permanentemente; con el estado Llamada, el LED parpadea. En el estado Llamada, se puede capturar pulsando la tecla correspondiente.

La señalización de los estados referidos a la conmutación de una extensión solo es posible si el Presence Manager puede ajustar un punto de monitoreo CSTA en dichas extensiones.

La configuración de las teclas corre a cargo del usuario. Al llevar a cabo la programación en el propio teléfono no se distingue si se trata de un número de teléfono interno o para toda la red.

El Gestor de presencia es un servicio sin interfaz de usuario. No hay que hacer ningún ajuste, ya que todos los datos se derivan automáticamente con una comparación.

El Gestor de presencia no es compatible con grupos. No tiene lugar la señalización LED y no es posible la telecaptura de llamadas. Por contra, el Gestor de presencia sí admite MULAP.

el Gestor de presencia no admite de forma activa teléfonos SIP ni S_0.

21.9 Estado de sincronización en la interred

En una interred, el estado de sincronización del portal de administración y el estado de registro de los distintos nodos se indica mediante botones de colores. La indicación del estado de sincronización vale para nodos del sistema de comunicación, no para nodos OpenScape 4000 ni OpenScape Voice.

Indicación del estado de sincronización

Indicación	Color	Significado para el maestro	Significado para el esclavo
Estado de sincronización (indicación en la página de inicio del portal de administración)	Rojo	-	La dirección IP del nodo maestro está configurada, pero el sistema esclavo no se ha podido registrar. A intervalos cíclicos, el esclavo intenta registrar en el maestro.
	Amarillo	-	El esclavo está registrado en el maestro, pero los números de teléfono no son consistentes en la interred. Puede producirse tras una proceso de copia de seguridad/restauración o tras el primer registro.
	Verde	Si un nodo está configurado como nodo maestro, el estado aparece en color verde.	
Estado de registro de los distintos nodos (indicación en el cuadro de diálogo Red>Vista de dominios)	Rojo	El esclavo está configurado; pero el sistema aún no se ha registrado.	El esclavo está configurado; pero el sistema aún no se ha registrado.
	Verde	El sistema está registrado.	El sistema está registrado.
Alive (indicación en el cuadro de diálogo Red>Vista de dominios)	Rojo	Mirada específica de nodo a la interred: no se puede acceder a todos los nodos marcados en rojo. El motivo pueden ser problemas de red o una caída del sistema de comunicación.	
	Verde	Se puede acceder al nodo (ajeno) a través de la red. El nodo propio siempre aparece en verde.	

21.9.1 Sincronización manual en la interred

Si después de configurar números de teléfono/nombres (números de teléfono de marcación directa o internos), éstos no se sincronizan automáticamente con los demás sistemas de una interred, se puede realizar una sincronización manual. La sincronización manual en la interred solo funciona en interconexiones homogéneas.

Maestro

Esclavo

El proceso de sincronización solo transmite cambios de configuración.

Si el indicador de estado del portal de administración está en "rojo", al accionar el botón de sincronización se puede iniciar la sincronización manual de los datos en el nodo maestro.

Si los sistemas ya configurados de la red no pueden establecer comunicación telefónica entre ellos, hay que determinar por otra vía la causa de la avería. Si el estado Alive de los distintos nodos es "rojo", indica un problema de red o que hay otros motivos por los que no se puede acceder a los nodos de la red. En estos casos, no vale de nada accionar el botón de sincronización.

Al realizar la activación en el nodo maestro, se solicita a los nodos esclavos actualizar los números de teléfono y nombres del sistema del maestro.

Al realizar la activación en un nodo esclavo, se actualizan los números de teléfono y nombres del sistema en el maestro. Al mismo tiempo, se renueva el registro del nodo esclavo en el nodo maestro.

21.9.2 Cómo iniciar la sincronización manual

Requisitos previos

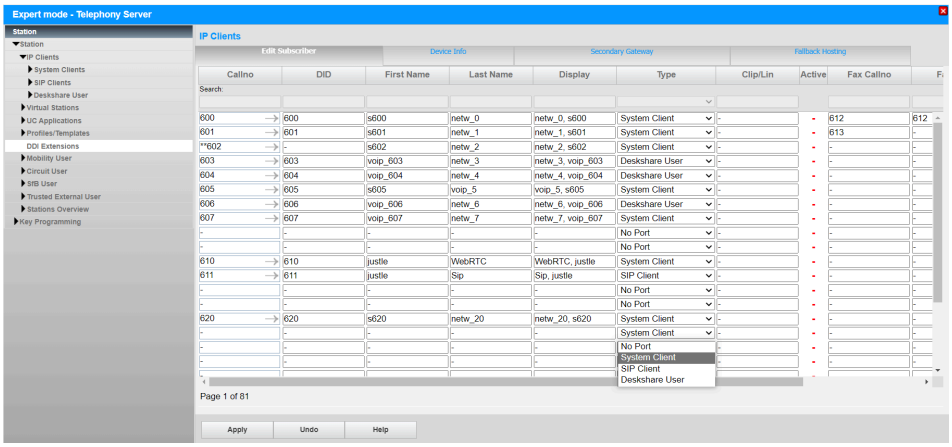
Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Reiniciar / Volver a cargar**.
3) Active el botón **Sync Network** (Sincronizar red) para iniciar la sincronización de forma manual.

21.10 Supervivencia

La supervivencia es una herramienta de la red de nodos de OpenScape Business. Si falla un nodo de OpenScape Business o no se puede acceder a él debido a un error en la red, los teléfonos del sistema (HFA) que estén conectados a dicho nodo podrán conectarse a otro diferente. Los números de los teléfonos del sistema se guardan después del nuevo acceso. Esto permite que la telefonía básica no se interrumpa. Sin embargo, otras opciones como el buzón de voz, los sistemas CTI o las aplicaciones, como myPortal, no estarán disponibles.



Cuando se pueda volver a acceder de forma segura al nodo de OpenScape Business que ha fallado, los teléfonos del sistema se conectarán a este automáticamente.

El tiempo para acceder a la pasarela de espera puede durar hasta 30 minutos.

En primer lugar, si se produce un error en el nodo de OpenScape Business, se intentará llevar a cabo la conexión de nuevo durante otros 10 minutos (en un tiempo predeterminado y no se puede modificar). Solo cuando haya

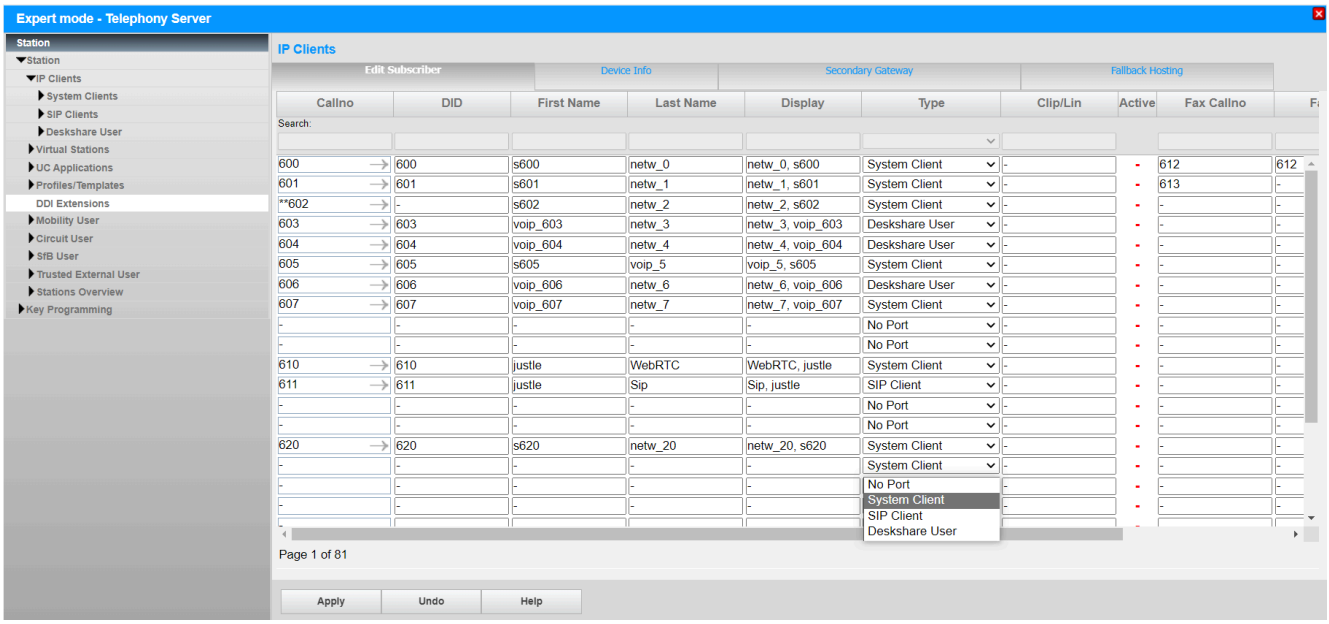
transcurrido este tiempo, los teléfonos del sistema afectados se registrarán en la pasarela de espera. El estado actual de los teléfonos registrados se puede ver en **Modo Experto** > **Registro de diagnósticos**.

Los ajustes de supervivencia están configurados en los teléfonos del sistema. Si se produce un error en el nodo de OpenScape Business, los teléfonos volverán a intentar conectarse a este varias veces. En el menú de Administración de los teléfonos, en el apartado «Redundancia del sistema», se puede configurar el tiempo de espera o la frecuencia con la que el teléfono intenta conectarse de nuevo. La configuración predeterminada para el tiempo de espera es de 30 segundos con un reintento. A continuación, los teléfonos se registran en la pasarela de espera. El registro automático en el nodo de OpenScape Business también se debe configurar en los teléfonos del sistema.

Nota: La opción de supervivencia requiere que el servicio POSTGRES funcione correctamente. Si el cortafuegos de aplicaciones está activado con una función para el servicio POSTGRES, es necesario asegurarse de que las direcciones IP de los demás nodos OpenScape Business que estén conectados a la red se añadan manualmente a esta función, ya que, de lo contrario, la función de supervivencia no funcionará.

Deben cumplirse los siguientes requisitos previos para la supervivencia:

- Debe haber suficientes puertos IP disponibles en la pasarela de espera para los teléfonos del sistema que estén conectados al nodo OpenScape Business y que deban «salvarse» cuando falle uno.
- Para dichos puertos libres, las estaciones deben configurarse sin nombre ni número de teléfono.

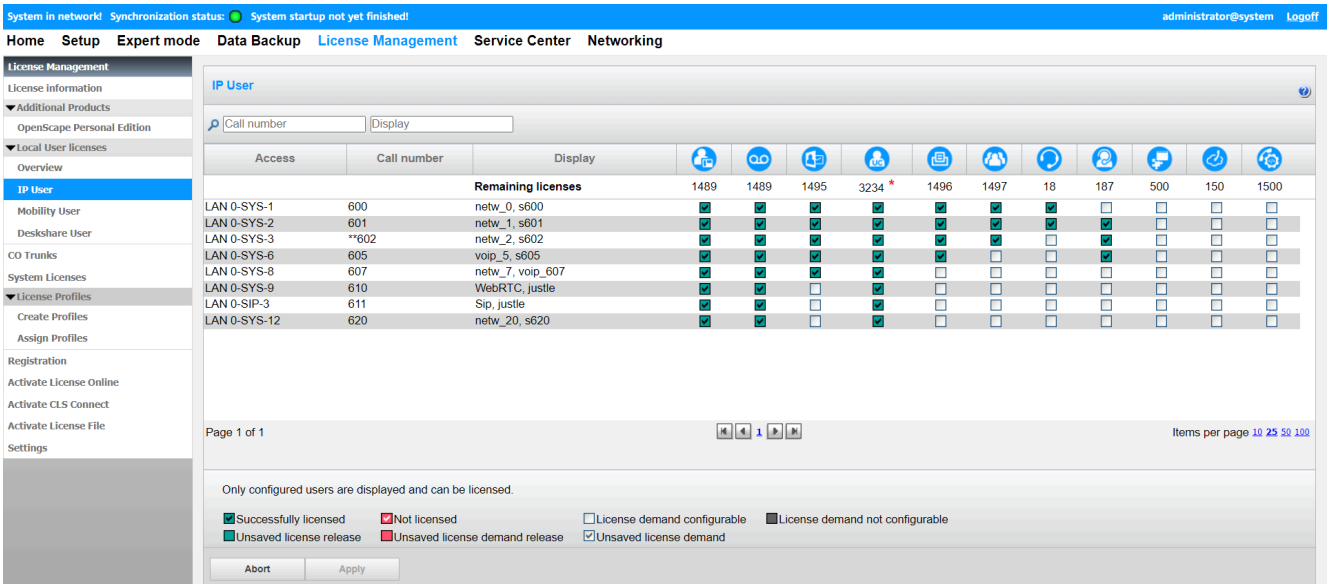


- Las estaciones deben estar configuradas como teléfonos del sistema (clientes del sistema) y tener una licencia de usuario de reserva. Si las licencias de reserva no están disponibles en el archivo de licencias activado,

se puede recurrir a las licencias de usuario IP. En caso de supervivencia, las estaciones solo pueden utilizar las funciones de telefonía.

Nota: Durante el tiempo de inactividad del nodo principal, puede haber problemas con los números de teléfono de redundancia HFA de los clientes hasta que dicho nodo vuelva a funcionar.

Nota: Si el sistema tiene asignadas licencias de usuario de reserva, no se podrán utilizar las licencias de usuario IP en caso de producirse un error.



21.10.1 Cómo configurar Survivability

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el grupo de menús, desplácese hasta **Extensiones** > **Clientes IP**. En un sistema OpenScape Business maestro, se muestra la ventana **Secondary Gateway** (Gateway secundario).
3) En **Node ID** (ID de nodo), seleccione el OpenScape Business que aplicará la extensión de OpenScape Business S en caso de emergencia.
4) Active la casilla de verificación **Emergency** (Emergencia) para la extensión de emergencia.
5) Las entradas de **Emergency Call no** (Número de llamada de emergencia) y **Call no DID** (Marcación directa de número de llamada) están prestablecidas y se pueden modificar en caso necesario.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

21.11 Eliminación de un nodo de la interred

Si desea retirar un nodo de la interred, es importante comprobar que no se pueda acceder a él en la configuración de red. De lo contrario, el nodo intentará de forma independiente registrarse de nuevo en la red y el nodo maestro intentará sincronizar los datos.

Procedimiento

Los nodos se borran a través del asistente Interconexión, y siempre hay que eliminar todos los nodos participantes.

- Interrumpa todos los tramos (encaminamiento) que vayan a los nodos que desea eliminar.
- Administración de la interred
- Introduzca "Ninguna red" en el nodo esclavo implicado en el asistente de redes del nodo esclavo.
- Retire el nodo esclavo de la lista de registro en el asistente de redes del nodo maestro.

Si el nodo no se elimina correctamente, los datos de un OpenScape Business se transfieren al otro y pueden producirse inconsistencias en el directorio interno. Es decir, los usuarios no aparecerán en el directorio de usuarios y, por tanto, tampoco podrán utilizar myPortal for Desktop, por ejemplo.

22 Equipo externo

Las conexiones son dispositivos externos (como, por ejemplo, un equipo de anuncios grabados o un portero eléctrico con abrepuertas) que se conectan a las interfaces del sistema de comunicación.

22.1 Equipo de anuncios grabados analógico

Un equipo de anuncios grabados analógico se puede conectar con una interfaz a/b para poder reproducir anuncios propios (p. ej., para el AutoAttendant central o para sustituir la música en espera).

Nota: Asegúrese antes de que el uso de anuncios grabados o de la música en espera no infringe ningún derecho de autor.

Por cada sistema de comunicación se pueden configurar hasta 16 fuentes de anuncios grabados como, por ejemplo, servidores de medios, equipos de anuncios grabados (Announcement Player) o contestadores analógicos.

En este caso se pueden utilizar los siguientes tipos de equipos de anuncios grabados:

- Equipos de anuncios grabados que al activarse comienzan siempre con el principio del texto del mensaje (p. ej. anuncio grabado de bienvenida)
- Equipos de anuncios grabados que tienen una reproducción continua (p. ej., para música en espera)

El equipo de anuncios grabados se debe comportar como una extensión, es decir: registrarse, reproducir el anuncio grabado y transferir la llamada (pasar a consulta, marcar y colgar).

Variantes de anuncio grabado

Están disponibles las siguientes variantes de anuncio grabado:

- Saludo (anuncio grabado antes de contestar)

  Antes de aceptar la llamada, el llamante escucha la reproducción de un saludo.
- AutoAttendant

  Si el AutoAttendant está activado, si el llamante no puede ser conmutado inmediatamente, puede insertarse música uu otros anuncios grabados.
- Marcación directa MF

  Si la Marcación directa MF está activada, un anuncio grabado ofrece al llamante la opción de marcación directa. Durante el anuncio grabado hay activo un receptor de códigos que detecta la marcación posterior del llamante y la transfiere.

Alternativas a la interfaz a/b (módulos SLA)

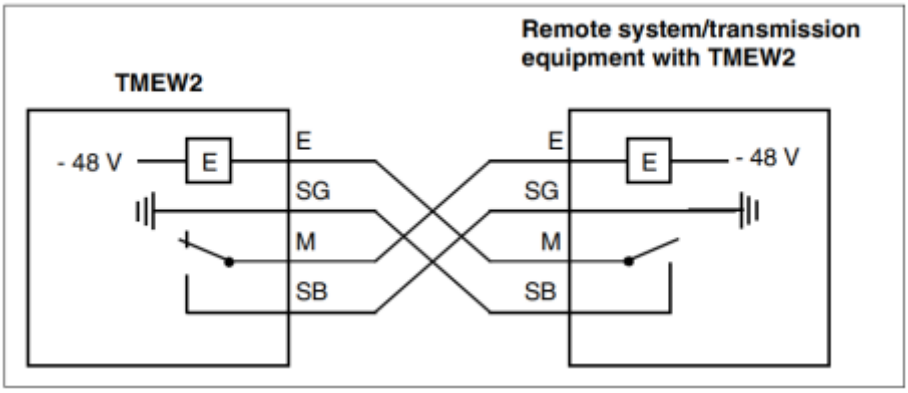
- OpenScape Business X8:módulo TMEW2
- OpenScape Business X5:módulo opcional STRB
- OpenScape Business X3:módulo opcional STRBR

Retraso de anuncio grabado

El valor de Retraso de anuncio grabado indica cuánto tiempo (ajustable entre 0 y 600 s) debe transcurrir para que las llamadas en espera se transfieran a un equipo de anuncios grabados.

Equipo de anuncios grabados Genius

Para la conexión del equipo de anuncios grabados Genius, el módulo TMEW2 puede ajustarse al tipo de interfaz 2. Encontrará la descripción del módulo TMEW2 y la ocupación de los conectores SIVAPAC en el panel trasero del equipo de anuncios grabados, en la Documentación de servicio, Montaje del hardware, capítulo "Módulos".



El equipo de anuncios grabados Genius se configura con el Manager E, en **Vista del sistema** > **Configuración** > **Conexiones** > **Anuncio grabado**.

22.1.1 Cómo añadir un equipo de anuncios grabados analógico

Requisitos previos

El equipo de anuncios grabados está conectado con una interfaz analógica.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Terminales / Extensiones**.
3) Haga clic en **Editar**, para iniciar el asistente **Terminales analógicas** . Aparece una lista de todas las extensiones analógicas.
4) En la línea del equipo de anuncios grabados, indique el nombre y el número de teléfono.
5) Si es necesario, en la línea del equipo de anuncios grabados haga otros ajustes de configuración.
6) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

22.1.2 Cómo modificar el retraso de anuncio grabado

La configuración se hace con el Manager E (véase también la ayuda online del Manager E):

Paso a paso

Vista de sistema, menú **Configuración** > **Parámetros del sistema** > **Parámetros de tiempo**: en la tabla de la entrada **Tiempo retardo anuncio antes de contestar** ajuste la **base** y el **factor** del Retraso de anuncio grabado como desee (valor estándar: 100 ms x 20).

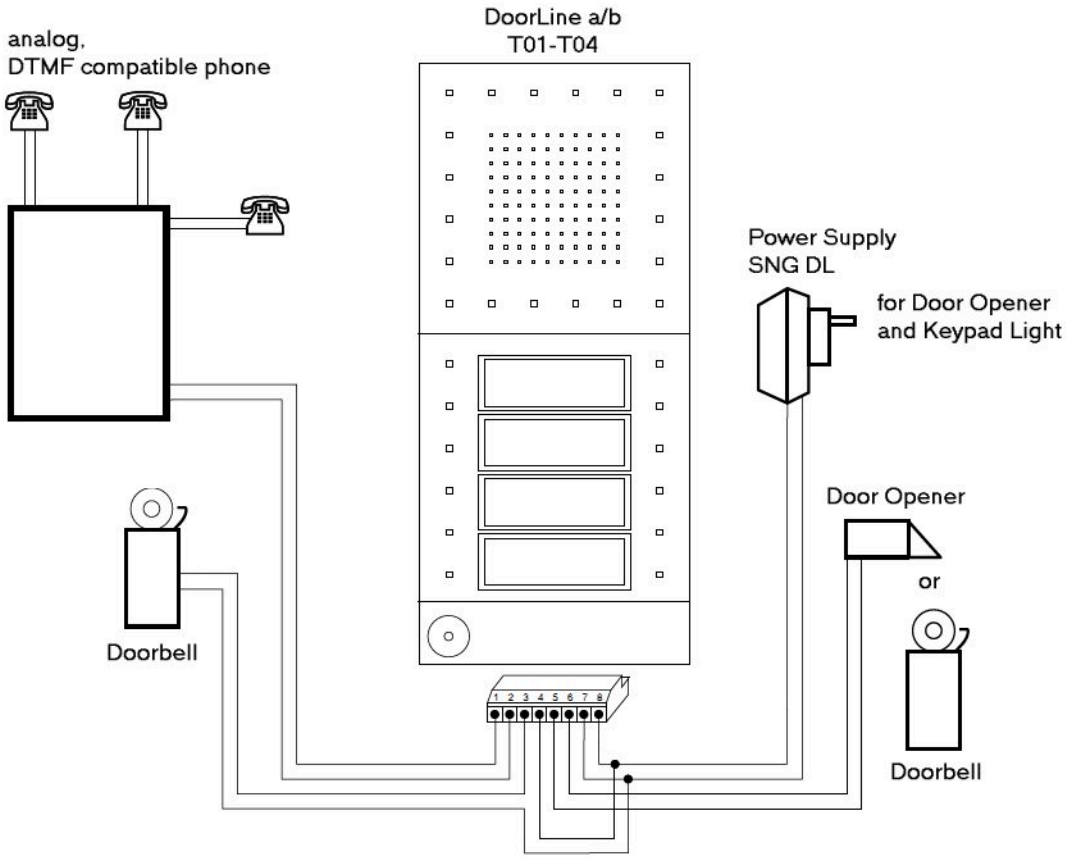
22.2 Portero eléctrico y Abrepuertas

Hoy en día, muchos fabricantes ofrecen funciones de portero eléctrico (PE). Las opciones de conexión disponibles son esenciales para la operación y las funciones de un PE. Aquí se describe como ejemplo el Doorline a/b T01-T04, que es parecido a otros porteros eléctricos de Behnke, Keil, 2n EntryCom, Auerswald, etc.

22.2.1 DoorLine a/b T01-T04

El portero eléctrico DoorLine a/b T01-T04 se conecta con una interfaz analógica. Equipa de 1 a 4 botones de llamada (según el modelo), se puede acceder a varias áreas residenciales o comerciales independientes. No solo se puede controlar desde cualquier teléfono sino que también ofrece la conexión para la fuente de alimentación del abrepuertas.

Gracias a la tecnología a/b de 2 hilos, el DoorLine a/b T01-T04 se puede montar de forma rápida y sencilla. Para sincronizar con el sistema de comunicación se puede configurar el procedimiento de marcación y ajustar el canal de voz. La apertura de puertas se hace mediante códigos del Doorline (por ejemplo, #9). Ya no es necesario utilizar un módulo de conexión especial como el Doorline M02, M03, M06 y M06/1.



Nota: Para este portero eléctrico no es necesario realizar más ajustes de configuración en OpenScape Business. Por motivos de seguridad se recomienda configurar la extensión como "Sin acceso al línea urbana" o "Acceso indirecto ".

22.2.1.1 Cómo configurar el puerto de extensión del Doorline a/b T01-T04

La configuración se hace con el Manager E (véase también la ayuda online del Manager E):

Paso a paso

1) **Vista del sistema**, menú **Configuración** > **Configurar estación** > **Extensiones**: para el puerto de extensión, seleccionar el tipo **Estándar**.
2) **Vista de extensión**, pestaña **Flags**: active el flag **Bloqueo de aviso de llamada en espera act.** del puerto de extensión.
3) **Vista del sistema**, menú **Configuración** > **Parámetros del sistema**, pestaña **Flags**: activar el flag **MF automático**.

22.2.1.2 Cómo configurar la extensión para Doorline a/b T01-T04

La configuración se hace con el Manager E (véase también la ayuda online del Manager E):

Paso a paso

1) **Vista de extensión**, pestaña **Flags**: desactive el flag **Bloqueo de aviso de llamada en espera act.** de la extensión.
2) **Vista de extensión**, pestaña **Flags**: active el flag **Salida lista de llamantes** de la extensión.

22.2.2 DoorCom Analog

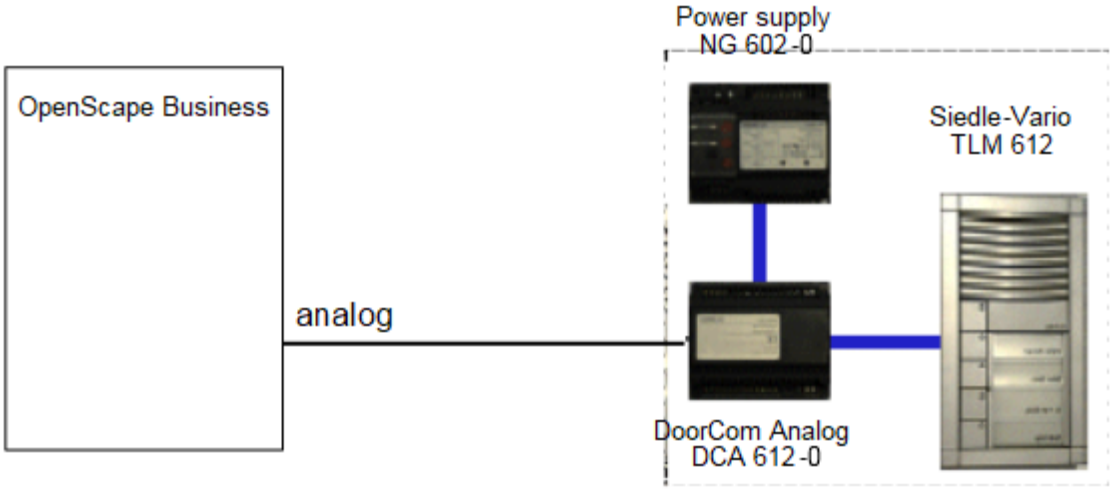
El producto DoorCom® Analog es una caja de adaptador universal TFE para los porteros eléctricos y abrepuertas de la empresa Siedle (p. ej. Vario TLM 612).

El DoorCom® analógico se conecta con una interfaz analógica del sistema de comunicación. Se comporta como un teléfono analógico con marcación MF, detección MF y control MF. El control solo es posible mediante señales MF.

DoorCom Analog solo puede funcionar con los siguientes componentes:

- DoorCom Analog DCA 612-0
- Portero eléctrico Siedle-Vario TLM 612
- Interfaz de conmutación por telecontrol DCSF 600

  Para la comunicación de voz de una extensión interna con el portero eléctrico. Sin este módulo no es posible realizar una devolución de llamada al portero eléctrico, p. ej. si se liberó una llamada del portero eléctrico por descuido.)
- Bloque de alimentación NG 602-0



Es posible programar las funciones de control del dispositivo (abrir puerta, acceder al portero eléctrico, etc.) en las teclas de procedimiento de un teléfono.

La secuencia de caracteres MF almacenada ahí se envía entonces al portero eléctrico/abrepuertas.

Nota: Para este portero eléctrico no es necesario realizar más ajustes de configuración en OpenScape Business. Por motivos de seguridad se recomienda configurar la extensión como "Sin acceso al línea urbana" o "Acceso indirecto ".

22.2.2.1 Cómo configurar el puerto de extensión del DoorCom analógico

La configuración se hace con el Manager E (véase también la ayuda online del Manager E):

Paso a paso

1) **Vista del sistema**, menú **Configuración** > **Configurar estación** > **Extensiones**: para el puerto de extensión, seleccionar el tipo **Estándar**.
2) **Vista de extensión**, pestaña **Flags**: active el flag **Bloqueo de aviso de llamada en espera act.** del puerto de extensión.
3) **Vista del sistema**, menú **Configuración** > **Parámetros del sistema**, pestaña **Flags**: activar el flag **MF automático**.

22.2.2.2 Cómo configurar la extensión para el DoorCom Analog

La configuración se hace con el Manager E (véase también la ayuda online del Manager E):

Paso a paso

1) **Vista de extensión**, pestaña **Flags**: desactive el flag **Bloqueo de aviso de llamada en espera act.** de la extensión.
2) **Vista de extensión**, pestaña **Flags**: active el flag **Salida lista de llamantes** de la extensión.

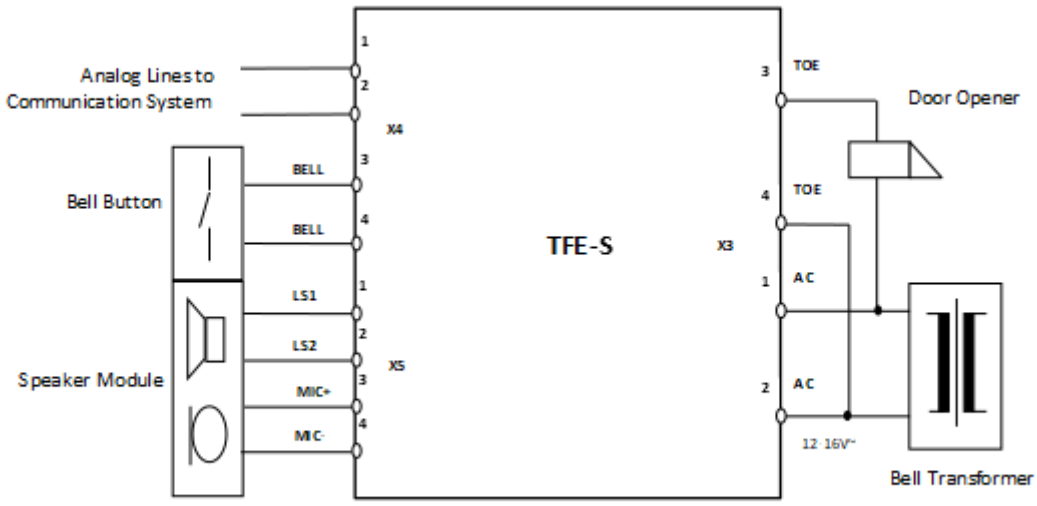
22.2.3 Dispositivo de portero eléctrico con amplificador (TFE-S)

El módulo TFE-S (S30122-K7696-T313) une una interfaz analógica del sistema de comunicación con un dispositivo de portero eléctrico, un abrepuertas y un timbre. El control se hace a través del sistema de comunicación.

Esto permite una conexión con porteros automáticos pasivos, comparables con los siguientes tipos:

- Marca Siedle (TLM511-01, 611-01)
- Marca Rito (5760)
- Marca Grothe (TS6216)

La amplificación se puede configurar de forma manual. El módulo TFE-S necesita una fuente de alimentación propia.



Datos técnicos

Parámetros	Valor
Fuente de alimentación	Transformador de timbre 12V - 16V CA, 50 hz
Consumo de corriente	máx. 150 mA
Interfaz de OpenScape Business	Extensión analógica
Dimensiones	100 mm x 160 mm
Temperatura ambiente	De 0°C a +45°C

Descripción del funcionamiento

Al accionar el timbre de la puerta, se señaliza en forma de llamada en el teléfono de una extensión definida (destino de portero eléctrico). Si la extensión acepta la llamada, se establece una conexión de voz con el portero eléctrico. Además, la extensión puede activar el abrepuertas con su teléfono.

Si no se puede acceder al destino de portero eléctrico, se produce una interceptación. Si la extensión de interceptación no está libre, se realiza una búsqueda del sistema a través de todos los teléfonos del sistema.

Consejo: Al señalizar una llamada del portero eléctrico no se tiene en cuenta el servicio nocturno.

Consejo: En el portero eléctrico no se puede usar la marcación abreviada central.

Opciones de configuración

Están disponibles las siguientes opciones de configuración:

- Abrepuertas:

  El abrepuertas se configura a través de una interfaz a/b. Para hacerlo el portero eléctrico debe tener conectado un adaptador. De esta forma, el usuario puede abrir la puerta pulsando una tecla del teléfono durante la conexión con el destino de portero eléctrico.
- MF (multifrecuencia):

  Este ajuste especifica si el abrepuertas se activa con un transmisor MF (MF: procedimiento de marcación por multifrecuencia), es decir, si el destino de portero eléctrico puede abrir la puerta con marcación posterior MF.
- Desvío de llamadas (AUL):

  Aquí se determina si la llamada debe ser transferida desde el portero eléctrico a un destino de desvío de llamada externo.

22.2.3.1 Cómo configurar el Portero eléctrico

El asistente **Portero eléctrico** permite establecer qué extensiones pueden accionar el abrepuertas. Puede configurar hasta diez porteros eléctricos.

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Portero eléctrico**. Se abre la ventana **Editar equipos de portero eléctrico**.
4) Seleccione una o varias **Ext. telef.**.
5) Introduzca el **Puesto dest.**.
6) En la casilla de verificación, active las funciones adecuadas, como **Abrepuertas**, **MF** y **AUL**.
7) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.
8) Para configurar cada portero eléctrico, siga los pasos del 1 al 7.

22.2.4 Altavoz

Se pueden conectar altavoces con el sistema de comunicación mediante amplificadores.

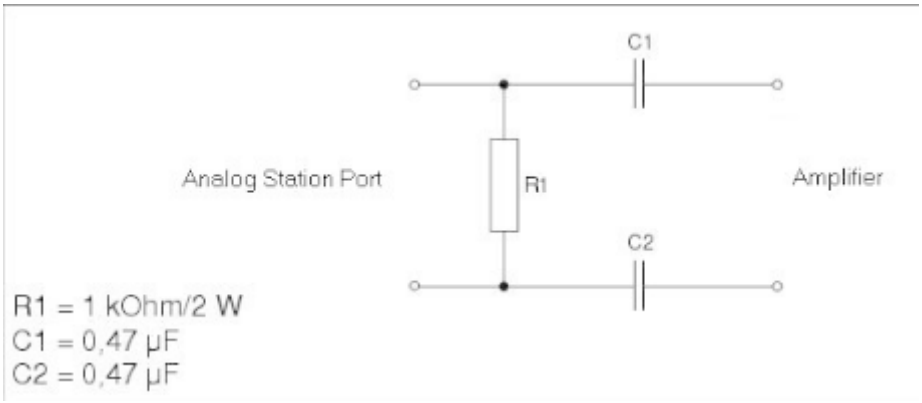
Para conectar un amplificador con altavoces, existen las siguientes opciones:

- **Conexión de un amplificador con una interfaz de extensión analógica**

  Puede ser necesario ajustar el nivel de volumen.



En su caso puede ser necesario utilizar una resistencia de bucle con la siguiente conexión:



- **Conexión del amplificador con el módulo TFE S**

  Se puede conectar un amplificador/sistema amplificador activo a través del módulo TFE S. La entrada del amplificador se conecta con la salida de altavoces del módulo TFE S.

  En su caso puede ser necesario utilizar otro contacto del módulo STRB para activar el amplificador o conmutar la señal de entrada (supresión de ruidos).

22.2.4.1 Cómo configurar la interfaz de extensión analógica para un altavoz

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Extensiones**.
3) En el grupo de menús, haga doble clic en **Extensiones** > **Extensiones analógicas**.
4) Seleccione la extensión analógica deseada (por ejemplo, 3011).
5) En la pestaña **Editar parámetros exten.**, modifique los datos de la extensión analógica según sea necesario.
6) En la lista desplegable **Tipo de ext.**, seleccione la entrada **Altavoz**.
7) Haga clic en **Aplicar**.

22.2.4.2 Cómo configurar la interfaz de extensión analógica para conectar un amplificador en el módulo TFE S

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Portero eléctrico**. Se abre la ventana **Editar equipos de portero eléctrico**.
4) Seleccione un **Ext. telef**.
5) Seleccione el **Puesto dest**.
6) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

22.3 Contactos

Los contactos (o "actuadores") son salidas de control y se activan o desactivan mediante señales de control del sistema de comunicación. Originan un cambio en el estado del equipamiento conectado y respaldan funciones de supervisión, alerta, control y regulación. Se utilizan principalmente en sistemas de seguridad y administración doméstica (p.ej, para Abrepuertas).

Los contactos se incluyen en módulos de relé de control opcionales. Todos los módulos de relé de control incluyen 4 salidas de control (contactos).

Módulos de relé de control posibles:

- REALS (OpenScape Business X8)
- STRB (OpenScape Business X3W/X5W)
- STRBR (OpenScape Business X3R/X5R)

Encontrará la descripción exacta de estos módulos (incl. asignaciones) en la Documentación de servicio, capítulo "Módulos".

Estas son las opciones para controlar los contactos:

- desde el teléfono, mediante códigos
- desde el teléfono del sistema, mediante un tecla
- por acceso remoto, a través de la línea urbana (DISA), mediante la extensión asignada a la función de relé
- por acceso remoto, mediante la prestación "Servicios asociados"

Los contactos se pueden activar o desactivar con las siguientes funciones:

Nota: Encontrará los códigos de control en el capítulo "Modo Experto".

- **Sin función**

  El contacto no está en servicio o no está registrado como timbre central (en "Configuración" - "Llamadas entrantes" - "Listas de destinos de llamada").

- **Act. y desact. manual**

  El contacto se puede activar o desactivar mediante la tecla o el código de encendido/apagado del interruptor seleccionado. Esta función se puede asignar a una extensión, a un grupo o a todas las extensiones.
- **Desact. autom. tras tiempo**

  El contacto se puede activar o desactivar como temporizador, mediante la tecla o el código de encendido/apagado del interruptor seleccionado. Esta función se puede asignar a una extensión, a un grupo o a todas las extensiones. Si se introduce como tiempo un valor superior a 0, el contacto se desactiva terminado ese tiempo.
- **Abrepuertas**

  El contacto se puede activar o desactivar como abrepuertas mediante la tecla o el contacto de encendido/apagado del interruptor seleccionado. Esta función se puede asignar a una extensión, a un grupo o a todas las extensiones. Si se introduce como tiempo un valor superior a 0, el contacto se desactiva terminado ese tiempo. En el display de todos los terminales asignados aparece el texto "Abrepuertas". Ejemplo para el factor con el tiempo de conmutación: 30*100 ms = 3 s.
- **Amplificador altavoz**

  El contacto se activa si se establece una conexión con el portero eléctrico/ abrepuertas/altavoz. Se desactiva en cuanto se interrumpe la conexión. De esta forma, es posible controlar un amplificador de portero eléctrico para que éste solo se active cuando se considere necesario. Esta función tiene que tener asignado el portero eléctrico o el puerto de altavoz.
- **Indicación de ocupado**

  El contacto se activa si la extensión asignada deja de estar en reposo (se descuelga el auricular, se activa el altavoz o el terminal de la extensión recibe una llamada). El contacto se desactiva cuando la extensión asignada vuelve a estar en reposo. El contacto se puede activar también directamente mediante una tecla o el código de encendido/apagado del interruptor seleccionado. En este caso se ignora el estado de la extensión asignada y el contacto solo se puede desactivar mediante de nuevo una tecla o un código. A esta función hay que asignarle una extensión determinada. Ejemplo de indicación de ocupado de la puerta: el Jefe telefonea y se enciende una lámpara sobre la puerta del Jefe para indicar que no quiere interrupciones.
- **Música de retención**

  El contacto se activa si al menos una extensión o una línea del sistema de comunicación no están en reposo. En este caso, se activa un equipo de anuncios grabados o un reproductor de CD. El contacto se desactiva si todas las extensiones y líneas del sistema de comunicación están en reposo. Esta función solo se puede asignar a todas las extensiones y solo puede estar presente una vez en el sistema de comunicación. Como tiempo de conmutación hay que introducir un valor superior a 0 (p. ej., 600*100 ms = 60 s). El contacto permanece activo y reproduce música hasta que termina el tiempo de conmutación o una señal de control lo desactiva.
- **Segundo timbre**

  El contacto se activa para la extensión asignada cuando esta recibe una llamada. Cuando se responde o finaliza la llamada, se desactiva el contacto. El contacto no es cronometrado. A esta función hay que asignarle una extensión determinada. Si se introduce un valor superior a 0 como tiempo

de conmutación, se puede retardar el apagado. El tiempo de conexión es un múltiplo de 3 segundos.

- **Impulso de tarificación**

  Este componente se sincroniza con el número de la extensión asignada en función de los impulsos o señales de tarificación entrantes. A esta función hay que asignarle una extensión determinada. El tiempo de conmutación es 150 ms de impulso y 150 ms de pausa, y no se puede modificar.
- **Extensión activa**

  El contacto se desactiva si la extensión asignada está activa (se descuelga el auricular o se activa el altavoz). El contacto se desactiva cuando la extensión asignada vuelve a estar en reposo. A esta función hay que asignarle una extensión determinada.

Nombre de contacto

Se puede asignar cualquier nombre a los contactos (máx. 16 caracteres).

22.3.1 Cómo configurar un contacto

Requisitos previos

Hay conectado un módulo de relé de configuración.

La configuración se hace con el Manager E (véase también la ayuda online del Manager E):

Paso a paso

1) **Vista del sistema**, menú **Configuración** > **Conexiones** > **Contactos**: en **Lista de contactos**, seleccionar el contacto que se va a configurar.
2) **Vista del sistema**, menú **Configuración** > **Conexiones** > **Contactos**: en **Tipo de contacto**, seleccionar la función del contacto.
3) **Vista del sistema**, menú **Configuración** > **Conexiones** > **Contactos**: en el campo **Nombre de contacto**, seleccionar un nombre cualquiera para el contacto (máx. 16 caracteres).
4) Si desea asignar a la función una extensión, un grupo o todas las extensiones, en el área **Extensión asignada** y en la lista **Número de teléfono**, seleccione el número de teléfono de la extensión o el número de llamada de grupo.

   Hay que marcar la entrada **ninguno** para todas las extensiones.
5) Si la función requiere un tiempo de conexión, en el área **Tiempo de conexión**, y en el campo **Factor**, introduzca el factor por el que se multiplicará el valor mostrado.

   Se pueden ver los valores 100 ms y 3 s.

22.4 Sensores

Los sensores son entradas de control y detectan un cambio de estado de la configuración activada. Puede activar o desactivar funciones del sistema de comunicación y, con ello, admitir funciones como supervisión, alarmas, control y reglas. Se utilizan fundamentalmente en sistemas de seguridad y

administración de edificios (p. ej., para control de temperatura o detectores de movimiento).

Los sensores van incluidos en módulos de relé de control opcionales. Todos los módulos de relé de control incluyen 4 entradas de control.

Módulos de relé de control posibles:

- REALS (OpenScape Business X8)
- STRB (OpenScape Business X3W/X5W)
- STRBR (OpenScape Business X3R/X5R)

Encontrará la descripción exacta de estos módulos (incl. asignaciones) en la Documentación de servicio, capítulo "Módulos".

Los sensores pueden activar o desactivar las siguientes funciones:

Nota: Encontrará los códigos de control en el capítulo "Modo Experto".

- Señalización de llamadas en los teléfonos
- Mensaje en pantalla en los teléfonos del sistema
- Activar/desactivar un equipo de anuncios grabados
- Control de un contestador automático
- Marcación automática con un número de llamada predefinido (número interno, número de llamada de grupo o número de llamada de destino externo)
- Activación de los siguientes servicios para un número de llamada (con código + número de llamada):
  - Contacto activado/desactivado
  - No molestar activado/desactivado
  - Desvío de llamadas activado/desactivado
  - Candado electrónico act./desact.
  - Enviar mensajes de texto
  - Retirar mensajes de texto
  - Servicio nocturno act./desact.
  - Transferencia de llamada act./desact.
- Activación directa de los siguientes servicios (solo con número de teléfono):
  - Contacto activado/desactivado
  - Utilizar el sistema de marcación abreviada
- Señalización de errores, que incluye:
  - la emisión de un mensaje de error programable (nombre de sensor, como máx. 10 caracteres: p. ej. Temp-Alarm) en el display de un determinado teléfono del sistema (sin señalización acústica).
  - llamada en un teléfono del sistema determinado con mensaje de error en el display durante la llamada (número de teléfono de destino)
  - registro de error en el historial de errores (registro en la memoria de errores = activar)

Número de llamada de destino

Un puerto analógico asignado puede programarse para los sensores. Este puerto es llamado por el sistema tan pronto como se recibe una señal de establecimiento de un enlace. La extensión llamante pasa por alto esta

conexión. Si hay un equipo de anuncios grabados conectado al puerto en cuestión, puede insertarse un anuncio grabado que informe a la extensión llamada de la activación del sensor. Un puerto analógico programado de este modo no puede ser activado desde el exterior. Si se ha programado un número de llamada externo para un sensor, pero no para un puerto analógico, el enlace externo se establecerá, pero no se transferirá ninguna señal acústica en relación con la activación del sensor. No obstante, si resulta necesario, la extensión llamada puede determinar el origen de la llamada a partir del número de llamada (CLIP).

Entrada de datos de control

Entrada de la cadena de caracteres de control con un máximo de 24 caracteres para el sistema Phonemail (número de llamada de buzón). En cuanto se establece el enlace se transmite la cadena de caracteres de control al puerto de anuncios grabados. Si no hay ningún puerto de anuncios grabados disponible, la cadena de caracteres de control se transfiere al destino.

23 Application Connectivity

Application Connectivity es compatible con el sistema, por ejemplo, con CSTA, TAPI y con Application Launcher.

23.1 CSTA

La interfaz CSTA permite la integración de aplicaciones CTI, de Contact Center y Comunicaciones Unificadas de alto rendimiento en OpenScape Business.

CSTA utiliza el protocolo TCP (Transmission Control Protocol). Se dispone de una conexión fija. La pérdida de paquetes de datos se detecta y corrige automáticamente.

Estándares

El protocolo CSTA implementado se basa en:

- ECMA-269 Services for Computer Supported Telecommunications Applications (CSTA) Phase III
- ECMA-285ASN.1 for Computer Supported Telecommunications Applications (CSTA) Phase III
- Ampliaciones específicas

Requisitos previos

Para usar CSTA se necesita UC Booster (Card o Server) o OpenScape Business S para el sistema conectado con aplicaciones CSTA. Los datos de inicio de sesión para las aplicaciones CSTA deben estar configurados en el sistema para activar automáticamente la interfaz CSTA. Las aplicaciones CSTA externas deben utilizar estos datos de inicio de sesión para acceder.

Prestaciones

CSTA ofrece las siguientes prestaciones:

- Acceso vía Ethernet LAN (TCP/IP)
- CSTA Phase III, codificación ASN.1
- Compatibilidad del protocolo CSTA XML para aplicaciones certificadas
- Amplia gama de teléfonos del sistema compatibles
- Supervisión a nivel de red y control de todos los recursos
- Multiplexing para puntos de supervisión

Dispositivos soportados

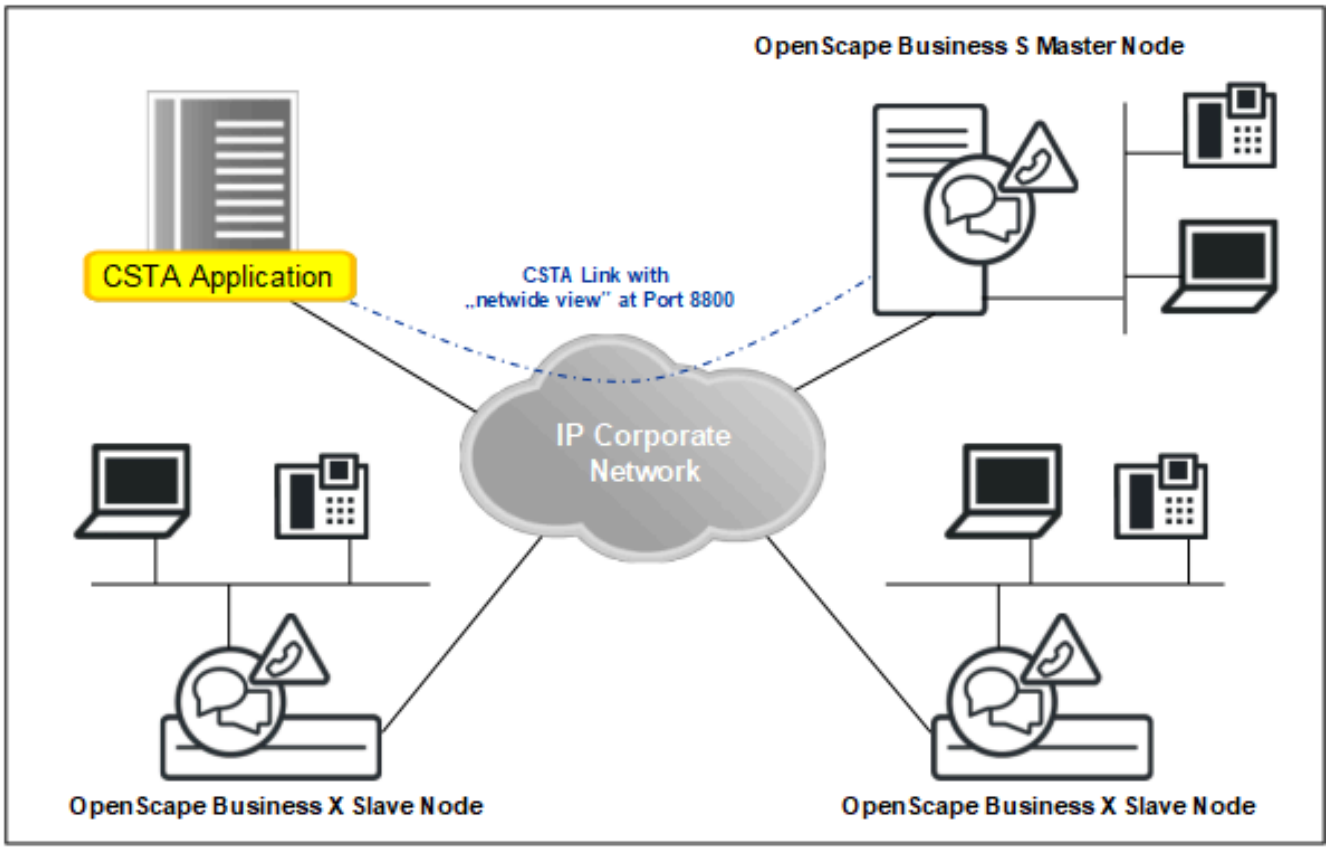
Además de con los teléfonos compatibles con el sistema, CSTA admite los siguientes dispositivos:

- ITSP

  Permite, p. ej., el uso de aplicaciones de Call Center con líneas urbanas SIP
- RDSI
- Línea urbana analógica
- Extensiones virtuales
- Grupos UCD
- MULAP

Nota: Encontrará información detallada sobre las prestaciones y los dispositivos compatibles en el manual de la interfaz CSTA.

Conexión para capa a nivel de red



Puertos

De forma predeterminada están disponibles los siguientes números de puerto:

Puerto	Número de puerto	Uso
CSP	8800	Cualquier aplicación CSTA
CMD	8900	Reservado para clientes TAPI 120; sea cual sea el número de clientes, se ocupa exactamente un enlace CSTA lógico

Las aplicaciones CSTA externas o los proveedores de servicio TAPI 120 deben utilizar la dirección IP del servidor UC o del sistema con el número de puerto correspondiente para establecer la conexión. La dirección IP correspondiente se muestra en la Gestión basada en Web (WBM), en Selección de aplicación.

Enlaces CSTA

De forma predeterminada, hay disponible un enlace CSTA del puerto CSP para aplicaciones CSTA externas. De forma predeterminadas hay otros tres enlaces CSTA asignados a las siguientes aplicaciones CSTA integradas o servicios:

- CMD (CSTA Message Dispatcher) para clientes TAPI 120 en el puerto CMD

- DSS (Direct Station Server)
- UC Suite

Si no se requieren estos servicios o estas aplicaciones CSTA, en caso necesario los enlaces CSTA correspondientes se pueden asignar a aplicaciones CSTA externas.

Nota: Un enlace CSTA proporciona el servicio TDS solo a los dispositivos locales. Los clientes deben tener un enlace CSTA con cada nodo en el que sea necesario para proporcionar el servicio TDS.

En general, las aplicaciones CSTA se pueden conectar a un sistema OpenScape Business a través de CSP, LAS (un componente del sistema) o PCC (un componente LDH).

Nota: Si una aplicación está conectada a través de CSP, también es necesario configurar las credenciales en CSP.

Más particular:

- Las aplicaciones UC Suite, OSCC, TAPI 170 y de terceros (externas) se conectan a través de CSP

  La conexión de aplicaciones CSTA de terceros (externas) que requieren información de troncales solo se puede realizar en modo UC Suite o consultando los propios puntos de monitoreo de troncales a través de CSTA, en su propia aplicación.
- UC Smart está conectado a través de LAS

Productos plus

En el sistema siempre están activados estos flags:

- Transferir siempre prefijo con los números de teléfono
- CSTA-CAUSE Handling avanzado
- Señalización CSTA CSP
- Supervisión MULAP

Conceptos relacionados

Teléfonos compatibles en la página 110

23.1.1 Cómo modificar el número de puerto para CSTA

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Administración de puertos**.

4) En la línea de **CSP**, y en el campo de entrada de la columna **Número puerto**, introduzca el número de puerto deseado.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
6) Reinicie el sistema.

Conceptos relacionados

OpenScape Business TAPI 120 en la página 1191

23.1.2 Cómo activar o desactivar el CMD para utilizar TAPI 120

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Middleware**.
3) En el grupo de menús, haga clic en **Middleware** > **CSTA Message Dispatcher (CMD)**.
4) Haga clic en la pestaña **Configuración - CSTA Message Dispatcher (CMD)**.
5) Elija una de estas opciones:
   - Si desea activar el CMD, en el área **Activación** active la casilla de verificación **El servicio se inicia automáticamente**.
   - Si desea desactivar el CMD, en el área **Activación** desactive la casilla de verificación **El servicio se inicia automáticamente**.
6) Elija una de estas opciones:
   - Si desea utilizar el registro automático para los clientes, en el área **Registro autom.** active la casilla de verificación **Registro autom. del cliente activado**.
   - Si no desea utilizar el registro automático para los clientes, en el área **Registro autom.** desactive la casilla de verificación **Registro autom. del cliente activado**.
7) Haga clic en **Aplicar**.

Conceptos relacionados

OpenScape Business TAPI 120 en la página 1191

23.1.3 Cómo activar o desactivar el servidor DSS para utilizar teclas DSS a nivel de red

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Middleware**.

3) En el grupo de menús, haga clic en **Middleware** > **Servidor DSS**.
4) Haga clic en la pestaña **Configuración - Servidor DSS**.
5) Elija una de estas opciones:
   - Si desea activar el servidor DSS, en el área **Activación** active la casilla de verificación **El servicio se inicia automáticamente**.
   - Si desea desactivar el servidor DSS, en el área **Activación** desactive la casilla de verificación **El servicio se inicia automáticamente**.
6) Haga clic en **Aplicar**.

23.1.4 Cómo activar o desactivar el CSP

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Middleware**.
3) En el grupo de menús, haga clic en **Middleware** > **CSTA Service Provider (CSP)**.
4) Haga clic en la pestaña **Configuración - CSTA Service Provider (CSP)**.
5) Elija una de estas opciones:
   - Si desea activar el CSP, en el área **Activación** active la casilla de verificación **El servicio se inicia automáticamente**. Indique también un ID de usuario CSTA y una contraseña de usuario CSTA para que una aplicación pueda utilizar CSTA.
   - Si desea desactivar el CSP, en el área **Activación** desactive la casilla de verificación **El servicio se inicia automáticamente**.

     Nota: ¡Si CSP está desactivado, no se pueden utilizar TAPI 120 (mediante CMD), TAPI 170, servidor DSS ni UC Suite!
6) Haga clic en **Aplicar**.

23.1.5 Cómo activar o desactivar el Media Extension Bridge

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Middleware**.
3) En el grupo de menús, haga clic en **Middleware** > **Media Extension Bridge (MEB)**.
4) Haga clic en la pestaña **Configuración - Media Extension Bridge (MEB)**.

5) Elija una de estas opciones:

- Si desea utilizar Media Extension Bridge, en el área **Activación** active la casilla de verificación **El servicio se inicia automáticamente**.
- Si desea liberar este enlace CSTA, en el área **Activación** desactive la casilla de verificación **El servicio se inicia automáticamente**.

6) Haga clic en **Aplicar**.

23.2 OpenScape Business TAPI 120/170

OpenScape Business TAPI 120 y OpenScape Business TAPI 170 son, junto a CallBridge Collection, dos TSP (Tapi Service Provider) optimizados para la arquitectura de sistema y la topología de redes de OpenScape Business y que ofrecen a las aplicaciones basadas en TAPI la interfaz Microsoft TAPI para la conexión con el sistema de comunicación OpenScape Business.

La integración con OpenScape Business se realiza exclusivamente mediante LAN. Los componentes adicionales de hardware y software, como CSTA Message Dispatcher (CMD) o CSTA Service Provider (CSP), no son necesarios para el funcionamiento con OpenScape Business. El registro de licencias está vinculado a la extensión y no distingue entre extensiones TAPI 120 o TAPI 170 de OpenScape Business. El registro de licencia es obligatorio desde la primera extensión TAPI.

La selección del TAPI Services Provider adecuado depende en lo esencial del número de los PC de cliente con aplicaciones TAPI, de la infraestructura de TI presente y de los teléfonos utilizados.

- **CallBridge Collection**

  se utiliza como First Party TAPI Serviceprovider clásico con teléfonos del sistema con una interfaz LAN o USB. Es adecuado para instalaciones con pocos PC. Para el funcionamiento de CallBridge Collection no se requiere una LAN. CallBridge Collection se instala en todos los PC en el que se use una aplicación TAPI. No son compatibles teléfonos analógicos, Cordless y del sistema sin interfaz USB/IP.

  No hay registro de licencia para integraciones de TAPI mediante CallBridge Collection.
- **OpenScape Business TAPI 120**

  se utiliza preferentemente como First Party TAPI Serviceprovider en redes de Microsoft con o sin Domain Controller, si se van a operar teléfonos analógicos, Cordless o del sistema sin interfaz USB/IP con la aplicación TAPI. El TAPI 120 Service Provider se instala en el cliente de PC en el que se utiliza una aplicación TAPI.

  Las integraciones de TAPI mediante OpenScape Business TAPI 120 requieren registro de licencia en OpenScape Business. Para la integración con OpenScape Business se requiere un enlace CSTA o un enlace con la interfaz WebServices, en función del modo de servicio o el tipo de integración, y sea cual sea el número de clientes TAPI 120. El volumen de funciones del lado de la TAPI depende del modo de servicio y del tipo de integración.
- **OpenScape Business TAPI 170**

  es un "Third Party" TAPI Service Provider clásico. Se instala en un servidor de la LAN y se integra de forma centralizada con el sistema OpenScape

Business. Como alternativa, TAPI 170 se puede utilizar como TAPI 120 si en la red de Microsoft hay un Domain Controller. Si se utiliza la función denominada Remote TAPI, no es necesario instalar el TAPI Service Provider en los PC de cliente. Esta función permite ahorrar mucho tiempo en instalaciones con muchos PC de cliente. Sin embargo, sí es obligatorio instalar OpenScape Business TAPI 170 en los siguientes escenarios.

– Integración de extensiones TAPI en sistemas OpenScape Business interconectados, si las extensiones TAPI están localizadas en diferentes nodos.
– Integración de aplicaciones TAPI que se usan en un servidor de terminal.
– Integración de aplicaciones TAPI basadas en servidor.

Las integraciones de TAPI mediante OpenScape Business TAPI 170 requieren registro de licencia en OpenScape Business. Para la integración con OpenScape Business se requiere un enlace CSTA, sea cual sea el número de clientes TAPI 170.

23.2.1 OpenScape Business TAPI 120

OpenScape Business TAPI 120 es un 1st Party Telephony Service Provider, que admite el abanico de funciones de Microsoft TAPI V2.1. OpenScape Business TAPI 120 permite a las aplicaciones CTI basadas en Windows supervisar y controlar un teléfono del sistema integrado con OpenScape Business.

Como alternativa, OpenScape Business TAPI 120 se puede integrar mediante la interfaz CSTA (modo CSTA) o mediante la interfaz WebServices WSI (modo UC Smart) con OpenScape Business. Al realizar la integración con un sistema no se admite el modo mixto. Si en el sistema OpenScape Business hay insertada una UC Booster Card o hay integrado un UC Booster Server, TAPI 120 solo se puede operar en modo CSTA. Los requisitos del sistema, el número máximo de extensiones TAPI y el volumen de funciones del lado de TAPI dependen de los modos de servicio.

Integraciones OpenScape Business TAPI 120

El software OpenScape Business TAPI 120 se instala en un PC cliente con Microsoft Windows. La conexión con el sistema OpenScape Business se realiza mediante LAN. No hace falta una conexión física entre el PC Windows y el teléfono.

- **Modo CSTA de TAPI 120**

  Todos los PC cliente TAPI 120 se integran con el mismo enlace CSTA de OpenScape Business. OpenScape Business multiplexa internamente todas las conexiones TAPI 120.

  En el modo CSTA, TAPI 120 admite OpenScape Business X3/X5/X8 y OpenScape Business S.

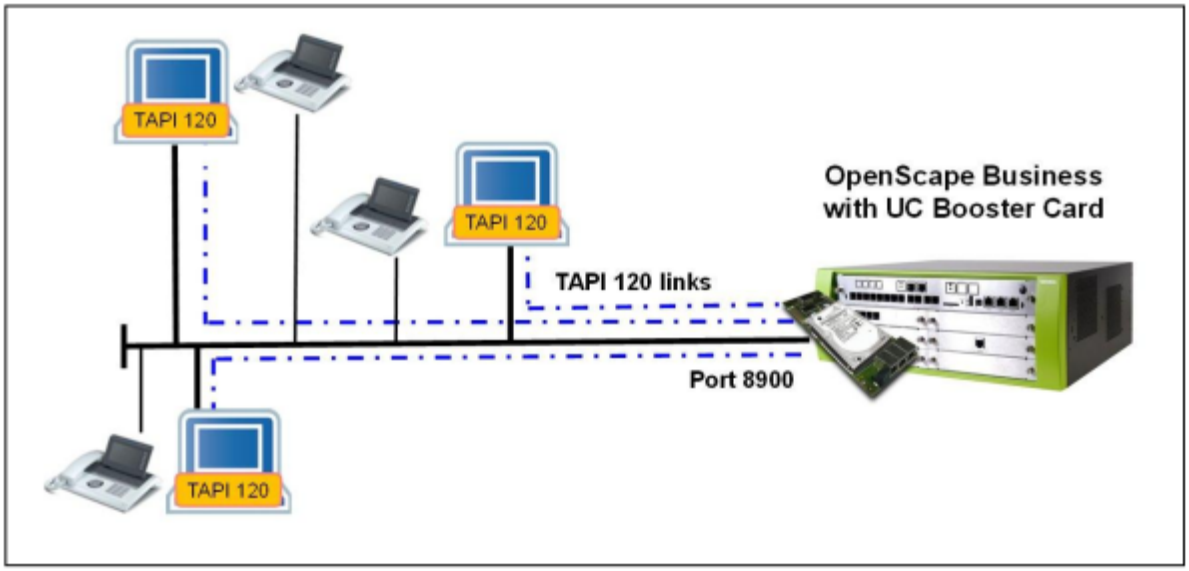


Figura 11: TAPI 120 en modo CSTA con OpenScape Business X5R y UC Booster Card

- **Modo UC Smart de TAPI 120**

  Todos los PC cliente TAPI 120 se integran mediante LAN y la interfaz WebServer con la placa base de OpenScape Business. OpenScape Business multiplexa internamente todas las conexiones TAPI 120.

  En el modo CSTA, TAPI 120 admite OpenScape Business X1/X3/X5/X8.

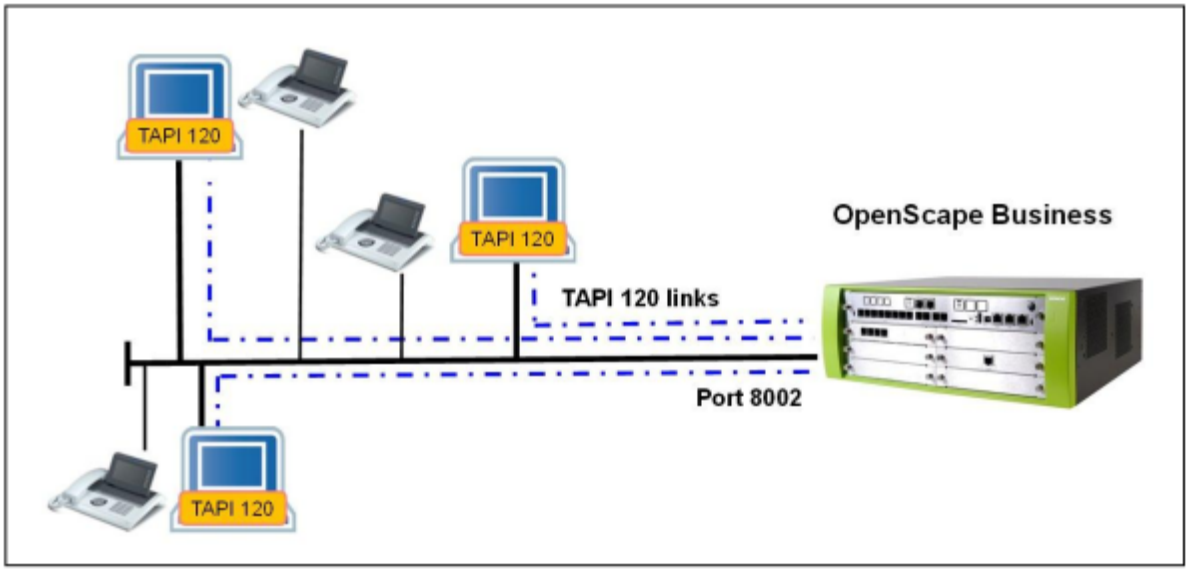


Figura 12: TAPI 120 en el modo UC Smart con OpenScape Business X5R

Prestaciones

Se admiten las siguientes prestaciones:

Prestación	TAPI 120 CSTA	TAPI 120 UC Smart
First-Party TAPI Service Provider integrado mediante LAN de forma central	X	X
Compatible con el estándar TAPI 2.1 de Microsoft	X	X
Integración con sistemas individuales OpenScape Business	X	X
Compatibilidad para el firewall OpenScape Business CTI	X	-
Funciones compatibles mediante TAPI		
Señalización de llamadas entrantes y salientes con identificación de los números de teléfono y del origen de la llamada	X	X
Información adicional en la señalización de llamadas con llamadas desviadas	X	X
Aceptación de llamadas internas y externas	X	X
Establecimiento de conexión controlado con colaterales internos y externos	X	X
Marcación manual/Marcación posterior MF	X	X
Liberación de llamadas existentes	X	X
Establecimiento de una llamada de consulta con interlocutores internos y externos	X	X
Alternar	X	X
Transferencia de llamada con seguimiento	X	X
Transferencia de llamada con seguimiento y marcación posterior del destino de consulta (One-Step Transfer)	X	X
Transferencia de llamada sin seguimiento (Blind-Transfer)	X	-
Establecer y borrar el desvío de llamadas	X	X
Establecer y borrar No molestar	X	X
Cómo iniciar una conferencia	X	-
Cómo ampliar una conferencia	X	-
Desviar llamada entrante	X	-
Telecaptura selectiva (Call Pickup)	X	-
Señalización de llamadas en grupo y telecaptura de llamada de grupo (Group Pickup)	X	-
Aparcamiento de llamadas existentes	X	-
Recuperar línea de llamadas aparcadas	X	-

Prestación	TAPI 120 CSTA	TAPI 120 UC Smart
Retención manual de llamadas existentes	X	-
Recuperar línea de llamadas retenidas manualmente	X	-
Establecer devolución de llamada	X	-
Respaldo de funciones controladas por código	X	-
Intercambio de datos relativo a llamadas entre aplicaciones TAPI	X	-
Control de teclas con teléfonos del sistema (HFA)	X	-
Control de amplificación de micrófono en teléfonos del sistema (HFA)	X	-
Control/Selección del uso de handset/altavoz/ auriculares con teléfonos del sistema (HFA)	X	-
Control del volumen de handset/altavoz/auriculares del teclado con teléfonos del sistema (HFA)	X	-
Acceso a displays y LED de optiPoint/OpenStage (límite de 50 displays activos por sistema)	X	-

Valores máximos

El número máximo de PC clientes TAPI 120 que se pueden integrar con OpenScape Business depende del modelo (véase Niveles de ampliación disponibles a través de Ventas).

Sistemas operativos aprobados

Los sistemas operativos aprobados actualmente para Microsoft Windows Server, el servidor de terminal y el PC cliente remoto aparecen enumerados en la información de ventas.

Con TAPI 120 solo se pueden utilizar sistemas operativos de Microsoft Windows.

En instalaciones en servidores de terminal, hay que utilizar OpenScape Business TAPI 170 en lugar de OpenScape Business TAPI 120.

Registro de licencia

Si se utiliza OpenScape Business TAPI 120 el registro de licencias se hace en base a extensión. Las licencias TAPI se administran dentro del sistema OpenScape Business y se pueden usar para ambos modos de TAPI 120. Si se utiliza la prestación MULAP, por cada extensión de la MULAP se requiere una licencia TAPI.

Nota: En el modo UC Smart, con TAPI 120 no se requieren licencias UC User.

Aprovisionamiento de software

El software OpenScape Business TAPI 120 se suministra en un soporte de datos propio. No se incluye con el software del sistema OpenScape Business.

Requisitos de hardware

El PC debe cumplir los requisitos del sistema indicados por Microsoft para el sistema operativo utilizado y los requisitos de la aplicación TAPI. Además, se requiere una interfaz LAN Ethernet.

- con TAPI 120 CSTA

  Sea cual sea el número de clientes TAPI 120 integrados se requiere un enlace CSTA de OpenScape Business. Para ello se requiere un OpenScape Business UC Booster (Card o Server).
- con TAPI 120 UC Smart

  Se requiere la interfaz WebServices. En el sistema no puede haber un OpenScape Business UC Booster (Card o Server).

Dispositivos compatibles

Los terminales y las prestaciones compatibles en estos terminales dependen del abanico de funciones CSTA o WSI del sistema OpenScape Business que se utilice. Esta información se incluye en la información de ventas de OpenScape Business.

Puerto IP/Dirección IP ocupado de forma predeterminada por TAPI 120

En el modo de servicio CSTA de TAPI 120, el enlace CSTA con OpenScape Business ocupa el puerto IP 8900.

En el modo de servicio UC Smart de TAPI 120, el enlace WSI con OpenScape Business ocupa el puerto IP 8802 para las conexiones cifradas (HTTPS) o el puerto 8801 para las conexiones sin cifrar (HTTP).

En la configuración TAPI 120, hay que introducir la dirección IP del sistema OpenScape Business según el modo de servicio. Esta dirección IP se muestra en la Gestión basada en Web (WBM), en **Selección de aplicación**.

Tareas relacionadas

Cómo modificar el número de puerto para CSTA en la página 1187

Cómo activar o desactivar el CMD para utilizar TAPI 120 en la página 1188

23.2.2 OpenScape Business TAPI 170

OpenScape Business TAPI 170 es un 3rd Party Telephony Service Provider, que respalda el volumen de funciones TAPI V2.1 de Microsoft. TAPI 170 permite a las aplicaciones CTI basadas en Microsoft Windows supervisar y controlar simultáneamente varios teléfonos integrados con OpenScape Business.

Prestaciones

OpenScape Business TAPI 170 ofrece las prestaciones siguientes:

- 3rd Party TAPI Service Provider con integración central
- Compatible con el estándar TAPI 2.1 de Microsoft
- Las funciones de telefonía están disponibles en todos los clientes de PC integrados mediante la arquitectura de cliente/servidor de TAPI 2.1
- No se requiere ningún software de cliente TSP adicional

- Funciones de telefonía compatibles:
  - Marcación entrante/saliente desde el PC
  - Transferencia del número de teléfono entrante, si se señaliza
  - Consulta y transferencia
  - Alternar
  - Conferencia
  - Desvío de llamadas
  - Transferir llamantes
  - Aceptar una llamada con la aplicación
  - Liberar una llamada con la aplicación
  - Transferencia antes/después de contestar
  - Transferencia de códigos de prestación
  - Supervisión del teléfono (estados de llamada, falla, etc.)
  - Aprovisionamiento de una interfaz ACD
  - Supervisión/acceso al teclado con teléfonos del sistema (HFA)
  - Control de display/LED con teléfonos del sistema (HFA)
  - Integración con sistemas individuales de OpenScape Business y sistemas interconectados
  - Soporte de números de teléfono/extensiones MULAP

Integraciones OpenScape Business TAPI 170

El software de OpenScape Business TAPI 170 se instala en un servidor de Microsoft Windows de la red. La conexión con OpenScape Business se realiza mediante un enlace CSTA. No hace falta una conexión física entre el PC Windows y el teléfono. OpenScape Business TAPI 170 se puede configurar en diferentes modos de servicio en sistemas individuales o en la red OpenScape Business. Los servidores y los clientes TAPI se administran desde el mismo Domain Controller de red.

- **Integración de aplicaciones TAPI basadas en servidor con OpenScape Business mediante TAPI 170**

  La aplicación de servidor y el software TAPI 170 se instalan en el denominado "servidor de telefonía" de la red. La aplicación de servidor ofrece a los clientes de la red las funciones de telefonía para las extensiones configuradas en OpenScape Business TAPI 170. El software TAPI 170 se integra mediante LAN con la interfaz CSTA de OpenScape Business. Para esta integración se requiere un enlace CSTA de OpenScape

Business y una licencia TAPI por cada extensión TAPI que haya configurada.

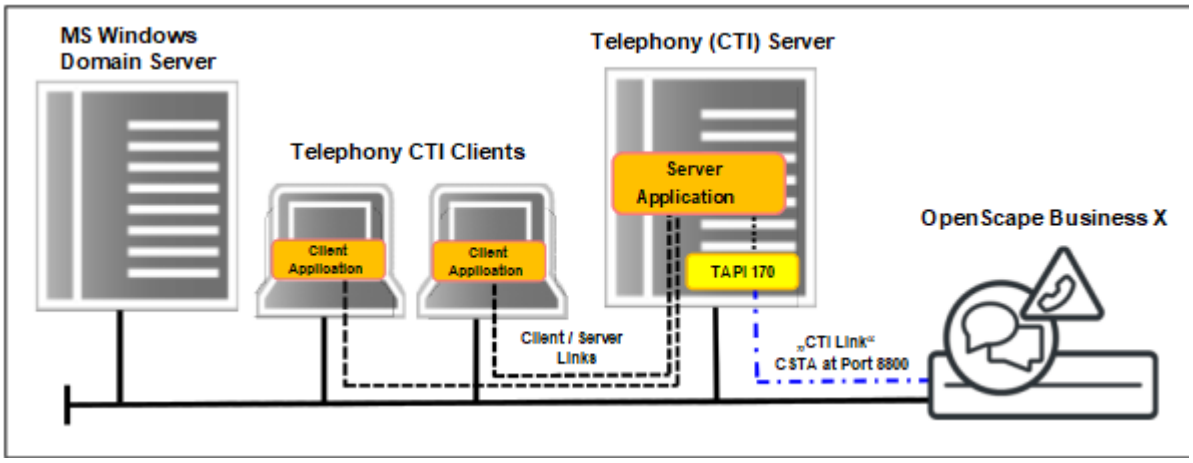


Figura 13: Aplicación TAPI basada en servidor mediante TAPI 170 con OpenScape Business

- **Integración de aplicaciones TAPI basadas en cliente con OpenScape Business mediante TAPI 170 con función "Remote TAPI"**

  En este escenario, el software de OpenScape Business TAPI 170 se instala en un servidor de la red. En los PC cliente con aplicaciones TAPI se habilita la denominada función "Remote TAPI" con la que la aplicación TAPI se comunica en el cliente con el software TAPI 170 en el servidor. Para ello, en el cliente no puede haber instalado software TAPI 170. El software TAPI 170 se conecta con la interfaz CSTA de OpenScape Business mediante LAN. Para esta integración se requiere un enlace CSTA de OpenScape Business y una licencia TAPI por cada extensión TAPI que haya configurada.

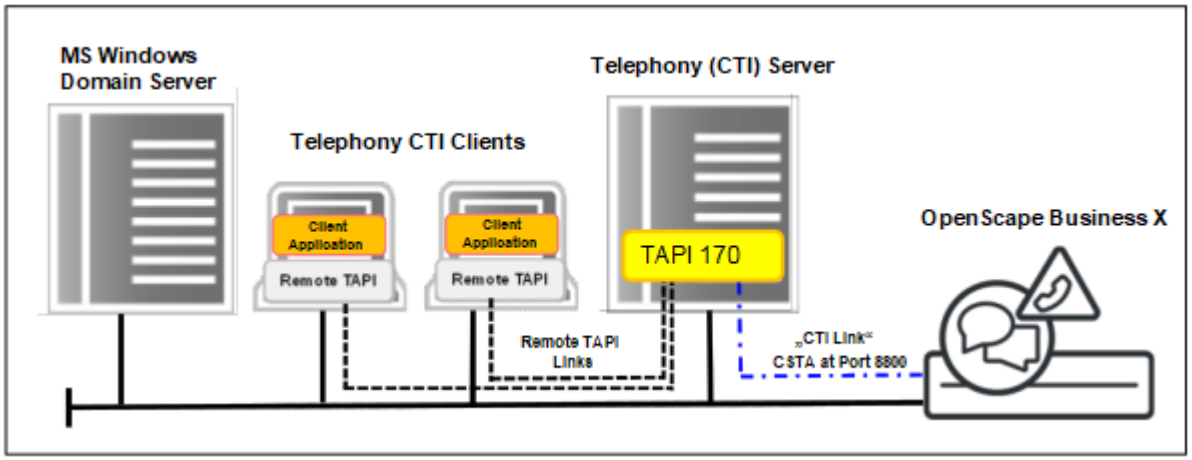


Figura 14: Aplicación TAPI basada en cliente mediante "Remote TAPI" con OpenScape Business

- **Integración de aplicaciones TAPI basadas en servidor de terminal con OpenScape Business mediante TAPI 170**

  En este escenario, las aplicaciones TAPI basadas en cliente se instalan en uno o varios servidores de terminal. En este caso, el software TAPI 170 se instala en el servidor de terminal. En el caso de un clúster integrado por varios servidores de terminal, el software TAPI 170 se debe instalar en cada servidor de terminal del clúster. Cada software TAPI 170 que haya instalado

se conecta con OpenScape Business mediante LAN. Por cada software TAPI 170 que haya instalado en un servidor de terminal, se requiere un enlace CSTA de OpenScape Business. Además, se requiere una licencia TAPI por cada extensión TAPI configurada.

No se puede superar el número máximo posible de servidores TAPI 170 OpenScape Business en conexión con OpenScape Business.

Nota: Solo se pueden controlar en el clúster tantos servidores de terminal como enlaces CSTA libres haya centro de OpenScape Business para integrar el software TAPI 170. El valor máximo de las interconexiones posibles se reduce si los enlaces CSTA de OpenScape Business están ocupados por otras aplicaciones CSTA.

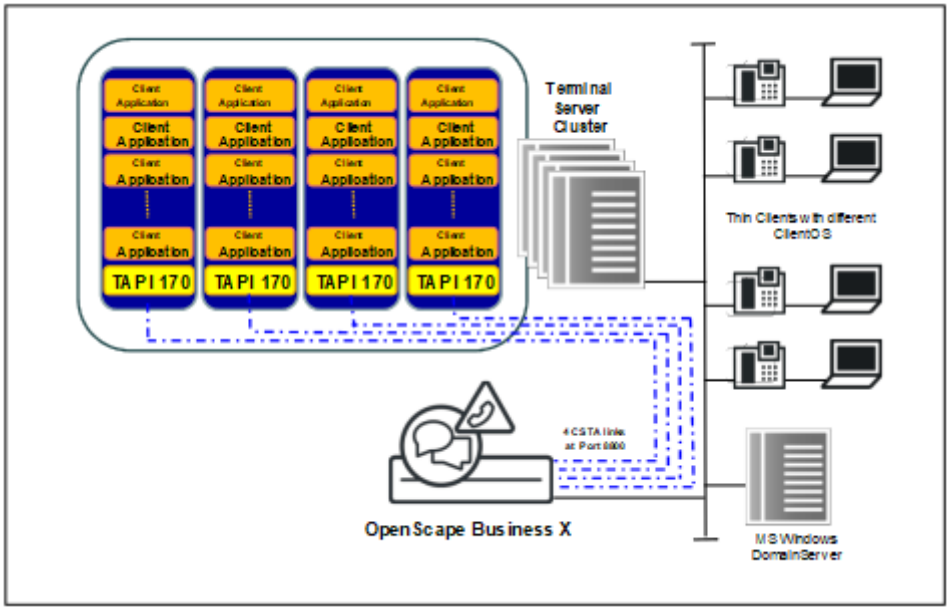


Figura 15: Aplicación TAPI basada en cliente en servidor de terminal con OpenScape Business

- **Integración de TAPI 170 en sistemas OpenScape Business interconectados**

  En los sistemas OpenScape Business interconectados, el software TAPI 170 se instala en un servidor integrado mediante LAN con la interfaz CSTA del nodo maestro. Esta integración depende de los modos de servicio indicados anteriormente del TAPI 170 Service Provider (Remote TAPI o integración basada en servidor). Para la implementación se requiere un enlace CSTA del nodo maestro OpenScape Business y una licencia TAPI por cada extensión TAPI de la red.

  Nota: Mediante el nodo maestro, el TAPI 170 puede acceder a nivel de red a todas las extensiones de la red. Con una integración de TAPI 179 en un nodo esclavo en lugar de un nodo maestro, TAPI 170 solo puede acceder a las extensiones del nodo esclavo. Si se utilizan varios TAPI 170

en un clúster de servidores de terminal, por cada TAPI 170 se requiere un enlace CSTA con el nodo maestro.

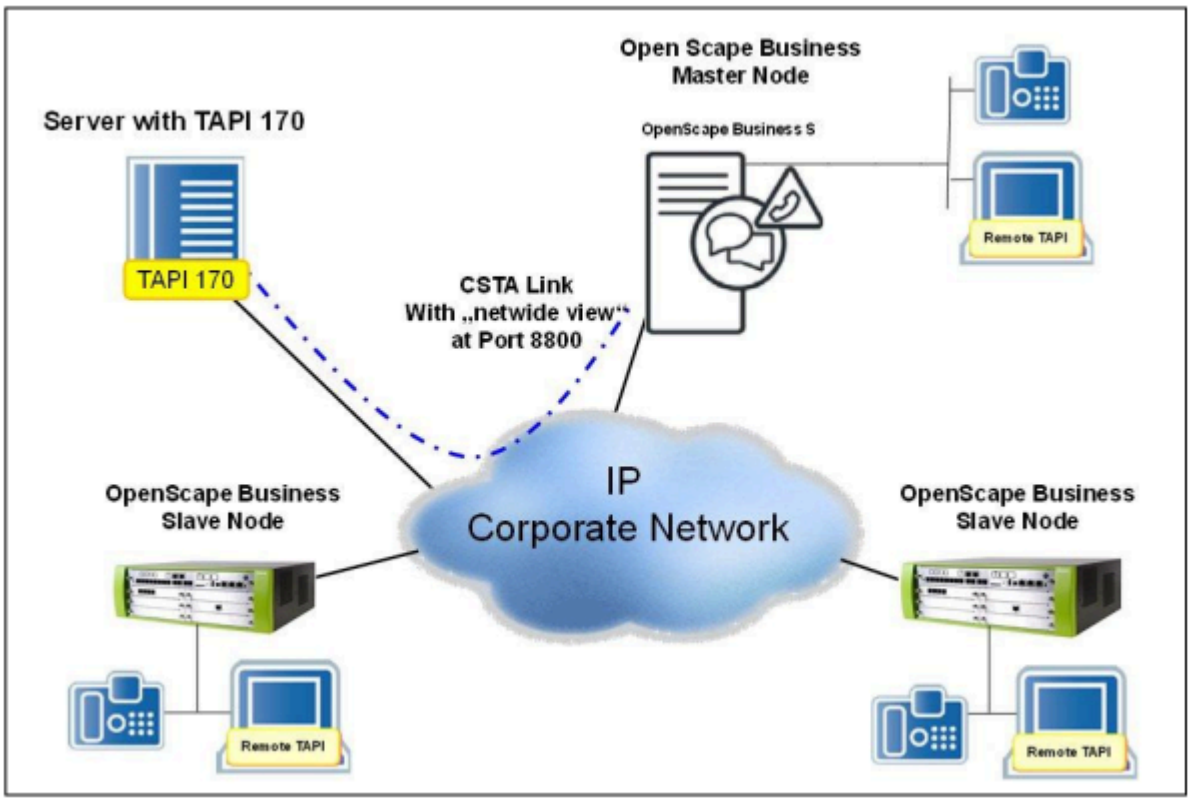


Figura 16: Integración de TAPI 170 en sistemas OpenScape Business interconectados

Límites de ampliación

El número máximo de PC cliente TAPI 170 que se pueden integrar con OpenScape Business depende del modelo. Puede obtener más información en el capítulo 1.3.9.4

Sistemas operativos aprobados

Los sistemas operativos aprobados actualmente para Microsoft Windows Server, el servidor de terminal y el PC cliente remoto aparecen enumerados en la información de ventas.

Con TAPI 170 solo se pueden utilizar sistemas operativos de Microsoft Windows.

El modelo de licencias de Microsoft requiere la licencia para el sistema operativo del servidor y tantas CAL de usuario o dispositivo de Microsoft como se necesiten para la ampliación planificada. Estas CAL no se entregan en el volumen de suministro de OpenScape Business TAPI 170 y se deben adquirir siempre por separado. En ciertas condiciones predeterminadas por Windows, para OpenScape Business TAPI 170 también se puede utilizar un "Windows Server for embedded systems" con la llamada licencia "Embedded Telco".

Registro de licencia

Si se utiliza OpenScape Business TAPI 170 el registro de licencias se hace en base a extensión. Las licencias se administran dentro del sistema OpenScape Business. Si se utiliza la prestación MULAP, por cada extensión de la MULAP se requiere una licencia TAPI.

Aprovisionamiento de software

El software OpenScape Business TAPI 170 se suministra en un soporte de datos propio. No se incluye con el software del sistema OpenScape Business.

Requisitos de hardware

Para la integración de OpenScape Business TAPI 170 se requiere un enlace CSTA de OpenScape Office, sin importar cuántos clientes TAPI 170 haya integrados. También es válido para sistemas OpenScape Business interconectados.

El PC debe cumplir los requisitos del sistema indicados por Microsoft para el sistema operativo utilizado, siempre que no se utilicen más aplicaciones de SW que no sean TAPI 170. Además, se requiere una interfaz LAN Ethernet.

Terminales compatibles

Los terminales y las prestaciones compatibles en estos terminales dependen del abanico de funciones CSTA o WSI del sistema OpenScape Business que se utilice. Esta información se incluye en la información de ventas de OpenScape Business.

23.3 Interfaz de Web Services

La interfaz integrada de Web Services permite la supervisión y el control de recursos de telefonía en sistemas con usuarios de UC.

Prestaciones

La interfaz de Web Services ofrece las siguientes prestaciones:

- Acceso vía Ethernet LAN (TCP/IP)
- Compatibilidad con HTTP y HTTPS
- Compatibilidad con sistemas individuales
- Funciones fáciles de usar y bien estructuradas para:
  - Control de llamadas
  - Control de dispositivos
  - Supervisión de dispositivos
  - Listines telefónicos
  - Diario de las extensiones
  - Presencia de las extensiones

Nota: En función del tipo de cliente WSI (Web Services Interface), el marcador de extensión Servicios asociados debe estar activado para habilitar la ejecución de algunos comandos WSI.

Sesiones web de WebServer

El número de sesiones de Web Server es común para todas las aplicaciones correspondientes como, por ejemplo, myPortal to go (Web Edition), Application Launcher, OptiClient Attendant (servidor) y OptiClient BLF.

Puntos de monitoreo internos

Los puntos de monitoreo internos no dependen de los puntos de monitoreo de la interfaz CSTA. Si varias aplicaciones supervisan al mismo usuario de UC mediante la Web Services Interface, el servidor Web utiliza un único punto de monitoreo interno.

Puertos

Están disponibles los siguientes números de puerto:

Puerto	Protocolo
8801	HTTP (sin cifrar)
8802	HTTPS (cifrado)

23.4 Open Directory Service

Open Directory Service (ODS) es un servicio de directorio abierto, integrado y basado en LDAP. Funciona como un servicio de metadirectorio, agregando los resultados de diferentes fuentes de directorio internas y externas a través de una única interfaz. En una empresa, se puede acceder al Open Directory Service mediante diferentes tipos de clientes, aplicaciones y dispositivos de comunicación.

El Open Directory Service realiza dos funciones:

1) Proporciona acceso a datos de contacto adicionales procedentes de fuentes externas mediante acceso a datos SQL u ODBC a bases de datos en la red del cliente que contienen datos de directorio
2) Expone tanto directorios internos como externos a clientes, dispositivos de comunicación y aplicaciones.

El Open Directory Service está desactivado por defecto. Al activarlo, asegúrese también de que los cortafuegos estén abiertos para el protocolo LDAP en el puerto TCP/389.

Servicio de directorio abierto en diferentes variantes de OpenScape Business

El Open Directory Service se ofrece con diferentes funcionalidades dependiendo de la plataforma OpenScape Business:

- Placas base OpenScape Business S, OpenScape Business X V3 Advanced, servidor Booster o tarjeta Booster:

  Se ofrece funcionalidad completa, de modo que se pueden utilizar fuentes de datos tanto internas como externas
- Placas base OpenScape Business X V3 Basic:

  La funcionalidad se limita a las fuentes de datos internas predeterminadas.

- Placas base OpenScape Business X V2:

  Se requiere una tarjeta Booster o un servidor Booster para utilizar el Open Directory Service.

Para conectarse al Open Directory Service a través del protocolo LDAP, utilice la dirección IP que se muestra en el portal de administración:

- En la parte derecha de la página de inicio de OpenScape Business Assistant, bajo **Aplicaciones**.
- En la página **Selección de aplicación** del asistente de **instalación inicial**, en**Configuración** > **instalación básica**

Fuentes de datos internas

Las siguientes fuentes de datos internas están disponibles de forma predeterminada en el Open Directory Service:

- Directorio externo
- Directorio interno
- Números de marcación rápida centrales

Para estas fuentes de datos internas, los nombres de los campos están permanentemente asignados al esquema de datos del Servicio de Open Directory.

Estas fuentes de datos internas no se pueden eliminar ni modificar. Para exponer fuentes de datos internas a través de ODS, se requiere una licencia "OpenScape Business OpenDirectory Base".

Fuentes de datos externas

Como administrador, puede integrar información de contacto de los siguientes tipos de bases de datos como fuentes de datos para acceso de solo lectura a través de SQL u ODBC.

- Fuentes de datos con controladores integrados (Microsoft SQL Server, PostgreSQL, Sybase SQL).
- Las fuentes de datos sin controladores integrados requieren un servidor ODBC Bridge instalado y configurado en el cliente ODS (descargable a través de WBM en **Centro de servicio** > **Software**).

Nota: Para una conectividad exitosa, es necesario definir un valor (este valor puede ser diferente del nombre de la fuente de datos, pero el campo no puede estar vacío) en el campo **Descripción**. En el caso de una fuente de datos de puente ODBC para Access, Firebird, Excel y Oracle, agregue el nombre de la fuente de datos, "access", "firebird", "excel" u "oracle", respectivamente, como valor del campo **Descripción** .

Nota: Para la integración de Microsoft Excel con la base de datos ODS, solo se admite el formato de archivo *.xsl* (pero no el *.xlsx*). En las versiones recientes de MS Office, evite editar o guardar los archivos de Excel para no dañar la codificación del archivo. Además, se requiere un controlador ODBC Bridge específico para Microsoft Excel.

Para acceder a fuentes de datos externas desde ODS, se requiere una licencia de "OpenScape Business OpenDirectory Connector" por cada fuente de datos conectada.

Número máximo de tipos diferentes de bases de datos: 3

Número máximo de fuentes de datos externas: 4

Asegúrese de que el Open Directory Service esté autorizado para acceder a la fuente de datos externa. Póngase en contacto con el administrador de la base de datos responsable con antelación para asegurarse de que esto sea así. Puede que sea necesario agregar un usuario independiente en la fuente de datos externa para que el sistema pueda acceder a ella.

Las fuentes de datos externas pueden utilizarse tanto en el contexto de las búsquedas en directorios como en la resolución de números de llamada en nombres.

Puede configurar el acceso directo a una tabla de base de datos desde una fuente de datos externa o una consulta SQL personalizada para la fuente de datos.

Cualquier columna que sirva como ID debe contener valores únicos y no nulos/no vacíos. Utilice la propiedad UNIQUE o PRIMARY KEY para asegurarse de que esto sea así.

En los casos en que se integren bases de datos externas, se aplicarán las siguientes restricciones:

- Los caracteres especiales `´[]'"` no son compatibles con ODS en nombres de tablas y nombres de columnas.
- Los tipos de columna "nchar" y "nvarchar" no son compatibles con ODS.
- Los caracteres de espacio en blanco intermedios (al menos en los últimos 4-5 dígitos) no son compatibles con el ODS para datos telefónicos.

Consultas SQL personalizadas para fuentes de datos externas

Las consultas SQL personalizadas también admiten tablas relacionadas, por ejemplo:

```
SELECT * FROM users LEFT OUTER JOIN phonenumbers ON
users.id = phonenumbers.uid;
```

La estructura de datos debe ser del tipo 1:1 o n:1, es decir, cada registro puede tener solo una fila.

El acceso mediante consultas SQL personalizadas a veces puede ser mucho más lento que el acceso directo a una tabla de la base de datos.

Las consultas SQL personalizadas con posibles riesgos de seguridad no se ejecutan; por ejemplo:

- Modificar datos
- Deteniendo el servidor SQL
- Ejecución de programas a través del servidor SQL
- Modificar los derechos de usuario

Por lo tanto, las consultas SQL personalizadas con los siguientes comandos SQL no se ejecutan:

- `PUNTO DE CONTROL`
- `CERRAR`
- `GRUPO`

- COMPROMETERSE
- COPIAR
- CREAR
- DESASIGNAR
- DECLARAR
- ELIMINAR
- DESCARTAR
- HACER
- ABANDONAR
- END
- EJECUTAR
- EXPLICAR
- BUSCAR
- CONCEDER
- INSERTAR
- CARGAR
- BLOQUEAR
- MOVER
- PREPARAR
- REASIGNACIÓN DE PROPIEDAD
- REINDEXAR
- PUESTA EN GUARDADO
- REINICIAR
- REVOCAR
- PUNTO DE GUARDADO
- ETIQUETA DE SEGURIDAD
- SELECCIONAR EN
- ESTABLECER
- MOSTRAR
- INICIAR TRANSACCIÓN
- TRUNCAR
- DEJAR DE ESCUCHAR
- ACTUALIZAR
- ASPIRAR
- VALUES

Asignación de campos para fuentes de datos

Para estas fuentes de datos, puede personalizar la asignación de nombres de campo al esquema de datos del Open Directory Service. Puede asignar cada campo del esquema de datos del Open Directory Service a no más de un campo de la fuente de datos externa. Sin embargo, puede asignar un campo de la fuente de datos externa a varios campos en el esquema de datos del Open Directory Service.

Asignaciones de salida de datos LDAP

Una asignación de salida de datos LDAP determina cuáles de los campos del esquema de datos del Open Directory Service se enviarán a través de LDAP, por ejemplo, para clientes LDAP específicos o para diferentes grupos de suscriptores que no desean ver todos los detalles, sino solo un subconjunto definido.

La interfaz **web** de mapeo de salida de datos LDAP está disponible de forma predeterminada y no se puede eliminar ni modificar. Todos los campos del esquema de datos en el Open Directory Service están asignados permanentemente a la salida LDAP en el mismo. También puede configurar otras asignaciones de salida de datos LDAP.

Los clientes LDAP pueden acceder a una asignación de salida de datos LDAP específica mediante el parámetro dc en el inicio de sesión LDAP; por ejemplo: `dc=web`.

Normalización de números de teléfono en formato canónico

Para cada fuente de datos, puede configurar la normalización de los números de teléfono en el formato canónico. Durante este proceso, se eliminan los espacios en blanco, los paréntesis, los guiones y las comas. Esto es necesario para identificar correctamente el nombre de la persona que llama y para la marcación desde ordenador. No debe omitir la normalización, a menos que los números de teléfono utilizados en la fuente de datos ya estén presentes en formato canónico. Puede configurar el sistema para que introduzca automáticamente los valores relacionados con la normalización, como el código de área, etc. Si la fuente de datos externa se encuentra en un sitio diferente al del sistema, es posible que deba ajustar estos valores.

Estado de las fuentes de datos

La visualización del estado bajo **OpenDirectory** > **Fuentes de datos** tiene el siguiente significado:

Color	Estado
verde	activo
rojo	ODBC y LDAP no funcionan correctamente; la configuración es incorrecta o la fuente de datos no está disponible
amarillo	LDAP no funciona correctamente: reinicie el Open Directory Service
gris	Configuración incompleta

Suministro de directorios

Los siguientes tipos de clientes, dispositivos de comunicación y aplicaciones pueden utilizar los directorios proporcionados por el Open Directory Service:

- Clientes UC
- Application Launcher
- Directorio del sistema
- OpenStage con soporte LDAP local
- Teléfonos IP DECT (a través de LDAP)
- Teléfonos SIP (a través de LDAP)
- Aplicaciones, por ejemplo, suites CRM como Microsoft Dynamics CRM (a través de LDAP, ODBC o exportación CSV de OpenLDAP)

El Open Directory Service puede identificar en los resultados de búsqueda la fuente de datos de la que se obtiene una coincidencia.

Conceptos relacionados

Requisitos para Application Launcher en la página 1216

23.4.1 Cómo activar o desactivar Open Directory Service

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **Open Directory Service**.
3) En el grupo de menús, haga clic en **Open Directory** > **Ajustes básicos**.
4) Elija una de estas opciones:
   - Si desea activar Open Directory Service, active la casilla de verificación **Activo**.
   - Si desea desactivar Open Directory Service, desactive la casilla de verificación **Activo**.
5) Haga clic en **Guardar**.
6) Haga clic en **Aceptar**.
7) Haga clic en **Aceptar**.

23.4.2 Cómo reiniciar Open Directory Service

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Open Directory Service está activo.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **Open Directory Service**.
3) En el grupo de menús, haga clic en **Open Directory** > **Mantenimiento**.
4) Haga clic en **Reiniciar**.
5) Haga clic en **Aceptar**.

23.4.3 Cómo configurar la contraseña ara acceder a Open Directory Service

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Siga estos pasos para establecer la contraseña con la que los clientes, los dispositivos de comunicación y las aplicaciones pueden acceder al Open Directory Service.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **Open Directory Service**.
3) En el grupo de menús, haga clic en **Open Directory** > **Ajustes básicos**.
4) Introduzca la **Contraseña LDAP** deseada.
5) Haga clic en **Guardar**.
6) Haga clic en **OK**.

23.4.4 Cómo configurar el ODBC-ODBC Bridge Server

Requisitos previos

El ODBC Bridge Server se ha descargado de la Gestión basada en Web (WBM), en **Centro de servicios** > **Software**, y se ha instalado en un PC con Windows (32 o 64 bits) con fuentes de datos que pueden acceder a bases de datos relacionales o no relacionales. El ODBC Bridge Server es necesario para que los controladores ODBC puedan acceder a la fuente de datos.

Nota:

Debido a las recientes actualizaciones de Windows 10/Windows Server de Microsoft, la interfaz ODBC del sistema operativo se ha modificado y, por lo tanto, solo los controladores de 32 bits son compatibles con ODBC to ODBC Bridge. Por el momento, se recomienda encarecidamente utilizar controladores ODBC de 32 bits para conectarse a fuentes de datos ODBC.

Se trata de una restricción temporal.

La fuente de datos se debe configurar como DSN en el cliente ODS mediante la administración de fuente de datos ODBC.

Conoce el nombre de usuario y la contraseña de la fuente de datos.

La configuración del ODBC Bridge Server se describe para la interfaz de usuario en idioma inglés. Por supuesto, la configuración también se puede realizar en otro idioma de interfaz (**Administrador de servidor** > **Idioma** tab).

Paso a paso

1) Haga clic con el botón secundario del ratón en el icono del ODBC Bridge Server de la bandeja de herramientas y seleccione la opción **Ajustes**.

2) Defina los ajustes generales del servidor:

a) Haga clic en la pestaña **Ajustes de servidor**.

b) En **Ajustes de conexión** seleccione la dirección IP con la que el cliente ODBC (OpenScape Business) accederá al ODBC Bridge Server en la lista desplegable **Interfaz de red**.

Al hacer la configuración ODS, esta dirección IP se debe introducir en la Gestión basada en Web (WBM) de OpenScape Business.

c) En **Puerto** indique el puerto al que llegarán las consultas del cliente ODBC (OpenScape Business).

Al hacer la configuración ODS, este puerto se debe introducir en la Gestión basada en Web (WBM) de OpenScape Business.

d) Si el servicio está detenido defina el **Estado de servicio** en **act.** (en **Control de servicios**) para activarlo, o seleccione **Iniciar servicio** en la bandeja de herramientas.

e) Si el servicio está conectado, defina el **Estado de servicio** en **desact.** para desactivarlo, o seleccione **Detener servicio** en la bandeja de herramientas.

f) En **Ajustes de red**, puede activar el cifrado definiéndolo en **act**.

g) En **Ajustes de red**, introduzca el número máximo de conexiones simultáneas a clientes ODBC (mínimo: 1, máximo: 20) en el campo **Conexiones máximas**.

h) Haga clic en **Guardar configuración**.

Nota: Cuando haya guardado los ajustes, deberá reiniciar el servicio.

---

3) Cree un usuario para el acceso del cliente ODBC a la fuente de datos:

a) Haga clic en la pestaña **Gestión de funciones**.

b) Haga clic en **Añadir usuario**.

c) En el campo **Nombre de usuario** asigne un nombre de usuario para el cliente ODBC.

d) En **Contraseña** y **Vuelva a introducir la contraseña** indique una contraseña para el cliente ODBC.

Hay que introducir estos mismos datos de usuario para la configuración ODS en la Gestión basada en Web (WBM) de OpenScape Business.

e) Seleccione el DSN al que podrá acceder el cliente ODBC; para ello, marque la casilla de la columna **Acceso**.

f) Introduzca el **Nombre de usuario de BD** y la **Contraseña**, si es necesario.

g) Haga clic en **Guardar configuración**.

4) Haga clic en la pestaña **Supervisión** para supervisar las conexiones. Aparecen los siguientes datos:

- Las versiones y los nombres de los controladores ODBC instalados.
- El nombre y la dirección IP del cliente ODS, el tiempo de la última conexión activa y el tiempo total de las conexiones activas.
- Las fuentes de datos ODBC disponibles (mediante el enlace **Abrir Administrador de fuentes de datos Windows**).

5) Haga clic en la pestaña **Registros** para permitir la creación de archivos de registro y definir los niveles de seguimiento del registro:
   a) Para activar el registro, defínalo en **act**.
   b) Seleccione el **Nivel de registro**: **Todo** para todos los registros, **Normal** para los registros de servicio o únicamente **Advertencias y Errores**.
   c) Seleccione el tipo de registro en la lista desplegable. Puede ver la carpeta de registros o la consola de registro.
6) Haga clic en la pestaña **Apariencia** para cambiar el aspecto:
   a) Seleccione un tema (claro u oscuro).
   b) Seleccione un estilo.
   c) Defina el idioma deseado.
   d) Seleccione si el servicio se ejecutará automáticamente al iniciar.
   e) Seleccione si el servicio se puede minimizar en la bandeja.
7) Haga clic en la pestaña **Acerca de** para ver los datos de servicio y las actualizaciones disponibles.

   Nota: Si hay disponible una nueva versión, haga clic en **Instalar** para ejecutar la actualización.

8) Seleccione **Salir** en la bandeja de herramientas para cerrar la configuración del servicio.

23.4.5 Cómo añadir una fuente de datos externa para Open Directory Service

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Tiene a su disposición los datos de acceso de la base de datos externa.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **Open Directory Service**.
3) En el grupo de menús, haga clic en **Fuentes de datos**.
4) Haga clic en **Agregar**.
5) Haga clic en la pestaña **Base de datos**.
6) Introduzca el **Nombre** de la fuente de datos.
7) Introduzca una **Descripción** de la fuente de datos.

8) Si desea agregar una base de datos SQL:
   a) Seleccione el tipo de **PostgreSQL** o **Microsoft SQL Server, Sybase SQL** o **ODBC Bridge** de la lista desplegable **ODBC driver**.
   b) En **Dirección de servidor de base de datos** introduzca la dirección IPv4 de la base de datos.
   c) Indique el **Puerto de servidor de base de datos**
   d) Ingrese el nombre de la **base de datos** en el caso correcto.
   e) Indique el **Inicio de sesión en base de datos** y asegúrese de utilizar correctamente mayúsculas y minúsculas.
   f) Introduzca la **Contraseña de base de datos** y asegúrese de usar correctamente mayúsculas y minúsculas.
   g) Si seleccionó el tipo **Microsoft SQL Server, Sybase SQL** en la lista desplegable del **controlador ODBC**, **ingrese también la versión del protocolo TDS.**
9) Si desea agregar una base de datos no SQL:
   a) En la lista desplegable **Controlador ODBC**, seleccione el tipo **ODBC Bridge**.
   b) En **Dirección de ODBC Bridge Server**, introduzca la dirección IPv4 de la base de datos.
   c) Introduzca el **Puerto de ODBC Bridge Server**.
   d) Ingrese el **DSN remoto del puente ODBC**
   e) Ingrese el **inicio de sesión de puente ODBC** correcto, que distinga entre mayúsculas y minúsculas.
   f) Ingrese la **contraseña de puente ODBC** correcta, que distinga entre mayúsculas y minúsculas.
10) Haga clic en **Comprobar acceso a base de datos** para probar el acceso.
11) Haga clic en **Guardar**.
12) Haga clic en la pestaña **Acceso a datos**.
13) Si desea utilizar una tabla de base de datos:
   a) Haga clic en **Selección simple - Acceso a una tabla**.
   b) Haga clic en **Consultar tablas de base de datos** y seleccione la tabla deseada en la lista **Tablas de base de datos**.

      Nota: Esta funcionalidad no es compatible con algunas fuentes de datos (por ejemplo, Oracle). Si es así, proporcione el nombre de la tabla manualmente.

   c) Haga clic en **Vista preliminar de tabla de base de datos** y, en la vista preliminar, desplácese por los bloques de datos utilizando los botones correspondientes.
14) Si desea utilizar una consulta SQL personalizada:
   a) Haga clic en **Consulta SQL autodefinida**.
   b) Introdúzcala en **Consulta SQL**.

      Nota: Al definir una nueva fuente de datos con una declaración SQL, debe formular la consulta de manera que garantice que los IDs de los registros sean constantes. Debe utilizar los atributos de ID incluidos en las tablas respectivas en lugar de calcular los IDs cuando se ejecuta la consulta. Evite cualquier declaración como "SELECT ROW_NUMBER() OVER

As ID" que crea IDs cuando se ejecuta la consulta y que entregará diferentes IDs dependiendo de la clasificación y la cantidad de registros. En caso de unir tablas con rangos de ID superpuestos con UNION ALL, mitigue el riesgo de IDs duplicados incrementando los IDs de las tablas existentes con un número diferente para cada tabla que se unirá (por ejemplo, "SELECT (table2.ID 1000) AS ID").

c) Haga clic en **Vista preliminar del resultado de la consulta** y, en la vista preliminar, desplácese por los bloques de datos utilizando los botones correspondientes.

15) Haga clic en la pestaña **Asignaciones de campo**.

Nota: Todas las columnas de la tabla seleccionada o todas las columnas que devuelve la consulta SQL definida por el usuario están disponibles para las asignaciones de campo.

16) Haga clic en **Agregar asignación de campo**.

17) En la lista desplegable que aparece a la izquierda del campo de la fuente de datos externa y en la lista desplegable que aparece a la derecha de la misma línea, seleccione el campo asignado del esquema de datos de Open Directory Service. Con fines de control, a la derecha se muestra una vista previa de los bloques de datos correspondientes; puede desplazarse por ella mediante los botones correspondientes.

Nota: El campo del **número de identificación** se debe asignar a un campo de la fuente de datos externa que sea exclusivo.

18) Si desea eliminar una fila de asignaciones de campos, haga clic en el icono de papelera a la izquierda.

19) Haga clic en la pestaña **Conversión de número**.

a) Active la casilla de verificación **Activo**.

b) Haga clic en **Consultar configuración de sistema**.

c) Si la base de datos externa no está en la misma ubicación que el sistema, indique: **Prefijo del país**, **Código de red local**, **Prefijo de marcación**, **Prefijo nacional** y **Extensión máxima de número interno**.

d) Elija una de estas opciones:

- Si desea eliminar un prefijo de marcación que pudiera haber en una fuente de datos externa, active la casilla de verificación **Eliminar prefijo de marcación**.

- Si no desea eliminar el prefijo de marcación, desactive la casilla de verificación **Eliminar prefijo de marcación**.

20) Haga clic en **Guardar**.

21) Haga clic en **Aceptar**.

Pasos siguientes

Reinicie Open Directory Service para aplicar los cambios.

Haga una vista previa del resultado de la búsqueda LDAP.

23.4.6 Cómo ejecutar una vista preliminar de los resultados de búsqueda LDAP para el Open Directory Service

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Para comprobar si un resultado de búsqueda LDAP de Open Directory Service ofrece los conjuntos de datos en la forma deseada y con el formato de número de teléfono correcto, siga estos pasos.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **Open Directory Service**.
3) En el grupo de menús **Open Directory** > **Usuarios de OpenScape Business** > **Fuentes de datos** haga clic en la fuente de datos deseada.
4) Haga clic en la pestaña **Prueba LDAP**.
5) Haga clic en **Ejecutar prueba**. En **Resultado de búsqueda LDAP**, se muestra una vista preliminar del resultado de la búsqueda.

Nota: El límite de respuestas estándar de OpenLDAP es 500 entradas. El motor back-end de Open Directory Service (ODS) también impone un límite de 500 entradas para cada fuente de datos.

La función de prueba LDAP de Open Directory Service (ODS) efectúa una consulta de búsqueda con un máximo de 500 entradas. El objetivo de la opción de prueba LDAP no es recuperar resultados, sino comprobar que la conectividad LDAP es la adecuada.

Por lo tanto, si hay más de 500 registros, es posible que las adiciones y modificaciones a los datos de LDAP no se reflejen en la Gestión basada en Web (WBM) después de ejecutar una prueba de LDAP.

23.4.7 Cómo borrar una fuente de datos externa para Open Directory Service

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **Open Directory Service**.
3) En el grupo de menús, haga clic en **Open Directory** > **Fuentes de datos**.
4) En el área de trabajo, haga clic en la fuente de datos correspondiente.
5) Haga clic en **Borrar**.

6) Haga clic en **Aceptar**.

Pasos siguientes

Reinicie Open Directory Service para aplicar los cambios.

23.5 Servicio de integración de Active Directory

Active Directory es un servicio de directorios de Microsoft para redes de dominio. Con el servicio de integración de Active Directory ofrecido, OpenScape Business puede leer la base de datos de Active Directory y sincronizar a los usuarios con su propia base de datos para simplificar la administración de usuarios y la configuración.

Requisitos previos

Para que se produzca la sincronización del servicio de integración de Active Directory deben cumplirse los siguientes requisitos:

- Existe un Active Directory Microsoft Server distribuido por el cliente
- Active Directory se utiliza como un punto de configuración único para los datos del empleado y, especialmente, para los datos del usuario. Se asignarán los siguientes campos entre Active Directory y OpenScape Business:
  - nombre
  - apellido
  - nombre en pantalla
- Este Active Directory solo se utiliza para añadir, cambiar o borrar datos de empleados.
- Se espera que todos los cambios de Active Directory se apliquen también en el sistema de comunicación.

Sincronización

El ID único de usuarios OpenScape Business empleado para la sincronización es el número de marcación directa (DID). Este número se sincroniza con el campo telephoneNumber del AD (Active Directory).

Cada cambio realizado en el Active Directory de la empresa se sincroniza inmediatamente con OpenScape Business. De esta forma, cada nuevo usuario añadido a AD también se añadirá a OpenScape Business y se asignará una licencia de usuario IP a ese usuario.

Cualquier cambio hecho en AD a usuarios ya sincronizados se refleja de inmediato en los usuarios de OpenScape Business.

Si se elimina un usuario sincronizado desde AD, el firstName (nombre), sn y displayName (nombre en pantalla) del usuario también se borrará de OpenScape Business, y se liberará la licencia de usuario IP. Sin embargo, el número de marcación directa y el número de llamada interno no se eliminan de OpenScape Business y permanece disponible para que se asigne a otro usuario.

Nota: El acceso al servicio de Active Directory es de solo lectura. Esto quiere decir que la sincronización de datos del usuario solo se realiza desde Active Directory a OpenScale

Business. Los cambios en la información de un usuario de OpenScape Business no se sincronizan de nuevo con Active Directory y los datos de Active Directory se sobrescribirán con la siguiente sincronización.

Asignación de campos

Puede personalizar la asignación de nombres de campo en el esquema de datos del servicio de Active Directory. De esta manera, puede controlar la forma en que se actualizan los campos en OpenScape Business a partir de los datos de Active Directory.

La asignación predeterminada de campos se indica en la tabla siguiente:

Campo OpenScape Business	Campo Active Directory
nombre	nombre
apellido	sn
nombre en pantalla	displayName
Marcación directa	telephoneNumber

Normalización de números de marcación directa

Los datos de ubicación de gateway del sistema OpenScape Business se utilizan para convertir el número de marcación directa de un usuario en un formato de número canónico.

Si es necesario, el formato de telephoneNumber en Active Directory también tiene que estar en formato canónico para que sea posible la sincronización automática.

23.5.1 Cómo configurar el servicio de Active Directory

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente del **Servicio de integración de Active Directory**.
4) Haga clic en la casilla de verificación **Activo** para activar el servicio de integración de Active Directory.
5) Establezca la **Dirección IP** del servidor de Active Directory, el **Nombre de usuario** y la **Contraseña** para un usuario válido.

   El **Nombre de usuario** solicitado aquí no es un nombre de usuario de OpenScape Business, sino un nombre de usuario de eActiveDirectory que se debe proporcionar en formato de especificación de directorio X.500. En este formato los usuarios se definen con lo siguientes nodos:

CN	Nombre común
OU	Unidad organizativa

DC	Componente de dominio

El nombre de usuario se describe a partir de la información más específica a la izquierda del más general de la derecha. Cada información se proporciona en forma de pares separados con un signo igual (**=**).

Un ejemplo de nombre de usuario sería `CN=John.doe,OU=Administrdores,DC=AlgunaCompañía`.

6) Haga clic en **Buscar DN** para buscar los DN disponibles y seleccione uno de ellos como base raíz de namingContext.

Si hay algún problema con las credenciales del usuario, verá un error `¡Error de autenticación! Compruebe sus credenciales`.

7) Si es necesario, edite los campos **Contenedor** y **Filtro**.

El valor estándar para un contenedor es `cn=Usuarios` y para un filtro es `(&(objectCategory=person)(objectClass=user))`

8) Haga clic en **Buscar datos**.

Se mostrarán las primeras 1000 entradas de AD, ordenadas por apellidos(sn).

9) Haga clic en un usuarios para comprobar los detalles.

10) Haga clic en **OK y Continuar** para ir a la pantalla **Asignación de campos**.

11) Realice las modificaciones necesarias en los valores de asignación de campos.

Los valores en la columna izquierda son el esquema de base de datos de OpenScape Business y los valores en la columna derecha corresponden a los atributos de Active Directory.

El **Número de teléfono** se utilizará para que coincida con el número de marcación directa de OpenScape Business.

12) Haga clic en **Finalizar** para completar la integración de Active Directory.

23.6 Application Launcher

Application Launcher es una aplicación Windows basada en Java para el control relativo a llamadas de aplicaciones en PC cliente de usuarios de la UC Suite y de myAgent. Application Launcher se puede utilizar por ejemplo para abrir automáticamente el formulario de contacto del usuario en un sistema CRM.

Application Launcher ofrece las siguientes prestaciones:

- La información relativa a la llamada sobre el número de teléfono (número de teléfono, nombre del interlocutor, ID de cliente, etc.) se toma del Open Directory Service o de los directorios del sistema
- Llamada desde aplicaciones Windows o aplicaciones Web en caso de llamadas entrantes y salientes
- Transferencia de información relativa a la llamada a aplicaciones Windows o aplicaciones Web
- Modo automático en segundo plano con llamadas entrantes
- Ventana emergente configurable y opcional en caso de llamadas entrantes con información relativa a la llamada y botones para acciones de usuario
- Lista de llamantes con función de llamada
- Funciones de vista previa para pruebas durante la configuración

- La configuración del primer cliente configurado se aplica fácilmente a todos los demás mediante el perfil de configuración del sistema

23.6.1 Requisitos para Application Launcher

Para utilizar Application Launcher, el PC cliente del usuario de UC Suite debe tener el software y el hardware adecuados.

La instalación requiere derechos de administrador en el PC cliente, pero no requiere actualizaciones automáticas.

Sistema operativo

Application Launcher se puede utilizar junto con los siguientes sistemas operativos:

- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bits o 64 bits)
- Microsoft Windows Vista (32 bits)

> **Consejo:** El sistema operativo utilizado requiere siempre la última versión de todas las actualizaciones disponibles (Service Packs y parches).

Windows Update

Los PC requieren siempre la última versión de todas las actualizaciones disponibles, incluidos los Service Packs.

Software adicional

Oracle Java 8 o superior, o bien OpenJDK 8 (véase**Service Center** > **Software**)

Web Services para teléfonos móviles

A fin de realizar la conexión de sistema, Web Services para teléfonos móviles debe estar activado en el sistema. En los firewalls de la LAN y de los PC cliente, deben estar abiertos los puertos configurados en el sistema.

Open Directory Service (opcional)

Si desea utilizar datos de Application Launcher desde Directory Service, este servicio debe estar configurado en el sistema. En los firewalls de la LAN y de los PC cliente, debe estar abierto el puerto configurado en el sistema.

Conceptos relacionados

Configuración de myPortal to go y Mobility Entry en la página 980
Open Directory Service en la página 1201

23.6.2 Perfil con datos de configuración de Application Launcher

Un perfil con datos de configuración de Application Launcher permite configurar rápida y fácilmente Application Launcher en todos los PC cliente.

El perfil incluye todos los datos de configuración, excepto los de conexión de sistema y del usuario. Una vez concluida la configuración de Application Launcher en un usuario, el administrador puede ofrecer ese perfil con los datos de configuración de Application Launcher en el sistema de comunicación. A continuación, todos los usuarios pueden importar el perfil y utilizarlo para configurar Application Launcher.

23.6.2.1 Cómo ofrecer un perfil con datos de configuración desde Application Launcher

Requisitos previos

Application Launcher está configurado para un usuario.

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Application Launcher**.
3) Haga clic en **Examinar** y seleccione este archivo: `C:\Documents and Settings\<Nombre del usuario Windows>\Application Data\Tray_Tool\profile.xml`.
4) Haga clic en **Abrir**.
5) Haga clic en **Cargar**.

Pasos siguientes

Todos los usuarios puede importar este perfil en el Application Launcher y usarlo para hacer la configuración.

23.7 Descripción general de myPortal for Teams

El plugin myPortal for Teams se utiliza para integrar la aplicación Microsoft Teams con OpenScape Business.

myPortal for Teams requiere una nueva placa base OpenScape Business V3 o un sistema OpenScape Business S y es compatible con la versión de software V3R1 FR2 y posteriores.

Con myPortal for Teams podrá:

- Filtrar y gestionar el historial de llamadas.
- Ver y buscar contactos.
- Organizar los contactos en grupos de favoritos.
- Enviar correos electrónicos a contactos.
- Seleccionar un dispositivo controlado (disponible para los usuarios de MULAP).
- Iniciar una llamada.
- Contestar, rechazar o desviar una llamada.
- Poner una llamada en espera.
- Transferir una llamada.
- Hacer una llamada de consulta.

- Alternar las llamadas.
- Realizar una transferencia asistida.

Nota: La búsqueda de contactos en directorios externos, como LDAP, no está disponible.

Nota: No hay compatibilidad con la función de Voz por IP, VoIP para myPortal for Teams.

23.7.1 Cómo configurar MyPortal para Teams

Requisitos previos

- Certificado oficial y de confianza de Microsoft para importar en OpenScape Business WBM
- ID de aplicación de Microsoft que debe generarse antes de configurar myPortal for Teams

Paso a paso

1) Desplácese hasta **Configuración> Servicios en la nube**.

2) Haga clic en Editar junto a **Complemento de cliente de Microsoft Teams**.

3) El nombre de dominio y el número de puerto en el campo **URL** ya están rellenados.

El nombre de dominio es el dominio de su sistema OpenScape Business.

El valor por defecto del número de puerto es 8805. Puedes cambiar el ID del dominio y el número de puerto si lo deseas.

4) Introduzca la **ID de aplicación**,

El administrador genera la ID de aplicación en el portal Microsoft Azure.

5) Haga clic en **OK y Descargar**.

El complemento se descarga como un archivo zip. El archivo descargado es un plugin personalizado basado en la configuración de su sistema.

Nota:

La pestaña de Microsoft Teams impide cargar el contenido web de un servidor que utiliza certificados autofirmados. Este es un aspecto de seguridad y el uso de certificados autofirmados es esencialmente una práctica insegura ya que esta interfaz está expuesta a Internet.

Por lo tanto, debe instalarse en el sistema un certificado de confianza de Microsoft. Para más información, véase también el capítulo.

23.7.2 Cómo cargar myPortal para Teams en la tienda de Teams

Requisitos previos

Debe tener derechos de administrador para la aplicación Microsoft Teams.

Paso a paso

1) Haga clic en **Aplicaciones** en la barra de navegación izquierda de la aplicación Microsoft Teams.
2) Haga clic en **Cargar una aplicación personalizada** y seleccione **Cargar para mi organización**.

   Seleccione el archivo que ha descargado de WBM y cárguelo.

Pasos siguientes

Una vez que se cargue el complemento myPortal para Teams, está disponible para que los usuarios lo añadan a su aplicación Microsoft Teams.

23.8 Unify Phone

Los usuarios de OpenScape Business pueden realizar llamadas telefónicas a través del cliente Unify Phone. Esta funcionalidad está disponible tanto desde el cliente de Unify Phone como a través del dispositivo. Para hacer eso, debe configurar la conectividad de Unify Phone con OpenScape Business y agregar los usuarios de Unify Phone.

La funcionalidad disponible de Unify Phone incluye:

- Realizar o responder llamadas
- Eliminar o rechazar llamadas
- Retener o recuperar llamadas
- Llamada Pull/Push
- Admisión de DTMF
- Swap de llamadas (alternativa)
- Desvío de llamadas
- Número alternativo
- Encaminamiento de llamadas
- Acceso al directorio y al diario
- Control de llamadas de terceros mediante los siguientes clientes de UC integrados: myPortal @work, myPortal for Desktop, myPortal for Outlook, myAttendant, my Agent y myPortal for Teams.

Además de las características mencionadas anteriormente, no se lanzan otras funciones, especialmente los códigos de función.

Nota: Actualmente, el control de llamadas de terceros (control CTI) solo es posible para el cliente de escritorio de Unify Phone. El control siempre se realiza a través del cliente de escritorio del Unify Phone (Web/PWA) y no está diseñado para el cliente móvil de Unify Phone. Es posible mover una llamada al cliente móvil de Unify Phone después de aceptar la llamada. Además, el control de llamadas de terceros no está diseñado para usarse junto con una función de "número alternativo" activa de Unify Phone.

23.8.1 Cómo configurar la conectividad del Unify Phone

Requisitos previos

Ha ingresado el valor **Upstream hasta (Kbps)** en **Configuración** > **Asistentes** > **Instalación básica** > **Instalación básica** > **Upstream de su conexión a Internet**, para poder realizar llamadas simultáneas. Por ejemplo, escriba “256” para realizar dos llamadas simultáneas.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Servicios en la nube**.
3) Haga clic en **Editar** junto a **Conectividad de Unify Phone**, para configurar los ajustes básicos de conectividad.
4) Seleccione la casilla de verificación **Habilitar Unify Phone** para activar la conectividad de Unify Phone.
5) En **Credenciales del Dominio Unify Phone**, ingrese los siguientes detalles:
   a) Seleccione el **Dominio** de la lista desplegable disponible.

      Existen las siguientes opciones:

      - phoneapp.unify.com
      - Personalizado

      Nota: Si Personalizado está seleccionado, rellene el campo **Dominio personalizado**.

   b) Ingrese la clave API que se genera para su inquilino en el campo **Clave API de Unify Phone**.
6) En **Llamadas simultáneas de Unify Phone**, seleccione la cantidad de llamadas telefónicas simultáneas de Unify en la lista desplegable disponible. El número depende del valor de flujo saliente que haya configurado anteriormente.

   Nota: Si la calidad de la llamada se deteriora, debe reducirse el número de llamadas simultáneas.
7) Haga clic en **Aceptar & Siguiente**.
8) En la ventana **Número de Ubicación de Unify Phone**, seleccione qué esquema de numeración desea utilizar. Esta selección afecta el formato de los números SIP y WSI.

   - Para utilizar números internacionales, active la casilla de verificación **Usar numeración internacional**.

     Si se eligen números internacionales, el asistente le pedirá que configure los números de ubicación que faltan en la ruta de Unify Phone, que se utilizarán para formar el número internacional. Además, los parámetros de ruta de Unify Phone para el tipo de número se actualizan según la selección.
   - Números internos
9) Haga clic en **Aceptar & Siguiente**.

10) Haga clic en **Ejecutar función** en la ventana emergente para crear una troncal SIP para Unify Phone.
11) Haga clic en **Aceptar & Siguiente** seguido de **Finalizar**.

Nota: Se sugiere guardar los datos de configuración, seleccionando **Copia de seguridad de datos** > **Copia de seguridad: inmediata** desde el menú principal.

Pasos siguientes

Si desea deshabilitar la conectividad de Unify Phone, primero debe eliminar todos los usuarios de Unify Phone como se describe en Cómo eliminar o eliminar usuarios de Unify Phone en la página 1224.

Nota: Es vital eliminar los usuarios activos de Unify Phone antes de, p. migraciones del sistema, para evitar discrepancias críticas entre la base de datos de OpenScape Business y la base de datos en la nube.

23.8.2 Cómo configurar la instancia de usuario de Unify Phone

Requisitos previos

La conectividad de Unify Phone está configurada.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Servicios en la nube**.
3) Haga clic en **Editar**, junto a **Instancia de usuario de Unify Phone**.
4) Haga clic en **Aceptar y Siguiente** y luego **Terminar**.

23.8.3 Cómo gestionar usuarios de Unify Phone

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Servicios en la nube**.
3) Haga clic en **Editar** junto a la **Instancia de usuario de Unify Phone**.

   Aparece una lista con los usuarios de Unify Phone configurados para el sistema específico.

Nota: Si ya hay usuarios registrados de Unify Phone se le pedirá que ejecute el asistente de Conectividad de Unify Phone sin cambiar la configuración.

23.8.3.1 Cómo crear nuevos usuarios de Unify Phone

Requisitos previos

La conectividad de Unify Phone está configurada.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Servicios en la nube**.
3) Haga clic en **Editar**, junto a **Instancia de usuario de Unify Phone**.
   Se muestran los usuarios de Unify Phone disponibles.
4) Haga clic en **Crear** junto a **Crear un nuevo usuario para Unify Phone**.
5) En la página de **creación de usuarios de Unify Phone**, haga lo siguiente:
   a) El **Código de acceso a la línea troncal Número de llamada del usuario de Unify Phone** es de sólo lectura y se genera automáticamente según el esquema de numeración seleccionado (internacional o interno).
   b) Ingrese el número de llamada del usuario de Unify Phone .
   c) Ingrese el **DID del usuario del Unify Phone**.
   d) Ingrese el **Nombre**.
   e) Ingrese el **Apellido**.
   f) Ingrese la **dirección de correo electrónico** del usuario de Unify Phone.
6) Haga clic en **Aceptar & Siguiente**.
7) Haga clic en **Salir**.
   Una vez que este proceso se completa con éxito, se envía un correo electrónico a la dirección de correo electrónico ingresada, lo que permite al usuario de Unify Phone completar la configuración.
8) Repita los pasos 4 a 6 para agregar más usuarios de Unify Phone.

23.8.3.2 Cómo agregar usuarios existentes de Unify Phone

Requisitos previos

La conectividad de Unify Phone está configurada.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Servicios en la nube**.
3) Haga clic en **Editar**, junto a **Instancia de usuario de Unify Phone**.
   Se muestran los usuarios de Unify Phone disponibles.
4) Haga clic en **Agregar** junto a **Agregar usuario existente para Unify Phone**.
5) En la página **Asignación de Usuario de Unify Phone**, los usuarios disponibles se muestran como íconos. Para agregar un usuario existente, haga lo siguiente:
   a) El **Código de acceso a la línea troncal Número de llamada del usuario de Unify Phone** es de sólo lectura y se genera automáticamente según el esquema de numeración seleccionado (internacional o interno).

b) Ingrese el número de llamada del usuario de Unify Phone .
c) Ingrese el **DID del usuario del Unify Phone**.
d) Puede buscar un usuario por **Nombre** o **correo electrónico**.
e) Seleccione un usuario de Unify Phone usando los íconos disponibles.

Hay tres tipos de íconos para los usuarios de Unify Phone:

- Iconos verdes: Usuarios disponibles que están activos.
- Iconos verdes atenuados: Usuarios no disponibles que no están activos.
- Icono verde atenuado en marco rojo: Usuarios no disponibles que no están activos, ya configurados con un número en Unify Phone.

Los campos **Nombre** y **Apellido** del usuario de Unify Phone se completan automáticamente.

6) Haga clic en **Aceptar & Siguiente**.

7) Repita los pasos 4 a 6 para agregar más usuarios de Unify Phone.

Pasos siguientes

Asigne licencias a los usuarios de Unify Phone como se describe en Cómo registrar licencias para suscriptores (independientes) en la página 323 o Cómo registrar licencia para extensiones (interred) en la página 334.

Al integrar un usuario de Unify Phone en un equipo (MULAP), tenga en cuenta lo siguiente:

- Solo se puede incluir un teléfono de escritorio IP o TDM en el equipo con el usuario de Unify Phone. La función de enrutamiento en Unify Phone se usa para determinar qué dispositivo final se debe usar para señalar una llamada entrante.
- El teléfono de escritorio del equipo con Unify Phone aún puede controlarse mediante aplicaciones externas a través de TAPI, WSI o CSTA. Esto también se aplica cuando Unify Phone se controla mediante aplicaciones de terceros.
- Los suscriptores inalámbricos no están aprobados en relación con Unify Phone.

23.8.3.3 Cómo editar los datos de usuario de Unify Phone

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Servicios en la nube**.

3) Haga clic en **Editar** junto al usuario de Unify Phone correspondiente.

4) Puede editar la siguiente información detallada:

a) El **Código para ocupación de línea urbana + Número de llamada de usuario de Unify Phone** es de únicamente lectura y se genera automáticamente según el esquema de numeración seleccionado (internacional o interno).
b) El **Número de llamada de usuario de Unify Phone**.
c) El **DID de usuario de Unify Phone**.
d) El **Nombre** de usuario de Unify Phone.

e) Los **Apellidos** de usuario de Unify Phone.

Nota: No se puede editar el campo Usuario de Unify Phone seleccionado que contiene la dirección de correo electrónico del usuario.

5) Haga clic en **OK y Continuar**.

23.8.3.4 Cómo eliminar o eliminar usuarios de Unify Phone

Hay escenarios en los que es absolutamente necesario eliminar usuarios de Unify Phone de su sistema OpenScape Business. Por ejemplo:

- Al migrar de un sistema de laboratorio de pruebas a un sistema real/en vivo.
- Al reemplazar una placa base de V2 H/W a V3 H/W o por fallas de H/W.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Servicios en la nube**.
3) Haga clic en **Editar**, junto a **Instancia de usuario de Unify Phone**.
4) Haga clic en **Editar** junto al usuario de Unify Phone correspondiente.
5) Haga clic en **Remover** o **Eliminar**.
6) Repita los pasos del 1 al 5 para eliminar más usuarios de Unify Phone.

Tenga en cuenta que eliminar usuarios administradores es diferente a eliminar usuarios no administradores de Unify Phone:

Cuando los usuarios de Unify Phone, con función de administrador o no, se eliminan del sistema, no se eliminan del inquilino de Unify Phone al que pertenecen. Estos usuarios todavía existen pero ya no tienen un número de teléfono asignado.

Cuando los usuarios de Unify Phone sin función de administrador se eliminan del sistema, también se eliminan del inquilino al que pertenecen.

Cuando los usuarios de Unify Phone con función de administrador se eliminan del sistema, no se eliminan del inquilino al que pertenecen. Estos usuarios todavía existen pero ya no tienen un número de teléfono asignado.

Nota: Si se configura un nuevo sistema mediante clonación o restauración de datos (migración), donde el sistema original tenía configurado un acceso al conector de Unify Phone, se debe garantizar que se evite cualquier discrepancia entre el estado de la nube UP y el de la base de datos OSBiz. Por esta razón, es esencial eliminar cualquier usuario de UP si es necesario y luego desactivar el conector de Unify Phone antes de clonar/hacer una copia de seguridad del sistema original.

23.8.3.5 Cómo configurar las opciones de número alternativo y encaminamiento de llamadas para interconectividad de Unify Phone

Para que las funciones de número alternativo y encaminamiento de llamadas de Unify Phone sean compatibles con OpenScape Business, debe establecer el siguiente ajuste en modo Experto.

Paso a paso

1) En el **modo Experto**, haga clic **Servidor de telefonía** > **Llamadas entrantes** > **Desvío de llamadas**.
2) Haga clic en la pestaña **Listas de destinos de llamada - Definición**.
3) En el apartado **Modificar Desvío de llamadas**, realice los siguientes ajustes de configuración:
   a) Para **Destino 1** seleccione `* Extensión llamada`.
   b) Parar **Destino 2** seleccione `** Definido por el usuario`.
   c) Como **Destino 3**, seleccione `Número de buzón de voz` (opcional).

23.9 Servicio Let's Encrypt

Let's Encrypt es una autoridad de certificación automatizada que ofrece certificados TLS/SSL gratuitos a través del protocolo del Entorno de gestión automática de certificados (ACME). El servicio verifica la propiedad del dominio mediante tokens y desafíos únicos, como el desafío HTTPS. Tras la verificación, los servidores Let's Encrypt proporcionan certificados firmados para una comunicación segura entre servidores y usuarios.

Para los sistemas de placas base V2 que utilizan OCAB o Booster Server, el certificado Let's Encrypt se sincroniza dentro del servidor Booster. Para facilitar la activación, se integra un mecanismo en la aplicación Java. El proceso de activación de los sistemas de placa base V2 puede requerir tiempo adicional ya que el certificado debe transferirse y activarse dentro del Booster (ya sea Tarjeta o Servidor). Debe anticipar un ligero retraso en el tiempo de activación debido a este proceso de sincronización. Cuando la función está desactivada, el certificado de servidor predeterminado se habilita para OCAB o Booster Server.

23.9.1 Cómo configurar el servicio Let's Encrypt

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Servicios en la nube**.
3) Haga clic en **Editar** junto al **Servicio Let's Encrypt**.
4) En **Configuración del nombre de dominio**, introduzca los siguientes datos:
   - Escriba el nombre de dominio en el campo **Nombre de dominio principal**.
   - Opcionalmente, escriba un segundo dominio en el campo **Nombre de dominio secundario (opcional)**.

5) En **Configuración de actualización automática de certificados**, establezca la hora para que se realice la actualización automática en el campo **Hora de actualización automática**.

> **Nota:** Los sistemas se reinician tras una actualización automática.

6) Haga clic en **Activar** para activar o **Desactivar** para desactivar el servicio.
7) En **Estado del servicio Let's Encrypt** podrá encontrar información detallada sobre el servicio y su estado:
   - **Estado del servicio** muestra si el servicio está actualmente `Activo` o `Inactivo`.
   - **Fecha de activación del certificado** muestra la fecha en la que se activó el certificado.
   - **Fecha de renovación** muestra la fecha de vencimiento para la renovación automática del certificado.
   - **Estado de renovación** muestra el estado del proceso de renovación automática.

> **Nota:** El protocolo Let's Encrypt utiliza el puerto HTTP TCP/80 para el desafío HTTP, durante la creación inicial del certificado o la actualización del certificado.

En la página de inicio de WBM se muestra un mensaje que informa a los administradores del sistema cuando el certificado caduca (X días) y cuando el intento de actualización del certificado no tuvo éxito.

23.10 CloudLink Service

CloudLink permite la comunicación entre los sistemas OpenScape Business locales y las aplicaciones Mitel basadas en la nube.

Conexión SIP

La función de conexión SIP se utiliza para conectar OpenScape Business a servicios en la nube como Workflow Studio.

Para habilitar esta función, consulte el capítulo Cómo configurar el conector SIP.

> **Consejo:** Antes de hacerlo, asegúrese de que la conexión a internet de subida esté configurada (consulte Cómo configurar el acceso a internet mediante un router externo.).

Compatibilidad con contenedores en OpenScape Business

OpenScape Business dispone de un entorno de ejecución de contenedores para dar soporte al contenedor CAS (Cloudlink Gateway). Debido a limitaciones de rendimiento/capacidad, solo está disponible en las siguientes versiones de OpenScape Business:

- Placas base V3 con disco NVMe conectado (sistemas integrados)
- Sistemas OpenScape Business S (variantes de servidor)

En los sistemas integrados, el entorno de ejecución de contenedores viene preinstalado como parte de la imagen de software empresarial OpenScape para hardware V3. No se inicia por defecto al arrancar el sistema para ahorrar recursos del sistema. Solo se activa una vez que el administrador habilita la compatibilidad con contenedores en la interfaz web de Cloudlink.

En las variantes de servidor, el entorno de ejecución del contenedor (paquete Docker) debe ser instalado por el administrador al instalar el sistema operativo SLES15.

Para configurar el servicio de soporte de contenedores, consulte el capítulo Cómo configurar la interfaz web de CloudLink Daemon.

23.10.1 Cómo configurar CloudLink Service

Paso a paso

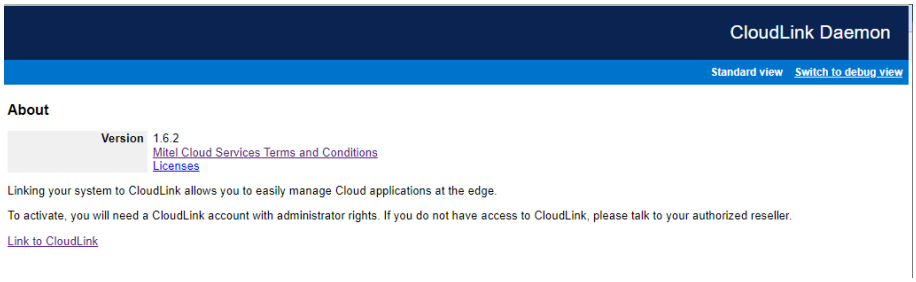
1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Servicios en la nube**.
3) Haga clic en **Editar** junto a **CloudLink Service**.
4) Haga clic en la casilla de verificación junto a **Habilitar CloudLink Service**.
5) Si es necesario, haga clic en la casilla de verificación junto a **Usar proxy**.
6) Escriba la dirección IP y el puerto del proxy en los campos **HTTP-Proxy** y **HTTP-Proxy Port** respectivamente.
7) Escriba sus credenciales en los campos **Nombre de usuario** y **Contraseña**.
8) Si es necesario, haga clic en la casilla de verificación junto a **Habilitar conector SIP**.
9) Haga clic en **Aplicar** para guardar su configuración.
10) Haga clic en **CloudLink** para abrir la ventana de la interfaz web de CloudLink Daemon.

23.10.2 Cómo abrir la interfaz web de CloudLink Daemon

La interfaz web de CloudLink Daemon permite la configuración e integración de sistemas en la nube y locales, mejorando las capacidades de las aplicaciones de comunicación OpenScape Business.

Paso a paso

1) Haga clic en **Enlace a CloudLink**.



   Será transferido al Portal CloudLink.
2) Proporcione su **nombre de usuario** y **contraseña** para iniciar sesión en CloudLink Portal.
3) Iniciar una conexión.

23.10.3 Cómo configurar la interfaz web de CloudLink Daemon

Puede realizar las siguientes acciones utilizando la vista Estándar o la vista Depurar. Para cambiar entre vistas, haga clic en **Cambiar a vista de depuración** o **Cambiar a la vista estándar**.

Paso a paso

1) Haga clic en **Términos y condiciones de los servicios en la nube de Mitel** para ver los términos y condiciones.
2) Haga clic en **Licencias** para ver las licencias relacionadas.
3) Haga clic en **CloudLink Portal**.

   Será transferido al CloudLink Portal.
4) Haga clic en **Desconectarse de CloudLink** para desconectarse del servicio.
5) Cambie el día y la hora para que se realicen las actualizaciones automáticas y haga clic en **Reprogramar**.
6) Haga clic en **Pausa** para pausar la siguiente actualización.
7) Haga clic en **Iniciar todos los túneles** y **Detener todos los túneles** para iniciar o detener túneles configurados.
8) Haga clic en **Iniciar** o **Detener** para iniciar o detener el acceso remoto a través del CloudLink gateway portal.
9) Para las placas base V3 OCCe con NVMe y los sistemas OpenScape Business S, puede configurar la función de soporte de contenedores haciendo lo siguiente:
   a) Haga clic en **Activar compatibilidad con contenedores**.
   b) En la ventana emergente de confirmación, haga clic en **Sí**.
   c) Si es necesario, haga clic en **Reiniciar** o **Desactivar la compatibilidad con contenedores**, para reiniciar o detener el servicio respectivamente.

23.10.4 Cómo habilitar/configurar el conector SIP para conectarse a Workflow Studio

Requisitos previos

La conexión a internet de subida está configurada (consulte Cómo configurar el acceso a internet mediante un router externo).

Se requiere una cuenta de CloudLink y es necesario establecer una conexión con CloudLink (consulte Cómo configurar la interfaz web de CloudLink Daemon).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Servicios en la nube**.
3) Haga clic en **Editar** junto a **CloudLink Service**.
4) Haga clic en la casilla de verificación junto a **Habilitar CloudLink Service**.
5) Si es necesario, haga clic en la casilla de verificación junto a **Usar proxy**.
6) Escriba la dirección IP y el puerto del proxy en los campos **HTTP-Proxy** y **HTTP-Proxy Port** respectivamente.
7) Escriba sus credenciales en los campos **Nombre de usuario** y **Contraseña**.
8) Si es necesario, haga clic en la casilla de verificación junto a **Habilitar conector SIP**.
   a) Seleccione un valor de la lista desplegable para el campo **Número de llamadas simultáneas a CloudLink**.
9) Haga clic en **Aceptar & Siguiente**.
   Los enlaces troncales se añaden (no se necesitan licencias para los enlaces troncales). CloudLink está configurado y se ha establecido una conexión.
10) En la ventana emergente puede ver el estado de la conectividad. Haga clic en **Salir**.

23.11 Números piloto de CloudLink

Llamar a cualquier número piloto de CloudLink configurado enruta la llamada a Workflow Studio para su posterior procesamiento.

El número de pilotos para los servicios Cloudlink por sistema OpenScape Business se limitará a 60 por sistema OpenScape Business.

Las líneas troncales por sistema OpenScape Business están limitadas por la capacidad total de líneas troncales de 250.

Además, las líneas troncales están limitadas por el ancho de banda ascendente definido en el asistente de instalación básico (128 Kbps por línea).

La interconexión troncal de Cloudlink ocupará 1 de las 10 rutas ITSP/Native-SIP dedicadas en un sistema OpenScape Business.

23.11.1 Cómo configurar los números piloto de CloudLink

Requisitos previos

El asistente de CloudLink está configurado.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Servicios en la nube**.
3) Haga clic en **Editar** junto a **Números piloto de CloudLink**.
4) Haga clic en **Agregar**.
5) Bajo la columna **Números piloto de CloudLink**, introduzca los números según sea necesario.
6) Para cada número, introduzca un nombre en la columna **Nombre para mostrar**.
7) Haga clic en **Aceptar & Siguiente**.
8) Si es necesario, haga clic en **Eliminar** o **Eliminar todo** para eliminar una o todas las entradas, pulse **Aceptar** para confirmar la eliminación.
9) Haga clic en **Aceptar & Siguiente** seguido de **Finalizar**.

24 Accounting

Accounting incluye el registro de datos de conexión y códigos de proyecto, la transmisión y visualización de datos de conexión, el control de gastos y Accounting Tools.

24.1 Datos de conexión

En Datos de conexión se incluye el registro de datos de conexión y códigos de proyecto.

24.1.1 Registro de datos de conexión

El sistema puede protocolizar los datos de conexión de sus líneas en uso.

Se graba un registro de datos de conexión por cada conexión finalizada o por cada conexión entrante. Por cada nuevo segmento de conexión (por ejemplo, resultado de una transferencia o desvío a otro usuario), se graba un registro de datos de conexión. Las conexiones internas no se protocolizan.

El administrador puede activar las siguientes opciones para registrar los datos de conexión:

- Registro activado/desactivado
- Duración de la conexión
- Importes o unidades de tarificación:

  La conversión de unidades de tarificación en importes se realiza con el factor configurable (importe económico por unidad de tarificación).
- Formato decimal

  Divide el importe total entre 100, por ejemplo, para mostrar 6 céntimos con el formato 0,06
- Suprimir las últimas cuatro cifras de los números de teléfono de destino
- Protocolizar conexiones entrantes
- Llamadas salientes sin conexión:

  La extensión recibe, por ejemplo, una prueba de que la extensión de destino no aceptó una llamada (identificada en el protocolo de salida con la hora de llamada 00:00:00). La opción solo es válida para conexiones RDSI y para todos los usuarios.
- Protocolo de conexión

  Iniciar registro al comienzo de la llamada
- Protocolizar MSN
- Emisión del número LCR saliente o del número marcado entrante
  - saliente:

    El número de teléfono enviado al PSTN desde LCR
  - entrante:

    El número de teléfono interno marcado en origen

Si ya hay gastos de conexión antes del establecimiento de conexión (como por ejemplo en Austria) se registran esté activa o no la protocolización de llamadas salientes sin conexión.

El sistema solo toma en cuenta conexiones a través de líneas QSIG si tienen configurado un código de línea.

No se hace protocolización en estos casos:

- interrupción prematura del intento de marcación
- conexiones no autorizadas (LCR, Listas de nos. prohibidos).

Conceptos relacionados

Códigos de proyecto en la página 1236

24.1.1.1 Cómo activar o desactivar el registro de datos de conexión

El asistente **Grabación de detalles de llamada** permite activar el registro de datos de conexión.

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Grabación de detalles de llamada**.
4) Elija una de estas opciones:
   - Si desea activar el registro de datos de conexión, active la casilla de verificación **Activar tarificación**.
   - Si desea desactivar el registro de datos de conexión, desactive la casilla de verificación **Activar tarificación**.
5) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

24.1.1.2 Cómo activar o desactivar el registro de la duración de la conexión

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Formato de salida**.

4) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Protoc. de la duración de llamada act.**.
   - Si desea desactivar la función, desactive la casilla de verificación **Protoc. de la duración de llamada act.**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.1.1.3 Cómo configurar la protocolización de importes o unidades de tarificación

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Formato de salida**.
4) Elija una de estas opciones:
   - Si desea que el sistema registre importes económicos, active la casilla de verificación **Reflejar Importes en vez de unidades**.
   - Si desea que el sistema registre unidades de tarificación, desactive la casilla de verificación **Reflejar Importes en vez de unidades**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.1.1.4 Cómo configurar Factor de tarificación, Moneda y Exactitud del cálculo

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Factores**.
4) Introduzca los valores adecuados para la dirección correspondiente en los campos **Factor** y **RDSI. múltip.**.
5) En el campo **Moneda**, que encontrará en el extremo inferior del formulario, indique el valor adecuado.
6) Por cada dirección correspondiente con el protocolo QSIG, seleccione una de estas opciones de acuerdo con el sistema de comunicación conectado:
   - Si se van a enviar y recibir importes monetarios, active la casilla de verificación **Importe**.
   - Si se van a enviar y recibir unidades de tarifas, desactive la casilla de verificación **Importe**.
7) En todas las líneas con una dirección con protocolo QSIG que envíen y reciban unidades de tarifas, en **Moneda** deje un espacio en blanco.

8) En la lista desplegable **Exactitud del cálculo**, seleccione la entrada **Ningún decimal**, **1 decimal**, **2 decimales**, **3 decimales** o **Mediante impulsos de tasación**.
9) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.1.1.5 Cómo activar o desactivar la protocolización de las cuatro últimas cifras

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Formato de salida**.
4) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Suprimir las últimas 4 cifras**.
   - Si desea desactivar la función, desactive la casilla de verificación **Suprimir las 4 últimas cifras**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.1.1.6 Cómo activar o desactivar la protocolización de llamadas salientes sin conexión

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Formato de salida**.
4) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Saliente sin conex.**.
   - Si desea desactivar la función, desactive la casilla de verificación **Saliente sin conex.**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.1.1.7 Cómo activar o desactivar la protocolización de conexiones entrantes

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Formato de salida**.
4) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Protocolizar llamadas entrantes**.
   - Si desea desactivar la función, desactive la casilla de verificación **Protocolizar llamadas entrantes**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.1.1.8 Cómo activar o desactivar el protocolo de conexión

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Formato de salida**.
4) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Protocolo de llamada act.**.
   - Si desea desactivar la función, desactive la casilla de verificación **Protocolo de llamada act.**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.1.1.9 Cómo activar o desactivar la protocolización de los MSN

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Formato de salida**.
4) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Salida de los MSN act.**.
   - Si desea desactivar la función, desactive la casilla de verificación **Salida de los MSN act.**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.1.1.10 Cómo activar o desactivar el formato decimal

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Formato de salida**.
4) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Formato decimal**.
   - Si desea desactivar la función, desactive la casilla de verificación **Formato decimal**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.1.2 Códigos de proyecto

Los códigos de proyecto (PRO) permiten asignar datos y gastos de conexión en función de proyecto. Para ello, el sistema protocoliza en los registros de datos de conexión correspondientes los códigos de proyecto que introducen las extensiones en el teléfono.

La prestación PRO se utiliza en combinación con el registro de datos de llamada y está a disposición de todas las extensiones.

Los usuarios pueden introducir un código de proyecto (PRO) en el teléfono antes de marcar o al finalizar la marcación. No se puede realizar la marcación desde un cliente que tenga un código de proyecto activado.

Un código de proyecto introducido durante una conferencia con extensiones externas se asigna a todas las líneas y conexiones implicadas.

El administrador puede configurar si se puede guardar un código de proyecto para la rellamada.

El listín telefónico personal puede guardar en un registro el código para la prestación PRO + un PRO + un número de teléfono de forma conjunta.

Procedimiento de entrada PRO

El administrador establece el procedimiento de entrada PRO en el plan de marcación LCR.

- Obligatorio

  El PRO debe introducirse antes del comienzo de la conexión (antes o después de la ocupación de una ruta).
- Opcional

  El PRO se puede introducir de forma opcional antes del comienzo de la conexión. En los clientes de terminales IP, también se puede hacer la entrada durante una conexión, incluidas las llamadas entrantes.

Procedimiento de prueba PRO

El sistema puede comprobar la validez de un código de proyecto de estas formas:

- Prueba de listas

  Solo son válidos PRO predefinidos. Después de introducir un código de proyecto válido, el usuario puede seguir marcando inmediatamente. El sistema asigna un código de proyecto no válido. En el display aparece "Entrada errónea" y suena un tono de confirmación negativo.
- Prueba de cantidad de posiciones

  Son válidos todos los códigos de proyecto posibles, teóricamente, con la cantidad de dígitos configurada. Después de introducir un código de proyecto válido, el usuario puede seguir marcando inmediatamente.
- Ninguna prueba

  No se comprueba la validez del PRO. El usuario debe separar los códigos de proyecto de menos de 11 posiciones de los demás dígitos marcados marcando "#". En los terminales RDSI, esta variante requiere siempre códigos de proyecto de 11 dígitos, de lo contrario no se realiza la marcación.

Si durante una conexión, la extensión averigua que el PRO asignado a una conexión no es correcto, puede introducir uno nuevo. El sistema sobrescribe el PRO actualmente ajustado. El registro de datos de conexión genera un registro de datos de conexión después de cada segmento. Por tanto, los segmentos de conexión finalizados con anterioridad se marcan con el PRO antiguo.

Conceptos relacionados

Registro de datos de conexión en la página 1231

24.1.2.1 Cómo configurar un código de proyecto

El asistente **Grabación de detalles de llamada** permite configurar códigos de proyecto.

Requisitos previos

Se ha registrado en la Gestión basada en Web (WBM).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Grabación de detalles de llamada**.
4) En los campos de entrada de la sección **Códigos de proyecto** indique los códigos de proyecto en la forma descrita en el asistente.
5) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

24.1.2.2 Cómo configurar un procedimiento de prueba de código de proyecto (PRO)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Códigos de proyecto**.
4) En la línea de la lista de códigos de proyecto correspondiente, y en la lista desplegable **Procedimiento de prueba**, seleccione la entrada deseada: **Ninguna prueba**, **Prueba de listas** o **Prueba de cant. posiciones**.
   a) En la lista desplegable **Cantidad de posiciones que deben ser comprobadas** seleccione el valor deseado.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.1.2.3 Cómo activar o desactivar la rellamada con PRO

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **Flags del sistema**.
4) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Rellamada con PRO**.
   - Si desea desactivar la función, desactive la casilla de verificación **Rellamada con PRO**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.2 Indicación y transferencia de datos de conexión

La indicación y transferencia de datos de conexión incluye distintas opciones para la indicación en el display de los teléfonos del sistema y para la transferencia de archivos.

24.2.1 Transmisión de importes (no para los EE. UU.)

El sistema puede mostrar en el display del teléfono el importe transmitido por el proveedor de red para la conexión externa en curso.

El proveedor de red debe admitir la transmisión de importes con la prestación Indicación de tasas (AOC-D o AOC-S). El sistema suma los importes de las unidades de tarifa correspondientes.

El importe puede transmitirse en estos momentos:

- al comienzo de la conexión y, en su caso, durante la conexión (AOC-S)
- durante la comunicación (AOC-D)

Con el parámetro Exactitud del cálculo, el administrador puede evitar inexactitudes en el registro de los datos de comunicación. La Exactitud del cálculo determina

- el número de decimales para la evaluación de los datos de comunicación (importe mínimo)
- el total máximo de los importes acumulados.

La Exactitud del cálculo configurada debe corresponderse al menos con la del RDSI. Si los tres decimales posibles máximos no son suficientes, se redondea automáticamente. Exactitud del cálculo puede aceptar los siguientes valores:

Exactitud del cálculo	importe mínimo	importe máximo
sin decimales	1	unos 4.300 millones
1 decimal	0,1	unos 430 millones
2 decimales (p. ej. para euros)	0,01	unos 43 millones
3 decimales (por ejemplo, libras esterlinas)	0,001	unos 4,3 millones

24.2.1.1 Cómo configurar la transmisión de importes

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Factores**.
4) Por cada ruta deseada, en la lista desplegable **Información de tasación**, seleccione la entrada **Ínterin**, **Final**, **Ínterin/final** o **Sin cargo**.
5) En la lista desplegable **Exactitud del cálculo**, que encontrará en el extremo inferior del formulario, seleccione el número de decimales a tomar en cuenta.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.2.2 Indicación de los gastos de conexión en el teléfono

El sistema puede mostrar información sobre los gastos de una conexión externa en curso en el display del teléfono, como importe.

El sistema suma los importes de las unidades de tarifa correspondientes. El importe se calcula a partir de las unidades de tarifa y del factor de tarifa configurado. El proveedor de servicios debe admitir la prestación Advice Of Charge (AOC).

La información sobre los gastos de conexión se puede transmitir en estos momentos:

- Al comienzo de la conexión y, en su caso, durante la conexión (AOC-S)
- Ínterin (AOC-D)
- Al final de la comunicación (AOC-E)

Al final de la comunicación, el display muestra las tasas definitivas de la conexión durante unos 5 segundos, siempre que el usuario no haya iniciado otra acción.

Al alternar siempre se muestran los gastos de conexión de la conexión actual.

Si la Transferencia ciega no se realiza correctamente, se muestra y calcula el importe total.

Las extensiones a las que se transfiere una conexión solo pueden ver y solo se les cargan los gastos de conexión que se produzcan a partir del momento de la transferencia.

24.2.3 Indicación de la duración de la conexión en el teléfono

El sistema puede mostrar la duración de las conexiones entrantes y salientes externas en el display del teléfono.

El formato es HH:MM:SS.

Si la indicación de la duración de la conexión está desactiva, el display del teléfono muestra en su lugar información sobre los costes de conexión del PSTN. Si no hay disponible información sobre los costes de conexión, el display muestra el número de teléfono del interlocutor, siempre que se identifique.

24.2.3.1 Cómo activar o desactivar la muestra la duración de la conexión

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **Display**.
4) Elija una de estas opciones:
   - Si desea activar la función, active la casilla de verificación **Indicación duración de llamada**.
   - Si desea desactivar la función, desactive la casilla de verificación **Indicación duración de llamada**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.2.4 Transmisión de datos de conexión

El sistema puede transmitir datos de conexión en un archivo por HTTPS.

Puede evaluar el archivo transmitido con un programa adecuado.

Solo se pueden emitir datos de conexión de forma permanente por CSTA.

El administrador puede seleccionar los siguientes formatos (ASCII de 8 bits) para los datos de conexión:

- Formato comprimido
- Formato sin compresión

Formato comprimido, estándar

Un conjunto de datos de conexión en formato comprimido incluye los siguientes campos separados por |, donde CRLF está siempre al final de cada conjunto:

Posición de campo	Duración	Descripción
1	8	Fecha al final de la conexión
2	8	Hora al final de la conexión
3	3	Número de línea urbana asignado
4	16	Número de extensión interno
5	8	Duración de timbre de la conexión entrante
6	8	Duración de la conexión
7	máx. 25	Número de teléfono externo marcado o recibido
8	11	Unidad de tarificación/Importe
9	2	Información adicional (p. ej., entrante, saliente, conexión transferida, conferencia, DISA, costes de establecimiento de conexión)
10	Máx. 11	Cód. proyecto
11	Máx. 11	Solo con acceso individual: MSN utilizado
12	6	LCR de código de acceso, código urbano
13	2	Ruta LCR utilizada, regla de marcación
14	25	Número de teléfono marcado o recibido (opcional)

Ejemplos de conjuntos de datos de conexión:

- Conexión saliente:

```
13.02.13|14:18:02|201|33388|00:02|00:00:07|0123456789||
1||||||
```

- Conexión entrante:

```
13.02.13|14:28:02|202|33388|00:05|00:00:12|0123456789||
1|||||
```

Formato comprimido, solo EE. UU.

Un conjunto de datos de conexión en formato comprimido incluye los siguientes campos separados por |, donde CRLF está siempre al final de cada conjunto:

Posición de campo	Duración	Descripción
1	8	Fecha al final de la conexión
2	8	Hora al final de la conexión
3	3	Número de línea urbana asignado
4	16	Número de extensión interno
5	8	Duración de timbre de la conexión entrante
6	8	Duración de la conexión
7	máx. 25	Número de teléfono externo marcado o recibido
8	11	Unidad de tarificación/Importe
9	2	Información adicional (p. ej., entrante, saliente, conexión transferida, conferencia, DISA, costes de establecimiento de conexión)
10	Máx. 11	Cód. proyecto
11	Máx. 11	Solo con acceso individual: MSN utilizado
12	6	LCR de código de acceso, código urbano
13	2	Ruta LCR utilizada, regla de marcación
14	2	Servicio de nodo PRI
15	1	PRI WATS band
16	3	PRI CIC
17	25	Número de teléfono marcado o recibido (opcional)

Nota: En las claves de registro *HKEY_LOCAL_MACHINE \SOFTWARE* de *Accounting Tool*, el valor de **DateFormat DWORD** debe definirse en 1 para el formato de fechas norteamericano (MM.DD.AA). El valor predeterminado es 0 y se corresponde con el formato de fechas de Europa/Latinoamérica (DD.MM.AA).

Nota: Los datos del registro de Accounting Manager en formato comprimido están separados por el delimitador |. Solo se puede configurar con Manager E.

Formato sin compresión

El formato sin compresión es apto para impresos. Además se emite un encabezado y un margen de página. Un conjunto de datos de conexión en formato comprimido incluye los siguientes campos separados por |:

Posición de campo	Posición de carácter, extensión	Descripción
1	1-8 (8)	Fecha al final de la conexión: DD.MM.AA (DD = día: rango de valores 01… 31, MM = mes: rango de valores 01… 12, YY = año: rango de valores 00… 99)
2	9-16 (8)	Hora al final de la sección de llamada o de una llamada entrante no respondida: hh:mm:ss (hh = horas: rango de valores 00… 23, mm = minutos: rango de valores 00… 59, ss = segundos: rango de valores 00… 59)
3	17-19 (3)	Línea: número de línea Rango de valores: 1… 250
4	20-35 (16)	Extensión: Número de extensión interno En el caso de las llamadas sin responder, siempre se emite la última extensión llamada (por ejemplo, línea colectiva, desvío de llamadas, transferencia automática diferida). En el caso de una llamada de grupo, se emite la última extensión registrada. En el caso de las llamadas con consulta, se indica la extensión. No se emiten los prefijos RNR programados (solo con interconexión). Si se ha traducido la numeración interna a un plan de numeración de 7 cifras como máximo, se emite el número de teléfono sin traducción. Al número de llamada interno de extensión se le puede anteponer un número de llamada de nodo de 7 cifras como máximo. Si la suma del número de nodo y del número de extensión es superior a siete cifras, solo se emiten las últimas siete cifras del número.
5	36-40 (5)	Duración de una conexión entrante: mm:ss (mm = minutos: rango de valores 00 ... 59; ss = segundos: rango de valores 00 ... 59) La indicación se realiza con todas las llamadas entrantes, siempre que en el sistema esté configurada la emisión de la duración de la llamada. En caso de desbordamiento del contador (duración > 59:59), se emite "59:59". Puede suceder, por ejemplo, en un cambio de fecha u hora durante el funcionamiento del sistema. En caso de llamada entrante en una extensión ocupada, la duración de la llamada tiene el valor “00:00".
6	41-48 (8)	Duración de la conexión o de la sección de llamada: hh:mm:ss (hh = horas: rango de valores 00… 23, mm = minutos: rango de valores 00… 59, ss = segundos: rango de valores 00… 59) Si en caso de una llamada entrante no se ha establecido conexión, se emiten 8 valores en blanco. En caso de desbordamiento del contador (duración > 23:59:59), se emite “23:59:59".

Posición de campo	Posición de carácter, extensión	Descripción
7	49-73 (25)	Número de teléfono marcado o, si está disponible, número de teléfono externo recibido: nnnnnnnnnnnnnnnnnnnnnnnnn (n = carácter marcado o recibido: rango de valores 0… 9, *, #, ?) La salida se ejecuta con llamadas entrantes y salientes, siempre que existan. En el caso de las llamadas salientes, se muestra el número de teléfono marcado o, si está disponible, el número de teléfono transmitido mediante COLP. Si la función de protección de datos está activada, los últimos cuatro caracteres mercados se sustituyen con "????" Si no hay disponible información sobre el número de teléfono, se emiten 25 espacios en blanco.
8	74-84 (11)	Unidades de tarificación para una sección de llamada: ddddddddddd (d = dígito: rango de valores 0… 9) Se puede elegir entre unidades de tarificación o importes. El importe de las unidades de tarificación en importes se calcula a partir del factor de tarificación definido como importe económico (con un suplemento necesario) por unidad de tarificación. Para configurar el factor de tarificación: • con exactitud del cálculo: factor de tarificación = 100% + suplemento correspondiente, si es el caso • sin cálculo exacto: factor de tarificación =importe/unidad + suplemento que pueda requerirse En función de la exactitud del cálculo, los costes de conexión se registran con o sin suplemento: La emisión se realiza siempre que se aplican costes de conexión a la sección de la llamada (por ejemplo, también con llamadas transferidas).

Posición de campo	Posición de carácter, extensión	Descripción
9	85-86 (2)	Elemento de información: información adicional Rango de valores 0 ... 9 Significado: • 1 = conexión entrante (Voice / 3.1 kHz Audio Call) • 2 = conexión saliente (Voice / 3.1 kHz Audio Call) • 3 = conexión entrante (otros servicios) • 4 = conexión saliente (otros servicios) • 5 = conexión entrante transferida • 6 = conexión saliente transferida • 7 = conferencia int/ext/ext con conexión entrante / Tránsito por transferencia externa • 8 = conferencia con conexión saliente / Tránsito por transferencia externa • 9 = conexión saliente mediante desvío de llamada a destino externo • 0 = información de conexión (lista de llamadas), se emite en cuanto se recibe una llamada entrante (la emisión se puede cancelar). Esto puede usar, por ejemplo para una búsqueda en la base de datos desde un PC. Si hay varias extensiones llamadas, por cada una de ellas se emite una línea (sin duración de llamada, duración de la comunicación ni información de tasas). • +10 = Desfase como identificación para llamadas en la lista negra • +20 = Desfase como indicador para los gastos del establecimiento de conexión (sin duración de la conexión) • +30 = Desfase como indicador para un registro de datos de seguimiento con – Duración de la conexión > 24 h. – secciones de llamada relacionadas con el mismo número de extensión/línea (por ejemplo, tras transferir una llamada, tras cancelar una conferencia). • +40 = desfase para un registro de datos con identificación de tránsito (por una extensión del sistema secundario). Puede darse en combinación con desfase +30. • +50 = desfase como indicador para Conexiones DISA • +70 = combinación de los desfases +30 y +40
10	87-97 (11)	Código de proyecto indicado por el usuario para esta conexión: pppppppppp (p = dígito del código de proyecto: rango de valores 0… 9) Las cifras faltantes se sustituyen por espacios en blanco.

Posición de campo	Posición de carácter, extensión	Descripción
11	98-108 (11)	MSN utilizado: mmmmmmmmmmm (m = dígito del MSN: rango de valores 0… 9) La indicación se realiza siempre que el usuario haya programado una tecla MSN. En las llamadas salientes de una extensión MULAP se emite el número de llamada de la extensión MULAP ocupada. Las cifras faltantes se sustituyen por espacios en blanco.
12	109-113 (5)	Código de asignación utilizado, Access Code: bbbbb (s = dígito del código de ruta: rango de valores 0… 9)
13	114-115 (2)	Ruta LCR utilizada: rr (r = dígito de la ruta seleccionada: rango de valores 0… 9)

Proceso de comunicación

Se puede solicitar la transferencia de datos de comunicación (Download Request), y el sistema emite una respuesta (Download Response).

A continuación se puede solicitar el borrado de los datos de conexión (Delete Request), y el sistema emite una respuesta (Download Response).

Download Request - Definition

Elemento	Contenido
HTTP header	Request method = GET
URL	https://<Dirección IP del sistema>/management/portlet
Parámetros	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=get
	username=<nombre de usuario>
	password=<contraseña>

Nota: Al consultar datos de tarifas con la interfaz de referencia, se aplican restricciones de solicitud HTTP GET. Los siguientes caracteres especiales no se pueden usar como palabras de paso al intentar obtener datos a través de una solicitud de URL:

:/?#[]@ !$&'()*+,;=

Ejemplo:

```
https://192.148.108.151/management/portlet/?portlet=
hipath-
accountingdownload::HiPathAccountingDownloadPortlet&
entity=accounting&action=get&username=xbert@system&
password=not4u;-)
```

Download Response - Definition

Elemento	Contenido
HTTP header	ContentType = "text / plain"
Parámetros	attachment filename = "<charging file>"
	data=<contenido del archivo de carga>

Response-Code	Significado
SC_OK(200)	Hecho
SC_BAD_REQUEST(400)	Parámetro incorrecto solicitado
SC_UNAUTHORIZED(401)	Inicio de sesión fallido o nombre de usuario/contraseña incorrectos
SC_INTERNAL_SERVER_ERROR(500)	Error interno

Delete Request - Definition

Elemento	Contenido
HTTP header	Request method = POST
URL	https://<Dirección IP del sistema>/management/portlet
Parámetros	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=delete
	username=<nombre de usuario>
	password=<contraseña>

Ejemplo:

```
https://192.148.108.151/management/portlet/?portlet=
hipath-
accountingdownload::HiPathAccountingDownloadPortlet&
entity=accounting&action=get&username=xbert@system&
password=not4u;-)
```

Delete Response - Definition

Response-Code	Significado
SC_OK(200)	Hecho
SC_BAD_REQUEST(400)	Parámetro incorrecto solicitado

Response-Code	Significado
SC_UNAUTHORIZED(401)	Inicio de sesión fallido o nombre de usuario/contraseña incorrectos
SC_INTERNAL_SERVER_ERROR(500)	Error interno

Conceptos relacionados

Accounting-Tools en la página 1250

24.2.4.1 Cómo seleccionar el formato

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Formato de salida**.
4) Elija una de estas opciones:
   - Si desea utilizar el formato comprimido, active la casilla de verificación **Formato de salida comprimido**.
   - Si desea utilizar el formato sin compresión, desactive la casilla de verificación **Formato de salida comprimido**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.2.4.2 Cómo activar o desactivar la transferencia de datos de conexión por HTTPS

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Tasas de llamada** > **Tasas de llamada - Formato de salida**.
4) En la lista desplegable **Salida**, seleccione una de estas opciones:
   - Si desea activar la prestación, seleccione la entrada **HTTPS**.
   - Si desea desactivar la prestación, seleccione la entrada **Ninguno**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.3 Control de gastos

El control de gastos incluye las prestaciones Aviso de rutas de enlace caras y Protección contra el abuso de tasas.

24.3.1 Aviso de rutas de enlace caras

Si no se puede acceder a un destino de llamada a través de la ruta de enlace más económica, el teléfono puede enviar un aviso de ruta de enlace cara a la extensión.

Así la extensión podrá decidir si continuar con la llamada a pesar del precio de la ruta en ese momento. El aviso se puede realizar de distintas formas:

- Texto en el display
- Tono
- Texto en el display y tono

Si en la tabla de rutas hay configurada una advertencia pertinente, y no se utiliza la ruta del Índice 1 de la tabla de rutas, el sistema advertirá de que se trata de una ruta de enlace poco económica.

El aviso en el display solo aparece si no hay configurado ningún nombre para la regla de marcación correspondiente. Si hay un nombre configurado aparecerá éste.

24.3.1.1 Cómo configurar una advertencia para rutas de enlace poco económicas

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **LCR**.
3) En el grupo de menús, haga clic en **Encaminamiento** > **LCR** > **Tabla de rutas** y en la tabla de rutas correspondiente.
4) Por cada ruta de enlace poco económica (columna **Ruta**), en la lista desplegable **Advertencia** seleccione la entrada deseada: **Tono**, **Display** o **Display + Tono**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.3.2 Protección ante abuso en las tarifas

El sistema puede supervisar conexiones para identificar posibles abusos de tasas (Toll Fraud Monitoring). Esto afecta a conexiones recibidas a través de una línea urbana o que salen a través de una línea urbana.

La primera extensión señaliza que se ha superado la duración de conexión configurada. Esto permite interrumpir la conexión si es necesario. En calidad de administrador puede configurar si se hará esta señalización y cuál será la duración de la conexión en su caso.

24.3.2.1 Cómo activar o desactivar la protección contra el abuso de tasas

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **Parámetros de tiempo**.
4) Elija una de estas opciones:
   - Si desea activar la protección contra el fraude en las tasas, en **Temporizador para Toll Fraud Monitoring** de la lista desplegable **Base**, seleccione la entrada deseada. En el campo **Factor** indique un valor que no sea 255. **Base** * **Factor** da como resultado el tiempo de conexión tras el cual se señalizará una conexión potencialmente fraudulenta.
   - Si desea desactivar la protección contra el fraude en las tasas, para **Temporizador para Toll Fraud Monitoring**, y en el campo **Factor**, indique 255.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

24.4 Accounting-Tools

Accounting Tools incluye Accounting Manager y Teledata Office.

Conceptos relacionados

Centro de servicios – Documentos en la página 130
Transmisión de datos de conexión en la página 1240

24.4.1 Accounting Manager

Accounting Manager es una aplicación Windows que permite consultar los datos de conexión a través de HTTPS. También permite evaluar dichos datos mediante tablas y gráficos.

Accounting Manager incluye documentación propia. Accounting Manager consulta los datos de conexión de los distintos nodos de red. También puede utilizar el Accounting Manager para probar la interfaz de datos de conexión. Puede descargar Accounting Manager en el **Centro de servicios** de la Gestión basada en Web (WBM). Accounting Manager requiere derechos de administración locales y la activación de TLS 1.2 en Microsoft Internet Explorer.

24.4.2 Teledata Office

Teledata Office es una aplicación de Windows para evaluar datos de conexión.

25 Mantenimiento

El sistema ofrece numerosas opciones de mantenimiento. Entre ellas, modificar los ajustes de telefonía, guardar y recuperar datos de configuración, actualización de software mediante update y upgrade y funciones de reinicio y recarga. Además, hay disponibles funciones para la determinación de estado, la supervisión y el mantenimiento. Distintos servicios remotos permiten acceder de forma remota al sistema.

Mantenimiento del UC Booster Server

Si además del sistema de comunicación se opera un UC Booster Server, este también ofrece algunas opciones de mantenimiento. Para mantener el UC Booster Server, al lanzar la Gestión basada en Web (WBM) el administrador no introduce la dirección IP del sistema de comunicación sino la del servidor Linux.

25.1 Configuración de telefonía

El sistema de comunicación ofrece distintas opciones de configuración para telefonía, por ejemplo: Fecha y hora, SNTP, Indicación en display personalizada y Música en espera.

25.1.1 Fecha y hora

El sistema de comunicación incluye un reloj del sistema con fecha y hora. myPortal for Desktop y todos los displays de un terminal muestran esta hora del sistema.

Puede definir o sincronizar la hora de sistema de esta forma:

- A través de un servidor temporal, con SNTP
- A través de una línea urbana RDSI, con una llamada saliente
- Configurándolo de forma manual

Después de activar un servidor SNTP, ya no se puede configurar de forma específica para el sistema la hora de sistema.

Si en un momento dado no se pudiera acceder a un servidor SNTP y los teléfonos el sistema HFA utilizan como origen para la hora otra fuente que no sea el sistema, la hora mostrada ahí puede ser distinta a la hora del sistema.

Una hora de sistema configurada de forma manual tras la inicialización del sistema, siempre se sobrescribe con la información horaria RDSI tras la primera comunicación RDSI saliente, siempre que el proveedor de red transmita la información. Si estando el sistema en funcionamiento, la diferencia entre la hora de sistema configurada manualmente y la información RDSI es de entre 2 y 70 minutos, se adopta la información horaria RDSI. De lo contrario, se mantiene la hora de sistema configurada de forma manual.

El administrador puede seleccionar uno de los siguientes formatos para la representación de la fecha en el display del teléfono. Además, el formato depende del tipo de teléfono:

Formato de fecha	OpenStage	OptiPoint 410, OptiPoint 420
Europa	Ma 20.11.07	20. NOV 07
EE. UU.	Ma 11/20/07	Ma NOV 20.07
International1	Ma 20.11.07	MA 20 NOV 07
International2	Ma 20.11.07	MA 20.11.07

Si en calidad de administrador establece por descuido una fecha anterior a 2007, no podrá seguir accediendo a la Gestión basada en Web (WBM). Solo podrá volver a hacerlo después de una operación de reinicio, con la que la fecha se restablezca al 01/01/2007.

25.1.1.1 Cómo configurar la fecha y hora manualmente

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Siga estos pasos si el sistema no consulta la fecha y la hora ni a través de líneas urbanas digitales ni mediante SNTP.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el área de navegación, haga clic en **Servidor de telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Fecha y hora** > **Fecha y hora**.
4) Indique la **Fecha y hora**.
5) Haga clic en **Aplicar**.
6) Haga clic en **Finalizar sesión**.
7) Finalice su sesión en la Gestión basada en Web (WBM) y vuelva a registrarse.

25.1.1.2 Cómo configurar la zona horaria

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el área de navegación, haga clic en **Servidor de telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Fecha y hora** > **Ajustes zona horaria**.
4) En la lista desplegable **Zona horaria**, seleccione la zona horaria.
5) Haga clic en **Aplicar**.

6) Finalice su sesión en la Gestión basada en Web (WBM) y vuelva a registrarse.

25.1.1.3 Cómo configurar el formato de fecha

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el área de navegación, haga clic en **Servidor de telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **Display**.
4) En la lista desplegable **Formato de fecha** seleccione el formato de fecha.
5) Haga clic en **Aplicar**.

25.1.2 SNTP

Mediante SNTP puede sincronizar la fecha y la hora de sus sistemas a nivel de red con los servidores horarios NTP.

SNTP (Simple Network Time Protocol) es una versión simplificada de NTP (Network Time Protocol), un estándar para sincronizar fecha y hora a través de redes de comunicación basadas en paquetes. Para sincronizar fecha y hora, el sistema necesita conectarse a un servidor NTP. Este servidor puede estar en su red local o en Internet. En Internet hay servidores NTP de acceso gratuito. Puede elegir uno localizado en su zona horaria. Cumpla con las condiciones de uso del correspondiente servidor y pida permiso para utilizarlo, si es necesario.

25.1.2.1 Cómo obtener la fecha y hora de un servidor SNTP

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Fecha y hora** > **Ajustes SNTP**.
4) Introduzca la **Dirección IP / Nombre DNS del servidor temp. externo**, por ejemplo, `0.de.pool.ntp.org`.
5) En la lista desplegable **Estado administrativo servicio del servidor SNTP**, seleccione la entrada **Activado**.
6) En la lista desplegable **Tiempo de interrogación para servidor de hora externo** seleccione el periodo deseado para asociar la fecha y la hora del servidor SNTP.
7) Haga clic en **Aplicar**.

8) Finalice su sesión en la Gestión basada en Web (WBM) y vuelva a registrarse.

25.1.3 Logotipos telefónicos

Los teléfonos de sistema con display pueden mostrar un logotipo personalizado como imagen de fondo de la interfaz telefónica.

En calidad de administrador puede importar, asignar o borrar del sistema logotipos telefónicos para teléfonos de sistema con display. Distintos tipos de teléfonos de sistema pueden utilizar distintos logotipos telefónicos.

Conceptos relacionados

Actualización de los teléfonos de sistema en la página 1283

25.1.3.1 Cómo cargar un logotipo telefónico en el sistema

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

El archivo de imagen con el logotipo telefónico cumple estos requisitos::

Teléfono	Formato	Color
OpenStage 40	112 x 32, BMP	monocromo
OpenStage 60 OpenStage 80	240 x 71, JPEG	monocromo o a color
OpenScape Desk Phone CP 400 OpenScape Desk Phone CP 400T/405T	112 x 32, BMP	monocromo
OpenScape Desk Phone CP 600/700/700X OpenScape Desk Phone CP 710	220 x 70, PNG	24 bits con alfa (transparencia)
OpenScape Desk Phone CP 600E	220 x 70, PNG	24 bits con alfa (transparencia) o 256 en escala de grises con alfa

Puede acceder al archivo de imagen con el logotipo telefónico en el sistema de archivos del PC de administración.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) Haga clic en **Mantenimiento** > **Imagen de software** en el árbol de navegación.
3) En el grupo de menús, haga clic en **Logotipos de imagen de teléfono** > **Cargar**.
4) Haga clic en **Examinar** para seleccionar un archivo de imagen apropiado.

5) Haga clic en **Cargar**.

25.1.3.2 Cómo distribuir un logotipo telefónico a teléfonos del sistema

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Imagen de software**.
3) En el grupo de menús, haga clic en **Logotipos de imagen de teléfono** > **Distribuir**.
4) Seleccione la casilla de verificación **Distribuir** en la línea del logotipo de teléfono que desee distribuir.
5) Seleccione el tipo de teléfono del sistema deseado en la lista desplegable **Distribuir en los workpoints con el tipo de dispositivo seleccionado**.
6) Haga clic en **Aplicar**.

25.1.3.3 Cómo borrar un logotipo telefónico

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Puede acceder al archivo de imagen con el logotipo telefónico en el sistema de archivos del PC de administración.

Para borrar un logotipo telefónico del sistema de comunicación, siga estos pasos:

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Imagen de software**.
3) En el grupo de menús, haga clic en **Logotipos de imagen de teléfono** > **Cargar**.
4) En la línea del logotipo telefónico que desea borrar, marque la casilla de verificación **Borrar**.
5) Si desea borrar más logotipos telefónicos, repita el paso anterior
6) Haga clic en **Borrar**. Se eliminan del sistema de comunicación todos los logotipos telefónicos marcados.

25.1.4 Indicación en display personalizada

Indicación en display personalizada permite, por ejemplo, mostrar el nombre de empresa en el display de los teléfonos del sistema en reposo.

Solo se puede modificar la parte derecha (máx. 18 caracteres) de la segunda línea de la pantalla, donde aparece de forma predeterminada "OpenScape". El texto se alinea a la izquierda de la fecha, siempre que lo permita su extensión:

```
16:30       VI 29.FEB 08         123456  Hotel de Correos >
```

25.1.4.1 Cómo modificar la indicación en display específica de cliente (Nombre del sistema)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Gateway**.
4) En el campo **Nombre del sistema** introduzca el nombre a mostrar.

Nota: No utilice otros caracteres que A-Z, a-z y 0-9.

---

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.1.5 Salida de texto multilingüe

El idioma de los mensajes de display puede seleccionarse para todo el sistema o también de forma individual para cada extensión.

Idiomas disponibles: alemán, alemán (Telekom), búlgaro, catalán, checo, chino, danés, eslovaco, esloveno, español, estonio, finés, francés, griego, holandés, húngaro, inglés (EE. UU.), inglés, italiano, letón, lituano, macedonio, noruego, polaco, portugués, rumano, ruso, serbio, serbo-croata, sueco y turco.

El ajuste del idioma básico se ejecuta al inicializar el sistema mediante la inicialización del país.

Conceptos relacionados

Configuración de las extensiones en la página 458

Tareas relacionadas

Cómo configurar extensiones IP y SIP en la página 202

25.1.6 Menús flexibles

Los menús flexibles permiten adaptar, de forma individualizada, las opciones de menú del display de los teléfonos de sistema.

En calidad de administrador puede ocultar o mostrar las distintas opciones de menú.

25.1.6.1 Cómo cambiar el menú flexible

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el grupo de menús, haga clic en **Ajustes básicos** > **Sistema** > **Menús flexibles**.
4) Para editar la **Lista de prestaciones ocultas** siga este procedimiento:
   - Para ocultar una opción de menú, active su casilla de verificación.
   - Para mostrar una opción de menú, desactive su casilla de verificación.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.1.7 Música en espera

El sistema de comunicación puede reproducir música en espera (Music on Hold, MOH) a los usuarios en espera durante los procedimientos de conmutación. Los llamantes escuchan la música en espera mientras son retenidos, aparcados o transferidos. También se hace con los llamantes que se encuentran en la cola de espera de la distribución de llamadas.

El sistema puede reproducir música en espera de estas fuentes:

- Música en espera
- EXMR

  Consulte Instalación de OpenScape Business X1/X1W, Documentación de servicio o Instalación de OpenScape Business X3/X5/X8, Documentación de servicio.
- Módulo insertable MUSIC

  Consulte Instalación de OpenScape Business X1/X1W, Documentación de servicio o Instalación de OpenScape Business X3/X5/X8, Documentación de servicio.
- Módulo MPPI-USB EXM (solo para OpenScape Business X3/X5)

  Véase Instalación de OpenScape Business X3/X5/X8, Documentación de servicio.

Archivos de sonido

El administrador puede transmitir archivos de sonido para la música en espera interna desde el PC al sistema de comunicación para utilizarlos como música en espera interna alternativa.

Nota: Antes de utilizar anuncios grabados o música de otra fuente, asegúrese de que el material no está protegido por derechos de copyright.

Importante: Si la extensión en espera es un cliente workpoint IP o una línea urbana IP, se utiliza la música en espera interna. La música en espera externa no es para su uso con IP.

Los archivos de sonido deben tener el formato `Wave` y las siguientes propiedades:

- 16 bits PCM
- Monoaural o estéreo
- Tasas de muestreo posibles: 8 / 22,05/ 24 / 32 / 40 / 44,1 o 48 kHz.
- El nombre de archivo de sonido puede tener, como máximo: 30 caracteres

Valores recomendados: **16 bits PCM - Mono - 8 kHz, 2 min. de duración aprox.**

Música en espera

Para el servicio nocturno y diurno se puede configurar diferente música en espera.

Nota: Para UC Suite, no se distingue entre archivos diurnos y nocturnos. Se utiliza **Archivo de música en espera - Noche**.

El administrador puede configurar las siguientes funciones:

- Música en espera con tono de llamada (tono de libre):

  El usuario retenido escucha la música en espera durante el proceso de consulta. Después de transferir al usuario retenido al destino, en lugar de la música en espera se reproduce el tono de llamada.
- Música en espera sin tono de llamada (tono de libre):

  El usuario retenido oye la música en espera hasta que el usuario llamado contesta la llamada.
- Sin música en espera:

  El usuario retenido no escucha nada (silencio). Si una llamada externa se transfiere a través de transferencia antes de contestar, el llamante escucha el tono de libre.

25.1.7.1 Cómo importar la música en espera interna

El asistente **Música en espera/Anuncios grabados** permite importar archivos de sonido al sistema de comunicación como música en espera interna.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM).

Los archivos de sonido para reproducir son archivos WAVE con el formato necesario.

Nota: Antes de usar este material, asegúrese de que no esté protegido por copyright.

Nota: Para UC Suite no se distingue entre archivos diurnos y nocturnos. Se utiliza el modo **Archivo de MoH diurna**.

Paso a paso

1) En la barra navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente **Música en espera / Anuncios grabados**.
4) Para el servicio diurno en **Archivo de MoH diurna** o para el servicio nocturno en **Archivo de MoH nocturna**, haga clic en **Examinar**.
5) Seleccione un archivo de sonido y haga clic en **Abrir**. La ruta del archivo de sonido seleccionado se muestra en **Archivo de MoH diurna** o en **Archivo de MoH nocturna**.
6) Haga clic en **Cargar**.
7) Para confirmar el mensaje, haga clic en **Aceptar** y, a continuación, en **OK y Continuar**.
8) Haga clic en **Salir**.

25.1.7.2 Cómo configurar la función de música en espera interna

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

El nombre de archivo de música en espera puede tener, como máximo, 30 caracteres.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Conexión**.
3) En el grupo de menús, haga clic en **Conexiones** > **Anuncios grabados / Música en espera**.
4) En la sección **Música en espera**, vaya a la lista desplegable **Tipo de MOH** y seleccione la entrada **Sin música en espera**, **Música esp. sin tono ll.** o **Música esp. con tono ll.**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.1.7.3 Cómo modificar la música en espera interna para cada grupo de relaciones de tráfico

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Servidor de telefonía > Conexiones**.
3) En el grupo de menús, haga clic en **Conexiones > Anuncios grabados / Música en espera**.
4) Haga clic en la pestaña **Modificar música en espera**.

5) En la línea del grupo de relaciones de tráfico correspondiente de la lista desplegable Archivo de sonido, seleccione la música en espera deseada.
6) Si un grupo no tiene asignada ninguna música en espera, se utiliza la música en espera interna.
7) En la línea del grupo de relaciones de tráfico correspondiente, introduzca una Descripción.
8) Haga clic en **Aplicar**.
9) Haga clic en **Aceptar**.

Nota: Esta función solo se aplica a sistemas OpenScape Business S y no se admite en OpenScape Business X.

25.1.8 Anuncio grabado

El sistema de comunicación permite reproducir anuncios en espera para las personas que llaman antes de contestar una llamada y también cuando se utiliza la distribución de llamadas y la marcación directa entrante DTMF. También puede reemplazar la melodía MOH en ciertas situaciones con un anuncio, por ejemplo, si una llamada se pone en espera o si un suscriptor está ocupado o está siendo enrutado.

El sistema puede importar anuncios de las siguientes fuentes:

- Anuncios internos
- Reproductor de anuncios (solo con la funcionalidad UC Booster)

  El reproductor de anuncios es un programa de software interno que está disponible junto con la funcionalidad UC Booster (UC Booster Card o UC Booster Server). Al llamar a un suscriptor, el reproductor de anuncios primero reproduce el anuncio deseado y luego establece la conexión con el suscriptor.
- Dispositivo de anuncio analógico

  Consulte la sección sobre Equipo auxiliar: dispositivo de anuncio analógico en la *documentación del administrador de OpenScape Business*.
- Módulo MPPI USB EXM (solo para OpenScape Business X3/X5)

  Para obtener más información, consulte *Instalación de OpenScape Business X3/X5/X8, Documentación del servicio*.

El administrador puede configurar anuncios para reproducción única (inicio/detención) o continua.

Un dispositivo de anuncio externo debe comportarse como una estación, es decir, anunciarse a sí mismo, reproducir el anuncio y conmutar la llamada (entrar en espera de consulta, marcar y colgar).

Archivos de audio

El administrador puede transferir archivos de audio con anuncios desde la PC al sistema de comunicación.

Nota: Antes de utilizar anuncios o música de otras fuentes, asegúrese de no infringir ningún derecho de autor.

Los archivos de audio deben estar disponibles como archivos `Wave` con las siguientes propiedades:

- PCM de 16 bits
- Mono o estéreo
- Posibles frecuencias de muestreo: 8 / 22.05 / 24 / 32 / 40 / 44.1 o 48 kHz
- Longitud máxima del nombre del archivo de audio: 30 caracteres

Recomendado: **PCM de 16 bits - Mono - 8 kHz, duración aproximada de 2 min**

25.1.8.1 Cómo configurar anuncios (UC Suite)& Refuerzo de UC)

El asistente **de Música en espera / Anuncios** se puede utilizar para configurar los anuncios.

Requisitos previos

- En **modo experto> Middleware> Reproductor de anuncios** seleccione la casilla de verificación **El servicio se iniciará automáticamente** para habilitar el reproductor de anuncios.
- Se debe configurar un número de llamada del reproductor de anuncios en el **modo experto> Configuración básica> Buzón de voz / Reproductor de anuncios**.
- Verifique que el número esté configurado correctamente en el **Modo Experto> LCR> Plan de marcado**, debajo del campo **Ann-Player**.
- La **tabla de enrutamiento** asociada está configurada en **12**, **UC Suite** está configurado para **Ruta** y **MEB** está configurado para **Regla de marcado**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.

3) Haga clic en **Editar** para iniciar el asistente de **Música en espera / Anuncios**.

4) Omita la selección de **Cargar música en archivos en espera a través de archivos HTTP**, haciendo clic en **Aceptar& Siguiente**.

Nota: Antes de utilizar anuncios o música, asegúrese de no infringir ningún derecho de autor.

---

5) Para transferir un archivo de audio al sistema de comunicación, proceda de la siguiente manera:

a) Haga clic en **Elegir archivo**.
b) Seleccione un archivo de audio.
c) Haga clic en **Abrir**.
d) Haga clic en **Cargar**.
e) Confirme el mensaje con **OK**.
f) Si desea cargar más archivos de audio al sistema, repita estos pasos.

6) Haga clic en **Aceptar & Siguiente**.

> **Consejo:** Los parámetros de configuración para **Anuncios** también se describen y se pueden configurar a través de **Modo Experto > Equipo Auxiliar > Anuncios**.

7) Seleccione el tipo de anuncio que se reproducirá en la columna **Tipo**.
8) Seleccione el puerto al que está conectado el dispositivo en la columna **Acceso**. Los destinos externos se pueden utilizar para direccionar dispositivos de anuncio en otro nodo del sistema.
9) Seleccione un archivo de anuncio de la lista desplegable en la columna **Archivo Wave** (solo para el tipo **Reproductor de anuncios** y en modo UC Suite).
10) Seleccione el tipo de reproducción de la lista desplegable en la columna **Modo**.
11) Haga clic en **Aceptar& Siguiente**, seguido de **Finalizar**.

25.1.8.2 Cómo configurar anuncios (UC Smart)

El asistente **de Música en espera / Anuncios** se puede utilizar para configurar los anuncios.

Requisitos previos

A los puertos analógicos que están configurados como puertos de anuncios se les debe asignar el valor **Contestador automático** en **Tipo de extensión**.

Los puertos EVM que están configurados como puertos de anuncio deben ser:

- se le asignó el valor **Estándar** en **Tipo de extensión**.
- eliminado del grupo de búsqueda del buzón de correo de voz.
- asignó un buzón de correo de voz al número de llamada del puerto en el Modo Experto **Modo Experto > Equipo Auxiliar > Smart VM**.

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **Telefonía central**.
3) Haga clic en **Editar** para iniciar el asistente de **Música en espera / Anuncios**.
4) Omita la selección de **Cargar música en archivos en espera a través de archivos HTTP**, haciendo clic en **Aceptar& Siguiente**.

> **Consejo:** Los parámetros de configuración para **Anuncios** se describen y se pueden configurar a través de Modo experto > Equipo auxiliar > Anuncios.

5) Seleccione el tipo de anuncio que se reproducirá en la columna **Tipo**.
6) Seleccione el puerto al que está conectado el dispositivo en la columna **Acceso**. Los destinos externos se pueden utilizar para direccionar dispositivos de anuncio en otro nodo del sistema.

7) Seleccione un archivo de anuncio de la lista desplegable en la columna **Archivo Wave** (solo para el tipo **Reproductor de anuncios** y en modo UC Suite).
8) Seleccione el tipo de reproducción de la lista desplegable en la columna **Modo**.
9) Haga clic en **Aceptar& Siguiente**, seguido de **Finalizar**.

25.1.9 Señalización de usuario a usuario

El sistema de comunicación permite la transmisión transparente de mensajes entre terminales (User to User Signalling, UUS). Se admite la variante UUS1 para el intercambio de información en mensajes de control del establecimiento y finalización de la conexión.

En una conexión con varios terminales, hay que garantizar que solo uno de los terminales transmita un mensaje a una llamada entrante.

25.1.10 Protección de señalización en el canal telefónico

El sistema de comunicación permite al administrador configurar un mecanismo de seguridad frente a la falsificación de datos a través de señales sonoras no deseadas en el canal de voz. La intercalación no es posible en una conexión así protegida. Todas las extensiones configuradas como fax tienen esta protección de señalización automáticamente.

Las llamadas recordatorias se posponen hasta que la extensión se libera.

Un usuario en retención siempre tiene protección de señalización.

25.1.11 Parámetros de tiempo

El sistema de comunicación ofrece al administrador distintas opciones de configuración para distintos parámetros de tiempo como, por ejemplo, la duración de devolución de llamada o el tiempo para la rellamada automática.

Los parámetros de tiempo serán preestablecidos en el sistema de comunicación y, por lo general, no es necesario modificarlos.

25.1.12 Control de prestaciones Centrex

Para controlar las prestaciones Centrex hay que transferir los signos de marcación * y # a RDSI e ITSP.

En calidad de administrador puede activar o desactivar esta prestación.

Los códigos se deben introducir en estado de marcación (por ejemplo, después de introducir el código de línea). La entrada comienza siempre con el carácter * o #, seguido por un dígito o combinación de dígitos, y finaliza con #.

25.1.12.1 Cómo activar o desactivar el control de prestaciones Centrex

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Telefonía** > **Ajustes básicos**.
3) En el árbol de navegación, desplácese hasta **Sistema** > **Flags del sistema**.
4) Elija una de estas opciones:
   - Si desea activar el control de prestaciones Centrex, active la casilla de verificación **Marcación de * y # en las interfaces de línea**.
   - Si desea desactivar el control de prestaciones Centrex, desactive la casilla de verificación **Marcación de * y # en las interfaces de línea**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.2 Capítulo 24.2 Copia de seguridad y recuperación de datos

Los datos de configuración del sistema de comunicación se pueden guardar y recuperar.

Los datos de configuración se almacenan en un conjunto de copias de seguridad. Cada proceso de almacenamiento crea un conjunto propio de copias de seguridad. La copia de seguridad se puede ejecutar de forma manual al instante o automáticamente en determinados momentos.

Nota: Se recomienda encarecidamente guardar periódicamente los datos de configuración como conjuntos de copias de seguridad.

Al hacer una actualización a una versión menor (minor release) hay que crear un nuevo conjunto de copias de seguridad.

Cada copia de seguridad se cifra mediante una clave específica del sistema.

Un conjunto de copia de seguridad cifrado solo se puede utilizar para restaurar el sistema que ha cifrado la copia de seguridad.

Se puede guardar en distintos medios de copia de seguridad (por ejemplo, en un soporte USB, una unidad de red o el disco duro de la UC Booster Card).

En función de la configuración del sistema, del uso del sistema de comunicación y del tipo de medio de copia de seguridad, la copia de seguridad o la restauración pueden requerir más tiempo (en algunos casos, en sistemas con la UC Suite se pueden necesitar hasta tres horas). Este proceso no se debe cancelar de forma manual ni reiniciando el sistema.

Si se cancela una restauración de datos, la configuración del sistema puede hacerse inhomogénea y no se podrá garantizar el correcto funcionamiento del sistema. Si se interrumpe una restauración, hay que repetir obligatoriamente el proceso, hasta que finalice correctamente. De lo contrario, puede ser necesario volver a configurar por completo el sistema. Si la restauración falla varias

veces, póngase en contacto con el servicio de atención al cliente y, mientras tanto, asegúrese de que la copia de seguridad de sus datos no se sobrescriba con otras copias. Para ello, desactive de forma provisional el almacenamiento de datos automático.

Conjunto de copias de seguridad para fines de diagnóstico

Para fines de diagnóstico se pueden crear conjuntos de copias de seguridad "más pequeños" que incluyan datos de diagnóstico para soporte técnico. A diferencia de lo que ocurre con los conjuntos de copias de seguridad normales, se crean volúmenes de datos considerablemente menores y eso permite, por ejemplo, enviarlos fácilmente por correo electrónico. Los conjuntos de copias de seguridad de diagnóstico incluyen, entre otros datos, los datos de configuración del sistema de comunicación y de la solución de UC instalada. No incluyen mensajes de voz, mensajes de fax ni anuncios grabados.

Directorio de copia de seguridad "Disco duro" (solo con UC Booster Card)

Si la UC Booster Card está insertada, los datos de configuración del sistema de comunicación se pueden guardar en una partición propia del disco duro de la UC Booster Card, en el directorio de copias de seguridad. Este directorio de copia de seguridad ya está preestablecido como archivo comprimido estándar "Disco duro".

Copia de seguridad de los datos de configuración del UC Booster Server

Si además del sistema de comunicación se opera un UC Booster Server, al hacer una copia de seguridad de los datos de configuración del sistema, también se deberían copiar los datos de configuración del UC Booster Server. La copia de seguridad de los datos del UC Booster Server es idéntica a la copia de seguridad de los datos del sistema de comunicación. La única diferencia es que al lanzar la Gestión basada en Web (WBM), el administrador no indica la dirección IP del sistema de comunicación sino la del servidor Linux.

25.2.1 Conjuntos de copias de seguridad

Los datos de configuración del sistema de comunicación se almacenan en un conjunto de copias de seguridad.

Además del conjunto de copias de seguridad, hay que guardar un archivo de texto relativo al conjunto de copias de seguridad. Este archivo incluye información sobre la fecha y la hora de la copia de seguridad y la versión de software con la que se hizo. Este archivo de texto es necesario para restaurar el conjunto de copias de seguridad.

Si se supera el número de conjuntos de copias de seguridad definido, se borran los conjuntos de copias de seguridad más antiguos.

Datos de conjunto de copias de seguridad

Estos son los datos que se presentan para un conjunto de copias de seguridad:

- **Nombre de archivo**: nombre del conjunto de copias de seguridad.
- **Tamaño**: tamaño del conjunto de copias de seguridad en bytes.
- **Fecha**: fecha en la que se creó el conjunto de copias de seguridad.

- **Comentario**: comentario que se introdujo en la creación del conjunto de copias de seguridad (optativo).

Destacados en color gris aparecen los conjuntos de copias de copias de seguridad que no se pueden restaurar.

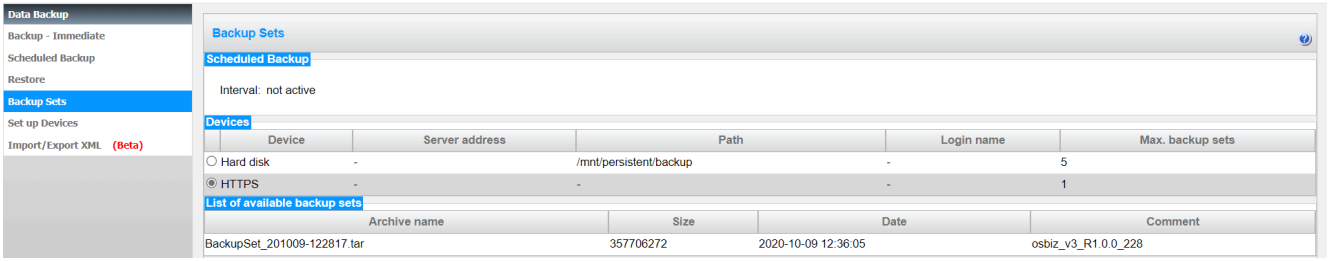
25.2.1.1 Cómo ver los conjuntos de copias de seguridad

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) Haga clic en **Copia de seguridad de datos** en la barra de navegación.
2) En el árbol de navegación, haga clic en **Conjuntos de copias de seguridad**.
3) En la sección **Dispositivos**, active el medio de copia de seguridad cuyos conjuntos de copias de seguridad desea mostrar. Aparecerá una lista de todos los conjuntos de copias de seguridad presentes en ese medio.



25.2.1.2 Cómo borrar conjuntos de copias de seguridad

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Almacenamiento de datos**.
2) En el árbol de navegación, haga clic en **Conjuntos de copias de seguridad**.
3) En la sección **Dispositivos**, active el medio de copia de seguridad cuyos conjuntos de copias de seguridad desea mostrar. Aparecerá una lista de todos los conjuntos de copias de seguridad presentes en ese medio.
4) Active la casilla de verificación del conjunto de copias de seguridad que desea borrar y haga clic en **Borrar**. El conjunto de copias de seguridad se borra.

25.2.2 Medios de copia de seguridad

Los conjuntos de copias de seguridad se almacenan en los medios de copia de seguridad seleccionados.

Se pueden utilizar estos medios de copia de seguridad:

- Soporte USB insertado
- Unidad de red
- PC cliente a través de HTTP (solo disponible con copia de seguridad inmediata)
- Disco duro de la UC Booster Card
- Servidores FTP/FTPS

En cada uno de los medios de copia de seguridad se puede establecer, de forma individualizada, el máximo de conjuntos de copias de seguridad que se pueden guardar en el directorio.

Soporte de almacenamiento USB

Para utilizar un soporte USB (por ejemplo, un disco duro o un stick USB) para la copia de seguridad, debe estar conectado a la interfaz de servidor USB del sistema de comunicación. Además, el soporte USB debe tener el formato FAT-32. Debido a la limitación del sistema de archivos, el tamaño máximo del conjunto de copias de seguridad no puede superar los 4 GB. En tales casos, se deben seleccionar medios de copia de seguridad alternativos. Los soportes USB con formato NTFS son de solo lectura. ¡Si hay varias particiones, solo se puede usar la primera partición para copia de seguridad!

No se admiten soportes USB de arranque.

Con OpenScape Business S y OpenScape UC Booster Server el soporte USB se conecta a la interfaz USB del servidor Linux.

Servidores FTP/FTPS y unidades de red

Los servidores FTP/FTPS y las unidades de red se pueden agregar como nuevos medios, editar o eliminar. Los servidores FTP/FTPS y las unidades de red también se pueden indicar varias veces para utilizar distintos directorios. Como protocolo de transferencia de archivos cifrado (FTPS) se admite el protocolo TLS 1.2.

Para realizar la copia de seguridad de los datos de configuración en un servidor FTP/FTPS, el usuario debe tener derechos de escritura para el directorio raíz. Para realizar la copia de seguridad en una unidad de red, basta con tener derechos de escritura para el directorio deseado.

Si la velocidad de transmisión al servidor FTPS es demasiado baja, se puede producir un error de funcionamiento en la copia de seguridad de los datos. En tal caso, hay que reiniciar la copia de seguridad.

Con FTPS se admiten certificados de hasta 2048 bits. Estos certificados son necesarios para la autenticación en el servidor FTPS.

25.2.2.1 Agregar un medio de copia de seguridad

Requisitos previos

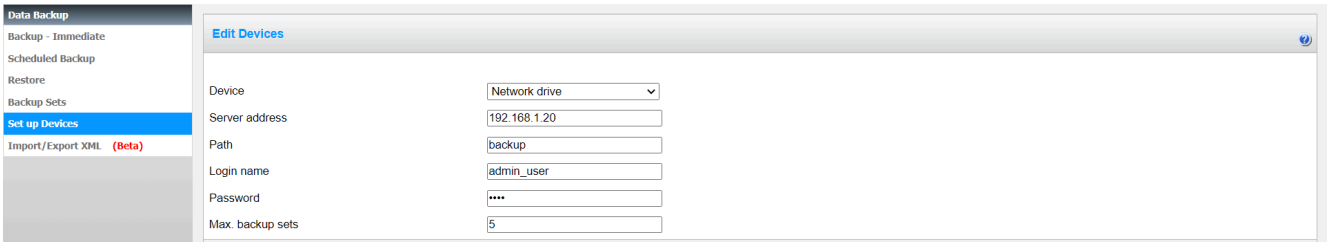
Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) Haga clic en **Copia de seguridad de datos** en la barra de navegación.

2) En el árbol de navegación, haga clic en **Configuración de dispositivo**.

3) Haga clic en **Agregar**.



4) En la lista desplegable de la columna **Equipo**, seleccione el medio de copia de seguridad deseado.
   - Si el destino de almacenamiento es un servidor FTP/FTPS, seleccione **(S)FTP**.
   - Si el destino de almacenamiento es una unidad de red, seleccione **Unidad de red**.

   Nota: La versión compatible de Samba es SMB2.

5) En **Dirección de servidor**, indique el nombre de host o la dirección IP del medio.
6) En **Directorio**, indique la ruta en la que desea almacenar el conjunto de copias de seguridad.
7) Si desea que el destino de almacenamiento sea un servidor FTP/FTPS, indique el **Nombre de usuario** y la **Contraseña** de acceso al servidor FTP/FTPS.

   Nota: El campo de contraseña admite los siguientes caracteres: `0-9 A-Z a-z ~ ! @ # $ % ^ _ - + = ? / , . :`

   La contraseña puede tener hasta 64 caracteres como máximo.

8) Si desea hacer una copia de seguridad en una unidad de red protegida, indique el **Nombre de usuario** y la **Contraseña** para acceder a la unidad de red.

   Nota: De forma predeterminada, se utiliza un dominio vacío para la autenticación. Si desea proporcionar el dominio, utilice como separador una barra diagonal (/) en el campo **Nombre de usuario**. Por ejemplo: `dominio/usuario`.

9) En **Número máximo de conjuntos de copias de seguridad** indique el máximo de conjuntos de copias de seguridad que almacenar en un directorio.
10) Haga clic en **OK y Continuar**. El medio de copia de seguridad recién creado aparece en la lista de medios de copia de seguridad disponibles.
11) En el árbol de navegación, haga clic en **Conjuntos de copias de seguridad**.
12) En el área **Dispositivos**, active el medio de copia de seguridad que acaba de añadir. Si en la lista de los conjuntos de copias de seguridad

disponibles no hay ninguna barra roja con un mensaje de error, significa que el medio de copia de seguridad está bien configurado.

13) Si aparece un mensaje de error, vuelva a comprobar sus datos (véase Cómo editar un medio de copia de seguridad en la página 1269

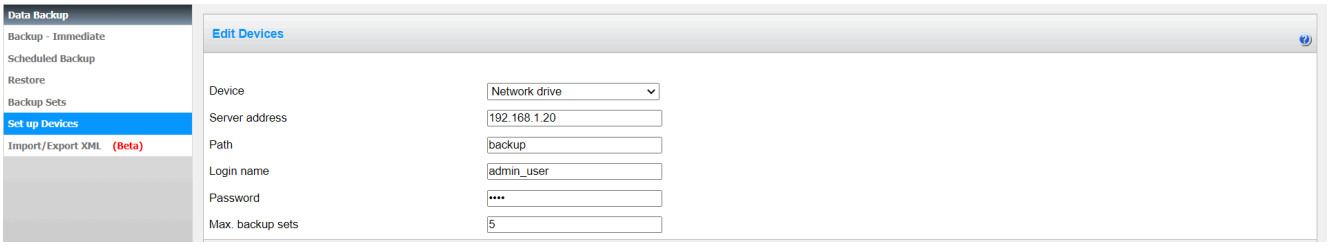
25.2.2.2 Cómo editar un medio de copia de seguridad

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) Haga clic en **Copia de seguridad de datos** en la barra de navegación.
2) En el árbol de navegación, haga clic en **Configuración de dispositivo**.
3) Active el medio de copia de seguridad que desea editar y haga clic en **Editar**.



4) Modifique los valores deseados.
5) Haga clic en **OK y Continuar**.

25.2.2.3 Cómo borrar un medio de copia de seguridad

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) Haga clic en **Copia de seguridad de datos** en la barra de navegación.
2) En el árbol de navegación, haga clic en **Configuración de dispositivo**.
3) Seleccione el medio de copia de seguridad que desea borrar y haga clic en **Borrar**.

   También se pueden seleccionar varios medios de copia de seguridad para borrar.
4) Confirme la consulta de seguridad con **Aceptar**. El medio de copia de seguridad se borra de la lista de medios de copia de seguridad disponibles.

25.2.3 Almacenamiento inmediato

Los datos de configuración se pueden guardar inmediatamente de forma manual.

Se pueden hacer copias de seguridad en diferentes medios de copia de seguridad. De forma predeterminada, está configurado el medio de copia de seguridad **HTTPS**. De esta forma puede almacenar el conjunto de copias de seguridad en todas las ubicaciones a las que tenga acceso el PC de cliente con el que se ha registrado en la Gestión basada en Web (WBM). También se debe poder acceder al lugar de almacenamiento seleccionado al restablecer el conjunto de copias de seguridad. Si hay un soporte USB conectado con el sistema de comunicación, se muestra como medio de copia de seguridad adicional **Dispositivo USB**. Si está insertada la UC Booster Card con disco duro, se muestra un medio de copia de seguridad adicional denominado **Disco duro local**.

El nombre del conjunto de copias de seguridad se asigna de forma automática en el proceso de copia. Incluye, entre otras cosas, la fecha en la que se ha ejecutado el proceso de copia. Además, estos datos también se recogen en un archivo de texto que se debe almacenar de forma adicional. Para poder identificar más fácilmente el conjunto de copias de seguridad en caso de recuperación, se puede introducir un comentario.

Conceptos relacionados

Copia de seguridad programada en la página 1271

Tareas relacionadas

Cómo modificar su propria contraseña de administrador en la página 123

25.2.3.1 Cómo guardar un conjunto de copias de seguridad inmediatamente

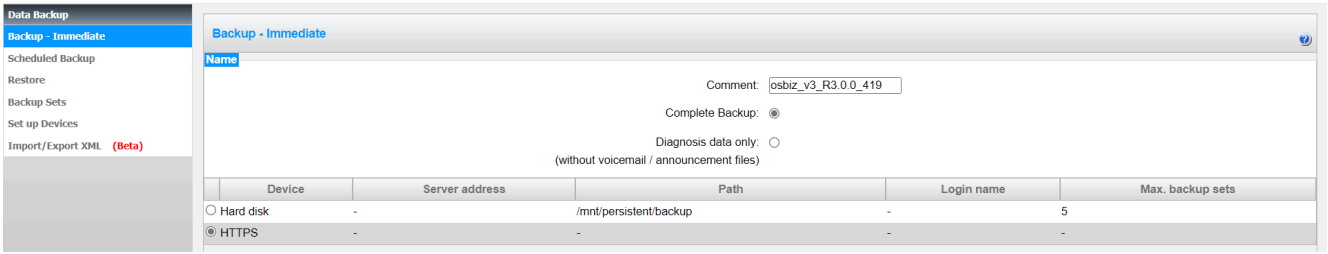
Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Solo cuando se utiliza UC Suite: UC Suite se ha iniciado correctamente.

Paso a paso

1) Haga clic en **Copia de seguridad de datos** en la barra de navegación.
2) En el árbol de navegación, haga clic en **Guardar - inmediatamente**.



3) En el campo **Comentario**, introduzca un comentario para el conjunto de copias de seguridad. Este comentario permitirá identificar con mayor facilidad el conjunto de copias de seguridad en caso de que sea necesaria una recuperación. Al hacer la entrada evite el uso de diéresis y caracteres especiales.
4) Si quiere crear un conjunto de copias de seguridad, incluyendo mensajes de voz y anuncios grabados, active la opción **Copia de seguridad completa**.

5) Si quiere crear un conjunto de copias de seguridad sin mensajes de voz y anuncios grabados, active la opción **Solo datos de diagnóstico**.
6) En el área **Equipos**, active la unidad de destino en la que desea guardar el conjunto de copias de seguridad.
7) Haga clic en **OK y Continuar**. Se abrirá una nueva ventana con el progreso del proceso de copia de seguridad.

Nota: Si el botón **OK&Continuar** no está activo (en gris), significa que no se han iniciado correctamente todas las aplicaciones (p. ej. UC Suite) cuyos datos se quieren copiar.

Si no tiene autorización para el directorio de archivo comprimido seleccionado, aparecerá un mensaje de error. Seleccione otra unidad de destino o modifique la ruta del archivo comprimido.

Si la unidad de destino no tiene suficiente espacio de almacenamiento libre para el conjunto de copias de seguridad, aparecerá un mensaje de error. Seleccione otra unidad de destino o borre un conjunto de copias de seguridad e inicie de nuevo la copia de seguridad.

---

8) La copia de seguridad se ha realizado correctamente si aparece el mensaje **¡La copia de seguridad se ha realizado con éxito!** Aparece **100 %**.
9) Si ha seleccionado **HTTPS** como medio de copia de seguridad, guarde el conjunto de copias de seguridad y el archivo de texto correspondiente al conjunto de copias de seguridad en el lugar que desee. En los demás medios de copia de seguridad, la ubicación se selecciona automáticamente. La ventana del navegador seguirá abierta hasta que concluya el proceso de guardado del conjunto de copias de seguridad del archivo de texto.

Nota: Si utiliza como soporte de copia de seguridad un soporte USB, espere hasta que el LED de dicho soporte deje de parpadear. Sólo entonces habrá finalizado correctamente la copia de seguridad en el soporte USB. A continuación, extraiga el soporte USB.

---

10) Haga clic en **Finalizar**.

25.2.4 Copia de seguridad programada

Los datos de configuración se pueden guardar automáticamente a través de una programación. Se pueden configurar el momento, la frecuencia y la ubicación del almacenamiento automático.

La copia de seguridad de datos programada se puede programar a diario o de forma semanal para una hora fija. Así, el proceso comenzará automáticamente en el momento establecido. Esta "solicitud de copia de seguridad" se puede configurar para un medio de copia de seguridad interno o externo. No se pueden configurar varias solicitudes de copia de seguridad.

Conceptos relacionados

Almacenamiento inmediato en la página 1269

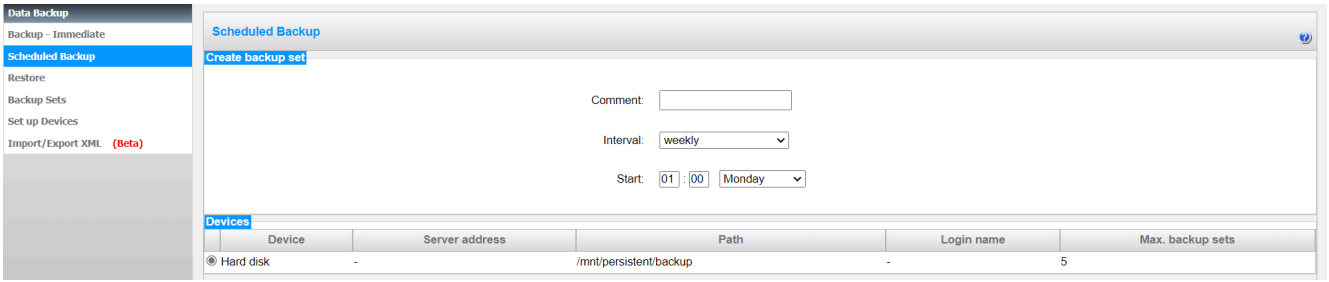
25.2.4.1 Cómo guardar un conjunto de copias de seguridad programado

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) Haga clic en **Copia de seguridad de datos** en la barra de navegación.
2) En el árbol de navegación, haga clic en **Copia de seguridad programada**.



3) En la sección **Crear conjunto de copias de seguridad**, y en el campo **Comentario**, introduzca un comentario para el conjunto de copias de seguridad para poder identificar más fácilmente el conjunto en caso de recuperación. Al hacer la entrada evite el uso de diéresis y caracteres especiales.
4) Establezca el intervalo de almacenamiento:
   - Copia de seguridad diaria: En la lista desplegable **Frecuencia**, seleccione el elemento **Diariamente** y, a continuación, introduzca cuándo debe iniciarse la copia de seguridad cada día en **Copia de seguridad el**.
   - Copia de seguridad semanal: En la lista desplegable **Frecuencia**, seleccione la opción **Semanal** y, a continuación, introduzca qué día de la semana y a qué hora debe iniciarse la copia de seguridad en **Copia de seguridad el**.
5) En el área **Equipos**, active la unidad de destino en la que desea guardar el conjunto de copias de seguridad.
6) Haga clic en **OK y Continuar**. La copia de seguridad de datos se inicia a diario o de forma semanal en el momento indicado.

25.2.5 Recuperar

Los datos de configuración se recuperan de forma manual mediante los conjuntos de copias de seguridad.

Se pueden recuperar todos los medios de copia de seguridad compatibles.

25.2.5.1 Cómo recuperar un conjunto de copias de seguridad

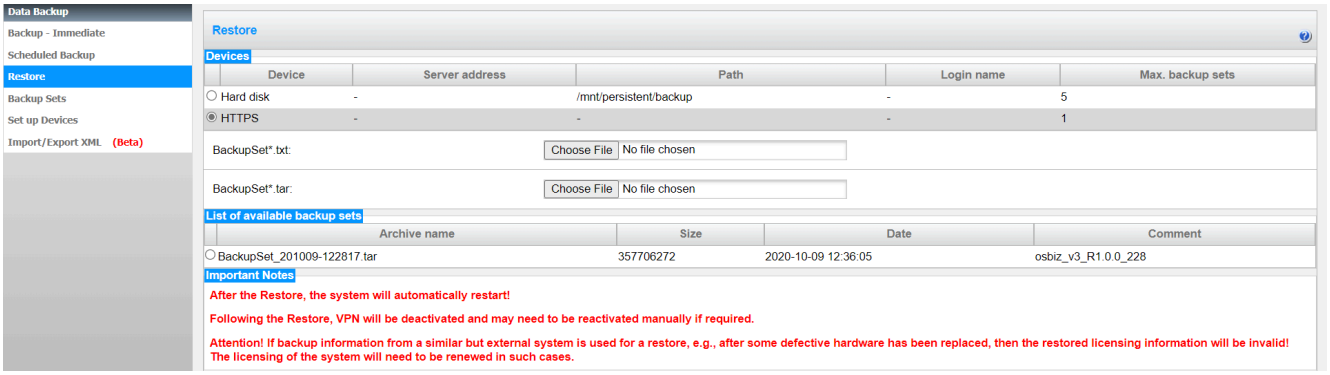
Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Solo cuando se utiliza UC Suite: UC Suite se ha iniciado correctamente.

Paso a paso

1) Haga clic en **Copia de seguridad de datos** en la barra de navegación.
2) En el árbol de navegación, haga clic en **Recuperar**.



3) En la sección **Equipo**, active el medio que contiene el conjunto de copias de seguridad que desea recuperar.
4) Si ha activado **HTTPS** como medio de copia de seguridad, desplácese hasta el lugar de almacenamiento del conjunto de copias de seguridad y seleccione el conjunto de copias de seguridad. A continuación, desplácese hasta el lugar de almacenamiento del archivo de texto y selecciónelo.
5) Si ha activado un medio de copia de seguridad que no es **HTTPS**, en el área **Lista de conjuntos de copias de seguridad disponibles**, seleccione el conjunto de copias de seguridad que contiene los datos de configuración que desea recuperar.
6) Espere hasta que los archivos terminen de cargarse en el sistema y, a continuación, haga clic en **OK & Continuar**. Se inicia el restablecimiento de los datos de configuración. Se muestra el progreso de la recuperación.
7) Cuando aparezca el mensaje **¡La recuperación ha finalizado!**, el sistema se reiniciará automáticamente. Cuando el sistema vuelva a estar en servicio, la recuperación habrá concluido correctamente.

25.3 Actualizaciones

Mediante las actualizaciones, se actualiza el software de los componentes de sistema dentro de una versión.

Para poder instalar actualizaciones, requiere el soporte de software de 3 años.

La versión del software instalado y la fecha de vencimiento del soporte de software aparecen indicadas en la página de inicio de la Gestión basada en Web (WBM). Si hay disponible un software más reciente, también se indica.

Nota: Al hacer una actualización a una versión menor (minor release) hay que crear un nuevo conjunto de copias de seguridad.

La actualización de software se realiza mediante la Gestión basada en Web (WBM). Con un modelo de hardware existe además la posibilidad de actualizar el software directamente mediante un soporte USB sin acceso a la Gestión basada en Web (WBM). En un sistema de comunicación con servidor UC Booster Server el modelo de hardware y el servidor UC Booster Server se actualizan por separado.

Mediante la Gestión basada en Web (WBM), se puede actualizar el software mediante el servidor Web de internet, mediante un servidor Web local o directamente mediante archivos de imagen.

Se actualizan los siguientes componentes del sistema:

- Software del sistema de comunicación
- Software de los clientes UC
- Software de los teléfonos de sistema (la actualización también se puede realizar de forma individual)
- Documentación

Junto con el software del sistema de comunicación también se actualiza el software de los clientes de UC. Si hay disponible un software más actualizado, los usuarios de los clientes UC recibirán un mensaje mediante la actualización automática. Este mensaje les indicará que hay disponible una actualización y la posibilidad de proceder a su instalación.

La actualización de software de los teléfonos IP del sistema se hace automáticamente, junto con la actualización del sistema de comunicación, pero también se puede realizar de forma manual. En los teléfonos de sistema UP0, la actualización se realiza de forma manual con el Manager E.

La actualización de software se puede iniciar inmediatamente o bien se puede establecer por separado el momento para la transmisión de software y para la activación de software. El software debería actualizarse fuera del horario comercial ya que el sistema de comunicación o los teléfonos de sistema tendrán que reiniciarse, y se interrumpirán las llamadas en curso y el uso de los clientes UC.

Si el software se ha transferido al sistema de comunicación, el software se activa en el momento seleccionado. A continuación, la imagen de teléfono más actual se carga automáticamente en los teléfonos IP del sistema. Después de reiniciar el sistema de comunicación y los teléfonos IP del sistema se activa el software recién cargado.

Nota: La actualización de software no debe realizarse simultáneamente en todos los sistemas y en diferentes versiones de software.

Archivos de imagen

Para actualizar los componentes del sistema se necesitan archivos de imagen que contengan el software de los componentes del sistema. Estos archivos de imagen se pueden descargar (por ejemplo, del servidor de software o servidor Web basado en Internet) y se pueden depositar en un servidor Web local, en

la red interna o en una llave USB. Hay un archivo de imagen propio para el sistema de comunicación sin tarjeta UC Booster y un archivo de imagen propio para un sistema con tarjeta UC Booster Card. Ambos archivos de imagen incluyen también el software para los teléfonos del sistema. No obstante, hay también un archivo de imagen propio para cada tipo de teléfono del sistema (por si hay que actualizar por separado los teléfonos del sistema).

Existen estos tipos de archivos de imagen:

- **tgz**: para el software del sistema de comunicación. En el archivo .tgz se encuentra un archivo .tar. El archivo tgz incluye un archivo tar. El archivo .tar se debe extraer del archivo .tgz con un archivo de compresión adecuado como, por ejemplo WinZip o 7-Zip. El archivo .tgz se ofrece para descarga porque durante la descarga desde el servidor de software se puede comprobar si el archivo está dañado.
- **tar**: para el software del sistema de comunicación. Incluye los archivos comprimidos para los distintos componentes del sistema.
- **app**: para el software del teléfono del sistema.

Servidor Web local

Si el software se actualiza mediante un servidor web, se accede al servidor de software (servidor web Internet) de forma predeterminada.

No obstante, también es posible utilizar para la actualización un servidor Web local. Para ello, el archivo de imagen debe estar depositado en el servidor Web local y la ruta con el servidor Web local debe estar configurada en la Gestión basada en Web (WBM).

Speed Upgrade

En el HiPath 3000 no se puede hacer un Speed Upgrade.

Importante: ¡Si la tarjeta SDHC se extrae durante el funcionamiento, se pueden perder datos!

Red - Licencias

Al actualizar/migrar sistemas en una red, donde el nodo maestro se utiliza para licenciar los nodos esclavos. Comience primero con los nodos esclavos antes que con el nodo maestro.

25.3.1 Uso de un servidor Web local

El software se puede actualizar mediante un servidor Web local.

Los archivos de imagen actuales deben estar almacenados en el servidor Web local. Además, hay que registrar los datos de acceso del servidor Web local en la Gestión basada en Web (WBM). Este cambio solo puede ser ejecutado por un administrador con el perfil **Experto**. Si se han introducido los datos de acceso del servidor Web local, se establecerán como valor estándar y para todas las demás actualizaciones del sistema de comunicación se utilizará el servidor Web local en lugar del servidor Web de Internet.

25.3.1.1 Cómo configurar el acceso al servidor Web local

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Hay disponible una conexión con el servidor Web local.

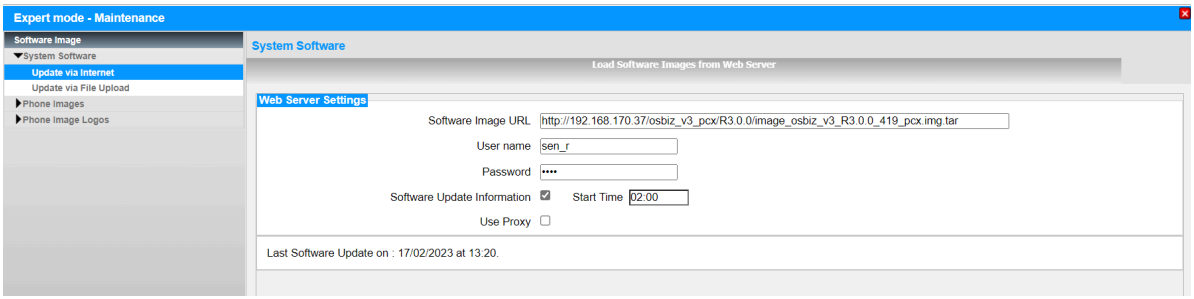
Necesitará la dirección Web (URL) y la identificación de acceso del servidor Web local, así como el nombre del archivo de imagen.

El archivo de imagen está almacenado en el servidor Web local como archivo .tar y se conoce el lugar de almacenamiento. En su caso, el archivo .tar debe ser descomprimido a partir del archivo .tgz.

Si desea utilizar un servidor proxy para la actualización necesitará sus datos (en su caso también el nombre de usuario y la contraseña).

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Imagen de software**.
3) En el grupo de menús, haga clic en **Software del sistema**.
4) Haga clic en **Actualización a través de Internet**.



5) Configure el acceso al servidor Web local:
   a) En **URL imagen de software** introduzca la dirección del servidor Web local, con la ruta y el nombre del archivo de imagen.

      Nota: El botón **Preajuste** permite restablecer los valores indicados a sus valores estándar.

   b) En el campo **Nombre de usuario** indique el nombre de usuario y en el campo **Contraseña** la contraseña para acceder al servidor Web local.
   c) Active la casilla de verificación **Información de actualización de software** y en Hora de inicio indique el **momento inicial** para buscar nuevo software en el servidor indicado arriba.
   d) Si desea utilizar un servidor proxy para la transmisión, active la casilla de verificación **Utilizar proxy** e introduzca los datos del servidor proxy.
6) Haga clic en **Aplicar**. Los datos de acceso del servidor Web local indicados se aplican como valor estándar.

   Si en el servidor Web local ya hay un nuevo archivo de imagen, comienza la actualización de software y aparece el acuerdo de licencia (véase Cómo actualizar el sistema a través de un servidor Web). Si es necesario todavía se puede anular el inicio de la actualización de software.

25.3.2 Actualización del sistema de comunicación

Al actualizar el sistema de comunicación, se actualiza el software del sistema de comunicación y se actualizan también las imágenes de software de los teléfonos del sistema memorizadas en el sistema de comunicación. De esta forma, la actualización completa de todos los componentes del sistema se realiza fácil y rápidamente.

Antes de hacer una actualización de software es conveniente hacer una copia de seguridad de los datos de configuración del sistema de comunicación (Copia de seguridad y recuperación de datos).

Actualización a través del servidor Web

Si el software se actualiza mediante un servidor web, se accede al servidor de software (servidor web Internet) de forma predeterminada.

Si se utiliza un servidor web local, el archivo de imagen debe estar depositado en el servidor web local.

En los sistemas de comunicación sin UC Booster Card no importa si se utiliza un archivo de imagen para un sistema con o sin UC Booster Card. Solo se instalan los componentes necesarios.

Después de establecer automáticamente una conexión con el servidor Web, se comprueba si hay disponibles nuevas actualizaciones de software. En los sistemas sin UC Booster se pueden desmarcar los paquetes de la actualización de software, para reducir el tiempo de descarga. Solo se transmiten los paquetes que se han modificado respecto a la versión de software instalada. Se pueden seleccionar el momento de inicio de la transferencia de software y de la activación de software. Si se alcanza el momento de la activación de software cuando la actualización todavía no se ha transferido del todo al sistema, la activación no se realiza automáticamente. En este caso hay que definir un nuevo momento de activación de forma manual.

Actualización mediante soporte USB

El archivo de imagen está depositado en un soporte USB. El soporte USB se inserta en la interfaz de servidor USB del sistema de comunicación. Este tipo de actualización solo pueden ejecutarlo administradores con el perfil **Experto** y no se puede ejecutar con OpenScape Business S ni OpenScape Business UC Booster Server.

Actualización mediante carga de archivo

El archivo de imagen está en un directorio de la red interna o en el PC de administración.

Actualización mediante soporte USB sin acceso a la Gestión basada en Web (WBM)

El sistema de comunicación se puede actualizar directamente sin acceso a la Gestión basada en Web (WBM) mediante un soporte USB. Para ello hay que insertar el soporte USB en la interfaz de servidor USB del sistema, y el archivo de imagen debe estar en el nivel superior de directorio del soporte USB. Si se reinicia el sistema de comunicación sin extraer el soporte USB, se inicia automáticamente la actualización de software. Este tipo de actualización no se puede hacer con OpenScape Business S. En un sistema con OpenScape Business UC Booster Server hay que actualizar además el servidor.

Actualización del UC Booster Server

Si además del sistema de comunicación se opera un UC Booster Server, al actualizar el software del sistema también hay que actualizar el software de comunicación del UC Booster Server. El software del sistema de comunicación y el del UC Booster Server siempre deben tener la misma versión. El software del UC Booster Server se actualiza del mismo modo que el software del sistema de comunicación. La única diferencia es que al lanzar la Gestión basada en Web (WBM), el administrador no indica la dirección IP del sistema de comunicación sino la del servidor Linux.

25.3.2.1 Cómo actualizar el sistema a través de un servidor Web

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

En la página de inicio de la Gestión basada en Web (WBM) se indica que hay disponible una nueva versión de software.

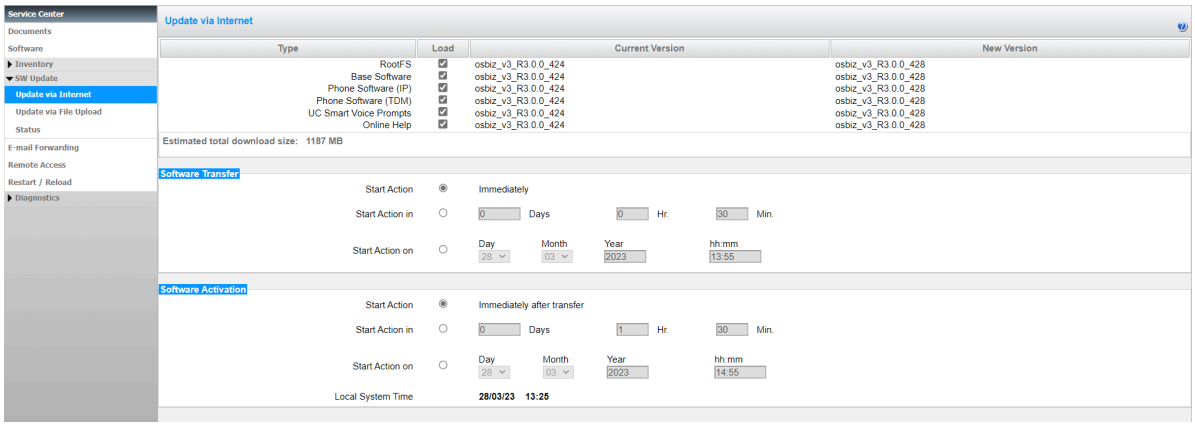
Hay disponible un acceso al servidor Web. De forma predeterminada, se establece conexión con el servidor Web de Internet. En lugar de ello, se puede configurar un servidor Web interno. (véase Uso de un servidor Web local).

Si la actualización se realiza a través de un servidor Web local, el archivo de imagen más actual debe guardarse en el servidor Web local.

Paso a paso

1) En la barra de navegación, haga clic en **Domicilio** y en el enlace **Puede obtener más detalles sobre los contenidos aquí: Enlace**. Se abre un archivo PDF con información importante sobre la nueva versión de software. Lea detenidamente la información y preste atención a la información sobre la actualización del sistema. A continuación, cierre la ventana.
2) En la barra de navegación, haga clic en **Centro de servicios**.
3) En el árbol de navegación, haga clic en **Actualización de software** > **Actualización a través de Internet**. Se muestra la versión de software instalada actualmente.
4) Haga clic en **OK y Continuar**.
5) Lea el acuerdo de licencia (EULA) y, a continuación, active el campo de opción **Acepto del acuerdo de licencia**.

6) Haga clic en **OK y Continuar**.



7) Si es necesario, en la columna **Cargar** desactive los paquetes que no desea actualizar. Por ejemplo, hay que hacerlo si las conexiones de Internet son lentas o se va a hacer una actualización de software mediante RDSI.

8) Seleccione los momentos de la transferencia y activación de software:

- **Iniciar acción - inmediatamente/inmed. tras transmisión**: el software se transfiere inmediatamente o se activa inmediatamente después de la transmisión. La actualización de software se carga en el sistema de comunicación en segundo plano. Después de reiniciar dos veces, el software está actualizado.
- **Iniciar acción en**: el software se transfiere o activa después de transcurrido un tiempo determinado. Indique el periodo en días, horas y minutos.
- **Iniciar acción el**: el software se transfiere o activa en un momento determinado. Indique la fecha y hora.

Nota: Si se alcanza el momento de la activación de software cuando la actualización todavía no se ha transferido del todo al sistema, la activación no se realiza automáticamente. En este caso hay que definir un nuevo momento de activación de forma manual.

---

9) Haga clic en **OK y Continuar**. La actualización de software se carga y activa en el sistema en segundo plano en el momento establecido. Para la activación de software el sistema se reinicia automáticamente dos veces seguidas.

Nota: Puede cerrar la ventana del navegador en cualquier momento.

---

10) Puede consultar el estado actual de la actualización con la Gestión basada en Web (WBM) en **Centro de servicios** > **Actualización de software** > **Estado**.

25.3.2.2 Cómo actualizar el sistema con un soporte USB

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

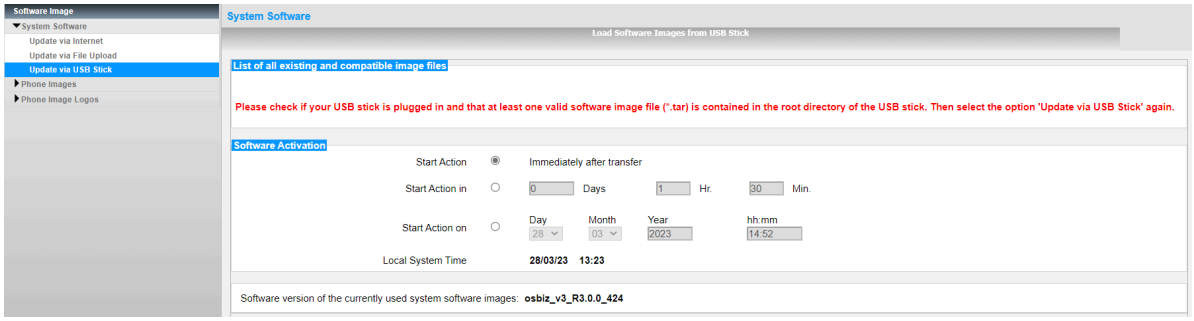
El soporte USB debe tener el formato FAT32.

Hay guardado un archivo de imagen actual en formato TAR en el soporte USB. También puede haber guardados varios archivos de imagen en distintos directorios.

Si el soporte USB tiene varias particiones, el archivo de imagen debe estar guardado en la primera partición.

Paso a paso

1) Inserte el soporte USB en la interfaz de servidor USB de la placa base.
2) En la barra de navegación, haga clic en **Modo Experto**.
3) En el árbol de navegación, haga clic en **Mantenimiento** > **Imagen de software**.
4) En el grupo de menús, haga clic en **Software del sistema**.
5) Haga clic en **Actualización via Stick USB**. Se muestran todos los archivos de imagen válidos guardados en el soporte USB, con el número de versión y el nombre de archivo.



6) Si hay guardados varios archivos de imagen, seleccione el archivo de imagen deseado; si no es así, el archivo de imagen está marcado automáticamente.
7) Seleccione el momento de la activación del software:
   - **Iniciar acción inmed. tras transmisión**: el software se activa inmediatamente después de la transferencia al sistema de comunicación.
   - **Iniciar acción en**: el software se transmite al sistema de comunicación de forma inmediata. El software se activa transcurrido un tiempo determinado. Indique el periodo en días, horas y minutos.
   - **Iniciar acción el**: el software se transmite al sistema de comunicación de forma inmediata. El software se activa en un momento determinado. Indique la fecha y hora.
8) Haga clic en **Cargar**. El archivo de imagen se transfiere al sistema de comunicación y se comprueba su coherencia. Para ambos procesos se requieren algunos minutos. Durante este tiempo, el soporte USB debe permanecer insertado.

9) Extraiga el soporte USB en cuanto lo indique la Gestión basada en Web (WBM) y haga clic en **Salir**. En el momento indicado de la activación de software se ejecutan consecutivamente dos reinicios de forma automática.

10) Puede consultar el estado actual de la actualización con la Gestión basada en Web (WBM) en **Centro de servicios** > **Actualización de software** > **Estado**.

25.3.2.3 Cómo actualizar el sistema mediante una carga de archivo

Requisitos previos

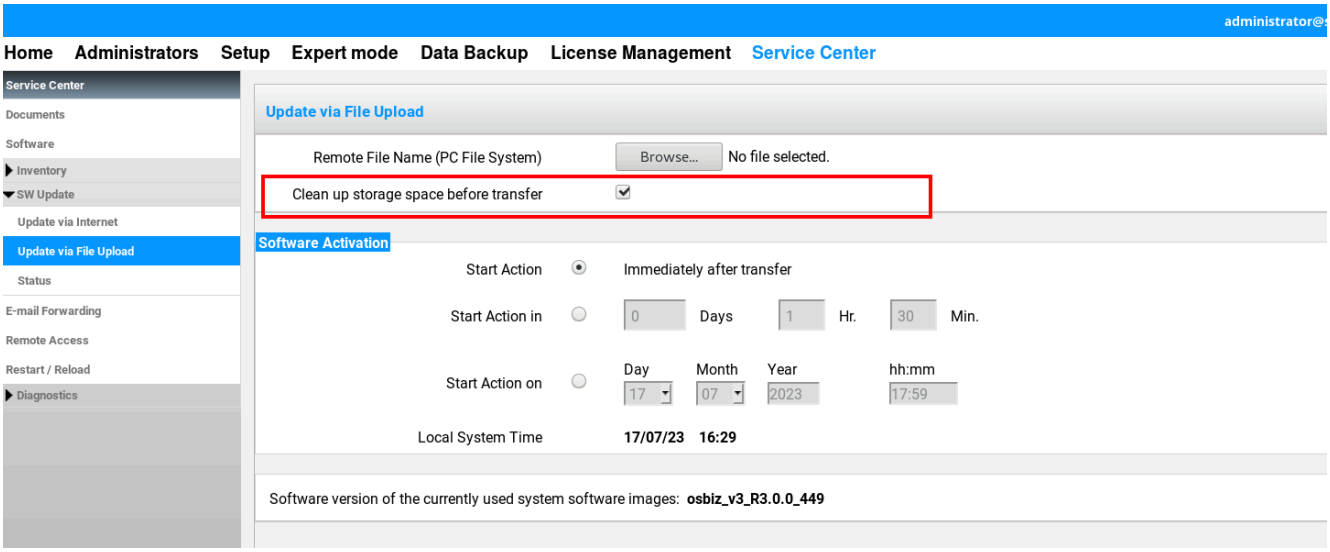
El archivo de imagen está depositado en la red interna en formato TAR o directamente en el PC de administración y se conoce la ubicación. Si hay un archivo TGZ, hay que extraer el archivo TAR del TGZ.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.

2) En el árbol de navegación, haga clic en **Actualización de software** > **Actualización a través de Carga de archivo**. Se muestra la versión de software instalada actualmente.

3) Haga clic en **OK y Continuar**.



4) Mediante el botón **Examinar** desplácese hasta la ubicación de almacenamiento del archivo de imagen (`*.tar`).

5) El flag **Limpiar el espacio de almacenamiento antes de la transferencia** está activado por defecto. Se activan las siguientes acciones, para liberar memoria de almacenamiento en preparación de la carga de archivos de software.

- Se eliminan todos los registros y rastros.
- Se borran todas las imágenes del software del teléfono.
- Se eliminan todos los volcados TCP.

6) Seleccione el momento de la activación del software:
   - **Iniciar acción inmed. tras transmisión**: El software se transmite inmediatamente al sistema de comunicación en segundo plano. Después de reiniciar dos veces, el software está actualizado.
   - **Iniciar acción en**: El software se transmite inmediatamente al sistema de comunicación en segundo plano. El software se activa transcurrido un tiempo determinado. Indique el periodo en días, horas y minutos.
   - **Iniciar acción el**: El software se transmite inmediatamente al sistema de comunicación en segundo plano. El software se activa en un momento determinado. Indique la fecha y hora.
7) Haga clic en **OK y Continuar**.
8) El archivo de imagen se transfiere al sistema de comunicación y se comprueba su coherencia. Para ambos procesos se requieren algunos minutos.

   Nota: Si cierra la ventana del navegador durante la transferencia de software, se interrumpe el proceso. Durante el control de consistencia puede seguir trabajando con la Gestión basada en Web (WBM) o cerrarla.
9) Si se va a activar el software inmediatamente, una vez hecha la comprobación de consistencia se hacen dos reinicios consecutivos.
10) Si el software no se activa de forma inmediata, una vez finalizada la transferencia haga clic en **Finalizar**. Para la activación de software el sistema se reinicia automáticamente dos veces seguidas.
11) Puede consultar el estado actual de la actualización con la Gestión basada en Web (WBM) en **Centro de servicios** > **Actualización de software** > **Estado**.

25.3.2.4 Cómo actualizar el sistema mediante un soporte USB sin acceso a la Gestión basada en Web (WBM)

Requisitos previos

El soporte USB debe tener el formato FAT32.

Hay un archivo de imagen actual en formato TAR guardado en el nivel de directorios superior del soporte USB. En ese nivel solo puede haber un archivo de imagen.

Si el soporte USB tiene varias particiones, el archivo de imagen debe estar guardado en la primera partición.

La versión de software del archivo de imagen debe ser más reciente que la del sistema. Atención: también se actualiza con versiones de software anteriores.

El sistema de comunicación está iniciado.

Paso a paso

1) Inserte el soporte USB en la interfaz de servidor USB de la placa base.

2) Mantenga pulsado el botón de Reset de 1 a 4 segundos. El sistema se apaga y se reinicia.

   Durante el arranque se comprueba el software. Si el soporte USB tiene un archivo de imagen adecuado, el archivo se carga en el sistema de comunicación. El LED rojo parpadea durante ese tiempo con impulsos de 1 Hz (0,5 s encendido/0,5 s apagado). Cuando finaliza el proceso de copia, se descomprime el software y los datos de cliente se aplican inmediatamente. Durante el proceso, el LED rojo parpadea con impulsos de 5 Hz (100 ms encendido/100 ms apagado).

3) Extraiga el soporte USB cuando el LED rojo parpadee con impulsos de 5 Hz.

4) Por último, el sistema se reinicia automáticamente dos veces seguidas. Cuando el LED verde parpadee con impulsos de 1 Hz (0,5 s encendido/0,5 s pagados) el sistema vuelve a estar listo para el servicio.

25.3.3 Actualización de los teléfonos de sistema

El software de los teléfonos del sistema se actualiza mediante un archivo de imagen. Hay un archivo de imagen propio por cada tipo de teléfono de sistema que incluye el software de teléfono de el tipo en cuestión. Estos archivos de imagen están incluidos en el software del sistema de comunicación y se cargan automáticamente en el sistema de comunicación al hacer una actualización.

De forma predeterminada, los teléfonos IP del sistema reciben automáticamente el software actualizado. Si en la Gestión basada en Web (WBM) se cambia la configuración de un teléfono de sistema IP (de **Cliente del sistema** a **Cliente SIP** o a la inversa), el software adecuado y almacenado en el sistema de configuración se carga automáticamente en el teléfono del sistema IP mediante el DLI. En los teléfonos del sistema que ya estaban operativos en el sistema o en otro sistema, hay que restablecer los ajustes de fábrica (Factory Reset) antes de ejecutar la actualización automática de software.

El administrador puede transferir software telefónico diferente del estándar a todos los teléfonos IP del sistema de un mismo tipo de forma manual. El software de los teléfonos del sistema UP0 se actualiza con el Manager E.

Si un software de teléfono (archivo de imagen) está marcado como estándar en Gestión basada en Web (WBM), la imagen se transfiere automáticamente a todos los teléfonos de sistema de ese tipo cuando se registren por primera vez en el sistema.

Al hacer una actualización manual, compruebe que el software de los teléfonos del sistema es compatible con la versión de software del sistema de comunicación (vea las notas de la versión).

Conceptos relacionados

Logotipos telefónicos en la página 1254

25.3.3.1 Cómo cargar el software de teléfono en el sistema

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Los archivos de imagen están almacenados en la red local y se conoce el lugar de almacenamiento. Se necesita un archivo de imagen propio para cada tipo de teléfono de sistema.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Imagen de software**.
3) En el grupo de menús, haga clic en **Imágenes de teléfono**.
4) Haga clic en **Cargar**. Aparece una lista con los archivos de imagen disponibles en el sistema de comunicación.
5) En **Nombre archivo remoto (sist. archivos PC)**, utilice **Examinar** para desplazarse al lugar de almacenamiento del archivo de imagen (`*.app`).
6) Haga clic en **Cargar**. Se carga el archivo de imagen y se comprueban errores.

Nota: En caso de error, podrá ver un mensaje de error. Compruebe los datos indicados y repita los pasos del 5 al 6.

---

7) Si la comprobación es positiva, confirme pulsando **Aceptar**. El archivo de imagen se incluye en la lista de los archivos de imagen disponibles en el sistema de comunicación.
8) Si desea cargar más archivos de imagen para otros tipos de teléfono de sistema, repita los pasos del 5 al 7.

25.3.3.2 Cómo distribuir el software telefónico a los teléfonos del sistema

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Imagen de software**.
3) En el grupo de menús, haga clic en **Imágenes de teléfono**.
4) Si desea distribuir una imagen de teléfono a todos los teléfonos de sistema de un tipo determinado:
   a) Haga clic en **Distribuir**. Aparece una lista con los archivos de imagen disponibles en el sistema de comunicación.
   b) Active la casilla de verificación **Distribuir** en las imágenes de teléfono deseadas.

5) Si desea distribuir una imagen de teléfono a un teléfono del sistema determinado:
   a) Haga clic en **Distribuir por dispositivo**. Aparecerá una lista de los teléfonos del sistema.
   b) En la lista desplegable **Software distribuible**, seleccione la imagen de teléfono para los teléfonos del sistema deseados.
6) Haga clic en **Aplicar**.

25.3.3.3 Cómo borrar el software telefónico

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Imagen de software**.
3) En el grupo de menús, haga clic en **Imágenes de teléfono**.
4) Haga clic en **Cargar**. Aparece una lista con los archivos de imagen disponibles en el sistema de comunicación.
5) En la línea de la imagen de teléfono que quiera borrar, active la casilla de verificación **Borrar**.
6) Si desea borrar más imágenes de teléfono, repita el paso anterior.
7) Haga clic en **Borrar**. Todas las imágenes de teléfono marcadas se eliminan del sistema de comunicación.

25.3.3.4 Cómo activar o desactivar la distribución automática del software telefónico

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Imagen de software**.
3) En el grupo de menús, haga clic en **Imágenes de teléfono**.
4) Haga clic en **Distribuir**. Aparece una lista con los archivos de imagen disponibles en el sistema de comunicación.
5) Si desea transferir el software telefónico automáticamente a los teléfonos del sistema, en la línea del archivo de imagen deseado active la casilla de verificación **Estándar** (ajuste estándar).
6) Si no desea transferir el software telefónico automáticamente a los teléfonos del sistema, en la línea del archivo de imagen deseado desactive la casilla de verificación **Estándar**.
7) Haga clic en **Aplicar**.

25.3.3.5 Cómo configurar la reactualización automática

El flasheo automático es una manera fácil de flashear el software HFA solo para el restablecimiento al funcionamiento original de fábrica. OpenScape Desk Phone IP 35G Eco y OpenScape Desk Phone CP 100/110/200/205/210/400/600/600E/700/700X/710, utilizando el servidor DLI del sistema.

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Nota: La reactualización automática solo es válida para dispositivos nuevos (de fábrica). En todos los demás dispositivos, hay que hacer una restauración ("restablecimiento de fábrica") para poder hacer una reactualización.

Paso a paso

1) Configure el dispositivo con un número y como cliente del sistema:
   a) En la barra de navegación, haga clic en **Modo Experto**.
   b) En el árbol de navegación, haga clic en **Servidor de telefonía > Extensión > Clientes IP**.
   c) En el campo **Nº llam**, introduzca el número interno.
   d) En el campo **N° llam. marc. directa** , introduzca el número público.
   e) Introduzca un nombre para el dispositivo.
   f) Seleccione **Cliente sist.** en el menú desplegable **Tipo**.
   g) Haga clic en **Aplicar**.

2) Configure el servidor DHCP para enviar la dirección IP del DLI mediante la opción DHCP:
   a) En la barra de navegación, haga clic en **Modo Experto**.
   b) En el árbol de navegación, haga clic en **Servidor de telefonía > Interfaces red > DHCP > Servidor DHCP > Editar parámetros globales**.
   c) Seleccione la opción **Utilizar DLI interno** en la sección **Servidor DNS**.

3) Conecte el dispositivo y especifique el número de terminal después de iniciar el teléfono.

4) El teléfono también se registra en la base de datos DLI. Para verificar el registro del dispositivo:
   a) En la barra de navegación, haga clic en **Modo Experto**.
   b) En el árbol de navegación, haga clic en **Mantenimiento > Imagen de software**.
   c) En el grupo de menús, haga clic en **Imágenes de teléfono**.
   d) Haga clic en **Distribuir por dispositivo**.

5) La reactualización automática comienza y carga en el dispositivo el software HFA almacenado en el sistema de comunicación.

Nota: No desconecte el dispositivo durante este proceso.

El dispositivo ya está configurado.

Nota: Si el dispositivo está configurado en SIP (en **Servidor de telefonía > Extensión > Clientes IP**), se actualizará con el software SIP más reciente, solamente si la actualización está disponible en la versión de software correspondiente.

Si un cliente SIP se convierte en cliente del sistema, hay que reiniciar el teléfono de forma manual para cargar el software HFA.

Nota: Si el proceso de reactualización no se completa correctamente, hay que restaurar los ajustes de fábrica (“restablecimiento de fábrica”) en el dispositivo.

25.3.4 Estado de software

El estado de software ofrece información sobre la versión de software y sus actualización.

Se pueden mostrar estos estados:

- Versión actual del software
- Hay una versión más reciente para actualizar
- Momento en el que se ejecutará la actualización de software
- El nuevo software se está cargando en el sistema
- Proceso de carga correcto o incorrecto

25.3.4.1 Cómo consultar el estado de software

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

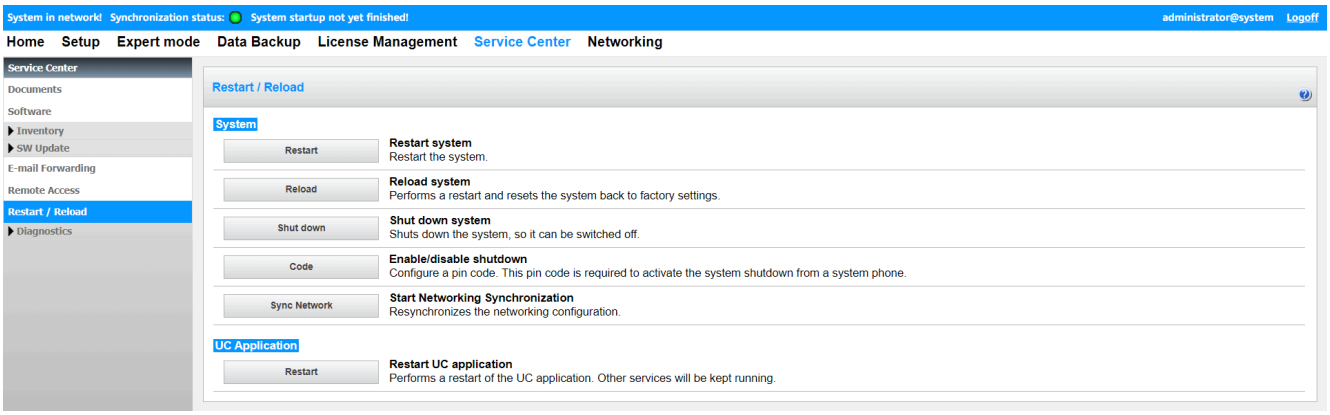
1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Actualización de software** > **Estado**. Podrá ver la versión actual del software. Esta información también aparece en la página de inicio de Gestión basada en Web (WBM).

   Se le informará si se está ejecutando una actualización de software en segundo plano.

   Se le informará si hay disponible una nueva actualización de software en el servidor Web. Esta información también aparece en la página de inicio de Gestión basada en Web (WBM).

25.4 Restart, Reload, Shutdown

A través de las funciones correspondientes se puede iniciar un reinicio (restart) y una recarga (reload) del sistema de comunicación OpenScape Business o de la tarjeta UC Booster Card. También se puede apagar de forma controlada (shutdown) el OpenScape Business X. Además se puede iniciar un reinicio (restart) de la aplicación de UC (UC Smart o UC Suite). Para poder hacer un apagado controlado de OpenScape Business X con un teléfono del sistema se puede definir un PIN.



Reiniciar y volver a cargar el UC Booster Server

Si además del sistema de comunicación se opera un UC Booster Server, también se puede reiniciar o volver a cargar el software de comunicación del UC Booster Server. El UC Booster Server se reinicia/recarga del mismo modo que el sistema de comunicación. La única diferencia es que al lanzar la Gestión basada en Web (WBM), el administrador no indica la dirección IP del sistema de comunicación sino la del servidor Linux.

Nota: Véase también Cómo eliminar o eliminar usuarios de Unify Phone en la página 1224.

25.4.1 Reinicio (Restart) de OpenScape Business

La función **Reiniciar sistema** permite reiniciar (Restart) de forma controlada OpenScape Business.

Hay que tener en cuenta las siguientes diferencias:

- OpenScape Business S y OpenScape Business X

  Se realiza un reinicio (Restart) controlado del sistema de comunicación. Después de la inicialización el sistema de comunicación vuelve a estar listo para el servicio.

  El tiempo de arranque depende de la estructura del sistema y del escenario de interconexión de OpenScape Business.

  Si OpenScape Business X3/X5/X8 equipa una tarjeta UC Booster Card (Tablero de aplicaciones OCAB), la aplicación de UC (UC Smart o UC Suite) se reinicia (Restart) de forma controlada.

- OpenScape Business UC Booster Server (servidor de aplicaciones)

  Se realiza un reinicio (Restart) controlado de la parte OpenScape Business y de la aplicación de UC (UC Suite). Tras la inicialización, la aplicación de UC vuelve a estar lista para el servicio.

Al reiniciar, se interrumpen las conexiones con todas las aplicaciones activas, por ejemplo, myPortal for Desktop y myAttendant. Una vez finalizado el inicio, se restablecen todas las condiciones automáticamente.

25.4.1.1 Cómo activar un reinicio (Restart) de OpenScape Business

La función **Reiniciar sistema** permite reiniciar (Restart) OpenScape Business.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Consejo: Al reiniciar, se interrumpen las conexiones con todas las aplicaciones activas, por ejemplo, myPortal for Desktop y myAttendant. Una vez finalizado el inicio, se restablecen todas las condiciones automáticamente.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Reiniciar / Volver a cargar**.
3) Haga clic en **Reiniciar sistema** y, a continuación, en **OK**. OpenScape Business se reinicia (Restart).

   OpenScape Business S y OpenScape Business X: Después de la inicialización, el sistema de comunicación vuelve a estar listo para el servicio.

   OpenScape Business UC Booster Server: Después de la inicialización, la aplicación de UC (UC Suite) vuelve a estar lista para pel servicio.

25.4.2 Recarga (Reload) de OpenScape Business

La función **Recargar sistema** permite volver a cargar (Reload) OpenScape Business.

Hay que tener en cuenta las siguientes diferencias:

- OpenScape Business S y OpenScape Business X

  Se realiza una recarga (Reload) del sistema de comunicación. Después de arrancar, el sistema de comunicación se encuentra en estado básico.

  – Todos los ajustes específicos del cliente y del país se eliminan (Distintivo de país del sistema = Alemania).
  – El sistema de comunicación tiene la dirección IP estándar 192.168.1.2 y el área de direcciones IP interna 192.168.3.xxx.
  – Se mantiene el registro de licencia.

  El tiempo de arranque depende de la extensión de sistema:.

- OpenScape Business UC Booster Server

  Se realiza una recarga de la parte OpenScape Business. Después de la inicialización la parte OpenScape Business se encuentra en estado básico.

  – Todos los ajustes específicos del cliente de la parte OpenScape Business (por ejemplo, el directorio de usuarios) se han borrado.
  – Se mantiene el registro de licencia.

  El sistema operativo no se restablece.

25.4.2.1 Cómo activar una recarga (Reload) de OpenScape Business

La función **Recargar sistema** permite activar una recarga (Reload) de OpenScape Business.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

OpenScape Business S y OpenScape Business X: Los datos de configuración del sistema de comunicación se han almacenado en un conjunto de copias de seguridad.

Nota:

La recarga restablece el sistema de comunicación al estado básico. Se eliminan todos los ajustes específicos del cliente y del país (Distintivo de país del sistema = Alemania). El sistema de comunicación recibe la dirección IP estándar 192.168.1.2.

OpenScape Business UC Booster Server: los datos de configuración de la parte de OpenScape Business están guardados en un conjunto de copias de seguridad.

Nota:

La recarga restablece la parte correspondiente a OpenScape Business al estado básico. Todos los ajustes específicos del cliente de la parte OpenScape Business (por ejemplo, el directorio de usuarios) se borran.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Reiniciar / Volver a cargar**.
3) Haga clic en **Recargar sistema** y, a continuación, en **Aceptar**. OpenScape Business se recarga.

Consejo: OpenScape Business S y OpenScape Business X: Después de arrancar, el sistema de comunicación se encuentra en estado básico. Una vez concluida la configuración de los ajustes básicos a través del asistente **Instalación inicial**, se pueden volver a cargar

los datos específicos del cliente y del país. Para obtener información sobre el procedimiento, consulte Recuperación.

OpenScape Business UC Booster Server: después del arranque, la parte de OpenScape Business está en el estado básico. Se pueden volver a cargar los datos específicos del cliente almacenados. Para obtener información sobre el procedimiento, consulte Recuperación.

25.4.3 Shutdown (apagado) de OpenScape Business X

Con la función **Apagar sistema** se puede iniciar un apagado controlado de los sistemas de comunicación OpenScape Business X.

25.4.3.1 Cómo apagar OpenScape Business X

La función **Apagar sistema** permite apagar de forma controlada los sistemas de comunicación OpenScape Business X.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Reiniciar / Volver a cargar**.
3) Haga clic en **Apagar sistema** y, a continuación, en **Aceptar**. El sistema de comunicación se apaga de forma controlada.

Consejo: OpenScape Business X1/X3/X5: El sistema de comunicación solo se puede volver a poner en servicio extrayendo y volviendo a enchufar la toma de red.

OpenScape Business X8: El sistema de comunicación solo se puede volver a poner en servicio apagando y volviendo a encender todas las fuentes de alimentación LUNA2.

25.4.4 PIN para el apagado controlado (Shutdown) de OpenScape Business X

La activación del apagado controlado mediante un teléfono del sistema está protegida por PIN.

En la activación mediante un teléfono del sistema siempre hay que introducir el PIN configurado en el sistema de comunicación. Este PIN lo configura un administrador con el perfil **Avanzado**.

25.4.4.1 Cómo configurar un PIN para el apagado controlado (Shutdown) de OpenScape Business X

El PIN permite activar un apagado controlado (Shutdown) con un teléfono del sistema.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Reiniciar / Volver a cargar**.
3) Haga clic en **Habilitar/Deshabilitar apagado**.
4) En el campo PIN, introduzca el **PIN** de seis dígitos deseado.
5) Haga clic en **Guardar** y a continuación en **Aceptar**.

Pasos siguientes

Para activar un apagado controlado (Shutdown) mediante un teléfono del sistema hay que introducir el código correspondiente (código estándar = *997) y a continuación introducir el PIN de seis dígitos.

- Para teléfonos IP: puede ejecutar el apagado controlado desde los primeros dos dispositivos configurados.
- Para teléfonos UP0: puede ejecutar el apagado controlado desde cada uno de estos teléfonos. En este caso, los clientes IP no tienen derechos para ejecutar un apagado.

25.4.5 Reiniciar (Restart) de la UC Booster Card (Tablero de aplicaciones OCAB)

La función Reiniciar tablero de aplicaciones permite a los administradores reiniciar de forma controlada el **Tablero de aplicaciones OCAB**, incluyendo la aplicación de UC (UC Smart o UC Suite).

Al reiniciar, se interrumpen las conexiones con todas las aplicaciones activas, por ejemplo, myPortal for Desktop y myAttendant. Una vez finalizado el inicio, se restablecen todas las condiciones automáticamente.

Además, también se reinician la interfaz CSTA, Presence Manager, Announcement Player, Media Extension Bridge y Open Directory Service.

25.4.5.1 Cómo iniciar un reinicio (Restart) de la UC Booster Card (Tablero de aplicaciones OCAB)

La función **Reiniciar tablero de aplicaciones** permite reiniciar (Restart) de forma controlada el tablero de aplicaciones OCAB, incluyendo la aplicación de UC (UC Smart o UC Suite).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Consejo: Al reiniciar, se interrumpen las conexiones con todas las aplicaciones activas, por ejemplo, myPortal for Desktop y myAttendant. Una vez finalizado el inicio, se restablecen todas las condiciones automáticamente.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Reiniciar / Volver a cargar**.
3) Haga clic en **Reiniciar tablero de aplicaciones** y a continuación en **OK**. La UC Booster Card (Tablero de aplicaciones OCAB) se reinicia (Restart).

25.4.6 Recarga (Reload) de la UC Booster Card (Tablero de aplicaciones OCAB)

Mediante la función **Recargar UC Booster Card** se puede iniciar una recarga del Tablero de aplicaciones OCAB, incluida la aplicación de UC (UC Smart o UC Suite).

La recarga de la UC Booster Card sirve para restablecer los ajustes de fábrica de la tarjeta y a continuación retirarla del sistema. Puede ser necesario, por ejemplo, si la tarjeta ya no se va a seguir utilizando en el sistema porque se ha cambiado al UC Booster Server o porque se va a utilizar la tarjeta en otro sistema OpenScape Business.

Todos los datos específicos del cliente y todos los datos del diagnóstico de la UC Booster Card se borran y el sistema se apaga. A continuación, el sistema de desconecta de la alimentación de red y se extrae la UC Booster Card.

Una vez extraída la UC Booster Card y reiniciado el sistema, hay que crear un nuevo conjunto de copias de seguridad, ya que los datos de configuración han cambiado y el conjunto de copias de seguridad anterior ya no es compatible. Si anteriormente se ha utilizado el disco duro de la UC Booster Card como soporte de copia de seguridad, hay que seleccionar otro soporte de copia de seguridad, por ejemplo, una unidad de red, un soporte de USB o un servidor FTP/FTPS (véase también el capítulo Guardar y Recuperar).

25.4.6.1 Cómo iniciar un recarga (reload) de la UC Booster Card (Tablero de aplicaciones OCAB)

La función **Recargar UC Booster Card** permite iniciar una recarga (Reload) del Tablero de aplicaciones OCAB, incluida la aplicación de UC (UC Smart o UC Suite).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Reiniciar / Volver a cargar**.
3) Haga clic en **Recargar UC Booster Card** y, a continuación, en **Aceptar**. La sesión de Gestión basada en Web (WBM) finaliza. Se restablecen los valores de fábrica de la tarjeta y, a continuación, el sistema se apaga.
4) En cuanto se apague por completo el RUN LED verde y los LED de controlador de la UC Booster Card, desconecte el sistema de la red eléctrica y retire la UC Booster Card (véase Guardar y Recuperar).

25.4.7 Reinicio (Restart) de la aplicación de UC

Con la función **Reiniciar aplicación UC** los administradores pueden iniciar (Restart) de forma controlada la aplicación de UC (UC Smart o UC Suite).

Al reiniciar la aplicación de UC, se interrumpen las conexiones con todas las aplicaciones activas (por ejemplo, myPortal for Desktop y myAttendant). Una vez finalizado el inicio, se restablecen todas las condiciones automáticamente.

25.4.7.1 Cómo activar un reinicio (Restart) de la aplicación de UC

La función **Reiniciar aplicación UC** permite reiniciar (Restart) de forma controlada la aplicación de UC (UC Smart o UC Suite).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Consejo: Al reiniciar, se interrumpen las conexiones con todas las aplicaciones activas, por ejemplo, myPortal for Desktop y myAttendant. Una vez finalizado el inicio, se restablecen todas las condiciones automáticamente.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Reiniciar / Volver a cargar**.
3) Haga clic en **Reiniciar aplicación UC** y a continuación en **Aceptar**. La aplicación de UC se reinicia (Restart).

25.5 Gestión de inventario

"Gestión de inventario" son las tareas destinadas a determinar el estado actual de los sistemas de comunicación OpenScape Business X y OpenScape Business S y de la configuración de hardware de los sistemas de comunicación OpenScape Business X.

25.5.1 Estado del sistema

El administrador puede determinar el estado actual de los sistemas de comunicación OpenScape Business X y OpenScape Business S mediante Gestión basada en Web (WBM). Se pueden recuperar informaciones sobre el estado de las extensiones, el establecimiento de conexión, los ITSP, VPN y la lista de direcciones IP configuradas.

Estado de extensión

El estado de extensión permite consultar esta información sobre las extensiones configuradas:

- Número de teléfono de extensión
- Nombre
- Tipo disposit.
- Dirección IP (en los teléfonos de sistema se muestra además un enlace con el que se puede abrir la Gestión basada en Web (WBM) del teléfono.)
- Dirección MAC
- Versión de software actual
- Versión de hardware
- Estado (Activado/Desactivado)

Estado del establecimiento de conexión

El estado del establecimiento de conexión permite consultar información relativa a las conexiones existentes con colaterales PSTN (Public Switched Telephone Network, tales como redes de telecomunicaciones privadas o públicas) del sistema de comunicación OpenScape Business X.

Estado de ITSP

El estado de ITSP permite consultar información sobre el estado actual de los ITSP (Internet Telephony Service Provider) configurados y agregados (si los hay). También aparecen indicadas los ITSP para los que están configuradas las extensiones.

El estado de cada ITSP activo aparece indicado con el color de sus respectivos rectángulos (verde = OK, naranja = como mínimo hay una extensión configurada sin errores).

Estado de la VPN

El estado de la VPN permite consultar informaciones sobre los túneles VPN configurados del sistema de comunicación OpenScape Business X.

Resumen de direcciones IP

Se muestran las direcciones IP configuradas en el sistema de comunicación OpenScape Business X.

Además se indica qué asistente y qué menús del Modo Experto permiten configurar las direcciones IP.

También se muestra un resumen del estado de la Booster Card y las interfaces Ethernet de la placa base.

25.5.1.1 Cómo consultar el estado de extensiones

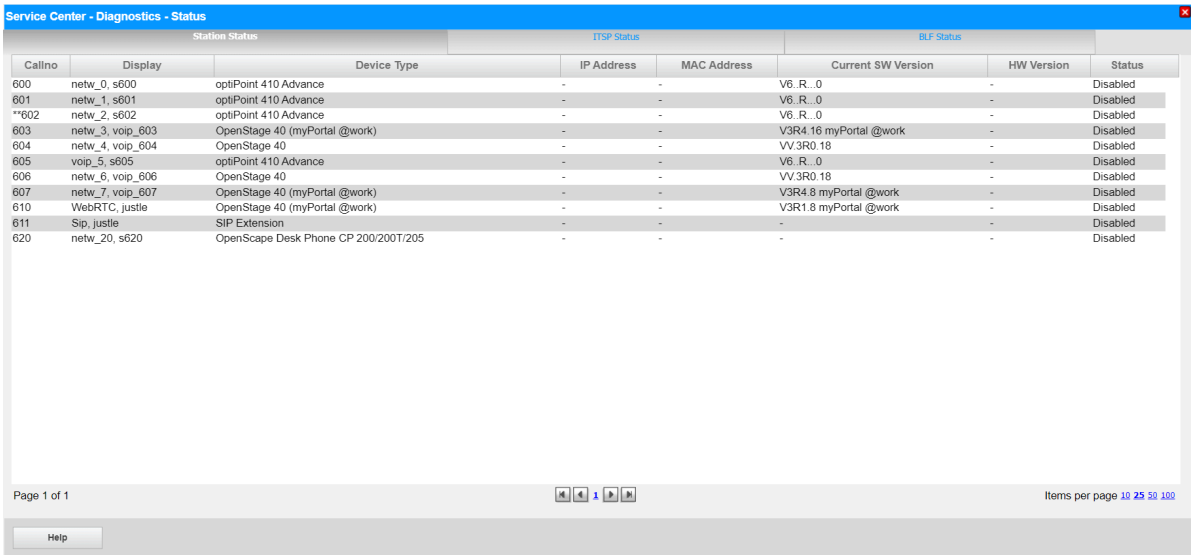
El asistente **Estado** permite registrar el estado actual de todas las extensiones configuradas.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Estado**.
3) Haga clic en la pestaña **Estado de extensión**. Aparece el estado de todas las extensiones configuradas.



4) Haga clic en **Salir**.

25.5.1.2 Cómo consultar el estado del establecimiento de conexión

El asistente **Estado** permite determinar el estado actual de los colaterales PSTN de un sistema de comunicación OpenScape Business X.

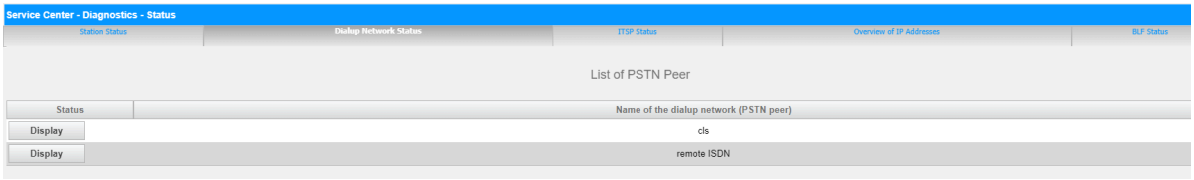
Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Estado**.
3) Haga clic en la pestaña **Estado de red de acceso telefónico**. Aparece la lista de los colaterales PSTN.

4) En la línea de la conexión deseada (Colateral PSTN) haga clic en **Mostrar**. Aparece el estado actual de la conexión (colateral PSTN).



5) Si desea consultar la información de estado de una nueva conexión (Colateral PSTN), siga el procedimiento descrito en el paso 3.
6) Haga clic en **OK** y, a continuación, en **Salir**.

25.5.1.3 Cómo consultar el estado de ITSP

El asistente **Estado** permite registrar el estado actual del ITSP (proveedor de servicios de telefonía por Internet).

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Estado**.
3) Haga clic en la pestaña **Estado ITSP**. Aparece el estado actual de los ITSP (Internet Telephony Service Provider) preconfigurados y agregados (si los hay) que estén activos.
4) Haga clic en **Diagnosticar** para obtener más información sobre la conexión SIP.
5) Haga clic en **Salir**.

25.5.1.4 Cómo mostrar direcciones IP

El asistente **Estado** permite consultar una vista general de las direcciones IP configuradas en un sistema de comunicación OpenScape Business X. Además se indica qué asistente y qué menús del Modo Experto permiten configurar las direcciones IP.

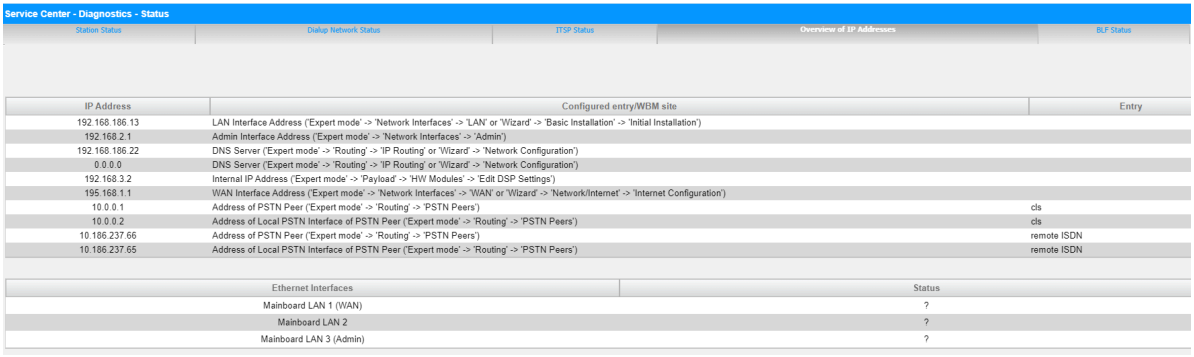
Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Estado**.

3) Haga clic en la pestaña **Resumen de direcciones IP**. Aparece un resumen de las direcciones IP configuradas en el sistema de comunicación.



4) Haga clic en **Salir**.

25.5.2 Inventario

El inventario permite a un administrador recuperar información sobre el hardware y el software de OpenScape Business X y el software de OpenScape Business S.

OpenScape Business X

Se pueden recuperar los siguientes detalles:

- Sistema de comunicación

  Entre otras cosas, se muestra la siguiente información:

  – Representación gráfica del sistema de comunicación y las tarjetas
  – Número de pieza de la placa base, dirección MAC, dirección IP, nombre de host y versión del software
  – Tipo de CPU y RAM (en GB) del sistema
  – Detalles sobre la cantidad de memoria, incluyendo el espacio disponible y utilizado en la tarjeta SDHC
  – Estado de todas las solicitudes
- Tableros

  La información mostrada incluye lo siguiente: ranura, tipo, número de pieza y estado de todas las placas instaladas.
- Tarjeta UC Booster (Tarjeta de Solicitud OCAB), si está disponible

  Entre otras cosas, se muestra la siguiente información:

  – Dirección MAC, dirección IP, nombre de host y versión de software
  – Detalles sobre la cantidad de memoria, incluyendo el espacio disponible y utilizado en el disco duro.
  – Estado de todas las solicitudes
  – Descripción general de todas las interfaces de Tarjeta de Refuerzo

  El enlace **Tarjeta de Refuerzo UC accesible** en la página de inicio de WBM, dirige al usuario a **Centro de Servicio >Inventario >Tarjeta de Refuerzo** para obtener una vista detallada. El enlace seguirá existiendo,

incluso si hay un problema con la Tarjeta de Refuerzo y el texto muestra **Tarjeta de refuerzo UC no accesible**.

Los siguientes mensajes de error se muestran en la página de inicio de WBM, dependiendo del error:

1) No es posible la conexión del circuito interintegrado con la tarjeta amplificadora
2) No es posible la conectividad con el protocolo de Internet v6 a la Tarjeta de Refuerzo
3) No es posible la conectividad con el protocolo de Internet v4 a la Tarjeta de Refuerzo
4) No es posible la conexión Secure Socket Shell a la Tarjeta de Refuerzo
5) No es posible la conectividad del sistema de archivos de red a la Tarjeta de Refuerzo
6) Una o más interfaces Ethernet están en modo semidúplex; se recomienda encarecidamente el modo dúplex completo

OpenScape Business S

Se pueden recuperar los siguientes detalles:

- Software

  Entre otras cosas, se muestra la siguiente información: Dirección MAC, dirección IP, nombre de host y versión de software.
- Información del disco duro

  Detalles sobre la cantidad de memoria, incluyendo la memoria disponible y la utilizada.
- Aplicaciones

  Se muestran todas las solicitudes y sus respectivos estados.

25.5.2.1 Cómo consultar el inventario de OpenScape Business X

El asistente **Inventario** permite determinar el estado actual del hardware y del software de los sistemas de comunicación OpenScape Business X.

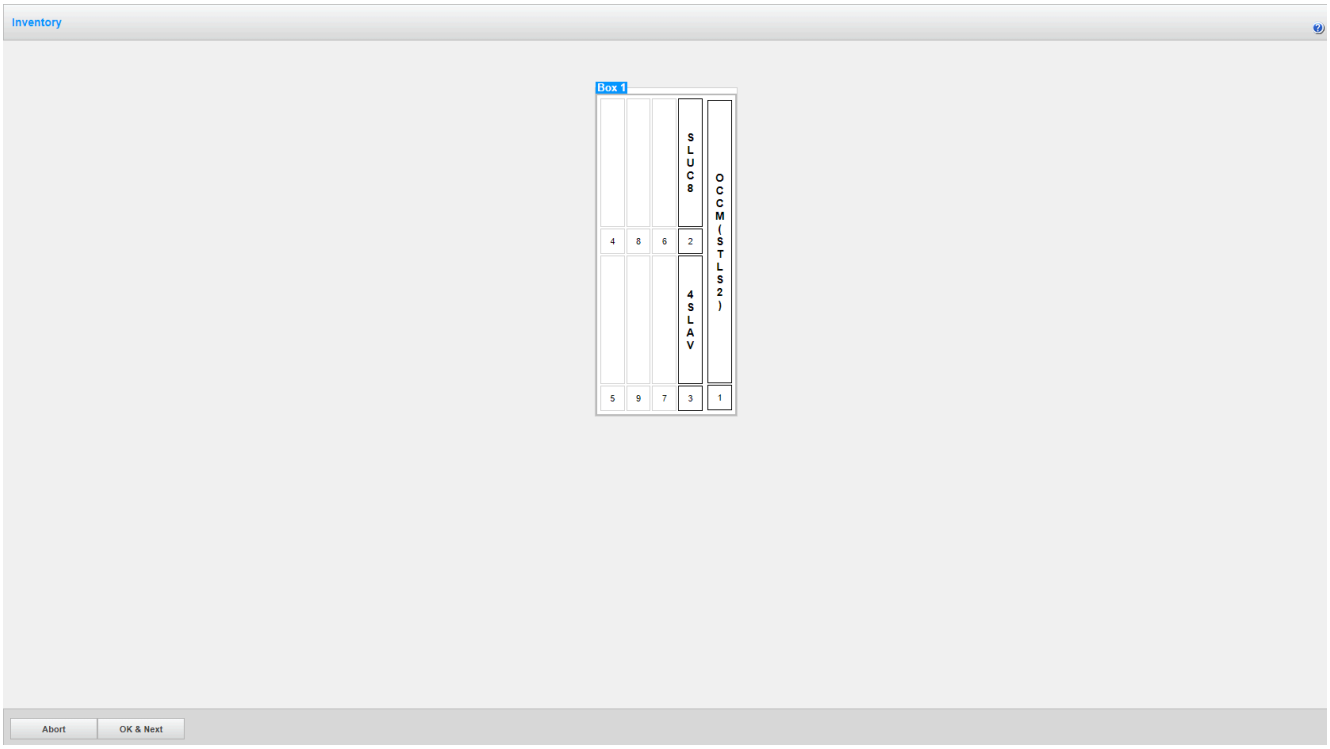
Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

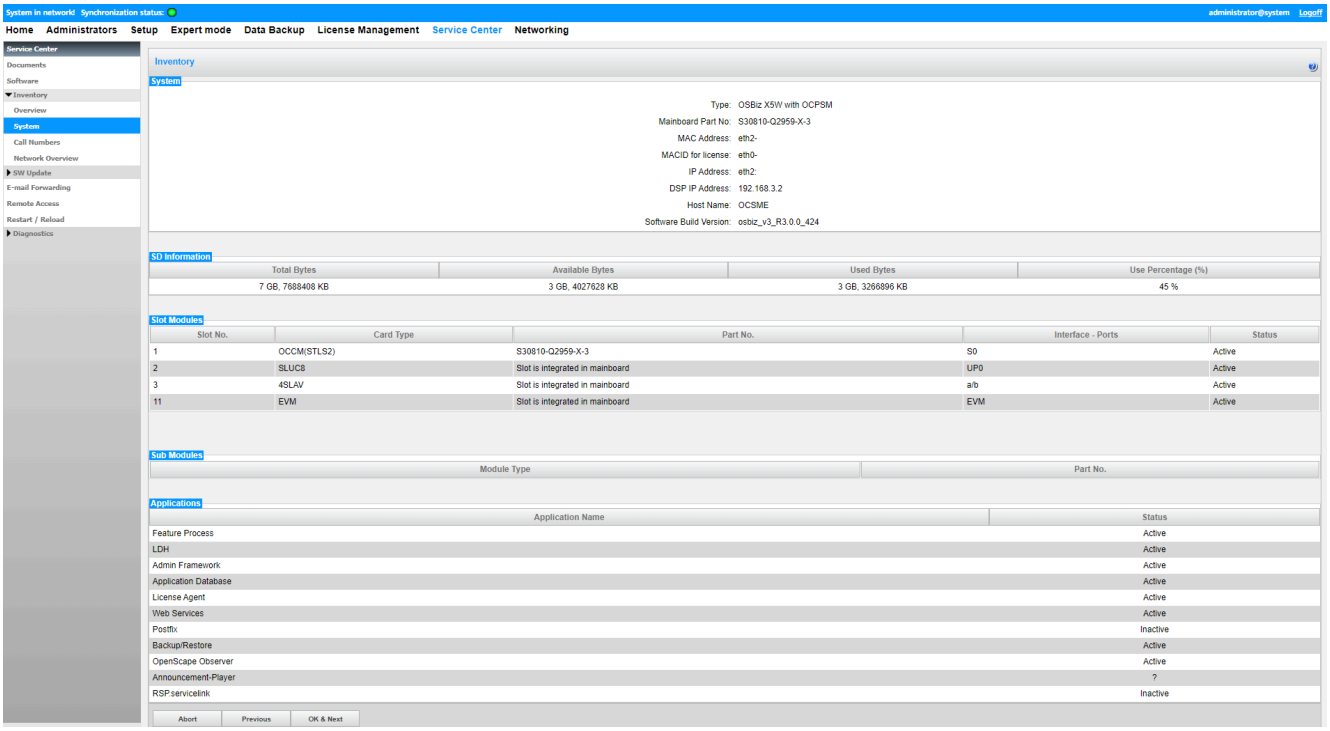
Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.

2) En el árbol de navegación, haga clic en **Inventario** > **Descripción general**. Se muestra una representación gráfica del sistema de comunicación y de los módulos.



3) Haga clic en **OK y Continuar**. Aparece información sobre el sistema de comunicación, sobre la memoria libre y en uso de la tarjeta SDHC, sobre los módulos y sobre el estado de la aplicación.



4) Haga clic en **OK y Continuar**. La información que aparezca a continuación depende de si el sistema de comunicación equipa una tarjeta UC Booster Card (Tablero de aplicaciones OCAB):
   a) Si su sistema de comunicación no está equipado con una Tarjeta UC Booster: Se muestra información sobre la asignación de números de llamada a los módulos.
   b) Si su sistema de comunicación está equipado con una Tarjeta UC Booster: Se muestra información sobre el módulo OCAB, sobre el espacio de almacenamiento disponible y utilizado en el disco duro y sobre el estado de la aplicación y de las interfaces de la Booster Card.

      Haga clic en **OK y Continuar**. Aparece información sobre la asignación de números de teléfono a los módulos.
5) Haga clic en **Finalizar**.

25.5.2.2 Cómo consultar el inventario de OpenScape Business S

El asistente **Inventario** permite consultar el estado actual del hardware y del software de OpenScape Business S.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Inventario**. Se muestra información sobre el software del sistema de comunicación, sobre el espacio libre y ocupado de los discos duros y sobre el estado de la aplicación.

25.6 Acciones automát.

Esta función permite definir acciones a ejecutar una vez o con regularidad. A continuación, el sistema de comunicación ejecuta dichas acciones en el momento determinado.

25.6.1 Acción automática Garbage Collection

La acción automática Garbage Collection permite realizar una limpieza de memoria automática en el sistema de comunicación periódicamente. Siempre que termina una limpieza de memoria, el sistema de comunicación se reinicia (Restart).

En la representación en el grupo de menús, el color de cada uno de los puntos de la lista indica el estado de la acción (verde = Acción activada, rojo = Acción no activada).

Seleccionando **Iniciar/Parar acción** se puede activar (iniciar) una acción no activa (de color rojo) y desactivar (parar) una acción activa (de color verde).

En la configuración estándar, la acción automática Garbage Collection no está activada.

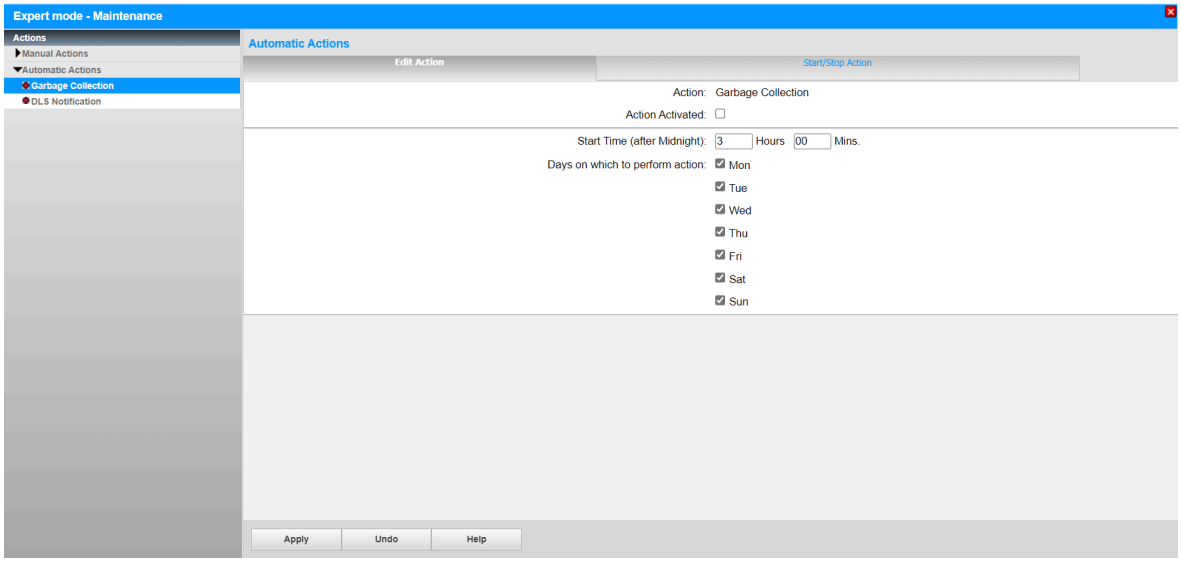
25.6.1.1 Cómo modificar la acción automática Garbage Collection

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Acciones**.
3) En el árbol de navegación, haga clic en **Acciones** > **Acciones automát.** > **Garbage Collection**.
4) Haga clic en la pestaña **Modificar acción**.



5) Seleccione el ajuste deseado:
   - Si desea que se ejecute la acción Garbage Collection, active la casilla de verificación **Acción activada**.
   - Si no desea que se ejecute la acción Garbage Collection, desactive la casilla de verificación **Acción activada**.
6) Si es necesario, modifique el **Inicio después de medianoche**.

   En el campo **Hrs.** indique las horas y en el campo **Min.** indique los minutos transcurridos los cuales se deberá iniciar la acción.

   Ejemplo: En el campo **h** se ha introducido `3` y en el campo **min.** `30`. Esto significa que la acción Garbage Collection se ejecutará mañana a las 3:30 h.
7) Si es necesario, modifique los días de la semana a través de **Ejecutar acción los sig. días de la semana**.

   Active la casilla de verificación de los días de la semana en los que se deberá ejecutar la acción. Desactive la casilla de verificación de los días de la semana en los que no se deberá ejecutar la acción.
8) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.6.1.2 Cómo iniciar la acción automática Garbage Collection (activación)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Acciones**.
3) En el grupo de menús, haga clic en **Acciones** > **Acciones automát.**. En el grupo de menús, aparecen los nombres de todas las acciones automáticas. Las acciones no activadas están identificadas con un punto de lista rojo. Las acciones activadas aparecen identificadas con un punto de lista verde.
4) En el grupo de menús, haga clic en **Garbage Collection**.
5) Haga clic en la pestaña **Iniciar/Detener acción**.
6) Haga clic en **Inicio** y a continuación en **Aceptar**.

25.6.1.3 Cómo detener la acción automática Garbage Collection (desactivación)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Acciones**.
3) En el grupo de menús, haga clic en **Acciones** > **Acciones automát.**. En el grupo de menús, aparecen los nombres de todas las acciones automáticas. Las acciones no activadas están identificadas con un punto de lista rojo. Las acciones activadas aparecen identificadas con un punto de lista verde.
4) En el grupo de menús, haga clic en **Garbage Collection**.
5) Haga clic en la pestaña **Iniciar/Detener acción**.
6) Haga clic en **Parada** y, a continuación, en **Aceptar**.

25.6.2 Acción automática Notificación DLS

La acción automática Notificación DLS permite iniciar el registro automático en un servidor DLS externo al arrancar el sistema de comunicación.

En la representación en el grupo de menús, el color de cada uno de los puntos de la lista indica el estado de la acción (verde = Acción activada, rojo = Acción no activada).

Seleccionando **Iniciar/Parar acción** se puede activar (iniciar) una acción no activa (de color rojo) y desactivar (parar) una acción activa (de color verde).

En la configuración estándar, la acción automática Notificación DLS no está activada.

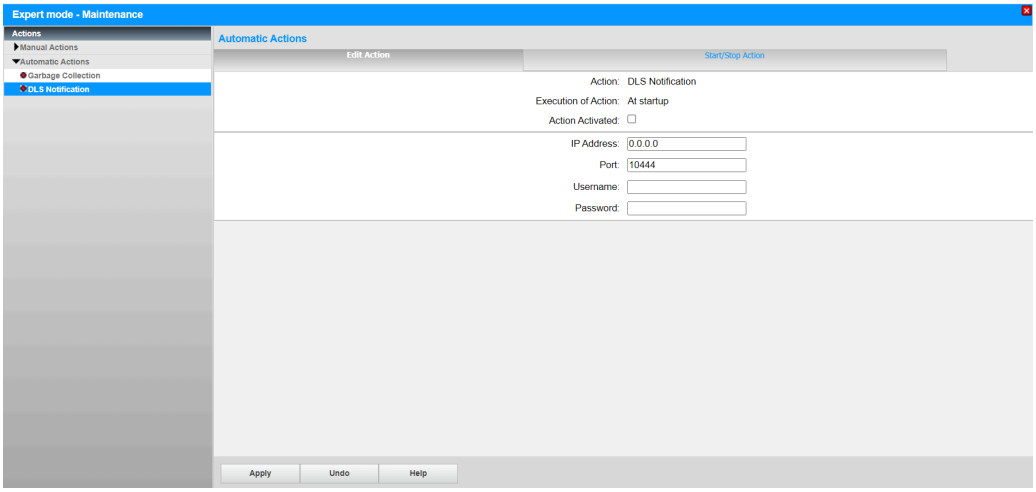
25.6.2.1 Cómo modificar la acción automática Notificación DLS

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Acciones**.
3) En el árbol de navegación, haga clic en **Acciones** > **Acciones automát.** > **Notificación DLS**.
4) Haga clic en la pestaña **Modificar acción**.



5) Seleccione el ajuste deseado:
   - Si desea que se ejecute la acción Notificación DLS, active la casilla de verificación **Acción activada**.
   - Si no desea que se ejecute la acción Notificación DLS, desactive la casilla de verificación **Acción activada**.
6) Si es necesario, en el campo **Dirección IP** modifique la dirección IP del servidor DLS externo.
7) Si es necesario, en el campo **Puerto**, modifique el puerto del servidor DLS externo.
8) Si es necesario, en el campo **Nombre de usuario** modifique el nombre de usuario para iniciar sesión en el servidor DLS externo.
9) Si es necesario, en el campo **Contraseña** modifique la contraseña para iniciar sesión en el servidor DLS externo.
10) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.6.2.2 Cómo iniciar la acción automática Notificación DLS (activación)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Mantenimiento** > **Acciones**.
3) En el grupo de menús, haga clic en **Acciones** > **Acciones automát.**. En el grupo de menús, aparecen los nombres de todas las acciones automáticas. Las acciones no activadas están identificadas con un punto de lista rojo. Las acciones activadas aparecen identificadas con un punto de lista verde.
4) En el grupo de menús, haga clic en **Notificación DLS**.
5) Haga clic en la pestaña **Iniciar/Detener acción**.
6) Haga clic en **Inicio** y a continuación en **Aceptar**.

25.6.2.3 Cómo detener la acción automática Notificación DLS (desactivación)

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Acciones**.
3) En el grupo de menús, haga clic en **Acciones** > **Acciones automát.**. En el grupo de menús, aparecen los nombres de todas las acciones automáticas. Las acciones no activadas están identificadas con un punto de lista rojo. Las acciones activadas aparecen identificadas con un punto de lista verde.
4) En el grupo de menús, haga clic en **Notificación DLS**.
5) Haga clic en la pestaña **Iniciar/Detener acción**.
6) Haga clic en **Parada** y, a continuación, en **Aceptar**.

25.6.3 Mecanismo de advertencia para la vida útil de la tarjeta SDHC

La acción automática "Mecanismo de advertencia para la vida útil de la tarjeta SDHC" es una forma de obtener información sobre el estado de mantenimiento de las tarjetas SDHC con una comprobación del sistema de archivos durante el arranque. Se inicia un asistente de la WBM que guía al técnico por todo el proceso de definir el momento en que el sistema debe reiniciarse y ejecutar la comprobación.

Nota: En caso de que la verificación no encuentre errores en el sistema de archivos, el **estado de la tarjeta** volverá a ser verde o amarillo incluso si se han notificado errores previamente.

Toda la información se registra en el Trace de cliente. La acción automática de mecanismo de advertencia para SDHC está desactivada de forma predeterminada

---

Nota: Esta opción activa un reinicio del sistema y muestra la alerta "`Nota: El sistema se reiniciará en cuanto pulse OK.`"

La pantalla de inicio de la WBM reconoce dos estados:

- Si la información del sistema está disponible, aparecerá un mensaje en la pantalla de inicio para informar del estado general de la tarjeta, **Estado de mantenimiento de la tarjeta** (verde, amarillo, rojo o gris).

  La vida útil general de la tarjeta se calcula según las especificaciones del fabricante y el promedio de ciclos de escritura del sistema. La vida útil de la tarjeta puede variar. Este dato se presenta junto con otra información en la página de comprobación de estado de SDHC en la WBM.

  La vida útil se estima en 4 años para tarjetas estándar y 10 años para tarjetas de larga duración.

  Nota: Los valores de vida útil estimados son una mera base para el mecanismo de advertencia del estado de mantenimiento de tarjeta integrado. Estos valores no implican automáticamente que una tarjeta sea defectuosa una vez superado el tiempo de vida útil.

  El estado verde indica que la tarjeta no ha alcanzado el fin de vida útil estimada y que no hay errores en el sistema de archivos.

  El estado amarillo significa que la tarjeta ha alcanzado el fin de la vida útil estimada.

  El estado rojo significa que hay más de 50 errores detectados en el sistema de archivos.

  El estado de mantenimiento gris significa que la tarjeta no es compatible o que no se puede recuperar información de la tarjeta. La tarjeta SDHC se debe sustituir por un tipo de tarjeta compatible.

  El mecanismo de advertencia para el estado amarillo se basa en la fecha de fabricación y la vida útil estimada para la tarjeta. Dado que las tarjetas pueden estar en stock durante un largo tiempo antes de empezar a utilizarse con OpenScape Business, la fecha de creación del sistema de archivos también se considera en el algoritmo de cálculo.

  A continuación, se muestra una tabla de cálculo del estado de una tarjeta con una vida útil estimada de 4 años.

Factor	**Años y ponderación**									
Fecha de fabricación	< 4 años	< 5 años		< 6 años		< 7 años		< 8 años		> 8 años
Antigüedad de sistema de archivos	< 4 años	< 4 años	4-5 años	< 4 años	4-6 años	< 3 años	3-7 años	< 2 años	2-8 años	-
Estado	Verde	Verde	Amarillo	Verde	Amarillo	Verde	Amarillo	Verde	Amarillo	Amarillo

- Si la información no está disponible, aparece el mensaje **Estado de mantenimiento de la tarjeta** desconocido.

  Nota: Si el sistema de archivos está dañado, se debe descargar una imagen de software del sistema adecuada desde el servidor de aprovisionamiento de software (SWS), y se debe copiar a la tarjeta SDHC usando la herramienta Card Manager. Después de haber iniciado el sistema con la tarjeta SDHC

nueva, se puede recuperar la configuración usando la copia de seguridad más reciente.

El mensaje "**Estado de mantenimiento de la tarjeta**" también incluirá un mensaje a la "página de acciones"

25.6.3.1 Cómo establecer una notificación en caso de errores en la tarjeta SDHC

En caso de que la función de verificación de archivos integrada notifique una cantidad de errores superior al umbral especificado (50 errores) o si el sistema no puede leer/escribir desde/hacia la tarjeta SDHC durante el funcionamiento normal, el sistema los notifica con un correo electrónico o evento SNMP.

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Sucesos**.
3) En el grupo de menús, haga clic en **Sucesos** > **Tabla reacción**. En el grupo de menús aparecen los nombres de Tabla reacción.
4) Seleccione **FP_EVT_HW_067** en el grupo de menús.
5) Seleccione una de las siguientes opciones disponibles:
   a) Enviar trap SNMP.
   b) Enviar e-mail.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Nota:

La dirección de correo electrónico debe configurarse en **Modo Experto > Mantenimiento > Sucesos > Correo electrónico.**

25.6.3.2 Cómo iniciar la acción automática "Mecanismo de advertencia para la vida útil de la tarjeta SDHC"

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) Guarde el sistema con la función de Copia de seguridad en un medio externo.
2) En la barra de navegación, haga clic en **Modo Experto**.
3) En el árbol de navegación, haga clic en **Mantenimiento** > **Acciones**.
4) En el grupo de menús, haga clic en **Acciones** > **Acciones automát.**. En el grupo de menús, aparecen los nombres de todas las acciones automáticas.

5) Haga clic en **Comprobación de mantenimiento SDHC** en el grupo de menús.

   Se muestran la fecha y la hora de **Hora del sistema local** y la **Última comprobación de estado**. También se muestra el contenido del **archivo de registro**.

6) Seleccione una de las siguientes opciones disponibles:
   a) Iniciar comprobación de mantenimiento inmediatamente.
   b) Iniciar comprobación de mantenimiento en una fecha determinada

7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.6.3.3 Cómo clonar y cambiar una tarjeta SDHC

Las tarjetas SDHC suelen tener una duración limitada. La vida útil depende principalmente del número de ciclos de escritura de la tarjeta SDHC. OpenScape Business tiene un mecanismo de detección de estado de mantenimiento SDHC para la vida útil de la tarjeta SDHC, y una función integrada de copia de seguridad de datos SDHC descrita a continuación para la sustitución de la tarjeta SDHC agotada y la creación de una tarjeta nueva totalmente operativa.

Nota: La función de copia de seguridad de datos SDHC puede copiar el contenido de la tarjeta SDHC actualmente insertada en el sistema sin tener que apagar este. Véase también Cómo eliminar o eliminar usuarios de Unify Phone en la página 1224.

Las copias de seguridad de los datos relevantes se pueden colocar en ubicaciones y soportes de almacenamiento diversos, como:

- Stick USB conectado al sistema.
- Lector USB de tarjetas SDHC conectado al sistema.
- Unidad Network File System (NFS).
- Unidad Network File System (NFS) vía USB.

Nota: Las opciones de stick USB o lector USB de tarjetas SDHC no están disponibles para OpenScape Business X1. En este caso, la copia de seguridad de datos SDHC debe almacenarse en una unidad NFS.

Si se utiliza un lector de tarjetas USB, cabe la posibilidad de que la tarjeta SDHC no sea accesible o formateable. De ser así, habrá que usar otro lector o stick USB.

Si se utiliza un lector USB con la nueva tarjeta SDHC insertada y conectado directamente al sistema, la función de copia de seguridad de datos SDHC integrada crea una tarjeta SDHC totalmente operativa. En los demás casos, se crea un archivo "tar" que contiene todos los datos del sistema y de configuración.

Nota: El archivo .tar no puede ser utilizado por la función de restauración del sistema.

El tamaño de la copia de seguridad de datos SDHC (archivo .tar) depende de los datos específicos del sistema y puede alcanzar varios GB si se almacenan archivos multimedia (mensajes de voz, registros de llamadas, etc.).

Para clonar y cambiar una tarjeta SDHC en un sistema activo, se debe seguir este procedimiento:

1) Crear un archivo de copia de seguridad de datos SDHC con un soporte adecuado (consulte Cómo crear un archivo de copia de seguridad de datos SDHC)
2) Cree una nueva tarjeta SDHC operativa que incluya todos los datos del sistema (consulte Cómo escribir con el Card Manager el software de comunicación en la tarjeta SDHC en la página 1371).
3) Apague el sistema, cambie la tarjeta SDHC y vuelva a encenderlo (consulte Cómo escribir con el Card Manager el software de comunicación en la tarjeta SDHC en la página 1371).

25.6.3.4 Cómo crear un archivo de copia de seguridad de datos SDHC

Requisitos previos

Un stick USB con al menos la misma capacidad que la tarjeta SDHC del sistema o un lector de tarjetas USB con una nueva tarjeta SDHC insertada cuyo tamaño sea al menos igual al de la tarjeta del sistema o una unidad Network File System (NFS) accesible desde el sistema.

Paso a paso

1) En la barra de navegación, haga clic en **Copia de seguridad de datos**.
2) Haga clic en **Copia de seguridad de datos SDHC** > **Copia de seguridad de datos** en el árbol de navegación.
3) Seleccione una de las siguientes opciones disponibles, según la ubicación y el soporte de medios disponible:
   a) NFS

      Se deben configurar una dirección de servidor válida, la ruta relevante y credenciales de inicio de sesión válidas.

      Haga clic en **Guardar y seleccionar**.

Nota: Hay disponible una copia de seguridad programada. Las acciones solo se pueden programar

de una en una y el usuario puede cambiar o cancelar la programación.

b) Lector de tarjeta

Esta opción crea una copia totalmente operativa de la tarjeta SDHC sin archivos de seguimiento y registro.

Antes de iniciar el proceso de copia, se debe conectar al sistema un lector USB de tarjetas SDHC con una tarjeta SDHC insertada.

Una vez iniciado el proceso, se formatea la tarjeta SDHC insertada y todos los archivos relevantes se transfieren a esa tarjeta.

Nota: No extraiga el lector USB de tarjetas SDHC ni la tarjeta SDHC insertada mientras se realiza el proceso.

Nota: La nueva tarjeta SDHC es totalmente operativa para su uso inmediato en el sistema OpenScape Business. La nueva tarjeta contiene todos los archivos y datos, excepto archivos de registro y seguimiento.

Nota: Hay disponible una copia de seguridad programada. Las acciones solo se pueden programar de una en una y el usuario puede cambiar o cancelar la programación.

c) NFS vía USB.

Se deben configurar una dirección de servidor válida, la ruta relevante y credenciales de inicio de sesión válidas.

Haga clic en **Guardar y seleccionar**.

Nota: Hay disponible una copia de seguridad programada. Las acciones solo se pueden programar de una en una y el usuario puede cambiar o cancelar la programación.

d) USB.

Debe haber un dispositivo USB vacío formateado con FAT32 conectado al sistema.

Nota: No extraiga el stick USB mientras se realiza el proceso.

Nota: El archivo de datos de copia de seguridad SDHC (archivo .tar) se puede utilizar en la herramienta Card

Manager para crear una tarjeta SDHC totalmente operativa para el sistema.

Nota: Hay disponible una copia de seguridad programada. Las acciones solo se pueden programar de una en una y el usuario puede cambiar o cancelar la programación.

4) Haga clic en **OK & Continuar**. Se abrirá una nueva ventana con el progreso del proceso de copia de seguridad.

Nota: Aparece un mensaje de error si no se puede montar el recurso compartido NFS o USB, o si no se puede formatear el soporte de almacenamiento.

5) El mensaje **Tarea de copia de seguridad finalizada correctamente** se muestra una vez realizado el proceso de copia del archivo de copia de seguridad.
6) Haga clic en **Finalizar**.

Nota: El proceso posterior dependerá de la ubicación de almacenamiento y el soporte elegidos.

En caso de utilizar el lector de tarjetas SDHC con una tarjeta SDHC, la nueva tarjeta SDHC puede utilizarse inmediatamente.

En los demás casos, el archivo de copia de seguridad de tarjeta SDHC generado debe utilizarse en combinación con la herramienta Card Manager para generar una nueva tarjeta SDHC.

Pasos siguientes

Siga el procedimiento de creación de una nueva tarjeta SDHC operativa y cámbiela en el sistema activo (consulte Cómo escribir con el Card Manager el software de comunicación en la tarjeta SDHC)

25.6.3.5 Cómo sustituir una tarjeta SDHC

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado).

Solo cuando se utiliza UC Suite: UC Suite se ha iniciado correctamente.

No se admite el paso a una versión de software anterior. Si se instala una tarjeta con software V2, solo se pueden recuperar versiones secundarias anteriores de V2.

Para evitar efectos secundarios, debe utilizarse la versión de software actual.

Nota: Si la tarjeta SDHC se rompe y el sistema se apaga, se debe utilizar una copia de seguridad anterior e ignorar los 10 primeros pasos del procedimiento siguiente. Véase también

Cómo eliminar o eliminar usuarios de Unify Phone en la página 1224.

Paso a paso

1) En la barra de navegación, haga clic en **Almacenamiento de datos**.
2) En el árbol de navegación, haga clic en **Guardar - inmediatamente.**
3) En el campo **Comentario**, introduzca un comentario para el conjunto de copias de seguridad. Este comentario permitirá identificar con mayor facilidad el conjunto de copias de seguridad en caso de que sea necesaria una recuperación. Al hacer la entrada evite el uso de diéresis y caracteres especiales.
4) Si quiere crear un conjunto de copias de seguridad, incluyendo mensajes de voz y anuncios grabados, active la opción **Copia de seguridad completa**.
5) En el área **Equipo**, active la unidad de destino en la que desea guardar el conjunto de copias de seguridad.
6) Haga clic en **OK y Continuar**. Se abrirá una nueva ventana con el progreso del proceso de guardado.

   Nota: Si el botón **OK&Continuar** no está activo (en gris), significa que no se han iniciado correctamente todas las aplicaciones (p. ej. UC Suite) cuyos datos se quieren copiar.

   Si no tiene autorización para el directorio de archivo comprimido seleccionado, aparecerá un mensaje de error. Seleccione otra unidad de destino o modifique la ruta del archivo comprimido.

   Si la unidad de destino no tiene suficiente espacio de almacenamiento libre para el conjunto de copias de seguridad, aparecerá un mensaje de error. Seleccione otra unidad de destino o borre un conjunto de copias de seguridad e inicie de nuevo la copia de seguridad.

   Nota: Si utiliza como soporte de copia de seguridad un soporte USB, espere hasta que el LED de dicho soporte deje de parpadear. Sólo entonces habrá finalizado correctamente la copia de seguridad en el soporte USB. A continuación, extraiga el soporte USB.

   Nota: Además del conjunto de copias de seguridad, hay que guardar un archivo de texto relativo al conjunto de copias de seguridad. Este archivo incluye información sobre la fecha y la hora de la copia de seguridad y la versión de software con la que se hizo.
7) La copia de seguridad se ha realizado correctamente si aparece el mensaje **¡La copia de seguridad se ha realizado con éxito! 100 %** .
8) Si ha seleccionado **HTTPS** como medio de copia de seguridad, guarde el conjunto de copias de seguridad y el archivo de texto correspondiente al conjunto de copias de seguridad en el lugar que desee. En los

demás medios de copia de seguridad, la ubicación se selecciona automáticamente. La ventana del navegador seguirá abierta hasta que concluya el proceso de guardado del conjunto de copias de seguridad del archivo de texto.

9) Haga clic en **Salir**.

10) Apague el sistema.

11) Extraiga la tarjeta SDHC existente.

12) Instale la nueva tarjeta SDHC.

13) Encienda el sistema.

Si se instala una tarjeta SDHC nueva, se instala automáticamente en el sistema la versión de software incluida en la tarjeta con la configuración predeterminada. Después de arrancar, el sistema tendrá la dirección IP predeterminada.

14) En la barra de navegación, haga clic en **Almacenamiento de datos**.

15) En el árbol de navegación, haga clic en **Recuperar**.

16) En la sección **Equipo**, active el medio que contiene el conjunto de copias de seguridad que desea recuperar.

17) Si ha activado **HTTPS** como medio de copia de seguridad, desplácese hasta el lugar de almacenamiento del conjunto de copias de seguridad y seleccione el conjunto de copias de seguridad. A continuación, desplácese hasta el lugar de almacenamiento del archivo de texto y selecciónelo.

18) Si ha activado un medio de copia de seguridad que no es **HTTPS**, en el área Lista de conjuntos de copias de seguridad disponibles, seleccione el conjunto de copias de seguridad que contiene los datos de configuración que desea recuperar.

19) Espere hasta que los archivos terminen de cargarse en el sistema y, a continuación, haga clic en **OK & Continuar**. Se inicia el restablecimiento de los datos de configuración. Se muestra el progreso de la recuperación.

20) Cuando aparezca el mensaje **¡La recuperación ha finalizado!**, el sistema se reiniciará automáticamente. Cuando el sistema vuelva a estar en servicio, la recuperación habrá concluido correctamente.

Nota: Después de la recuperación, el dispositivo debe eliminarse del servidor RSP y luego debe reconfigurarse.

25.7 Gestión de energía

La gestión de energía pone automáticamente el sistema de comunicación en modo de ahorro de energía en función de la carga del sistema. Así se reduce el consumo de energía del sistema y se protege el medio ambiente. Se puede configurar el horario en el que el sistema puede pasar al modo de ahorro de energía (p.ej., por la noche).

La gestión de energía solo se puede activar si las interfaces LAN del sistema están en el modo Ethernet-Link **Auto**. En el modo de ahorro de energía, las interfaces LAN del sistema de comunicación cambian automáticamente al modo dúplex completo de 100Mbit/s. Las interfaces LAN de la infraestructura conectada también deben estar en modo de detección automática.

Modos de servicio

- Modo activo (Active Mode)

  En el modo activo se utilizan las funciones del sistema de comunicación y entre el sistema y la infraestructura conectada se produce una transferencia de datos significativa.
- Modo de espera (Idle Mode)

  En modo de espera apenas se utilizan funciones del sistema de comunicación y entre el sistema y la infraestructura conectada no hay una transferencia de datos significativa. Si se inicia una función, el sistema cambia del modo de espera al modo activo.
- Modo de ahorro de energía (Low Power Mode)

  El modo de ahorro de energía tiene un consumo de energía más bajo que el modo de espera. El sistema se encuentra en el modo dúplex completo de 100Mbit/s.

También es posible operar el sistema permanentemente en el modo Ethernet-Link de dúplex completo 100Mbit/s o semidúplex 100Mbit/s.

25.7.1 Cómo activar o desactivar la gestión de energía

Requisitos previos

La interfaz LAN de la placa base mediante la que el sistema se conecta con la interfaz LAN se encuentra en el modo Ethernet-Link **Auto**.

Solo si hay insertada una UC Booster Card: la interfaz LAN de la UC Booster Card, mediante la que la UC Booster Card se conecta con la interfaz LAN, se encuentra en el modo Ethernet-Link **Auto**.

Las interfaces LAN de la infraestructura conectada (p.ej. teléfonos IP) se encuentran en modo de detección automática.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.

2) En el árbol de navegación, haga clic en **Asistentes** > **Configuración básica**.

3) Haga clic en **Editar** para iniciar el asistente **Gestión de energía**.

4) Si desea activar la gestión de energía:

a) Active la casilla de verificación **Activar/Desactivar la gestión de energía**.

b) En **Comienzo del modo de ahorro de energía** y **Final del modo de ahorro de energía** indique el intervalo de horas durante el que el sistema de comunicación debe cambiar al modo de ahorro de energía.

5) Si desea desactivar la gestión de energía, desactive la casilla de verificación **Activar/desactivar la gestión de energía**.

6) Haga clic en **OK & Continuar**. Se aplican los ajustes.

7) Haga clic en **Salir**.

25.7.2 Cómo modificar el modo Ethernet-Link de las interfaces LAN

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Telefonía** > **Interfaces de red**.

3) Seleccione el modo Ethernet-Link para la interfaz LAN de la placa base:

a) En el grupo de menús, haga clic en **Placa base** > **LAN 2**. El sistema se conecta con la infraestructura LAN mediante la interfaz LAN 2.

b) Si desea desactivar la gestión de energía, en la lista desplegable **Modo Ethernet-Link** seleccione la entrada **Auto**.

c) Si desea poner el sistema permanentemente en el modo de ahorro de energía, en la lista desplegable **Modo Ethernet-Link**, seleccione la entrada **100HDX** o **100FDX**.

Nota:

Con los modos Ethernet-Link **100HDX**, **100FDX** y **1000FDX** no se puede activar la gestión de la alimentación.

---

d) Haga clic en **Aplicar**.

4) Solo si hay insertada una UC Booster Card: seleccione el modo Ethernet-Link para la interfaz LAN de la UC Booster Card:

a) En el grupo de menús, haga clic en **Tablero de aplicaciones** > **LAN 2** o **LAN 1**, según la interfaz LAN que se use para conectar la UC Booster Card con la infraestructura LAN (indicada por el signo de verificación de la casilla **Interfaz activada**).

b) Si desea desactivar la gestión de energía, en la lista desplegable **Modo Ethernet-Link** seleccione la entrada **Auto**.

c) Si desea poner el sistema permanentemente en el modo de ahorro de energía, en la lista desplegable **Modo Ethernet-Link**, seleccione la entrada **100HDX** o **100FDX**.

Nota:

Con los modos Ethernet-Link **100HDX**, **100FDX** y **1000FDX** no se puede activar la gestión de la alimentación.

---

d) Haga clic en **Aplicar**.

25.8 Supervisión y mantenimiento de OpenScape Business

OpenScape Business ofrece distintas funciones para supervisar el estado actual del sistema, y localizar y resolver errores.

25.8.1 Comprobación de una conexión de red de OpenScape Business X

Una solicitud de ICMP (Internet Control Message Protocol) permite comprobar la conexión de red entre el sistema de comunicación OpenScape Business X y la dirección de destino mediante paquetes de solicitud eco.

Los paquetes de solicitud eco se pueden enviar mediante la función **Ping** y mediante la función **Traceroute**. Los mensajes de respuesta se visualizan junto con los tiempos de ida y vuelta.

Mediante la función **Traceroute** se envían los paquetes de solicitud eco con distintos valores TTL (Time-To-Live) crecientes.

25.8.1.1 Cómo enviar ping

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Diagnóstico de IP**.
3) En el grupo de menús, desplácese hasta **Placa base** > **Solicitud ICMP** > **Ping**.
4) En el campo **Dir. destino**, indique la dirección IP del destino deseado.
5) En el campo **Cant. de solicit. eco por enviar**, indique la cantidad deseada (valor estándar = 3).
6) Haga clic en **Enviar**.

   A continuación, se muestran los mensajes de respuesta junto con los tiempos de ida y vuelta.

25.8.1.2 Cómo comprobar Traceroute

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Diagnóstico de IP**.
3) En el grupo de menús, desplácese hasta **Placa base** > **Solicitud ICMP** > **Ejecutar traceroute**.
4) En el campo **Dir. destino**, indique la dirección IP del destino deseado.
5) En el campo **Byte TOS**, indique el valor deseado (valor estándar = 0).
6) Haga clic en **Enviar**.

   A continuación, se muestran los mensajes de respuesta junto con los tiempos de ida y vuelta.

25.8.2 SNMP (Simple Network Management Protocol)

El SNMP (Simple Network Management Protocol) es un protocolo de redes que permite supervisar y controlar los componentes de red (por ejemplo, router, servidor, conmutadores, impresora, PC) desde una extensión central (consola de administración). El protocolo controla la comunicación entre los componentes supervisados y la extensión de supervisión.

SNMP describe la estructura de los paquetes de datos que pueden enviarse, y el proceso de comunicación. SNMP fue diseñado para que todos los dispositivos con capacidad de red pudieran ser incluidos en la supervisión. Entre las tareas de la administración de red por SNMP se incluyen

- la supervisión de componentes de red,
- el control y configuración remotos de componentes de re,
- la identificación y notificación de errores.

Para la supervisión se utilizan los denominados "agentes". Se trata de programas que se ejecutan directamente en los componentes supervisados. Estos programas pueden registrar el estado de los componentes y realizar por sí mismos ajustes de configuración o activar acciones. SNMP permite a la consola de administración central comunicarse con los agentes a través de una red.

Nota: OpenScape Business admite SNMPv2c, pero también responde a consultas SNMPv1 snmpget.

Bases de datos de información de gestión MIB

El volumen de datos que puede administrarse por SNMP se establece en las bases de datos de información de gestión (MIBs). Las MIB son modelos de datos que describen de forma preestablecida los componentes de red a ser administrados. La MIB de los sistemas de comunicación OpenScape Business X se puede descargar mediante la Gestión basada en Web (WBM) (Centro de servicios).

Los sistemas de comunicación disponen de un agente SNMP propio que permite acceder auna serie de datos de sistema almacenados en su base de datos de información de gestión (MIB). La MIB proporciona informaciones básicas de sistema, informaciones de estado, datos relativos a sucesos e informaciones sobre el hardware instalado (slots) y conexiones configuradas (puertos).

El protocolo SNMP permite la supervisión y administración centralizadas de los componentes de red, incluyendo los propios sistemas de comunicación. De este modo es posible

- comunicarse con un sistema de comunicación por TCP/IP.
- acceder a datos a través de aplicaciones de administración externas.
- implementar tareas de mantenimiento remoto.
- visualizar el estado de servicio del sistema de comunicación.
- transmitir fallos relevantes para el servicio (traps).

Comunidades

El acceso a los datos SNMP (MIB) se controla por comunidades. Se distingue aquí entre comunidades de lectura, de escritura y Trap. Cada comunidad tiene una dirección IP.

Para, por ejemplo, permitir a un PC el acceso de lectura a los datos SNMP (MIB), hay que registrar su dirección IP en la lista de comunidades de lectura. Para obtener acceso de lectura y escritura, la dirección IP debe registrarse en la lista de comunidades de escritura.

Las comunidades Trap se utilizan para administrar a los destinatarios de los mensajes de error (Traps).

Traps

Las traps se generan en caso de problemas del sistema de comunicación y su función es informar de errores y fallos de funcionamiento. Estos son los tipos de traps:

- Traps de sistema = Errores de sistema que necesitan medidas de resolución inmediatas.
- Traps de rendimiento = Informaciones sobre problemas de rendimiento, que no necesitan ser resueltos.

Las traps se clasifican por su efecto y las puede consultar un administrador con el perfil **Experto** a través de Gestión basada en Web (WBM). Se muestra una lista de todas las traps recibidas. La lista incluye esta información:

Columna	Significado
VarBind1 (Severidad)	Clase de efecto de la trap Estas son las entradas posibles: Crítico: Mensaje de error El error es causa de problemas. Mayor: (Major) Mensaje de error. El error puede tener causar problemas. Menor: (Minor) Mensaje de error. El error no causa problemas. Advertencia: (Warning) Mensaje sobre un procedimiento o estado potencialmente problemático, pero ningún mensaje de error. Eliminado Información: (Information) Mensaje de estado puro, ningún mensaje de error. Estado intermedio Otras traps
VarBind2 (Nombre)	Nombre de la trap
Nombre genérico	Designación general como, por ejemplo Enterprise Specific
Nombre específico	Tipo de la trap (1 = Software, 2 = Hardware)
Empresa	–

Columna	Significado
Tiempo	Momento del error
Índice	Número de lista

La presentación de las trapas se actualiza cada 30 segundos. Las traps se ordenan según su orden de aparición.

Al pulsar sobre un nombre de trap aparecen los datos detallados de la misma.

Código SNMP	Entrada en el protocolo de sucesos	Significado	Medidas necesarias	Observación
Clase de error 01 - Mensajes generales				
	Reinicio del sistema	Reinicio completo (restablecimiento) de todo el sistema con el CDB actual.	Ninguno	
FP_EVT_ADM_002	recarga de slot firmado	recarga de slot firmado		
FP_EVT_ADM_003	reinicio del sistema	reinicio del sistema		
FP_EVT_ADM_010	Reinicio del sistema SNMP	Reinicio de todo el sistema a través de SNMP.	Ninguno	
FP_EVT_ADM_014	Cambios en la base de datos local SNMP	Cambios "in situ" en la base de datos.	Ninguno	
FP_EVT_ADM_015	Cambios en la base de datos remota SNMP	Cambios "remotos" en la base de datos.	Ninguno	
FP_EVT_ADM_016	Resultado SNMP APSXF	Mensaje de acuse de recibo de transferencia APS a través de SNMP.	Ninguno	
FP_EVT_ADM_017	Fallo de autenticación SNMP	Intento de acceso no autorizado.	Compruebe la configuración del firewall en OpenScape Business/ Manager E (Firewall de red).	
FP_EVT_ADM_019	Sensor de alarma	La temperatura de la carcasa de OpenScape Business es demasiado alta.	Compruebe el ventilador y el suministro de aire en la carcasa de 19'. Tenga en cuenta la temperatura ambiente.	
FP_EVT_ADM_020	Límite del búfer CDR alcanzado	Desbordamiento en el búfer CDR (información CDR).	Compruebe que las interfaces (V.24, LAN), los puertos y la conexión funcionan o lea los datos de la llamada.	

Código SNMP	Entrada en el protocolo de sucesos	Significado	Medidas necesarias	Observación
FP_EVT_ADM_024	aplicación no autorizada	Intento de acceso a través de una aplicación no autorizada.	Compruebe la configuración del firewall en OpenScape Business/ Manager E (Firewall de red).	
FP_EVT_ADM_025	conmutación manual desde HiPath Manager			
Clase de error 02 - Mensajes de gestión de licencias				
Clase de error 09 - Mensajes del módulo de hardware				
FP_EVT_HW_034	pérdida de trama activada (STMD)	pérdida de trama activada (STMD)		
FP_EVT_HW_035	pérdida de trama desactivada (STMD)	pérdida de trama desactivada (STMD)		
FP_EVT_HW_036	deslizamiento detectado (STMD)	Se ha producido un deslizamiento de bits en una línea RDSI.	Compruebe la línea S0. Si es necesario, vuelva a cargar la placa o realice un reinicio completo. Si el error persiste, establezca una traza RDSI.	El problema puede deberse a la asincronía de las frecuencias de reloj interna y externa. Posible pérdida de datos/conexión interrumpida.
FP_EVT_HW_039	señal de indicación de alarma error desactivada (TMS2M)	Indicación de alarma: Se ha corregido el error S2M.	Ninguno	
FP_EVT_HW_040	error por minuto degradado activado (TMS2M)	error por minuto degradado activado (TMS2M)		
FP_EVT_HW_041	error por minuto degradado desactivado (TMS2M)	error por minuto degradado desactivado (TMS2M)		
FP_EVT_HW_042	ningún error de señal activado (TMS2M/ STMD)	Indicación de alarma: Se ha producido un error S2M. No hay conexión física disponible.	Compruebe la línea S2M y la placa. Si es necesario, vuelva a cargar la placa o realice un reinicio completo. Si el error persiste, establezca una traza RDSI.	
FP_EVT_HW_043	ningún error de señal desactivado (TMS2M/ STMD)	Indicación de alarma: Se ha corregido el error S2M.	Ninguno	

Código SNMP	Entrada en el protocolo de sucesos	Significado	Medidas necesarias	Observación
FP_EVT_HW_046	error de segundos gravemente erróneos activado (TMS2M)	error de segundos gravemente erróneos activado (TMS2M)		
FP_EVT_HW_047	error de segundos gravemente erróneos desactivado (TMS2M)	error de segundos gravemente erróneos desactivado (TMS2M)		
FP_EVT_HW_052	reloj utilizable como ref. (TMS2M/STMD)	reloj utilizable como ref. (TMS2M/STMD)		
FP_EVT_HW_053	reloj no utilizable como referencia	reloj no utilizable como referencia		
FP_EVT_HW_060	Error de alimentación de acceso activado (SLMO)	Error de alimentación de acceso activado (SLMO)		
FP_EVT_HW_063	Error ELIC activado (SLMO/SLMC)	Error ELIC activado (SLMO/SLMC)		
FP_EVT_HW_064	Error ELIC desactivado (SLMO/SLMC)	Error ELIC desactivado (SLMO/SLMC)		
FP_EVT_HW_067	Error OCTAT activado (SLMC)	Error OCTAT activado (SLMC)		
FP_EVT_HW_096	error desconocido de LW	error desconocido de LW		
Clase de error 11 - Mensajes generales				
FP_EVT_DEV_041	L1 asíncrono activado	L1 asíncrono activado		
FP_EVT_DEV_042	L1 asíncrono desactivado	L1 asíncrono desactivado		
FP_EVT_DEV_043	Error de sobrecarga activado	Error de sobrecarga activado		
FP_EVT_DEV_044	Error de sobrecarga desactivado	Error de sobrecarga desactivado		
FP_EVT_DEV_045	Error de comprobación activado	Error de comprobación activado		
FP_EVT_DEV_046	información optiPoint	información optiPoint		
FP_EVT_DEV_048	Error de capa 2 detectado	Error de capa 2 detectado		
FP_EVT_DEV_049	Error de capa 3 detectado	Error de capa 3 detectado		
FP_EVT_DEV_052	Otros errores	Otros errores		
FP_EVT_DEV_057	NO TEI disponible	NO TEI disponible		

Código SNMP	Entrada en el protocolo de sucesos	Significado	Medidas necesarias	Observación
FP_EVT_DEV_058	Demasiados errores L1	Demasiados errores de capa 1.	Compruebe las líneas, el terminal y el puerto. Puede haberse producido un cortocircuito.	
FP_EVT_DEV_059	Acceso no configurado	Acceso no configurado		
Clase de error 16 - Mensajes del sistema operativo				
FP_EVT_GEN_002	Error en el grupo de liberación	Error en el grupo de liberación	Establezca un trace utilizando la información de BLS (Soporte de segundo nivel). Cree un volcado de pila. Guarde una instantánea.	
FP_EVT_GEN_004	Error en OSF-Send	Error en OSF-Send	Establezca un trace utilizando la información de BLS (Soporte de segundo nivel). Cree un volcado de pila. Guarde una instantánea.	
FP_EVT_GEN_005	Error en OSF-Timer	Error en OSF-Timer	Establezca un trace utilizando la información de BLS (Soporte de segundo nivel). Cree un volcado de pila. Guarde una instantánea.	
FP_EVT_GEN_010	REINICIADO: restablecimiento manual	REINICIADO: restablecimiento manual	Establezca un trace utilizando la información de BLS (Soporte de segundo nivel). Cree un volcado de pila. Guarde una instantánea.	

Código SNMP	Entrada en el protocolo de sucesos	Significado	Medidas necesarias	Observación
FP_EVT_GEN_011	REINICIADO: recarga manual	REINICIADO debido a una recarga manual	Establezca un trace utilizando la información de BLS (Soporte de segundo nivel). Cree un volcado de pila. Guarde una instantánea.	
FP_EVT_GEN_012	REINICIADO: Apagado	REINICIADO por apagón	Establezca un trace utilizando la información de BLS (Soporte de segundo nivel). Cree un volcado de pila. Guarde una instantánea.	
FP_EVT_GEN_013	Copia de seguridad KDS no realizada	Copia de seguridad KDS no realizada	Establezca un trace utilizando la información de BLS (Soporte de segundo nivel). Cree un volcado de pila. Guarde una instantánea.	
FP_EVT_GEN_014	REINICIADO: reinicio desconocido. Ind. Hardware: incompatible	REINICIADO debido a reinicio desconocido. Ind. Hardware: incompatible	Establezca un trace utilizando la información de BLS (Soporte de segundo nivel). Cree un volcado de pila. Guarde una instantánea.	

Código SNMP	Entrada en el protocolo de sucesos	Significado	Medidas necesarias	Observación
FP_EVT_GEN_015	registro general de errores	registro general de errores	Establezca un trace utilizando la información de BLS (Soporte de segundo nivel). Cree un volcado de pila. Guarde una instantánea.	
FP_EVT_GEN_020	CSTA: longitud fuera de rango	CSTA: longitud fuera de rango	Establezca un trace utilizando la información de BLS (Soporte de segundo nivel). Cree un volcado de pila. Guarde una instantánea.	
FP_EVT_GEN_024	inactivo tras reiniciar	inactivo tras reiniciar	Establezca un trace utilizando la información de BLS (Soporte de segundo nivel). Cree un volcado de pila. Guarde una instantánea.	
FP_EVT_GEN_030	super. de pts. mon. CSTA	super. de pts. mon. CSTA	Establezca un trace utilizando la información de BLS (Soporte de segundo nivel). Cree un volcado de pila. Guarde una instantánea.	
Clase de error 19 - Mensajes de servicios de red				
FP_EVT_NWS_011	Cliente SNTP en PCS no se puede activar	Cliente SNTP en PCS no se puede activar		
Clase de error 20 - Mensajes de procesamiento de llamadas				
FP_EVT_CP_002	RS232: DSR no listo	La interfaz RS232/V.24 está averiada.	Compruebe la interfaz, la línea y la aplicación.	

Código SNMP	Entrada en el protocolo de sucesos	Significado	Medidas necesarias	Observación
FP_EVT_CP_013	vías no conectadas	Se ha superado el número máximo de rutas de conexión permitidas.	Utilice la herramienta de planificación del proyecto para probar la configuración del sistema. Establezca un trace utilizando la información de BLS. Cree un volcado de pila. Guarde una instantánea.	
Clase de error 21 - Mensajes del Device Handler				
FP_EVT_DH_004	Puerto fuera de servicio	Puerto fuera de servicio		
FP_EVT_DH_005	Puerto en servicio	Puerto en servicio		
FP_EVT_DH_016	Nombre en mens. S0/ S2M descart.	Nombre en mens. S0/ S2M descart.		
FP_EVT_DH_017	mens. demasiado largo L3S int->ext	mens. demasiado largo L3S int->ext		
FP_EVT_DH_018	mens. demasiado largo L3S ext->int	mens. demasiado largo L3S ext->int		
FP_EVT_DH_022	Auto PRI detec prot DMS250	Auto PRI detec prot DMS250		
FP_EVT_DH_023	Detec PRI autom prot NI2		Detec PRI autom prot NI2	I
FP_EVT_DH_024	Detec PRI autom prot 4ESS prot		Detec PRI autom prot 4ESS prot	
FP_EVT_DH_026	desbordamiento del módulo clave	desbordamiento del módulo clave		
FP_EVT_DH_027	Límite de Can-B alcanzado	Límite de Can-B alcanzado		
Clase de error 23 - Mensajes de Device Handler				
FP_EVT_NW_060	sistema en espera, no hay búfer disponible	Sistema en espera, no hay más búfer libre disponible.	Establezca un trace utilizando la información de BLS. Cree un volcado de pila. Guarde una instantánea.	
Clase de error 26 - Mensajes de administración de la placa				

Código SNMP	Entrada en el protocolo de sucesos	Significado	Medidas necesarias	Observación
FP_EVT_PR_001	tarjeta fuera de servicio	La placa especificada está fuera de servicio.	Ninguno	
FP_EVT_PR_003	otro tipo de tarjeta distinto del antiguo	Tipo de placa incompatible. La ranura ya está preasignada con un tipo de placa diferente.	Sustituya la tarjeta o utilice el Assistant T para borrar el tipo de tarjeta preasignado de modo que se reconozca la nueva tarjeta.	
FP_EVT_PR_004	tarjeta en servicio	La placa especificada está operativa.	Ninguno	
FP_EVT_PR_005	error durante la lectura de la base de datos	error durante la lectura de la base de datos		
Clase de error 28 - Mensajes de recuperación				
FP_EVT_RC_008	Falta APS en EventLog B	Falta APS en EventLog B	Ninguno	La versión actual de APS se introduce al copiar la memoria B del protocolo de sucesos. Esto facilita el análisis.
Clase de error 30 - Mensajes del software de la placa				
FP_EVT_LW_095	no hay conexión USBS al sistema	no hay conexión USBS al sistema		
Mensajes relativos al gestor de recursos				
FP_EVT_RM_001	Error de configuración del gestor de recursos	Error de configuración del gestor de recursos		
Mensajes sobre UPM				
FP_EVT_UPM_010	UPM: reiniciado	UPM: reiniciado		

Código SNMP	Entrada en el protocolo de sucesos	Significado	Medidas necesarias	Observación
MSG_DLSC_BOOTSTRAP_OK	Cliente DLS arrancado con éxito.	Cliente DLS arrancado con éxito.		
MSG_STRC_STOP	Trace seguro detenido.	Trace seguro detenido.		
MSG_STRC_START	Trace seguro iniciado para protocolos.	Los traces seguros han sido activados por el usuario para los protocolos mencionados.		
MSG_SPE_CERT_MISSING	Falta el certificado SPE.	No hay certificado SPE instalado.	Importe el certificado SPE y la clave privada (archivo PKCS#12).	
MSG_SPE_CERT_AVAIL	Certificado SPE disponible.	Ya está disponible el certificado SPE.		

Código SNMP	Entrada en el protocolo de sucesos	Significado	Medidas necesarias	Observación
MSG_SPE_CERT_UPDATED	El certificado SPE se ha actualizado correctamente.	El certificado SPE se ha actualizado correctamente.		
MSG_SPE_CERT_EXPIRED	Certificado SPE caducado.	Se ha superado el periodo de validez del certificado SPE instalado.	Instale un nuevo certificado válido.	
MSG_SPE_CRL_EXPIRED	SPE CRL para una CA específica ha caducado.	CDP inaccesible o CRL recuperada caducada.	Importe un certificado CA SPE con CRL válidas configuradas en CDP.	
MSG_SPE_CRL_UPDATED	SPE CRL para CA se ha actualizado correctamente.	SPE CRL para CA se ha actualizado correctamente.		
MSG_SPE_ALL_CRLS_UPTODATE	Todas las CRL de SPE vuelven a estar actualizadas.	Todas las CRL de SPE vuelven a estar actualizadas.		
MSG_MIKEY_REBOOT	Mikey Stack: aserción fallida.	Mikey Stack: aserción fallida.		
MSG_IPSEC_REBOOT	Error fatal en la pila IPSec.	Error fatal en la pila IPSec.		
MSG_CAT_H323_REBOOT		Reiniciar con H.323		
MSG_CAT_HSA_REBOOT		Reiniciar con HAS		
MSG_GW_SUCCESSFULLY_STARTED				
MSG_IP_LINK_FAILURE				
MSG_IP_LINK2_FAILURE		IP-Link 1 arriba/abajo		
MSG_IP_LINK3_FAILURE				
MSG_NEW_SW_AVAILABLE				
MSG_ADMIN_REBOOT		Reinicio con WBM/CLI-Admin, actualización de software o restauración de datos		
MSG_SYSTEM_REBOOT		Reinicio automático, por ejemplo con Garbage Collection		
MSG_EXCEPTION_REBOOT		Reiniciar con excepción de SW		
MSG_GW_OBJ_MEMORY_EXHAUSTED		Sin memoria		
MSG_TLS_POOL_SIZE_EXCEDED		Se acabaron los grupos internos		
MSG_OAM_RAM_THRESHOLD_REACHED		Límite de RAM alcanzado		

Código SNMP	Entrada en el protocolo de sucesos	Significado	Medidas necesarias	Observación
MSG_OAM_DMA_RAM_THRESHOLD_REACHED		Límite de DRAM alcanzado		
MSG_OAM_THRESHOLD_REACHED		Límite alcanzado, por ejemplo, para memoria flash o pools de IP		
MSG_OAM_HIGH_TEMPERATURE_EXCEPTION		Temperatura límite alcanzada (demasiado caliente)		
MSG_HACKER_ON_SNMP_PORT_TRAP		Acceso no autorizado al puerto SNMP		
MSG_DVMGR_LAYER2_SERVICE_TRAP		Canal B arriba/abajo		
MSG_SSM_NUM_OF_CALL_LEGS_2BIG	Más de 2 llamadas Leg: ¡no se permite! CSID: %x/%x	No se permiten más de dos Llamadas Legs por sesión. Esto ha provocado que el software se vuelva inestable. Se ejecuta el reinicio necesario.		
MSG_SSM_SESSION_CREATION_FAILED	Error en la creación de la sesión	La señalización ya no es posible porque no se ha podido crear una sesión. Se ejecuta el reinicio necesario. Se genera una trap SNMP.		
MSG_IPNCV_STARTUP_ERROR	Puesta en marcha del IPNCV: Fallo en la creación de IPNCV Manager	No se ha podido iniciar IPNCV. Se genera una trap SNMP.	Crear un TR/MR	
MSG_IPNCV_STARTUP_SHUTDOWN	Inicio/parada de IPNCV: IPNCV Manager creado con éxito o inicio/parada IPNCV: Apagado satisfactorio de IPNCV Manager	IPNCV se ha iniciado o detenido correctamente		
MSG_IPNCV_ERROR_INTERNO	Error interno de IPNCV: %s	Error de software: se encontraron datos internos inválidos. Se generará una trap SNMP con el perfil IPNCV-Detallado.		
MSG_IPNCV_MEMORY_ERROR	Memoria IPNCV: %s	Desbordamiento de memoria: se genera una trap SNMP.	Reinicie la gateway. Crear un TR/MR.	
MSG_IPNCV_SIGNALING_ERROR	Error de señalización IPNCV: %s	Error de software: se han encontrado datos internos no válidos.		

Código SNMP	Entrada en el protocolo de sucesos	Significado	Medidas necesarias	Observación
MSG_CAR_ALIVE_IP_CONNECTION_LOST	CAR: Alive: conexión ip %d.%d.%d.%d perdida	CAR: Alive: Conexión IP perdida.		
MSG_LIC_DATA_ACCEPTED		Datos de licencia aceptados		
MSG_LIC_DATA_CORRUPTED		Datos de licencia incompletos		
MSG_LIC_DATA_NOT_ACCEPTED		Datos de licencia aceptados		
MSG_SPE_CERT_MISSING	¡No hay certificado SPE instalado!	Falta el certificado SPE.	Instalar certificado SPE.	

Nota: Existen eventos SNMP no documentados en esta guía.

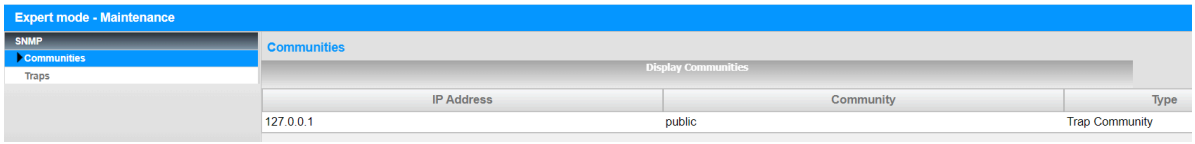
25.8.2.1 Cómo mostrar todas las comunidades

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **SNMP**.
3) En el grupo de menús, haga clic en **SNMP** > **Comunidades**. Aparece un listado de todas las comunidades con sus correspondientes datos (dirección IP, comunidad, tipo).



25.8.2.2 Cómo añadir comunidad

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **SNMP**.

3) Seleccione la comunidad deseada:
   - Si desea agregar una comunidad de lectura, en el grupo de menús haga clic en **SNMP** > **Comunidades** > **Comunidades lectura**. Haga clic en la pestaña **Añadir comunidad de lectura**.
   - Si desea agregar una comunidad de escritura, en el grupo de menús haga clic en **SNMP** > **Comunidades** > **Comunidades escritura**. Haga clic en la pestaña **Añadir comunidad de escritura**.
   - Si desea agregar una comunidad trap, en el grupo de menús haga clic en **SNMP** > **Comunidades** > **TRAP Comunidades**. Haga clic en la pestaña **Añadir comunidad trap**.
4) En el campo **Dirección IP** introduzca la dirección IP de la nueva comunidad.
5) En el campo **Comunidad** introduzca el nombre de la nueva comunidad.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.8.2.3 Cómo editar comunidad

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **SNMP**.
3) En el grupo de menús, bajo **SNMP** > **Comunidades** > **...**, navegue hasta la comunidad deseada.
4) Haga clic en la pestaña **Editar comunidad**.
5) Modifique la Comunidad.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.8.2.4 Cómo borrar comunidad

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **SNMP**.
3) En el grupo de menús, bajo **SNMP** > **Comunidades** > **...**, navegue hasta la comunidad deseada.
4) Haga clic en la pestaña **Borrar comunidad**.
5) Haga clic en **Borrar** y a continuación en **Aceptar**.

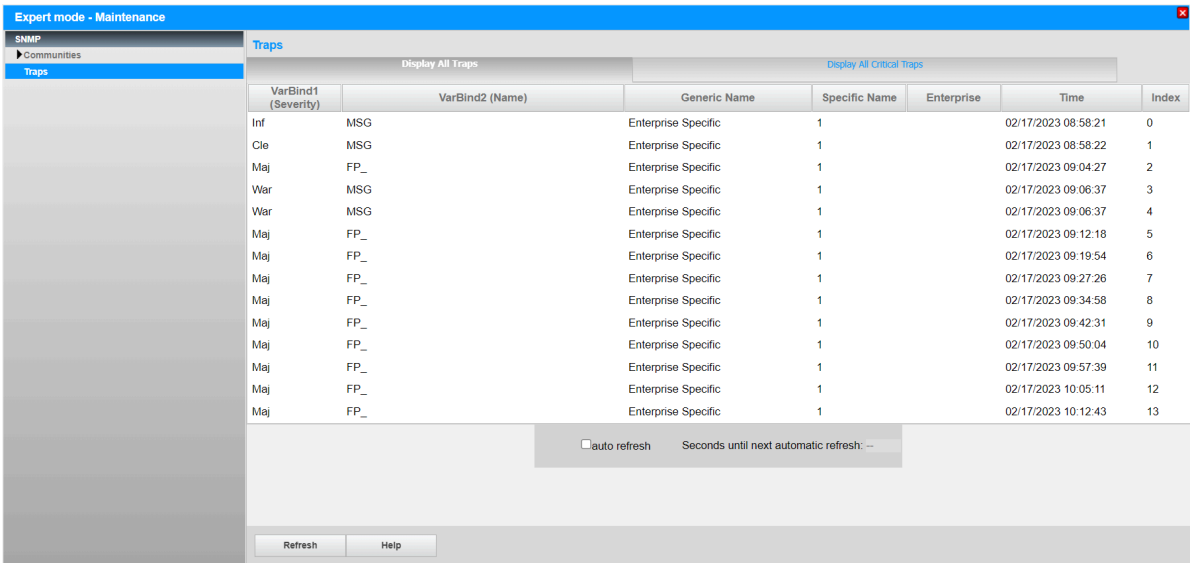
25.8.2.5 Cómo mostrar traps

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **SNMP**.
3) En el grupo de menús, haga clic en **SNMP** > **Traps**.
4) Elija una de estas opciones:
   - Si desea mostrar una lista de todas las traps, haga clic en la pestaña **Mostrar todas traps**.



   - Si desea mostrar una lista de todas las traps críticas, haga clic en la pestaña **Mostrar todas traps críticas**.

25.8.2.6 Cómo mostrar detalles de una trap

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **SNMP**.
3) En el grupo de menús, haga clic en **SNMP** > **Traps**.
4) Haga clic en la pestaña **Mostrar todas traps**. Aparece un listado de todas las traps con sus datos correspondientes.
5) Haga clic en el nombre de la trap deseada. Aparecerán los datos de la trap.
6) Haga clic en la pestaña **Mostrar todas traps**, para ver un listado de todas las traps críticas.

25.8.3 Acciones manuales

Las acciones manuales permiten cargar distintos datos de protocolo (datos y protocolos de diagnóstico).

Los administradores con el perfil **avanzado** pueden cargar datos de diagnóstico (Protocolos de diagnóstico) mediante el asistente **Trace**.

Los administradores con el perfil de **experto**, pueden cargar protocolos de diagnóstico a través del **Modo Experto**.

Se pueden cargar estos protocolos:

Protocolo	Explicación	Caso de aplicación
Protocolo trace	Archivo Trace estándar, al activar perfiles Trace. Se puede seleccionar entre las siguientes opciones: • **Todo el protocolo**: se descargan todos los archivos de protocolo de de trace del sistema existentes. • **Protocolo de hoy**: se descargan los archivos de protocolo de trace del sistema del día de hoy (a partir de las 00:00 horas). • **Selección propia**: **Desde:** XXX **Hasta:** YYY: se descargan los archivos de protocolo de trace del sistema del periodo seleccionado.	Ningún uso especial
Protocolo sucesos	Acciones/Sucesos del sistema de comunicación (Reset, Encendido/Apagado, etc.)	Ningún uso especial
Protocolo admin.	Mensajes a través de procesos de administración en el sistema de comunicación (intentos de inicio de sesión, etc.)	Ningún uso especial
Protocolos de licencia	Mensajes sobre componentes del sistema de comunicación que necesitan licencia	Problemas en la obtención de licencia (el archivo de licencia no se puede activar, etc.)
Trace de cliente	Los mensajes para el seguimiento de clientes se presentan en un formato más detallado que, por ejemplo, en el protocolo Trace (registro remoto, registro ITSP, etc.).	Problemas con la conexión de ITSP (proveedor de servicios de telefonía Internet) o con el inicio de sesión remoto
Protocolo Framework	Mensajes de WBM	Problemas con el registro de licencia, al realizar una copia de seguridad (Backup) o al restaurar (Restore) o con la Gestión basada en Web (WBM)
Protocolo de diagnóstico	Registros de diagnóstico del sistema de comunicación (FP/LDH)	Caída o apagado no controlado del sistema de comunicación

Protocolo	Explicación	Caso de aplicación
Protocolos de UC Suite	Mensajes de la UC Suite del sistema de comunicación (protocolos de la UC Suite, CSP y MEB) Se puede seleccionar entre las siguientes opciones: • **Todo el protocolo**: se descargan todos los archivos de protocolo existentes de UC Suite, CSP y MEB. • **Protocolo de hoy**: se descargan los archivos de protocolo de UC Suite, CSP y MEB del día de hoy (a partir de las 00:00 horas). • **Selección propia**: **Desde:** XXX **Hasta:** YYY: se descargan los archivos de protocolo de UC Suite, CSP y MEB del periodo seleccionado. Todos los archivos de protocolo se agrupan en un archivo comprimido. Para los protocolos OpenScape Business se aplican las siguientes designaciones de archivo: archivos de protocolo de UC Suite = `vs_aaaa_mm_dd.log`, archivos de protocolo CSP = `csptrace_aaaa_mm_dd.log`, archivos de protocolo MEB = `mebtrace_aaaa_mm_dd.log`. ***Información***: solo se pueden descargar datos de diagnóstico si se opera con UC Booster Card OCAB. Si se utiliza el OpenScape Business UC Booster Server, los datos de diagnóstico se deben descargar a través del propio servidor.	Problemas con la UC Suite y/o los clientes (myPortal for Desktop, myAttendant, etc.)
Protocolos de aplicaciones	Mensajes de la parte de aplicaciones del sistema de comunicación (por ejemplo, protocolos CSP) Los administradores con el perfil **Experto** pueden utilizar el **modo Experto** para elegir entre las siguientes opciones: • **Todo el protocolo**: se descargan todos los archivos de protocolo disponibles • **Protocolo de hoy**: se descargan los archivos de protocolo del día de hoy (a partir de las 00:00 horas). • **Selección propia**: **Desde:** XXX **Hasta:** YYY: se descargan los archivos de protocolo del periodo seleccionado. Todos los archivos de protocolo se agrupan en un archivo comprimido.	Problemas con la parte de aplicaciones del sistema de comunicación
Protocolos de diagnóstico del sistema	Registros de diagnóstico del sistema de comunicación	Ningún uso especial
Protocolo PPP	Mensajes para el protocolo Point-to-Point	Problemas en las conexiones de acceso telefónico (Dial-In) o de desconexión (Dial-Out)

Protocolo	Explicación	Caso de aplicación
Protocolo CoreLog	Los CoreLog se generan al reiniciar, etc. (como los volcados de memoria de un PC).	Caída o apagado incontrolado de OpenScape Business

Después de seleccionar los protocolos deseados, se genera un archivo comprimido y se guarda en un directorio indicado.

25.8.3.1 Cómo descargar Datos de diagnóstico / Protocolos de diagnóstico

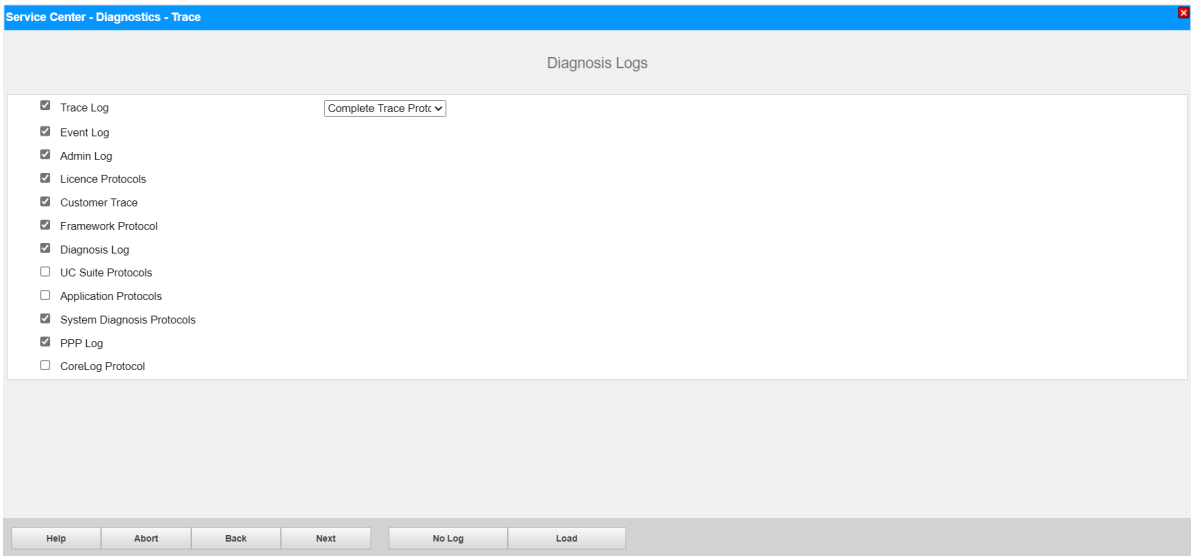
El asistente **Trace** permite descargar datos de diagnóstico (protocolos de diagnóstico) de los sistemas de comunicación.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Trace**.
3) Haga clic en **Protocolos de diagnóstico**.



4) Active la casilla de verificación de los protocolos que desea cargar. Desactive la casilla de verificación de los protocolos que no desea descargar.
5) Haga clic en **Cargar** y, a continuación, en **Aceptar**. Se abre la ventana de descarga de archivos.
6) Guarde el archivo en el directorio deseado. A continuación, cierre la ventana que confirma la descarga del archivo.
7) Haga clic en **Continuar** y, a continuación, en **Salir**.

25.8.4 Traces

Gracias a los Traces, se pueden registrar los pasos de programa y sus resultados durante la ejecución de un programa. En conexión con otros datos de diagnóstico se puede rastrear un programa con errores hasta la causa del fallo. A través de los perfiles y componentes trace se configura el nivel de detalle con el que se registrarán los Traces.

Consejo: La activación de Traces tiene un efecto negativo en el rendimiento del sistema y solo deberían realizarla administradores expertos y previa consulta con el soporte técnico responsable.

Especialmente, el Trace consolas ocupa recursos de sistema esenciales por lo que influye considerablemente en el rendimiento del sistema de comunicación.

Redes

Para el diagnóstico de los sistemas de comunicación interconectados, se deben crear datos de seguimiento (Trace) por separado para cada nodo. No se puede realizar el registro central de datos de seguimiento de los sistemas interconectados.

Configuración del formato de seguimiento

A través de la función Configuración de formato trace, los administradores con el perfil **Experto** pueden definir qué datos de encabezado deberán incluirse en la salida Trace y el formato que deberán tener los datos Trace.

Datos de encabezado para la salida Trace (en la configuración estándar están activadas todas las opciones):

- Ajustes globales formato de encabezam. trace

  Si esta opción está activada, se pueden activar o desactivar estos datos de encabezado.
- ID subsist.
- Nombre tarea
- ID tarea
- Hora
- Nombre mód.
- N.° de línea

Preparación de los datos trace (formateo):

- Formateo completo con expansión de parámetros (estándar) = gran volumen de datos, rendimiento Trace normal. Ajuste estándar
- Restringido (tipos de mensajes binarios, especial para X-Tracer) = volumen de datos medio, rendimiento Trace rápido.
- Restringido (solo expansión de tipos de datos elementales) = volumen de datos bajo, rendimiento Trace muy rápido.
- Trace con rendimiento optimizado sin expansión de parámetros = volumen de datos muy bajo, rendimiento Trace extremadamente alto.

Consejo:

Hay que tener en cuenta que los datos de encabezado Trace adicionales y un formato de datos Trace exhaustivo, reducen el rendimiento global de un Trace.

Interfaces de salida trace

Esta función permite a los administradores con el perfil **Experto** definir las interfaces para la salida Trace. Se puede activar el Trace de archivo o el Trace vía LAN, también se pueden desactivar las dos interfaces.

Interfaz de salida trace	Explicación	Ajuste estándar
Trace archivo	**Act. trace archivo** Los mensajes Trace se registran en el sistema de comunicación en un archivo de protocolo. Si la opción está activada se aplican estos ajustes de configuración: **Cuota de seguimiento máxima (kByte)**: Indica el tamaño máximo de la memoria de seguimiento **Estrategia en caso de cumplirse la cuota máxima**. Se puede elegir entre **Saltar (eliminar archivo trace más antiguo)** y **Detener temporalmente el archivo trace**. **Tiempo transcurrido entre la creación de nuevos archivos trace (s):** 900 **Margen de tiempo durante el que están disponibles los archivos trace:** aparece indicado el margen de tiempo real.	Activado
Seguimiento vía LAN	**Act. trace vía LAN** Los mensajes Trace se transfieren a través de la interfaz LAN. Si la función está activada se aplica esta configuración: **valor del temporizador =** 25 s (tiempo de retardo para la transmisión de datos.)	No activado

Protocolo trace

Si la interfaz de salida Trace Trace archivo está activada, los administradores con el perfil **Experto** pueden valerse de ella para borrar o transferir los archivos de protocolo resultantes en un PC.

Loopback digital

Los loopbacks digitales se utilizan para comprobar los canales B de las interfaces S_0, S_{2M} y T1 de los módulos que pudiera haber. Los loopbacks digitales solo se tienen que activar si así lo solicita el proveedor de servicios.

Los loopbacks digitales solo se pueden configurar con Manager E.

Visor de sucesos / Protocolo trace de cliente

Los administradores con el perfil **Avanzado** pueden iniciar la indicación de sucesos (Trace de cliente) a través del asistente **Visor de sucesos**. Además, se puede borrar o transferir el archivo de protocolo trace de cliente de un PC.

Se describe el procedimiento a seguir para las siguientes funciones que se pueden iniciar a través del asistente:

- Cómo mostrar o modificar el protocolo Visor de sucesos / protocolo Trace de cliente
- Cómo descargar o abrir protocolo Visor de sucesos / protocolo Trace de cliente
- Cómo borrar protocolo Visor de sucesos / protocolo trace de cliente

Los administradores con el perfil **Experto** pueden iniciar la indicación del archivo de protocolo de Trace (seguimiento) de cliente a través del **Modo Experto**. Además, se puede borrar o transferir el archivo de protocolo trace de cliente de un PC.

Componente trace M5T

Esta función permite supervisar la pila SIP a los administradores con el perfil **Experto**. Por cada componente trace M5T se puede definir el nivel de detalle del registro mediante niveles trace (0=nivel mínimo a 4=nivel máximo).

Seguimiento seguro

Esta función permite registrar flujos de datos de señalización y de uso de VoIP cifrados a los administradores con el perfil **Experto**.

Si la prestación Signaling and Payload Encryption (SPE) está activada, se cifran los flujos de datos de señalización y de uso de VoIP recibidos y emitidos por el sistema de comunicación y entre teléfonos IP.

Para garantizar un análisis en caso de error, se pueden transmitir en la LAN informaciones trace adicionales (**Secure Trace**) durante un periodo de tiempo limitado. Con ello se generan archivos Secure Trace con cifrado asimétrico, que solo pueden ser descifrados y analizados por desarrolladores.

Para restringir el uso de la función Secure Trace, se han implementado estas características de seguridad:

- Un técnico de servicio debe importar una clave pública (certificado) en el sistema de comunicación correspondiente. Este certificado forma parte de un archivo X.509 y es necesario para poder generar un Secure Trace. El equipo de desarrollo despliega el archivo X.509. El certificado incluido es válido durante un mes como máximo.
- El inicio y el final del Secure Trace están protegidos por una contraseña especial (passphrase). Esta contraseña solo la conoce el cliente.

Así, el certificado es la clave del técnico de servicio y la contraseña (passphrase) es la clave del cliente. Se necesitan ambas claves para activar la función Secure Trace.

Proceso para generar un Secure Trace:

1) Un técnico de servicio determina un problema en la LAN de clientes. Junto con el equipo de desarrollo responsable se determina si es necesario generar un Secure Trace.
2) Se informa sobre esa necesidad al cliente que debe confirmar que ha recibido esa información. A continuación, el cliente emite un pedido para generar un Secure Trace, dando a conocer la fecha y la hora de inicio y final de la supervisión.

3) Un desarrollador crea un par de claves, compuesto por una clave pública y otra privada. Con este par de claves solo se puede crear un único Secure Trace. Los certificados se utilizan de esta forma

   - El certificado con la clave privada es estrictamente secreto y solo lo pueden utilizar desarrolladores autorizados.

     Se necesita la clave privada para descifrar los archivos Secure Trace.
   - El certificado con la clave pública se transfiere al técnico de servicio en un archivo X.509, en formato PEM o binario.

     Para importar este certificado en el sistema de comunicación afectado es necesario que se pueda generar un Secure Trace.

4) El técnico de servicio informa al cliente de que se va a comenzar a generar el Secure Trace. El cliente debe informar a las extensiones afectadas.

   Nota: Si no se notifica a las extensiones previamente, la grabación de llamadas y de datos de conexión va en contra de la ley.

5) El técnico de servicio importa el certificado con la clave pública en el sistema de comunicación correspondiente.
6) Para iniciar Secure Trace, el cliente introduce la contraseña (passphrase). Se generan los archivos Secure Trace.

   El sistema registra el inicio y el final del Secure Trace.
7) Una vez finalizada la creación del Secure Trace, se informa al cliente al respecto. El técnico de servicio retira el certificado del sistema de comunicación.
8) Los archivos Secure Trace se ponen a disposición del equipo de desarrollo.
9) Un desarrollador descifra los archivos Secure Trace mediante la clave primada. A continuación, se analizan los datos descifrados.

   Nota: Una vez finalizado el análisis, hay que destruir todos los datos correspondientes de forma segura. Este proceso incluye la destrucción de la clave privada, para que si existe una copia no autorizada, no se puedan volver a descifrar los archivos Secure Trace.

Seguimiento de pila H.323

Esta función permite a los administradores con el perfil **Experto** establecer la configuración Trace pila H.323. El nivel de detalle de la grabación se puede definir por niveles Trace (0 = nivel de detalle mínimo a 4 nivel de detalle máximo). Para la salida Trace pila H.323 se pueden elegir estas opciones de configuración:

Interfaz de salida trace	Explicación	Ajuste estándar
Trace consolas	**Act. trace consolas** Los mensajes Trace pila H.323 se emiten en la consola.	No activado

Interfaz de salida trace	Explicación	Ajuste estándar
Trace archivo	**Act. trace archivo** Los mensajes Trace pila H.323 se registran en un archivo de protocolo. Si la opción está activada se aplican estos ajustes de configuración: Tamaño máx. búfer trace (bytes) = 50000 Bytes (cantidad de datos almacenados en la memoria intermedia). Tamaño máx. archivo trace (bytes) = 1000000 Bytes (tamaño máximo del archivo de protocolo). Temporizador Trace = 60 s (tiempo de retardo para escribir los datos en el archivo de protocolo).	No activado

La activación y/o desactivación de los módulos H.323 permite definir qué componentes del trace pila H.323 deberán ser recogidos en la información de estado y de proceso. El estado de todos los módulos H.323 aparece indicado con el color del punto de lista correspondiente (verde = módulo H.323 activado, rojo = módulo H.323 no activado).

El protocolo trace pila H.323 se puede transferir o borrar de un PC.

Trace de componentes de licencia

Esta función permite a los administradores con el perfil Experto supervisar el agente de licencia interno del sistema (CLA, Customer License Agent). El nivel de detalle del registro se puede definir mediante niveles Trace (Bajo=nivel mínimo (ajuste estándar); Estándar=nivel medio; Todo=nivel máximo).

En la configuración estándar, el Trace de componentes de licencia está activado (nivel Trace = Bajo).

Si se modifican los niveles de Trace, repercute negativamente en el rendimiento del sistema y solo deberían hacer esos cambios administradores expertos y previa consulta con el soporte técnico responsable.

Perfiles trace

Los perfiles Trace establecen el nivel de detalle con el que se registran los datos. Un perfil Trace tiene asignados componentes trace. De esta forma se establecen los componentes del sistema para los que un perfil Trace debe registrar información de estado y de proceso.

Hay disponibles perfiles Trace predefinidos, que abordan todos los escenarios estándar. Además, los administradores con el perfil **Experto** pueden crear sus propios perfiles trace. Al iniciar un perfil Trace el registro se activa a través de él. Para desactivarlo, hay que detener el perfil.

- El asistente **Trace** permite a los administradores con el perfil **avanzado**, iniciar y/o detener perfiles Trace. El estado de cada perfil Trace se indica a través del color del punto de lista correspondiente (verde = Perfil Trace activado, rojo = Perfil Trace no activado). Seleccionando **Iniciar/Detener**

se puede activar (iniciar) un perfil Trace no activo (punto de lista rojo) y desactivar (detener) un perfil Trace activo (punto de lista verde)

Con **Cargar Trace** se pueden transferir y abrir los archivos de protocolo resultantes de un PC.

Con **Borrar Trace** se pueden borrar los archivos de protocolo resultantes.

Se describe el procedimiento a seguir para las siguientes funciones que se pueden iniciar a través del asistente:

- Cómo descargar un archivo de protocolo de de trace del sistema
- Cómo borrar un archivo de protocolo de trace del sistema
- Cómo mostrar todos los perfiles de seguimiento
- Cómo iniciar o detener un perfil trace
- Cómo descargar Datos de diagnóstico / Protocolos de diagnóstico

- Los administradores con el perfil **Experto** pueden detener todos los perfiles Trace al mismo tiempo a través del **Modo Experto** e iniciar y/o detener perfiles Trace por separado.

  En la representación en el grupo de menús, el color de cada uno de los puntos de lista indica el estado del perfil Trace (verde = Perfil Trace activado, rojo = Perfil Trace no activado). Seleccionando **Iniciar/Detener perfil** trace se puede activar (iniciar) un perfil Trace no activo (punto de lista rojo) y desactivar (detener) un perfil Trace activo (punto de lista verde).

  Seleccionando **Mostrar perfil trace** se muestran los datos detallados del perfil Trace deseado: estos datos incluyen el nombre de perfil, indicaciones relativas a la protección contra la escritura y al estado del perfil e información sobre los problemas a los que va orientado el uso del perfil Trace. También se indican los componentes trace pertenecientes al perfil Trace.

Perfil trace	Caso de aplicación
Actors_Sensors_Door-Opener	¡Todavía no hay información disponible!
Básico	¡Todavía no hay información disponible!
Calls_with_Analog_Subscriber_Trunks	¡Todavía no hay información disponible!
Calls_with_ISDN_Subscriber_Trunks	¡Todavía no hay información disponible!
Calls_with_System_Device_HFA	¡Todavía no hay información disponible!
Calls_with_System_Device_Upn	¡Todavía no hay información disponible!
CDR_Charging_data	¡Todavía no hay información disponible!
CMI	¡Todavía no hay información disponible!
CSTA_application	¡Todavía no hay información disponible!
Problemas de visualización	¡Todavía no hay información disponible!
Gateway_Stream_detailed	¡Todavía no hay información disponible!
Gateway_Stream_overview	¡Todavía no hay información disponible!
IP_Interfaces	¡Todavía no hay información disponible!
License_problem	¡Todavía no hay información disponible!
Network_Call_Routing_LCR	¡Todavía no hay información disponible!
Peripheral_cards	¡Todavía no hay información disponible!

Perfil trace	Caso de aplicación
RAS_or_Internal_access	¡Todavía no hay información disponible!
Ressources_MOH_Conferencing	¡Todavía no hay información disponible!
SIP_Interconnection_Subscriber_ITSP	¡Todavía no hay información disponible!
SIP_Registration	¡Todavía no hay información disponible!
Smart_VM	¡Todavía no hay información disponible!
UC_Smart	¡Todavía no hay información disponible!
Voice_Fax_connection	¡Todavía no hay información disponible!
VPN	¡Todavía no hay información disponible!
Web_based_Assistant_Expert_Mode	¡Todavía no hay información disponible!

Componentes trace

Con ayuda de los componentes trace se registra la información de estado y de proceso de los distintos componentes del sistema de comunicación.

Los administradores con el perfil **Experto** pueden detener al mismo tiempo todos los componentes trace, o iniciarlos y detenerlos por separado. Al iniciar un componente trace se activa el registro. Para desactivarlo hay que detener el componente. El nivel de detalle del registro se puede configurar a través de niveles Trace (0 = Nivel mínimo de detalle a 9 = Nivel máximo de detalle).

En la representación en el grupo de menús, el color de cada uno de los puntos de la lista indica el estado del componente trace (verde = Componente activado, rojo = Componente no activado). Seleccionando **Iniciar/Detener componente trace** se puede activar (iniciar) un componente trace no activo (de color rojo) y desactivar (detener) un componente trace activo (de color verde).

En la indicación de un componente trace se indica el nombre del subsistema, el índice componentes trace, el nivel Trace configurado e información de estado se haya iniciado o no el componente trace. Si desea editar un componente Trace, puede modificar el nivel Trace y el inicio o parada de los componentes Trace.

25.8.4.1 Cómo descargar un archivo de protocolo de de trace del sistema

El asistente **Trace** permite descargar archivos de protocolo de trace del sistema.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Trace**.
3) Haga clic en **Protocolos de diagnóstico**.

4) Haga clic en **Ningún protocolo**, para desactivar las casillas de verificación de todos los protocolos.
5) Active la casilla de verificación **Protocolo trace**.
6) Elija una de estas opciones:
   - Si desea descargar todo el protocolo de trace del sistema existente, en la lista desplegable seleccione **Todo el protocolo**.
   - Si desea descargar el protocolo de trace del sistema del día en curso, en la lista desplegable seleccione **Protocolo de hoy**.
   - Si desea descargar el protocolo de trace del sistema de un periodo determinado, en la lista desplegable seleccione **Selección propia**. En la lista desplegable **Desde:** seleccione el inicio y en la lista desplegable **Hasta:**, el final del periodo deseado.
7) Haga clic en **Cargar** y, a continuación, en **Aceptar**. Se abre la ventana de descarga de archivos.
8) Guarde el archivo en el directorio deseado. A continuación, cierre la ventana que confirma la descarga del archivo.
9) Haga clic en **Continuar** y, a continuación, en **Salir**.

25.8.4.2 Cómo borrar un archivo de protocolo de trace del sistema

El asistente **Trace** permite borrar archivos de protocolo de trace del sistema.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Trace**.
3) Haga clic en **Borrar Trace** y, a continuación, en **Aceptar**.
4) Haga clic en **Continuar** y, a continuación, en **Salir**.

25.8.4.3 Cómo restablecer los valores estándar de los ajustes Trace

El asistente **Trace** se puede usar para restablecer el estado estándar de los archivos de registro de seguimiento del sistema.

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Avanzado** o **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Trace**.
3) Haga clic en el botón **Default Trace Settings** y luego en **Aceptar** en el siguiente mensaje emergente que notifica que la acción se ha completado.

4) Haga clic en **Continuar** y, a continuación, en **Finalizar**.

Nota: La función Trace hace un amplio seguimiento que aumenta la carga general del sistema y no debe estar permanentemente activo. Se deberían restablecer los ajustes estándar de Trace, haciendo clic en el botón **Default Trace Settings** en cuanto se haya creado correctamente los seguimientos requeridos**.**

Nota: Si hay activos ajustes de seguimiento amplio, se le notificará al respecto en la página de inicio de WBM, en la sección **Notificaciones**. Además hay un enlace directo a los ajustes en el Centro de servicios.

25.8.4.4 Cómo mostrar todos perfiles trace

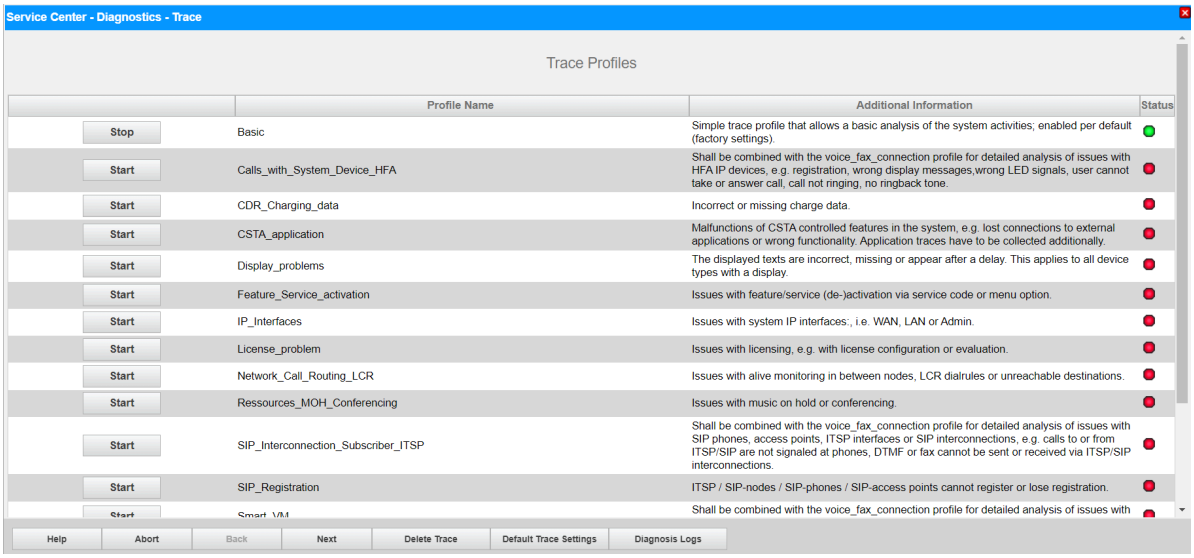
El asistente **Trace** permite obtener información sobre el estado de todos los perfiles Trace.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Trace**. Aparece un listado de todos los perfiles Trace, indicando los perfiles Trace iniciados y no iniciados.



3) Haga clic en **Continuar** y, a continuación, en **Salir**.

25.8.4.5 Cómo iniciar o detener un perfil trace

El asistente **Trace** permite iniciar y detener perfiles Trace.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Trace**. Aparece un listado de todos los perfiles Trace. Un punto de lista de color rojo identifica los perfiles Trace que se pueden iniciar. Un punto de lista de color verde identifica los perfiles Trace que se pueden detener.
3) Elija una de estas opciones:
   - Si desea iniciar un perfil trace, haga clic en **Inicio**. El color del punto de lista que indica el estado del perfil Trace correspondiente pasa de rojo a verde.

     Nota: Los perfiles trace iniciados tienen un efecto negativo en el rendimiento del sistema. Por este motivo, detenga todos los perfiles trace una vez finalizadas las actividades de diagnóstico, excepto el perfil trace **Estándar**. El perfil trace **Estándar** debe permanecer activo.
   - Si desea detener un perfil trace, haga clic en **Parada**. El color del punto de lista que indica el estado del perfil Trace correspondiente pasa de verde a rojo.
4) Haga clic en **Continuar** y, a continuación, en **Salir**.

25.8.4.6 Cómo mostrar o modificar la configuración de formato trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

El soporte técnico responsable requiere que se modifique la configuración de formato trace.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Configuración de formato trace**. Aparecen los ajustes actuales de la configuración de formato Trace.
4) Si es necesario, modifique la configuración deseada.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.8.4.7 Cómo mostrar o modificar las interfaces de salida trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

El soporte técnico responsable requiere que se modifiquen las interfaces de salida trace.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Interfaces de salida trace**. El SNMP (Simple Network Management Protocol) es un protocolo de redes que permite supervisar y controlar los componentes de red (por ejemplo, router, servidor, conmutadores, impresora, ordenador) desde una extensión central (consola de administración).
4) Si es necesario, modifique la configuración deseada.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.8.4.8 Cómo mostrar o modificar el protocolo Visor de sucesos / protocolo Trace de cliente

El asistente **Visor de sucesos** permite iniciar la indicación de sucesos (Trace de cliente) y modificar los ajustes de actualización.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Visor de sucesos**.
3) Haga clic en la pestaña **Mostrar**.
4) Seleccione el ajuste deseado:
   - Si desea que el protocolo se actualice automáticamente, active la casilla de verificación **Actualización autom**.
   - Si no desea que el protocolo se actualice automáticamente, desactive la casilla de verificación **Actualización autom**.
5) Si es necesario, haga clic en **Actualizar**, para actualizar manualmente el protocolo Trace de cliente.
6) Haga clic en **Salir**.

25.8.4.9 Cómo descargar o abrir protocolo Visor de sucesos / protocolo Trace de cliente

El asistente **Visor de sucesos** permite transferir el archivo de protocolo Trace de cliente a un PC o abrir dicho archivo.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Visor de sucesos**.
3) Haga clic en la pestaña **Cargar vía HTTP**.
4) Haga clic en **Cargar** y, a continuación, en **Aceptar**. Se abre la ventana de descarga de archivos.
5) Elija una de estas opciones:
   - Si desea descargar el archivo de protocolo, haga clic en **Guardar como**. Guarde el archivo en el directorio deseado y, a continuación, cierre la ventana que confirma la descarga del archivo.
   - Si desea abrir el archivo de protocolo, haga clic en **Abrir**. A continuación, se muestra el contenido del archivo de protocolo comprimido.
6) Haga clic en **Salir**.

25.8.4.10 Cómo borrar protocolo Visor de sucesos / protocolo trace de cliente

El asistente **Visor de sucesos** permite borrar el archivo de protocolo de Trace de cliente.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Visor de sucesos**.
3) Haga clic en la pestaña **Borrar protocolo sucesos**.
4) Haga clic en **Borrar protocolo** y, a continuación, en **Aceptar**.
5) Haga clic en **Salir**.

25.8.4.11 Cómo mostrar los componentes trace M5T

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Componente trace M5T**. Aparece una lista de todos los componentes trace M5T con su configuración actual. Además, en el grupo de menús aparecen los nombres de todos los componentes trace M5T. Un punto de lista coloreado indica el estado de cada uno de los componentes trace M5T.

25.8.4.12 Cómo iniciar o detener un componente trace M5T

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

El soporte técnico responsable responsable requiere que se inicie o se detenga un componente trace M5T.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Componente trace M5T**. En el grupo de menús aparecen los nombres de todos los componentes trace M5T. Un punto de lista de color rojo identifica los componentes trace M5T que se pueden iniciar. Un punto de lista de color verde identifica los componentes trace M5T que se pueden detener.
4) En el grupo de menús, haga clic en el componente trace M5T deseado.
5) Haga clic en la pestaña **Inicia/Detener componente trace**.
6) Elija una de estas opciones:
   - Si desea iniciar un componente trace M5T, haga clic en **Inicio** y a continuación en **Aceptar**.
   - Si desea detener un componente trace M5T, haga clic en **Parada** y, a continuación, en **Aceptar**.

25.8.4.13 Cómo editar componentes M5T-Trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

El soporte técnico responsable requiere que se modifiquen los componentes M5T-Trace.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Componente trace M5T**. Aparece una lista de todos los componentes trace M5T con su configuración actual.
4) Modifique los ajustes de configuración deseados.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.8.4.14 Cómo iniciar o detener Secure Trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Secure trace**.
4) Haga clic en la pestaña **Iniciar/Detener Secure Trace**.
5) Elija una de estas opciones:
   - Si desea iniciar el Secure Trace, siga este procedimiento:

     En el campo **Frase de contraseña de activación Secure Trace** introduzca la contraseña del Secure Trace.

     En el campo **Duración de Secure Trace (min.)** introduzca el tiempo (en minutos) durante el que estará activo el Secure Trace.

     Active las casillas de verificación de los protocolos para los que desea generar el Secure Trace. Desactive las casillas de verificación de los protocolos para los que no desea generar el Secure Trace.

     Haga clic en **Iniciar Secure Trace** y, a continuación, en **Aceptar**.
   - Si desea detener Secure Trace, haga clic en **Terminar SecureTrace** y, a continuación, en **Aceptar**.

25.8.4.15 Cómo consultar el estado de Secure Trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Secure trace**.
4) Haga clic en la pestaña **Estado Secure Trace**. A continuación se muestra el estado actual de Secure Trace.

25.8.4.16 Cómo modificar la contraseña para el Secure Trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Secure trace**.
4) Haga clic en la pestaña **Modificar frase de contraseña Secure Trace**.
5) En el campo **Frase de contraseña actual** introduzca la contraseña actual para el Secure Trace.
6) La En los campos **Nueva frase de contraseña** y **Confirmar nueva frase de contraseña** introduzca la nueva contraseña para Secure Trace. Debe tener entre cinco y doce posiciones.
7) Haga clic en **Aplicar**.

25.8.4.17 Cómo importar el certificado para el Secure Trace a partir de un archivo X.509

Requisitos previos

Hay un archivo X.509 en formato binario PEM o binario.

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Secure trace**.
4) Haga clic en la pestaña **Importar archivo X.509 para Secure Trace**.
5) Haga clic en **Examinar** para seleccionar el archivo X.509 deseado.
6) Haga clic en **Abrir**.
7) Haga clic en **Importar certif. de archivo**.

25.8.4.18 Cómo mostrar o modificar una configuración Trace de pila H.323

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

El soporte técnico responsable requiere que se modifique la configuración trace de pila H.323.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Trace pila H.323**.
4) Haga clic en la pestaña **Editar config. trace pila H.323**. Aparece la configuración actual de la configuración Trace de la pila H.323.
5) Si es necesario, modifique la configuración deseada.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.8.4.19 Cómo editar módulos H.323

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

El soporte técnico responsable requiere que se modifiquen los módulos H.323.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Trace pila H.323**.
4) Haga clic en la pestaña **Editar todos mód. H.323**.

5) Seleccione la configuración deseada para **Trace act.**:
   - Si desea activar el seguimiento Trace para determinados módulos H.323, active las casillas de verificación correspondientes. Desactive la casilla de verificación de los módulos H.323 para los que desea desactivar el Trace.
   - Si desea desactivar el seguimiento Trace de todos los módulos H.323, haga clic en **Ninguno**.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.8.4.20 Cómo descargar o abrir Protocolo trace de pila H.323

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Trace pila H.323**.
4) Haga clic en la pestaña **Cargar protocolo trace pila H.323 vía HTTP**.
5) Haga clic en **Cargar** y, a continuación, en **Aceptar**. Se abre la ventana de descarga de archivos.
6) Elija una de estas opciones:
   - Si desea guardar el archivo de protocolo de Trace pila H.323, haga clic en **Guardar como**. Guarde el archivo en el directorio deseado y, a continuación, cierre la ventana que confirma la descarga del archivo.
   - Si desea abrir el archivo de protocolo de Trace pila H.323, haga clic en **Abrir**. A continuación, el archivo aparece en el editor de texto.

25.8.4.21 Cómo borrar protocolo trace pila H.323

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Trace pila H.323**.
4) Haga clic en la pestaña **Borrar protocolo trace pila H.323**.
5) Haga clic en **Borrar protocolo** y, a continuación, en **Aceptar**.

25.8.4.22 Cómo modificar el trace de componentes de licencia

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

El soporte técnico responsable requiere que se modifique el trace de componentes de licencia.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Componente de licencia** > **CLA**.
4) Elija una de estas opciones:
   - Si desea detener el trace de componentes de licencia, en la lista desplegable **Nivel trace**, seleccione la entrada **Desact**.
   - Si desea utilizar un nivel de detalle bajo para el registro trace, en la lista desplegable **Nivel trace**, seleccione la entrada **bajo**.
   - Si desea utilizar un nivel de detalle medio para el registro trace, en la lista desplegable **Nivel trace**, seleccione la entrada **Estándar**.
   - Si desea utilizar un nivel de detalle alto para el registro trace, en la lista desplegable **Nivel trace**, seleccione la entrada **Todo**.
5) Haga clic en **Aplicar**.

25.8.4.23 Cómo mostrar detalles de un perfil Trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Perfiles trace**. Aparece un listado de todos los perfiles Trace. Además, en el grupo de menús aparecen los nombres de todos los perfiles Trace. Un punto de lista coloreado indica el estado de cada uno de los perfiles Trace.
4) En el grupo de menús, haga clic sobre el nombre del perfil Trace que desee. Aparecen los datos detallados del perfil Trace.

25.8.4.24 Cómo detener todos los perfiles trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Perfiles trace**.
4) Haga clic en la pestaña **Detener todos perfiles trace**.
5) Haga clic en **Detener todos** y a continuación en **Aceptar**.

25.8.4.25 Cómo agregar perfil Trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Perfiles trace**.
4) Elija una de estas opciones:
   - Si desea agregar un perfil trace vacío, haga clic en la pestaña **Añadir perfil trace (perfil vacío)**.
   - Si desea agregar un perfil trace que contenga los componentes trace de todos los perfiles trace iniciados en ese momento, haga clic en la pestaña **Añadir perfil trace (con ajustes trace actuales)**. Seleccione cuáles de los componentes trace mostrados deberán incluirse en el nuevo perfil Trace.
5) En el campo **Nombre perfil** introduzca el nombre del nuevo perfil Trace.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.8.4.26 Cómo mostrar los componentes trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Componentes trace**.
4) Elija una de estas opciones:
   - Si desea mostrar la lista de todos los componentes trace, haga clic en la pestaña **Mostrar todos componentes trace**.
   - Si desea mostrar la lista de todos los componentes trace iniciados, haga clic en la pestaña **Mostrar componentes trace iniciados**.
   - Si desea mostrar la lista de todos los componentes trace detenidos, haga clic en la pestaña **Mostrar componentes trace parados**.

25.8.4.27 Cómo mostrar detalles de un componente Trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.

3) En el grupo de menús, haga clic en **Traces** > **Componentes trace**. Aparece una lista de todos los componentes trace. Además, en el grupo de menús aparecen los nombres de todos los componentes trace. Un punto de lista coloreado indica el estado de cada uno de los componentes trace.
4) En el grupo de menús, haga clic sobre el nombre del componente trace que desee. Aparecen los datos detallados del componente trace.

25.8.4.28 Cómo iniciar o detener un componente trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Componentes trace**. En el grupo de menús aparecen los nombres de todos los componentes trace. Un punto de lista de color rojo identifica los componentes trace que se pueden iniciar. Un punto de lista de color verde identifica los componentes trace que se pueden detener.
4) En el grupo de menús, haga clic en el componente trace deseado.
5) Haga clic en la pestaña **Inicia/Detener componente trace**.
6) Elija una de estas opciones:
   - Si desea iniciar un componente trace, haga clic en **Inicio** y a continuación en **Aceptar**.
   - Si desea detener un componente trace, haga clic en **Parada** y, a continuación, en **Aceptar**.

25.8.4.29 Cómo detener todos los componentes trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Componentes trace**.
4) Haga clic en la pestaña **Detener todos los componentes trace**.
5) Haga clic en **Detener todos** y a continuación en **Aceptar**.

25.8.4.30 Cómo restablecer los valores estándar de los ajustes Trace

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Componentes trace**.
4) Haga clic en la pestaña **Ajustes de Trace estándar**.
5) Haga clic en el botón **Default Trace Settings** y luego en **Aceptar** en el siguiente mensaje emergente que notifica que la acción se ha completado.

Nota: La función Trace hace un amplio seguimiento que aumenta la carga general del sistema y no debe estar permanentemente activo. Se deberían restablecer los ajustes estándar de Trace, haciendo clic en el botón **Default Trace Settings** en cuanto se haya creado correctamente los seguimientos requeridos**.**

Nota: Si hay ajustes de seguimiento amplio activos, se le notificará al respecto en la página de inicio de WBM, en la sección **Notificaciones. Además habrá un enlace directo a los ajustes.**

25.8.4.31 Cómo editar componentes trace

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) En el grupo de menús, haga clic en **Traces** > **Componentes trace**.
4) Haga clic en la pestaña **Editar componentes trace**. Aparece una lista de todos los componentes trace con su configuración actual.
5) Modifique los ajustes de configuración deseados.
6) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.8.4.32 Cómo reenviar archivos de protocolo del sistema automáticamente

Puede activar la opción de reenviar automáticamente los archivos de protocolo del sistema a un sistema de administración externo/servidor de syslog.

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en, haga clic en **Mantenimiento > Traces > Transferencia de Syslog**.
3) Indique la **Dirección IP** y el **Puerto** del sistema de administración en el que se reenviará el archivo syslog.
4) Haga clic en **Iniciar** para guardar los cambios en la configuración e iniciar el proceso.

   Si la conexión con el portal de administración/servidor de syslog se establece correctamente, el **Estado de conexión** mostrará un círculo verde a modo de indicador.

   Si la conexión con el portal de administración/servidor de syslog no se establece correctamente, el **Estado de conexión** mostrará un círculo rojo a modo de indicador.
5) Haga clic en **Detener** para desactivar el proceso.

   Si el **Estado de conexión** está establecido como desactivado, se mostrará con un círculo gris a modo de indicador.
6) Si cambia los ajustes de configuración, haga clic en **Aplicar** para que los cambios se hagan efectivos.

25.8.4.33 Cómo iniciar el servicio de datos Kernel Crash

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Su sistema de comunicación tiene una placa base (OCCLA, OCCMA(R), OCCMB(R)).
Asegúrese de que hay suficiente espacio libre en el disco de almacenamiento para que el servicio funcione correctamente. El servicio requiere 200 MB de espacio de almacenamiento. Los discos afectados son:

- SSD SATA de 16 GB (si no se monta una SSD NVMe)
- SSD NVMe

Se recomienda eliminar los rastros antes de iniciar el servicio si se quiere liberar espacio de almacenamiento.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) Haga clic en **Componentes trace > Datos de Kernel Crash**.
4) Haga clic en **Inicio**.

Se inicia el servicio de datos Kernel Crash y se desencadena automáticamente un reinicio del sistema. El servicio conserva el estado tras el reinicio del sistema.

25.8.4.34 Cómo detener el servicio de datos de Kernel Crash

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Su sistema de comunicación tiene una placa base (OCCLA, OCCMA(R), OCCMB(R)).

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) Haga clic en **Componentes trace > Datos de Kernel Crash**.
4) Haga clic en **Detener**.

Se detiene el servicio de datos Kernel Crash y se desencadena automáticamente un reinicio del sistema. El servicio conserva el estado tras el reinicio del sistema.

25.8.4.35 Cómo iniciar el Trace del servidor de medios

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.
3) Haga clic en **Trace del servidor de medios**.
4) Seleccione una opción de la lista desplegable **Nivel de trace** para definir el nivel de detalle del trace.
5) Haga clic en **Inicio**.

Nota: Los traces activos aumentan la carga general del sistema y pueden tener un impacto negativo en su rendimiento. Por lo tanto, el Trace del servidor de medios debe desactivarse tan pronto como termine sus actividades de diagnóstico.

25.8.4.36 Cómo detener el Trace del servidor de medios

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Mantenimiento** > **Traces**.

3) Haga clic en **Trace del servidor de medios**.

4) Haga clic en **Detener**.

25.9 TCP Dump

Un TCP Dump permite supervisar y evaluar el tráfico de datos en una interconexión IP.

Consejo: La activación de un TCP-Dump afecta negativamente en el rendimiento del sistema y solo deberían realizarla administradores expertos y previa consulta con el soporte técnico responsable.

Los archivos TCP Dump se guardan en el sistema de comunicación. Para hacer el diagnóstico de los archivos se requiere una aplicación adecuada.

Los TCP Dump se suelen utilizar para

- generar un Trace LAN por un breve periodo de tiempo (por ejemplo, para obtener una imagen de error reproducible).
- permitir a los técnicos de servicio autorizados acceder de forma remota a un Trace LAN.

Ventajas respecto a los daemon RPCAP: se puede acceder de forma remota, no hay que enviar los archivos Trace por correo electrónico

Desventajas respecto a los daemon RPCAP: no es una solución muy útil para realizar seguimientos (Traces) a largo plazo, espacio de almacenamiento limitado, no se puede definir un filtro de capturas, gestión más compleja y costosa si hay muchos Traces

25.9.1 Cómo iniciar TCP Dump

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Traces** > **TCP Dump**.

3) Haga clic en **Iniciar TCP Dump**.

4) Seleccione los ajustes deseados.

5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.9.2 Cómo detener TCP Dump

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Traces** > **TCP Dump**.
3) Haga clic en **Terminar TCP Dump**.
4) Haga clic en **Aceptar**.

25.9.3 Cómo borrar TCP Dump

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Traces** > **TCP Dump**.
3) Haga clic en **Borrar TCP Dump**.
4) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.10 Daemon RPCAP

Un daemon RPCAP (Remote Packet Capture) permite supervisar y evaluar el tráfico de datos en una interconexión IP.

Consejo: La activación de un daemon RPCAP repercute negativamente en el rendimiento del sistema y solo deberían realizarla administradores expertos y previa consulta con el soporte técnico responsable.

El daemon RPCAP permite el acceso remoto de aplicaciones externas a los paquetes TCP/IP de las interfaces LAN del sistema de comunicación.

A menudo, los daemon RPCAP se utilizan para realizar seguimientos (Traces) a largo plazo, ya que los archivos Trace se almacenan en un PC y no en el sistema de comunicación.

Ventajas respecto a TCP Dump: gestión más rápida y sencilla, se pueden hacer seguimientos (Traces) a largo plazo, se puede configurar libremente el número o tamaño de los archivos Trace, se puede hacer un Trace de la LAN interna

Desventajas respecto a TCP Dump: se duplica el tráfico de datos en la red y, con ello, la carga de las interfaces LAN del sistema de comunicación; se requiere una liberación de puertos especial (en el firewall)

25.10.1 Cómo activar RPCAP Daemon

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

El RPCAP Daemon se ha desactivado.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Traces** > **RPCAP Daemon**.
3) Seleccione los ajustes deseados.
4) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.10.2 Cómo desactivar RPCAP Daemon

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

El RPCAP Daemon se ha activado.

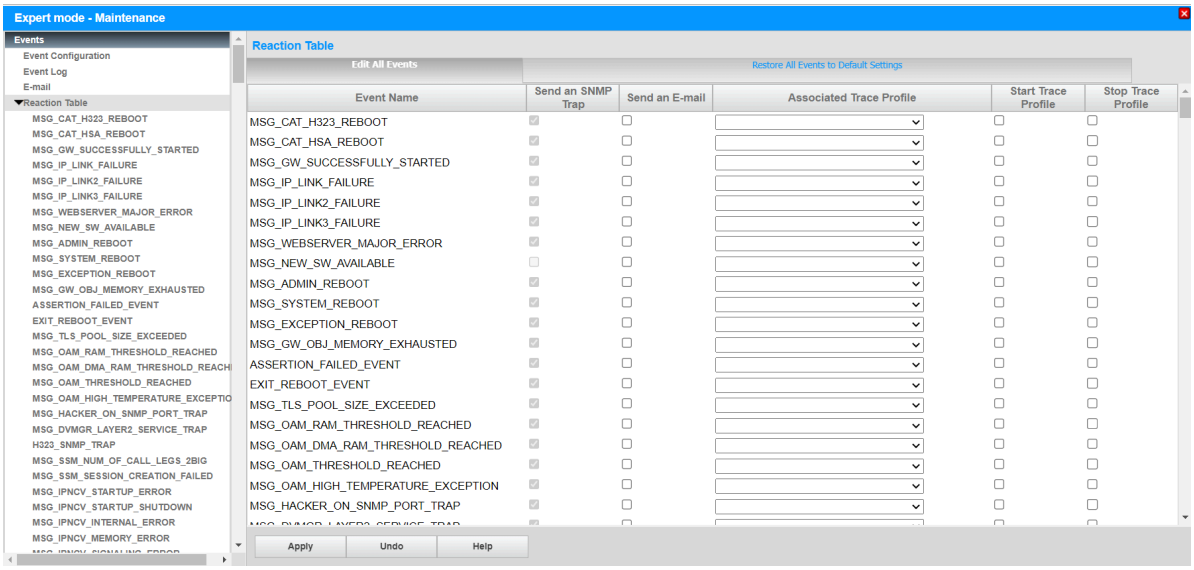
Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Traces** > **RPCAP Daemon**.
3) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.11 Sucesos

Los sucesos informan sobre deficiencias del sistema. Todos los sucesos se escriben en un archivo de protocolo de tamaño limitado. Si se supera el tamaño máximo del archivo, se crea uno nuevo. Puede haber hasta siete archivos.

En función de la configuración de la tabla de reacción y de la clase de problema, los sucesos pueden generar un trap SNMP, borrar un correo electrónico y/o iniciar/detener una supervisión Trace. La Gestión basada en Web (WBM) permite evaluar, configurar y guardar el protocolo de sucesos (el visor de sucesos).



Para interpretar el archivo de protocolo de sucesos, el archivo tiene que descargarse y extraerse en el PC con Gestión basada en Web (WBM). A continuación, el archivo se puede abrir, editar o imprimir desde cualquier editor de texto. Después de transferir el archivo de protocolo de sucesos, se puede eliminar de la memoria del sistema de comunicación.

Los sucesos que activan acciones se definen con estas propiedades:

- Código de suceso:

  Identifica un suceso como, por ejemplo, `MSG_ADMIN_LOGGED_OUT` = Información sobre el fin de sesión de un administrador.
- Tipo de suceso:

  Estos son los tipos de suceso:

  – Información: (Information) Mensaje de estado puro, ningún mensaje de error.
  – Advertencia: (Warning) Mensaje sobre un procedimiento o estado potencialmente problemático, pero ningún mensaje de error.
  – Menor: (Minor) Mensaje de error. El error no causa problemas.
  – Mayor: (Major) Mensaje de error. El error puede tener causar problemas.
  – Crítico: Mensaje de error El error es causa de problemas.
  – Limpio: (Cleared) Mensaje de error. El error ya fue resuelto por el sistema de comunicación.
  – Indeterminado: (Indeterminate) Mensaje de error. Aún no se ha determinado con exactitud la causa del error.

- Texto de suceso

  Algunos textos de suceso incluyen distintas variables. Estas variables se identifican de esta forma:

  – %s: cadena de caracteres
  – %u: número decimal positivo o negativo
  – %f: número en punto flotante
  – %p: indicador (dirección de memoria)
  – %x: número hexadecimal (en minúsculas)
  – %X: número hexadecimal (en mayúsculas)
  – %c: un único carácter
  – %d y %i: números decimales positivos

Tabla reacción

Los administradores con el perfil **Experto** pueden valerse de la tabla de reacción para definir las reacciones ante todos los eventos posibles por separado.

Se puede definir si se enviará un trap SNMP, si se deberá reiniciar el sistema de comunicación, si se deberá enviar un correo electrónico o si deberá iniciarse/pararse un perfil Trace. Si el suceso tiene asignado un perfil Trace, se muestra su nombre.

Ajustes de correo electrónico

Valiéndose de estos ajustes, un administrador con el perfil **Experto** puede hacer ajustes para el envío de correos electrónicos en caso de sucesos.

Protocolos de diagnóstico

El sistema de comunicación protocoliza determinadas acciones de procesos en protocolos de diagnóstico. Un administrador con el perfil **Experto** puede evaluar estos archivos de protocolo para fines de diagnóstico.

Señalización de alarma con exceso de temperatura

En el sistema de comunicación hay memorizados dos valores de temperatura críticos. Si la temperatura de sistema supera el primer valor, se emite una advertencia por trap SNMP o correo electrónico para advertir que la temperatura del sistema es muy alta. Además, este mensaje también se puede mostrar en el display de hasta 3 teléfonos del sistema (UP0 y HFA) Cómo definir los destinos para la señalización de alarmas. Si se supera el segundo valor, los módulos responsables del sobrecalentamiento (p.ej. OpenScape Business Booster Card) se apagan de forma controlada o se desconectan (p.ej. SLAV/SLAD). Para borrar la alarma y poner los módulos de nuevo en servicio, hay que apagar y encender de nuevo el sistema.

Se puede configurar qué 3 destinos (teléfonos del sistema) serán notificados en caso de que haya un exceso de temperatura.

25.11.1 Cómo modificar la protocolización de sucesos por LAN

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Sucesos**.
3) En el grupo de menús, haga clic en **Sucesos** > **Config. sucesos**.
4) Seleccione el ajuste deseado:
   - Si desea transmitir la protocolización de sucesos a través de una LAN, active la casilla de verificación **Act. protocoliz. sucesos vía LAN**.
   - Si no desea transmitir la protocolización de sucesos a través de una LAN, desactive la casilla de verificación **Act. protocoliz. sucesos vía LAN**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.11.2 Cómo descargar el archivo de protocolo de sucesos

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Sucesos**.
3) En el grupo de menús, haga clic en **Sucesos** > **Protocolo sucesos**.
4) Haga clic en la pestaña **Cargar vía HTTP**.
5) Haga clic en **Cargar** y, a continuación, en **Aceptar**. Se abre la ventana de descarga de archivos.
6) Guarde el archivo en el directorio deseado. A continuación, cierre la ventana que confirma la descarga del archivo.

25.11.3 Cómo borrar archivo de protocolo de sucesos

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Sucesos**.
3) En el grupo de menús, haga clic en **Sucesos** > **Protocolo sucesos**.
4) Haga clic en la pestaña **Borrar protocolo sucesos**.
5) Haga clic en **Borrar protocolo** y, a continuación, en **Aceptar**.

25.11.4 Cómo modificar configuración de correo electrónico por sucesos

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Transferencia de correos electrónicos se debe configurar para que todos los sistemas utilicen la opción **Destinatario de notificaciones de emergencia**. Para obtener más información, véase Cómo configurar el envío de correo electrónico en la página 208

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Sucesos**.
3) En el grupo de menús, haga clic en **Sucesos** > **Correo electrónico**.
4) En **Asunto**, indique lo que deberá aparecer en el campo Asunto del correo electrónico.

   Consejo: El Asunto debería indicar de forma clara e inequívoca que se trata de un correo electrónico emitido en razón de un suceso.

5) En los campos **Receptor 1** a **Receptor 5**, indique las direcciones de correo electrónico a las que se debe enviar el correo electrónico.
6) En el campo **Destinatario de emergencia**, indique la dirección de correo electrónico de un responsable de seguridad *in situ* a quien se le enviará un correo electrónico al marcar un número de emergencias.

   El asunto del correo electrónico es "Nueva llamada de emergencia". El número de llamada y el nombre del llamante, de estar configurados, se incluyen en el correo electrónico recuperándose de la base de datos del sistema.
7) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.11.5 Cómo mostrar la Tabla reacción sucesos

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Sucesos**.
3) En el grupo de menús, haga clic en **Sucesos** > **Tabla reacción**. Aparece la tabla de reacción con todos los posibles sucesos y su configuración.

25.11.6 Cómo modificar la configuración de reacción de un suceso

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Sucesos**.

3) En el grupo de menús, haga clic en **Sucesos** > **Tabla reacción**. Aparece la tabla de reacción con todos los posibles sucesos y su configuración. Además, en el grupo de menús aparecen los nombres de todos los posibles sucesos.
4) En el grupo de menús, haga clic sobre el nombre del suceso que desee.
5) Haga clic en la pestaña **Editar suceso**. Aparecen los ajustes de reacción del suceso deseado.

Consejo: Los ajustes de reacción **Reiniciar gateway** e **Informar a OpenScape** no se pueden modificar. El ajuste **Enviar trap SNMP** no se puede modificar en todos los sucesos.

---

6) Si es posible, seleccione el ajuste para **Enviar trap SNMP**:
   - Si desea enviar un trap SNMP en caso de suceso, active la casilla de verificación **Enviar trap SNMP**.
   - Si no desea enviar un trap SNMP en caso de suceso, desactive la casilla de verificación **Enviar trap SNMP**.
7) Seleccione el ajuste para **Enviar e-mail**:
   - Si desea enviar un correo electrónico en caso de suceso, active la casilla de verificación **Enviar e-mail**.
   - Si no desea enviar un correo electrónico en caso de suceso, desactive la casilla de verificación **Enviar e-mail**.
8) En la lista desplegable **Perfil trace asignado** seleccione el perfil Trace deseado.
9) Seleccione la configuración para el inicio o parada del perfil Trace:
   - Si desea iniciar el perfil trace seleccionado en caso de suceso, active la casilla de verificación **Iniciar perfil trace**.
   - Si desea detener el perfil trace seleccionado en caso de suceso, active la casilla de verificación **Parar perfil trace**.
10) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.11.7 Cómo modificar la configuración de reacción de varios sucesos

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Sucesos**.
3) En el grupo de menús, haga clic en **Sucesos** > **Tabla reacción**. Aparece la tabla de reacción con todos los posibles sucesos y su configuración de reacción.

Consejo: Los ajustes de reacción **Reiniciar gateway** e **Informar a OpenScape** no se pueden modificar. El ajuste **Enviar trap SNMP** no se puede modificar en todos los sucesos.

---

4) Modifique la configuración de reacción del suceso deseado de la tabla de reacción:
   - Si es posible, seleccione el ajuste para **Enviar trap SNMP**:

     Si desea enviar un trap SNMP en caso de suceso, active la casilla de verificación **Enviar trap SNMP**.

     Si no desea enviar un trap SNMP en caso de suceso, desactive la casilla de verificación **Enviar trap SNMP**.
   - Seleccione el ajuste para **Enviar e-mail**:

     Si desea enviar un correo electrónico en caso de suceso, active la casilla de verificación **Enviar e-mail**.

     Si no desea enviar un correo electrónico en caso de suceso, desactive la casilla de verificación **Enviar e-mail**.
   - En la lista desplegable **Perfil trace asignado** seleccione el perfil Trace deseado.
   - Seleccione la configuración para el inicio o parada del perfil Trace:

     Si desea iniciar el perfil trace seleccionado en caso de suceso, active la casilla de verificación **Iniciar perfil trace**.

     Si desea detener el perfil trace seleccionado en caso de suceso, active la casilla de verificación **Parar perfil trace**.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.11.8 Cómo descargar o abrir protocolos de diagnóstico

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Sucesos**.
3) En el grupo de menús, haga clic en **Sucesos** > **Protocolos diagnóstico**.
4) Haga clic en la pestaña **Extraer protocolos diagnóstico**. Aparece una lista de todos los protocolos disponibles con sus correspondientes nombres de archivo, tamaño de archivo en Bytes, momento de la última modificación y atributos de archivo.
5) En **Nombre de archivo**, haga clic en el nombre del protocolo de diagnóstico deseado. Se abre la ventana de descarga de archivos.
6) Guarde el archivo en el directorio deseado. A continuación, cierre la ventana que confirma la descarga del archivo.

25.11.9 Cómo borrar protocolos diagnóstico

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Mantenimiento** > **Sucesos**.
3) En el grupo de menús, haga clic en **Sucesos** > **Protocolos diagnóstico**. Aparece una lista de todos los protocolos disponibles con sus correspondientes nombres de archivo, tamaño de archivo en Bytes, momento de la última modificación y atributos de archivo.
4) Haga clic en la pestaña **Borrar protocolos diagnóstico**.
5) Haga clic en **Borrar protocolo** y, a continuación, en **Aceptar**.

25.11.10 Cómo definir los destinos para la señalización de alarmas

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Sucesos**.
3) En el grupo de menús, haga clic en **Sucesos** > **Señalización de alarmas**.
4) En las listas desplegables **Extensión 1-3**, seleccione los tres destinos (teléfonos del sistema con display, UP0 y HFA) donde aparecerá una notificación en pantalla si la temperatura del sistema supera un valor crítico definido.
5) Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

25.12 Datos de configuración para el diagnóstico

Para fines de diagnóstico se pueden crear conjuntos de copias de seguridad "más pequeños" que incluyan datos de diagnóstico para soporte técnico. A diferencia de lo que ocurre con los conjuntos de copias de seguridad normales, se crean volúmenes de datos considerablemente menores y eso permite, por ejemplo, enviarlos fácilmente por correo electrónico.

Los conjuntos de copias de seguridad de diagnóstico incluyen, entre otros, los datos de configuración del sistema de comunicación y de la aplicación UC (UC Smart o UC Suite). No incluyen mensajes de voz, mensajes de fax ni anuncios grabados.

Para almacenar los conjuntos de copia de seguridad de diagnóstico, se pueden utilizar estos medios:

- **Dispositivo USB**

  Los datos se pueden guardar, por ejemplo, en una unidad USB o un stick USB conectados.

  Nota: Si para la copia de seguridad se utiliza un disco duro USB, una partición de un disco duro USB o un stick USB, deberán tener formato FAT-32. Debido a la limitación del sistema de archivos, el tamaño máximo del conjunto de copias de seguridad no puede superar los 4 GB. En tales casos, se deben seleccionar medios de copia de seguridad alternativos. Los soportes USB con formato NTFS son de

solo lectura. ¡Si hay varias particiones, solo se puede usar la primera de ellas para copia de seguridad!

Si se utiliza como destino de almacenamiento un soporte USB con capacidad de arranque, hay que extraerlo de forma segura después de la copia de seguridad.

- **HTTPS**

  Los datos se pueden guardar mediante HTTPS en el disco duro del PC cliente.
- **Disco duro** (solo para OpenScape Business X3/X5/X8 con UC Booster Card (Tablero de aplicaciones OCAB))

  Los datos se pueden guardar en el disco duro del tablero de aplicaciones OCAB.

Consejo: No se puede hacer una copia de seguridad en el disco duro del sistema de comunicación.

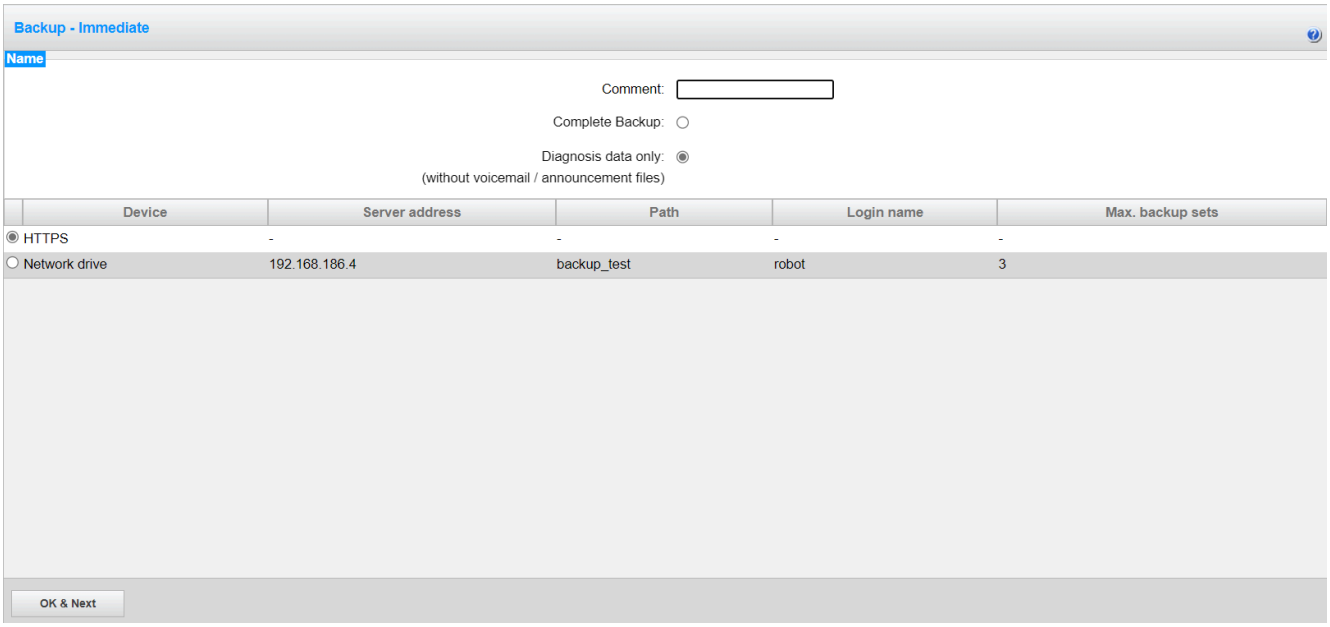
25.12.1 Cómo crear datos de configuración para el diagnóstico

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Avanzado**.

Paso a paso

1) Haga clic en **Copia de seguridad de datos** en la barra de navegación.
2) En el árbol de navegación, haga clic en **Copia de seguridad de datos** > **Guardar inmediatamente**.



3) Active la casilla de verificación **Diagnóstico**.

4) Seleccione el dispositivo en el que desea almacenar el conjunto de copias de seguridad de diagnóstico. Tiene las siguientes opciones:
   - Si desea guardar los datos en un disco duro o stick USB conectados, active el campo de opción **Dispositivo USB**.
   - Si desea guardar los datos por HTTPS en el disco duro del PC cliente, active el campo de opción **HTTPS**.
   - Solo para OpenScape Business X3/X5/X8 con Tarjeta UC Booster (Tablero de aplicaciones OCAB): Si desea guardar los datos en el disco duro del Tablero de aplicaciones OCAB, seleccione el campo de opción **Disco Duro**.
5) Si es necesario, en el campo **Comentario** introduzca un comentario sobre el conjunto de copias de seguridad de diagnóstico. Al hacer la entrada evite el uso de diéresis y caracteres especiales.
6) Haga clic en **OK y Continuar**. Se abrirá una nueva ventana con el progreso del proceso de copia de seguridad.
7) El mensaje `¡La copia de seguridad ha finalizado!` aparece si la copia de seguridad se ha realizado con éxito.
8) Si ha seleccionado **HTTPS** como medio de copia de seguridad, debe guardar el conjunto de copias de seguridad de diagnóstico y el archivo de texto correspondiente en una ubicación de su elección. En los demás medios de copia de seguridad, la ubicación se selecciona automáticamente. La ventana del navegador debe seguir abierta hasta que finalice el proceso de guardado del conjunto de copias de seguridad de diagnóstico y del archivo de texto.

   Nota: Si utiliza como medio de copia de seguridad un **Dispositivo USB**, espere hasta que el LED de dicho soporte deje de parpadear. Solo entonces habrá terminado de guardarse el conjunto de copias de seguridad de diagnóstico en el soporte USB. A continuación, extraiga el soporte USB.
9) Haga clic en **Finalizar**.

Pasos siguientes

Ya puede, por ejemplo, enviar el conjunto de copias de seguridad de diagnóstico para la búsqueda de errores al servicio técnico responsable en forma de correo electrónico.

25.13 Card Manager

OpenScape Business se suministra con medios de arranque que contienen el software del sistema. El Card Manager es una herramienta diseñada para crear un nuevo software del sistema en una tarjeta SDHC, en M.2 SATA SSD y en discos duros (HDD) de la UC Booster Card vacíos. Para ello se necesita tener el software del sistema de comunicación como archivo de imagen compatible.

El software de la tarjeta SDHC, M.2 SATA SSD o HDD es un software estándar de sistema, sin datos de cliente. No se puede utilizar para actualizaciones de software ni para hacer copias de seguridad de datos de cliente. Solo es posible en el caso de la tarjeta SDHC, que esta incluya un archivo de copia de seguridad durante la creación.

El Card Manager se puede iniciar como una imagen .ISO en un DVD de arranque Linux, en un lápiz USB de arranque Linux o en un entorno virtual.

El software Card Manager está disponible a través del Partner Portal.

Ejemplos de aplicación

- Antes de proceder a la entrega del sistema, hay que sustituir el software por la versión más reciente.
- El dispositivo de almacenamiento está dañado y hay que sustituirlo por uno nuevo en el que todavía no se ha guardado software.
- El software utilizado está defectuoso y hay que volver a instalarlo. En el proceso se borran todos los datos de cliente.

  Si para la restauración de los datos de cliente hay disponible un conjunto de copias de seguridad, el nuevo software instalado debe coincidir con la versión de software con la que se hizo el conjunto de copias de seguridad para que los ajustes incluidos en el conjunto sean compatibles con el software instalado y se puedan editar.

25.13.1 Cómo escribir con el Card Manager el software de comunicación en M.2 SATA SSD

Puede escribir con el Card Manager el software de comunicación de OpenScape Business V3 en M.2 SATA SSD.

Requisitos previos

La memoria de trabajo del PC debe ser al menos de 3 GB.

Disponible: un PC con una unidad de DVD de sistema operativo Windows 10 y al menos 2 USB 2.0 o interfaces posteriores.

Herramienta Card Manager V3 o posterior totalmente operativa en un PC.

Disponible: un adaptador USB para SATA SSD. El adaptador debe ser compatible con la Llave M y la Llave B.

Disponible: una tarjeta M.2 SATA SSD cualificada.

Disponible: una imagen de software de sistema en la versión correcta como archivo .tar. La versión de software debe coincidir con la versión del sistema de destino. Debe ser exactamente la misma versión que está en uso en el dispositivo de almacenamiento actual del sistema.

Aplicación Card Manager como archivo .ISO de DVD.

El archivo .ISO de Card Manager se debe grabar en un DVD.

Paso a paso

1) Almacene el archivo de imagen .tar actual en un lápiz USB y arranque la aplicación Card Manager desde el archivo .ISO de DVD.

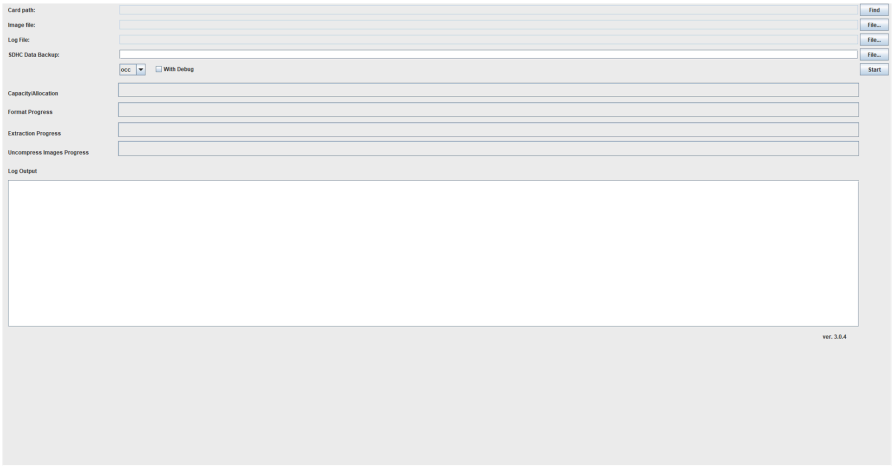
2) Conecte el adaptador USB para SATA SSD a una interfaz USB en el PC.

3) Introduzca la tarjeta M.2 SATA SSD en el adaptador y haga clic en **Aceptar** en la ventana emergente para confirmar la selección.

   El Card Manager borrará todos los datos de la tarjeta SSD introducida.

   No introduzca ningún dispositivo USB adicional en el PC, ya que se reconocerá como un medio de almacenamiento de OpenScape Business y se borrarán todos los datos.

4) En la aplicación Card Manager, haga clic en **Buscar** junto a **Ruta de tarjeta**.



5) Introduzca el lápiz USB con el archivo de imagen y haga clic en **Archivo...** junto al **Archivo de imagen** y seleccione el archivo de imagen .tar almacenado en el lápiz USB.

6) Seleccione **OCCe** desde el menú desplegable para crear la tarjeta M.2 SATA SSD.

7) Si lo desea, también puede crear un archivo de registro para posibles errores de programa. Para ello, haga clic en **Archivo...** junto a **Archivo de registro** y desplácese hasta la ubicación del archivo de registro. Asigne un nombre al archivo de registro y haga clic en **Guardar**.

8) Haga clic en **Inicio**.

   Se inicia el proceso de escritura y el progreso de cada paso se muestra en una barra de progreso.

9) Haga clic en **Aceptar** una vez finalizada la instalación y retire la tarjeta M.2 SATA SSD del adaptador.

10) Retire el adaptador de la interfaz USB.

11) Apague el sistema de comunicación.

12) Introduzca la nueva M.2 SATA SSD en el sistema de comunicación apagado.

13) Encienda el sistema de comunicación. El sistema se inicia con la nueva M.2 SATA SSD y la misma versión de software y configuración, listo para entrar en funcionamiento al empezar a parpadear el LED verde a 1 Hz (0,5 s encendido/0,5 s apagado).

Nota: Si la tarjeta M.2 SATA SSD se introduce en un sistema de comunicación OpenScape Business, el sistema se inicia en el estado de suministro, que incluye, entre otras cosas, la dirección IP predeterminada `192.168.1.2`.

Restaure una copia de seguridad del sistema. La copia de seguridad debe tener la misma versión secundaria que la del sistema instalado.

25.13.2 Cómo escribir con el Card Manager el software de comunicación en la tarjeta SDHC

Puede escribir con el Card Manager el software de comunicación de OpenScape Business V3 en una tarjeta SDHC.

Requisitos previos

Disponible: un PC con una unidad de DVD de sistema operativo Windows 10 y al menos 2 USB 2.0 o posterior.

Herramienta Card Manager V3 o posterior totalmente operativa en un PC.

Disponible: lector USB de tarjetas SDHC externo.

Disponible: una tarjeta SDHC apta.

Opcional: un archivo de copia de seguridad de datos SDHC (archivo .tar) almacenado en un lápiz USB junto con el sistema de imagen.

Protección contra escritura de la tarjeta SDHC desactivada.

Disponible: una imagen de software de sistema en la versión correcta como archivo .tar. Puede ser el archivo de imagen pequeño (OCC) o grande (OCAB). La versión de software debe coincidir con la versión del sistema de destino. Debe ser exactamente la misma versión que está en uso en la tarjeta SDHC actual del sistema.

Aplicación Card Manager como archivo .ISO de DVD.

El archivo .ISO de Card Manager se debe grabar en un DVD.

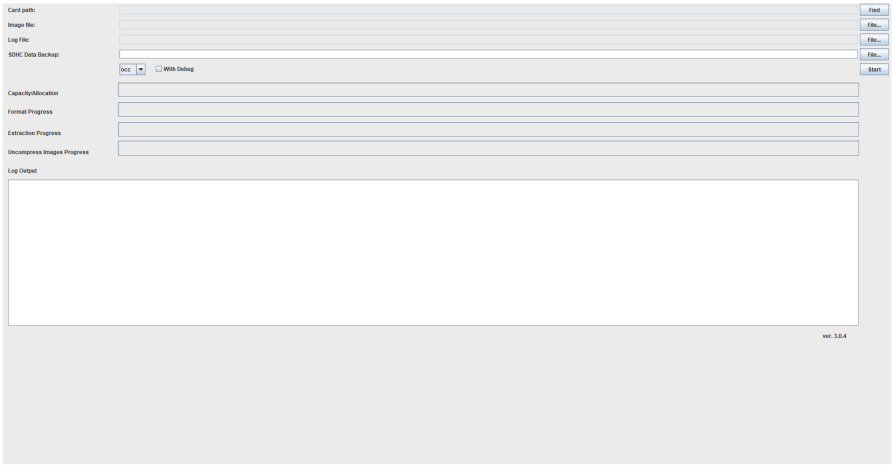
Paso a paso

1) Almacene el archivo de imagen .tar actual en un lápiz USB y arranque la aplicación Card Manager desde el archivo .ISO de DVD.
2) Conecte el lector de tarjetas SDHC por USB a una interfaz USB en el PC.
3) Desconecte el lector de tarjetas, introduzca la tarjeta SDHC, vuelva a conectar el lector y haga clic en **Aceptar** en la ventana emergente. La ruta de la tarjeta SDHC aparece bajo **Ruta de tarjeta**.

   El Card Manager borrará todos los datos de la tarjeta SSD introducida.

   No introduzca ningún dispositivo USB adicional en el PC, ya que se reconocerá como un medio de almacenamiento de OpenScape Business y se borrarán todos los datos.

4) En la aplicación Card Manager, haga clic en **Buscar** junto a **Ruta de tarjeta**.



5) Introduzca el lápiz USB con el archivo de imagen y haga clic en **Archivo...** junto al **Archivo de imagen** y seleccione el archivo de imagen .tar almacenado en el lápiz USB.

6) Seleccione **OCC** desde el menú desplegable para crear la tarjeta SDHC.

7) Si lo desea, también puede crear un archivo de registro para posibles errores de programa. Para ello, en **Archivo de registro** haga clic en **Archivo...** y desplácese hasta la ubicación del archivo de registro. Asigne un nombre al archivo de registro y confírmelo con **Guardar**.

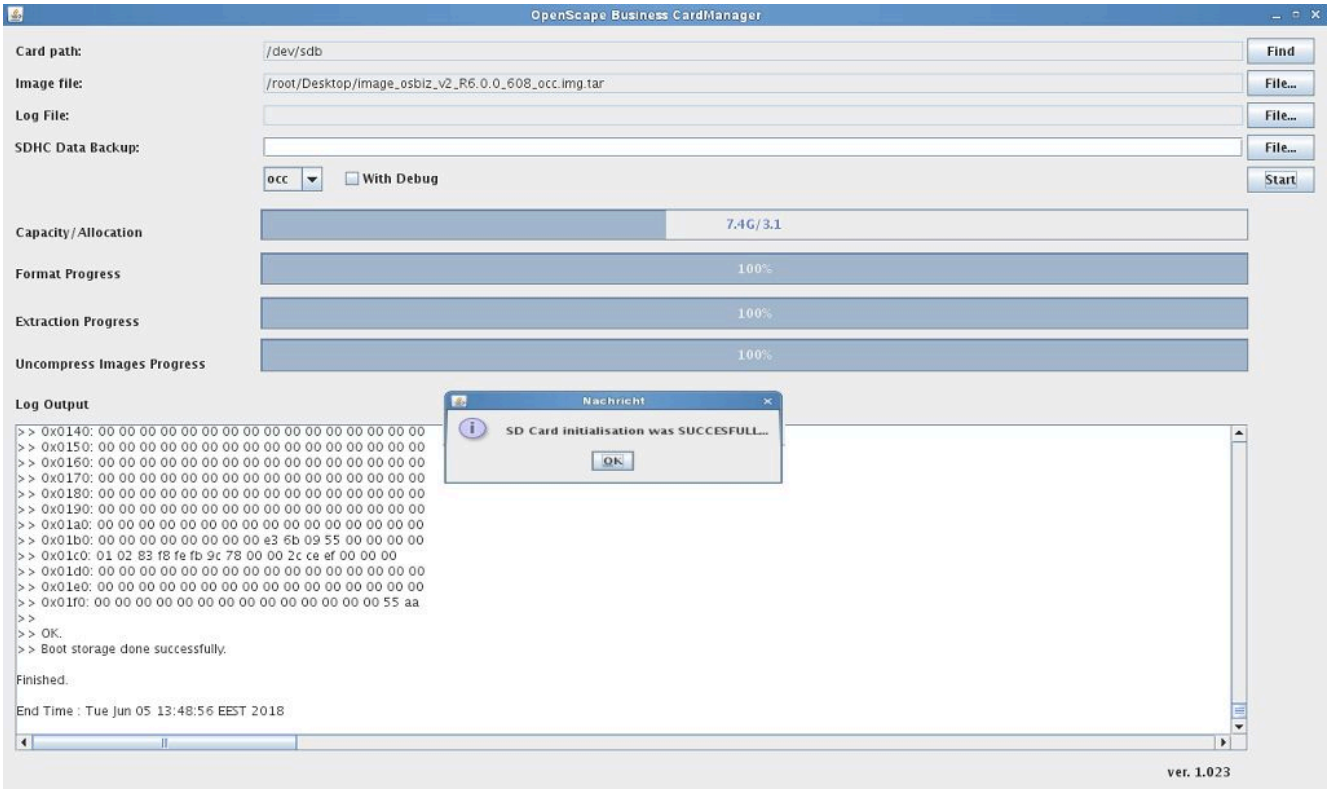
8) También puede hacer clic bajo **Copia de seguridad de datos SDHC** en **Archivo...** y seleccionar el archivo .tar con un archivo de copia de seguridad de datos SDHC específico de cliente. La ruta del archivo .tar aparece bajo **Copia de seguridad de datos SDHC.**

9) Haga clic en **Inicio**.

   Se inicia el proceso de escritura y el progreso de cada paso se muestra en una barra de progreso.

Nota: Si se rellena el campo texto (**Copia de seguridad de datos SDHC**), Card Manager primero compara la versión del archivo de copia de seguridad de datos de tarjeta SDHC con la versión del archivo de imagen de software del sistema. En caso de discrepar, aparece un mensaje de error y el proceso se interrumpe. En caso de coincidir, el Card Manager escribe la imagen seleccionada y luego extrae el archivo .tar especificado en la tarjeta SDHC. Si no hay ninguna copia de seguridad de datos

SDHC disponible, el campo de texto debe permanecer vacío.



10) Haga clic en **Aceptar** una vez finalizada la instalación y retire la tarjeta SDHC del lector.
11) Retire el lector de tarjetas de la interfaz USB.
12) Apague el sistema de comunicación.
13) Inserte la nueva tarjeta SDHC en la ranura SD del sistema de comunicación apagado.
14) Encienda el sistema de comunicación. El sistema se inicia con la nueva tarjeta SDHC y la misma versión de software y configuración, listo para entrar en funcionamiento al empezar a parpadear el LED verde a 1 Hz (0,5 s encendido/0,5 s apagado).

Nota: Si la tarjeta SDHC se introduce en un sistema de comunicación OpenScape Business, el sistema se inicia en el estado de suministro, que incluye, entre otras cosas, la dirección IP predeterminada `192.168.1.2`.

25.13.3 Cómo escribir con el Card Manager el software de comunicación en el disco duro OCAB

Puede escribir con el Card Manager el software de comunicación de OpenScape Business V3 con OCAB en el disco duro OCAB.

Requisitos previos

Disponible: un PC con una unidad de DVD de sistema operativo Windows 10 y al menos 2 USB 2.0 o interfaces posteriores.

Herramienta Card Manager V3 o posterior totalmente operativa en un PC.

Disponible: un adaptador para el disco duro OCAB. El adaptador debe ser compatible con la Llave M y la Llave B.

Disponible: un disco duro OCAB cualificado.

Disponible: una imagen de software de sistema (OCAB) en la versión correcta como archivo .tar. La versión de software debe coincidir con la versión del sistema de destino. Debe ser exactamente la misma versión que está en uso en el dispositivo de almacenamiento actual del sistema.

Aplicación Card Manager como archivo .ISO.

El archivo .ISO de Card Manager se debe grabar en un DVD.

Paso a paso

1) Almacene el archivo de imagen .tar actual en un lápiz USB y arranque la aplicación Card Manager desde el archivo .ISO de DVD.

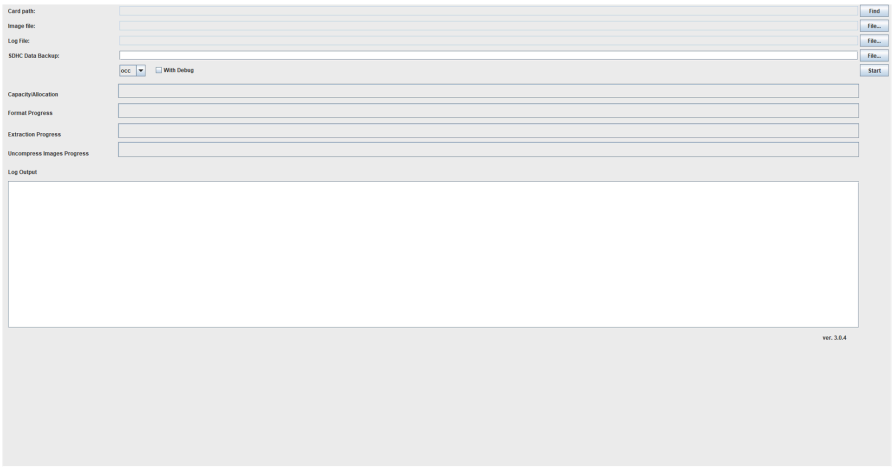
2) Conecte el adaptador a una interfaz USB en el PC.

3) Introduzca el disco duro OCAB en el adaptador y haga clic en **Aceptar** en la ventana emergente para confirmar la selección.

El Card Manager borrará todos los datos del disco duro introducido.

No introduzca ningún dispositivo USB adicional en el PC, ya que se reconocerá como un medio de almacenamiento de OpenScape Business y se borrarán todos los datos.

4) En la aplicación Card Manager, haga clic en **Buscar** junto a **Ruta de tarjeta**.



5) Introduzca el lápiz USB con el archivo de imagen y haga clic en **Archivo...** junto al **Archivo de imagen** y seleccione el archivo de imagen .tar almacenado en el lápiz USB.

6) Seleccione **OCAB** desde el menú desplegable para crear el disco duro OCAB.

7) Si lo desea, también puede crear un archivo de registro para posibles errores de programa. Para ello, haga clic en **Archivo...** junto a **Archivo de**

registro y desplácese hasta la ubicación del archivo de registro. Asigne un nombre al archivo de registro y haga clic en **Guardar**.

8) Haga clic en **Inicio**.

Se inicia el proceso de escritura y el progreso de cada paso se muestra en una barra de progreso.

9) Haga clic en **Aceptar** una vez finalizada la instalación y retire el disco duro OCAB del adaptador.

10) Retire el adaptador de la interfaz USB.

11) Apague el sistema de comunicación.

12) Monte el nuevo disco duro OCAB en la UC Booster Card y, a continuación, introdúzcala en el sistema de comunicación apagado.

13) Encienda el sistema de comunicación. El sistema se inicia con la nuevo disco duro OCAB y la misma versión de software y configuración, listo para entrar en funcionamiento al empezar a parpadear el LED verde a 1 Hz (0,5 s encendido/0,5 s apagado).

Nota:

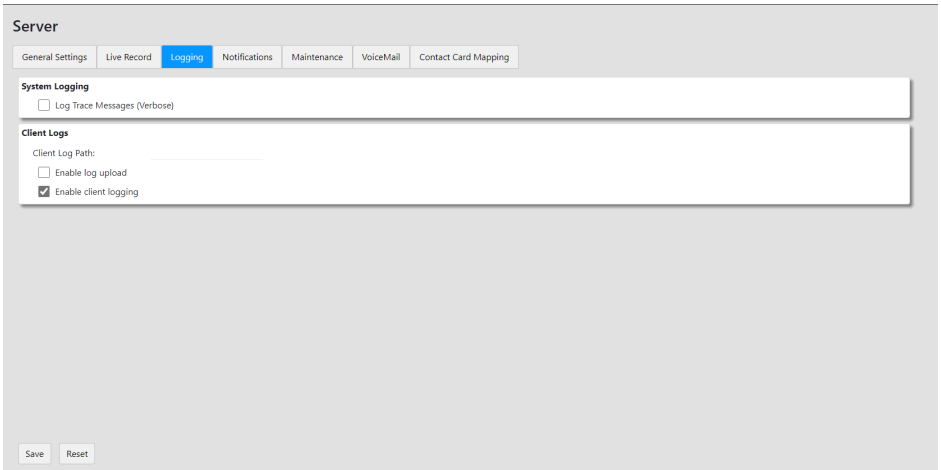
Todos los datos multimedia del cliente se pierden. Puede restaurar un conjunto de copias de seguridad del sistema y recuperar estos datos.

25.14 Supervisión y mantenimiento de la UC Suite

La Gestión basada en Web (WBM) ofrece a los administradores con el perfil **Experto** diferentes funciones para la supervisión y el mantenimiento de la UC Suite.

25.14.1 Protocolización

La ejecución de la UC Suite se supervisa de forma interna al sistema. La Protocolización de sistema permite configurar si se va a realizar una grabación. Además, se realiza una protocolización de las actividades de la UC Suite (por ejemplo, el inicio de un cliente de la UC Suite) en Client Logs (Registros de cliente).



Protocolización de sistema

Se puede activar o desactivar el siguiente protocolo de sistema:

Protocolo de sistema	Ajuste estándar
Mensajes de protocolo Trace (detallados)	No activado

Los resultados de todos los protocolos de sistema activos se registran diariamente en un archivo de protocolo con la designación vs-aaaa-mm-dd.log (por ejemplo, vs-2013-01-222.log) y se almacenan en el sistema de comunicación en la ruta /var/system/trace_log/vsl/log.

Consejo: Sólo desarrollo puede evaluar los archivos de protocolo.

Registros de cliente

Registros de cliente son los archivos de protocolo de la UC Suite. Por cada cliente de la UC Suite (myPortal for Desktop, myAttendant, etc.) y por cada extensión (usuario) se crea un directorio donde se almacenan los archivos de protocolo correspondientes. Se registran en él las actividades de una extensión como, por ejemplo, el inicio del cliente y las llamadas entrantes y salientes.

Consejo: El almacenamiento de Client Logs solo se admite en clientes de UC Suite que se utilizan con sistemas operativos Windows de Microsoft.

Se puede definir la ruta en la que se quiere almacenar el directorio de CC-Logs con los directorios de los distintos clientes de la UC Suite. Al hacerlo se puede elegir si el directorio deberá almacenarse en el directorio de cada uno de los PC cliente o en un PC o servidor central conectado en red.

Por defecto, el directorio `CC-Logs` se almacena en la siguiente ruta: `<Drive>:\N-Documentos y configuraciones//CC-Logs`

El periodo de retención de los registros de cliente es de 5 días. No se puede modificar este valor.

De forma predeterminada, la protocolización de las actividades de la UC Suite está activada en Client Logs. Los administradores con el perfil avanzado

pueden desactivar la protocolización a nivel de extensión mediante el asistente Directorio de usuario. Los administradores con el perfil de experto pueden activar o desactivar la protocolización a nivel de sistema a través del Modo Experto.

En función del escenario en cuestión, los registros de cliente se depositan de forma predeterminada en el disco duro de la tarjeta UC Booster Card (OCAB), del servidor UC Booster Server o del sistema de comunicación OpenScape Business S. Los administradores con el perfil Experto pueden utilizar el Modo Experto para desactivar el almacenamiento de los registros de cliente en el disco duro.

Los administradores con el perfil Avanzado pueden utilizar el asistente Trace para descargar los archivos de protocolo (Client Logs) de los clientes de la UC Suite utilizados por las extensiones internas (myPortal for Desktop, myAttendant, etc.).

Los administradores con el perfil Experto pueden utilizar el Modo Experto para descargar los archivos de protocolo (Client Logs) de los clientes de la UC Suite utilizados por las extensiones internas (myPortal for Desktop, myAttendant, etc.).

25.14.1.1 Cómo activar o desactivar el registro de los protocolos de sistema

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en Servidor y a continuación en Protocolos.
4) En la sección Fax T.38 seleccione una de estas opciones:
   - Si desea grabar los mensajes de seguimiento (Trace) diariamente en un archivo de protocolo, active la casilla de verificación Mensajes de protocolo Trace (detallados).
   - Si no desea grabar los mensajes de seguimiento (Trace) en un archivo de protocolo, desactive la casilla de verificación Mensajes de protocolo Trace (detallados).
5) Haga clic en **Guardar**.

25.14.1.2 Cómo activar o desactivar el registro de los Client-Logs a nivel de sistema

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.

3) Haga clic en Servidor y a continuación en Protocolos.
4) En la sección Fax T.38 seleccione una de estas opciones:
   - Si desea registrar Client-Logs, active la casilla de verificación Activar protocolización de cliente.
   - Si no desea registrar Client-Logs, desactive la casilla de verificación Activar protocolización de cliente.

   Consejo: La grabación de registros de cliente solo se admite para los clientes de la UC Suite que se utilizan con sistemas operativos Windows de Microsoft.
5) Haga clic en **Guardar**.

25.14.1.3 Cómo activar o desactivar el registro de los Client-Logs a nivel de extensión

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Configuración**.
2) En el árbol de navegación, haga clic en **Asistentes** > **UC Suite**.
3) Haga clic en **Editar** para iniciar el asistente **Directorio de usuario**.
4) Seleccione la extensión deseada en el directorio de usuarios y haga clic en **Editar**.
5) En el grupo de menús, haga clic en **Mis preferencias** > **Varios**.
6) Elija una de estas opciones:
   - Si desea registrar Client-Logs para la extensión deseada, active la casilla de verificación **Protocolizar mensajes de depuración (detallados)**.
   - Si no desea registrar los Client-Logs para la extensión deseada, desactive la casilla de verificación **Protocolizar mensajes de depuración (detallados)**.

   Consejo: La grabación de registros de cliente solo se admite para los clientes de la UC Suite que se utilizan con sistemas operativos Windows de Microsoft.
7) Haga clic en **Guardar**.
8) Si desea activar o desactivar el registro de los Client-Logs para otra extensión, repita los pasos del 4 al 7.

25.14.1.4 Cómo configurar la ruta de almacenamiento para los archivos de registro de cliente

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en Servidor y a continuación en Protocolos.
4) En el campo Ruta de registro de cliente, indique la ruta de almacenamiento en la que desea almacenar el directorio CC-Logs, con los subdirectorios de los distintos clientes de UC Suite y sus archivos de registro de cliente. Elija una de estas opciones:
   - Si desea crear un directorio CC-Logs en todos los PC cliente, introduzca, por ejemplo, <Unidad>:\<Ruta>. `<Drive>:\<Path>`.
   - Si desea almacenar el directorio de CC-Logs en un servidor o en un PC central conectado en red, introduzca, por ejemplo, \\<Dirección IP>\<Unidad>\<Ruta>. `\\\\<IP address><Drive><Path></Drive></IP><IP address><Drive>.</Drive></IP>`

   Consejo: El almacenamiento de Client Logs solo se admite en clientes de UC Suite que se utilizan con sistemas operativos Windows de Microsoft.
5) Haga clic en **Guardar**.

25.14.1.5 Cómo activar o desactivar la memorización central de los registros de cliente en el disco duro

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en Servidor y a continuación en Protocolos.
4) En la sección Fax T.38 seleccione una de estas opciones:
   - Si desea depositar registros de cliente en el disco duro de la tarjeta UC Booster Card (OCAB), del servidor UC Booster Server o del sistema de comunicación OpenScape Business S, active la casilla de verificación Habilitar carga de protocolos.
   - Si no desea depositar registros de cliente en el disco duro de la tarjeta UC Booster Card (OCAB), del servidor UC Booster Server o del sistema de comunicación OpenScape Business S, desactive la casilla de verificación Habilitar carga de protocolos.

   Consejo: La grabación de registros de cliente solo se admite para los clientes de la UC Suite que se utilizan con sistemas operativos Windows de Microsoft.
5) Haga clic en **Guardar**.

25.14.1.6 Cómo descargar Client Logs de todas las extensiones internas

El asistente **Trace** permite descargar los archivos de protocolo (Client Logs) de los clientes de la UC Suite que utilizan las extensiones internas (myPortal for Desktop, myAttendant, etc.). Los Client Logs solo son compatibles con los clientes de la UC Suite que se utilizan con sistemas operativos Windows de Microsoft.

Requisitos previos

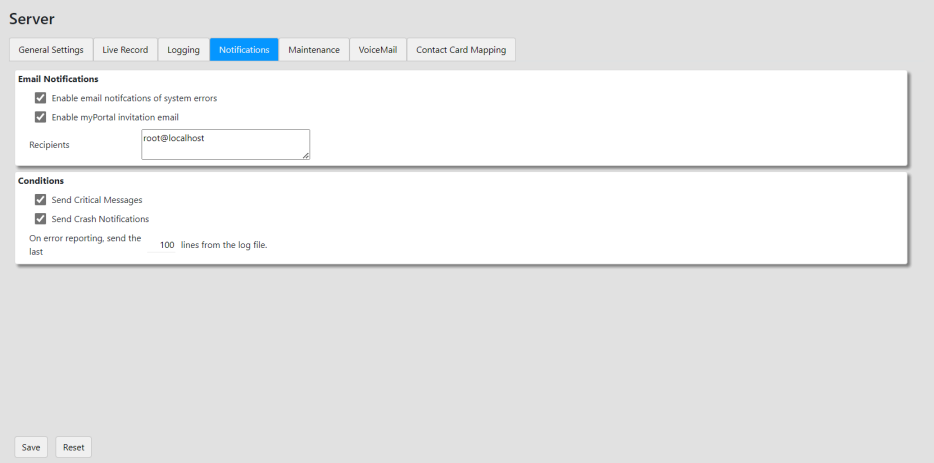
Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Diagnostico** > **Trace**.
3) Haga clic en **Protocolos de diagnóstico**.
4) Haga clic en **Ningún protocolo**, para desactivar las casillas de verificación de todos los protocolos.
5) Active la casilla de verificación **Protocolos de aplicaciones**.
6) Elija una de estas opciones:
   - Si desea descargar todo el protocolo existente, en la lista desplegable seleccione **Todo el protocolo**.
   - Si desea descargar el protocolo del día en curso, en la lista desplegable seleccione **Protocolo de hoy**.
   - Si desea descargar el protocolo de un periodo determinado, en la lista desplegable seleccione **Selección propia**. En la lista desplegable **Desde:** seleccione el inicio y en la lista desplegable **Hasta:**, el final del periodo deseado.
7) Haga clic en **Cargar** y, a continuación, en **Aceptar**. Se abre la ventana de descarga de archivos.
8) Guarde el archivo en el directorio deseado. A continuación, cierre la ventana que confirma la descarga del archivo.
9) Haga clic en **Continuar** y, a continuación, en **Salir**.

25.14.2 Notificación

Se pueden enviar **notificaciones de email** a los **Destinatarios** indicados para advertir por anticipado sobre niveles de uso crítico del disco duro o sobre errores.



El envío de correos electrónicos se puede vincular a las siguientes **condiciones**:

Condiciones	Ajuste estándar
Enviar mensajes críticos	Activado
Enviar notificaciones de caída del sistema	Activado

Es conveniente activar y enviar notificaciones y avisos importantes sobre las caídas del sistema. Estos mensajes advierten a sus destinatarios sobre un posible problema que debe ser comunicado al servicio técnico responsable.

Además, se puede definir cuántas líneas del final del archivo de protocolo se enviarán con el correo electrónico. Se pueden notificar los siguientes errores del sistema (solo en inglés):

Error del sistema
NULL monitor
Could not notify CallHandler
Terminate call failed
Unable to load VM Structure from file
Alsa stuck
Alsa cancel failed
MEN CallID 0
NULL alsa handle
Database connection failed
Rules engine logic failure
Config schema format failure
90% Disk usage mark
Principal: Could not connect to the database !
Principal: Could not load the configuration from the database!
Principal: Could not open configuration file !
Principal: Could not read the settings from the configuration file !

Error del sistema
A segmentation fault was detected.
Database logic error
Database schema error
ConnectionServer failed to start
MultisiteSync failed to start
Multisite failed to start
TransferManager failed to start
IPC failed to start
ConferenceManager failed to start
CallManager failed to start
MediaProcessing failed to start
Queues failed to start
Import failed to start
Data client failed to start
DirectoryClient failed to start
DirectoryServer failed to start
FV failed to start
IM failed to start
Switch failed to start
No Switches
Exchange Integration failed to start
Outbound Fax failed to start
SQL connection pool failed to start
Task scheduler failed to start
Trunks failed to start
Unknown switch type
Users failed to start
MEB has been disconnected
MEB ACK timeout
Switch Heartbeat timeout

25.14.2.1 Cómo configurar notificaciones por correo electrónico de errores del sistema

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor** seguido de **Notificaciones**.
4) Seleccione la configuración deseada para la notificación por correo electrónico, en el área **Notificaciones por correo electrónico**:
   - Si desea recibir notificaciones por correo electrónico, active la casilla de verificación **Habilitar notificaciones de errores del sistema**.
   - Si no desea notificaciones por correo electrónico, desactive la casilla de verificación **Habilitar notificaciones por correo electrónico de errores del sistema**.
5) Introduzca las direcciones de correo electrónico de las personas a las que se enviarán las notificaciones por correo electrónico en el campo **Destinatarios**. Diferentes direcciones de correo electrónico deben estar separadas por una coma `","` seguido de un espacio `" "`.
6) Seleccione la configuración deseada para mensajes críticos
   - Si desea recibir notificaciones por correo electrónico para mensajes críticos, active la casilla de verificación **Enviar mensajes críticos**.
   - Si no desea notificaciones por correo electrónico para mensajes críticos, desactive la casilla de verificación **Enviar mensajes críticos**.
7) Seleccione la configuración deseada para notificaciones de bloqueo
   - Si desea recibir notificaciones por correo electrónico de fallos del sistema, active la casilla de verificación **Enviar notificaciones de fallos**.
   - Si no desea recibir notificaciones por correo electrónico de fallos del sistema, desactive el **envío de notificaciones de fallos**.
8) Introduzca el número de líneas de archivo de registro que se enviarán con un correo electrónico en el campo **Enviar líneas de archivo de registro**.
9) Haga clic en **Guardar**.

25.14.3 Mantenimiento

Mediante el mantenimiento se pueden definir periodos de retención para los mensajes, la información sobre llamadas del diario, las llamadas grabadas con myAgent, los faxes y correos electrónicos recibidos y enviados, los correos electrónicos del Contact Center y los archivos de protocolo.

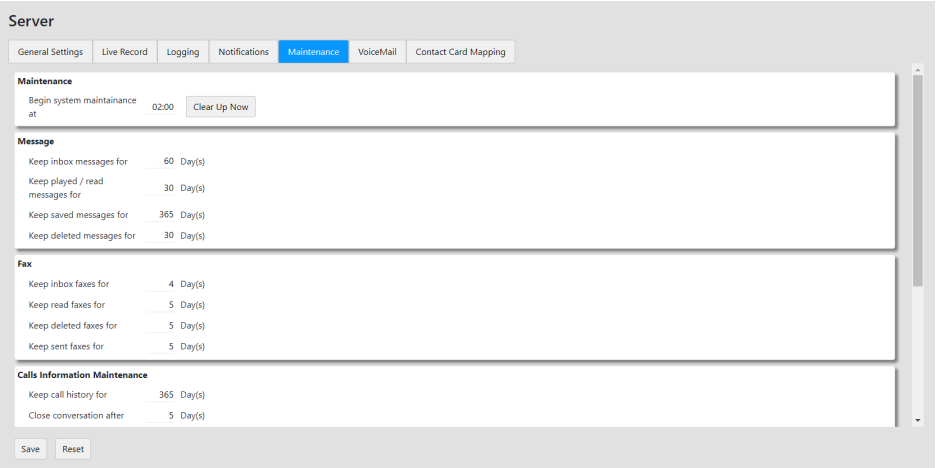
Además se puede configurar a qué hora se borrarán estos datos (una vez superados los tiempos de retención establecidos):

- Mensajes
- Información de llamada en el diario de llamadas (Historial de llamadas)
- Llamadas grabadas con myAgent (Contact Center)
- Faxes y correos electrónicos recibidos y enviados del Contact Center
- Archivos de protocolo

El ajuste estándar es 2:00 horas.

Además es posible iniciar inmediatamente el mantenimiento del sistema y, con ello, iniciar el borrado inmediato de los datos indicados (una vez superados los tiempos de retención establecidos). Esto puede ser necesario, por ejemplo, si

el disco duro del sistema de comunicación ha alcanzado un nivel de llenado crítico.



Para obtener más información sobre **Mantenimiento de mensajes**, consulte Buzón de voz.

Para obtener información sobre **Mantenimiento de mensajes de fax**, consulte Buzón de fax.

Para obtener más información sobre **Mantenimiento de información de llamadas**: Historial de llamadas, consulte Diario.

Con **Mantenimiento de información de llamadas**: **Contact Center**, se borran las llamadas grabadas de myAgent y los faxes y correos electrónicos enviados y recibidos del Contact Center que hayan superado el periodo de retención definido. El ajuste estándar para el periodo de retención de los datos del Contact Center son 60 días.

Consejo: Los periodos de conservación para el mantenimiento de información de llamadas son independientes unos de otros.

Los informes de Contact Center se basan en el historial de llamadas. Si para el historial de ha llamado se ha configurado un periodo de retención más corto que para los datos del Contact Center, es posible que algunos informes ya no estén disponibles.

Durante el **Mantenimiento de archivo de protocolo**, se eliminan los archivos de protocolo que hayan superado el periodo de retención establecido. El ajuste estándar para el tiempo de conservación de los archivos de protocolo es de 10 días.

25.14.3.1 Cómo configurar la hora para el mantenimiento

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.

2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor** y luego en **Mantenimiento**.
4) Introduzca la hora a la que se debe llevar a cabo el mantenimiento diario en el campo **Comenzar mantenimiento de sistema a las**, en la sección **Mantenimiento**. A la hora aquí definida se comenzarán a borrar los mensajes, la información de llamada del diario de llamadas y los archivos de protocolo que hayan superado los periodos de retención establecidos.
5) Haga clic en **Guardar**.

25.14.3.2 Cómo configurar el periodo de retención de los archivos de protocolo

Requisitos previos

Ha iniciado sesión en WBM con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor** y luego en **Mantenimiento**.
4) Introduzca el periodo de retención en días en el campo **Conservar información de protocolo para**, en la sección **Mantenimiento de archivo de protocolo**. Los archivos de protocolo se eliminan una vez superado el periodo de retención establecido.
5) Haga clic en **Guardar**.

25.14.3.3 Cómo ejecutar un mantenimiento del sistema inmediato

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor** y luego en **Mantenimiento**.
4) Haga clic en **Borrar ahora**, en la sección **Mantenimiento**.

Consejo: Se eliminan los mensajes, la información de llamadas del diario, las llamadas grabadas con myAgent, los faxes y correos electrónicos recibidos y enviados del Contact Center y los archivos de protocolo que hayan superado los periodos de retención definidos.

---

5) Haga clic en **Aceptar** para confirmar la eliminación.

25.14.3.4 Cómo configurar el tiempo de retención para los datos del Contact Center

Requisitos previos

Ha iniciado sesión en WBM (Gestión basada en Web) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **OpenScape Business UC Suite**.
3) Haga clic en **Servidor** y luego en **Mantenimiento**.
4) Introduzca el periodo de retención en días en el campo **Contact Center**, en la sección **Mantenimiento de información de llamadas**. Las llamadas grabadas con myAgent y los faxes y correos electrónicos para el Contact Center enviados y recibidos se borran cuando superan el tiempo de retención definido aquí.
5) Haga clic en **Guardar**.

25.15 Supervisión de UC Smart

Los administradores con el perfil **Experto** pueden consultar el estado actual de UC Smart mediante la Gestión basada en Web (WBM).

25.15.1 Cómo consultar el estado actual de UC Smart

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

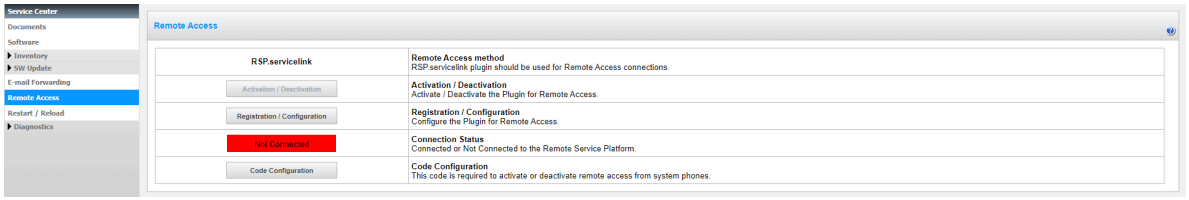
Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Aplicaciones** > **UC Smart**.
3) Haga clic en **Estado**.

   Se muestra el estado actual del servidor de aplicaciones y el número de conexiones activas de los distintos clientes de UC.

25.16 Servicios remotos

Distintos servicios remotos permiten a los técnicos de servicio autorizados acceder de forma remota al sistema de comunicación y a los componentes conectados. De esta forma se pueden realizar tareas de mantenimiento de forma económica y los usuarios reciben asistencia in situ para la resolución de problemas.



Debido a los elevados estándares de seguridad, es preferible el servicio remoto mediante RSP.servicelink. Para obtener más información, véase RSP.servicelink.

25.16.1 RSP.servicelink

Acceso remoto con RSP.servicelink (**R**emote **S**ervice **P**latform) ofrece a los técnicos de servicio autorizados de un RSP la posibilidad de administrar el sistema de comunicación (incluidas las aplicaciones UC Booster) de forma remota, cómoda y segura. Para configurar RSP.servicelink, solo se requiere una conexión a Internet, un navegador Web, el Partner ID y la contraseña de su colateral de servicio remoto. RSP.servicelink garantiza una conexión de banda ancha con alta seguridad.

RSP.servicelink utiliza tecnología OpenVPN. Utiliza el cifrado y el protocolo SSL/TLS, y proporciona un grado máximo de seguridad con un certificado de cliente adicional. El término RSP.servicelink se abrevia como RSP en la documentación.

Nota: RSP utiliza el rango 100.64.0.1 - 100.127.255.254 para la interfaz tun0, cuando RSP está activo, lo que significa que si es necesario acceder a una IP externa dentro de este rango, se debe agregar una ruta estática en el sistema Open Scape Business para encaminar el tráfico a través de la interfaz deseada.

Combinado con OpenScape Business, RSP ofrece estas importantes ventajas:

- Alta seguridad mediante conexión de Internet saliente

  El establecimiento de conexión remoto se inicia siempre mediante el sistema de comunicación. Esto significa que el firewall de la red de clientes solo debe autorizar una conexión HTTPS con una única dirección del centro de servicios remotos (puerto 443). En condiciones normales no hace falta modificar las políticas de seguridad del cliente ni de sus firewalls, ya que por norma general este puerto ya suele estar abierto en el firewall del cliente. De esta forma se garantiza una gran seguridad para la red de clientes.

  RSP permite al administrador del sistema de comunicación controlar la conexión remota mediante la activación y desactivación del acceso. En el caso de RSP.servicelink, se instala también automáticamente un certificado de cliente.
- Elevado ancho de banda

  En caso de error, la conexión de Internet de banda ancha permite transmitir rápidamente los datos de diagnóstico, aumentando así la calidad del servicio.

- Configuración sencilla y económica

  El software del sistema de comunicación ya incluye un RSP.servicelink. Al activar el plugin de servicio se introduce el Partner ID y la contraseña de su colateral de servicio remoto.

  Todos los proveedores de servicios remotos que utilizan RSP.servicelink tienen un Partner ID propio.

  El plugin RSP.servicelink se debería desactivar y reactivar antes de realizar una actualización de software.
- Seguridad de cara al futuro

  RSP es la base para servicios futuros (servicios de valor añadido) como, por ejemplo, la automatización de copias de seguridad, generación de informes y supervisión.

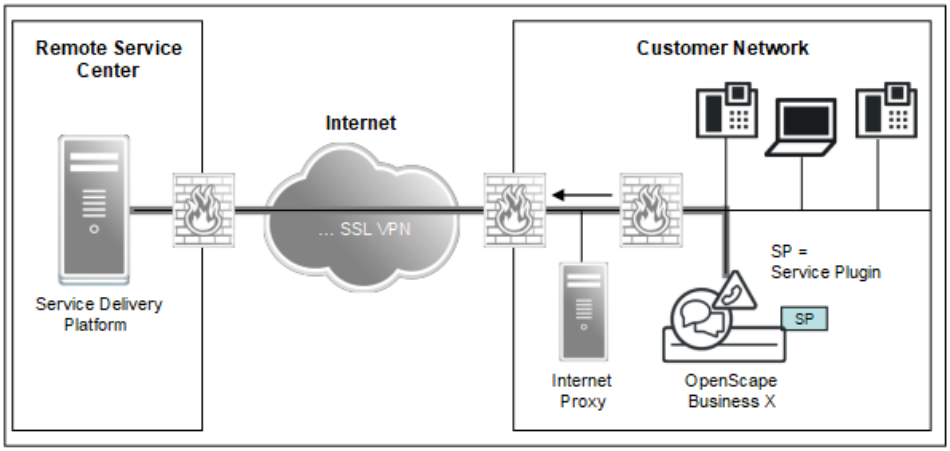


Figura 17: RSP – Vista general para OpenScape Business X

RSP es compatible con los estándares de Web Services, entre ellos, HTTPS (Hypertext Transfer Protocol Secure), SOAP (Simple Object Access Protocol) y XML (Extensible Markup Language).

Para RSP.servicelink, la comunicación entre el lado del cliente y el centro de servicios remoto se garantiza siempre con un cifrado AES-256-CBC.

Plugins de servicio

El plugin RSP.servicelink plugin se puede activar o desactivar de forma individual.

Después de sustituir la placa base hay que restablecer el plugin RSP.servicelink. Al hacer el restablecimiento se borra toda la configuración RSP y se desactiva el plugin de servicio.

Nota: Si el sistema no está en modo DTAG y el plugin RSP.servicelink está activo, no es posible modificar la configuración de proxy. El botón **Registro/Configuración** está deshabilitado.

En modo DTAG, si el plugin RSP.servicelink está activo, al pulsar el botón Registro/Configuración se muestra directamente la página de configuración de proxy con los botones Anular/Salir. También es posible hacerlo desde el servidor remoto.

Administración de dispositivos (dispositivo administrado)

En sistemas de comunicación sin UC Booster, se puede habilitar el acceso remoto a otros dispositivos en la LAN del cliente mediante la configuración en el lado de SIRA. En el lado SIRA se pueden configurar teléfonos IP con la función "Dispositivos gestionados".

Consejo: El acceso remoto a otros sistemas de comunicación OpenScape Business presentes en la LAN de clientes no es posible. Hay que configurar para acceso remoto todos los OpenScape Business.

Activación / Desactivación

Para activar o desactivar los plugins de servicio, existen las opciones siguientes:

- con el asistente **Habilitar / Deshabilitar**

  Para los plugins de servicio RSP, existe un asistente propio para la activación o desactivación.
- introduciendo un código en el teléfono del sistema (valores estándares: activación con *996 y desactivación con #996)

  Por motivos de seguridad, en la activación o desactivación mediante un teléfono del sistema hay que introducir además un PIN de cuatro dígitos. Este PIN se configura en la Gestión basada en Web (WBM) del sistema de comunicación con el perfil **Advanced**.

Copia de seguridad y recuperación de datos

Las credenciales de RSP se almacenan en el conjunto de seguridad del sistema.

Si se configura un nuevo sistema OpenScape Business mediante clonación o restauración de datos (migración), y el sistema original tenía configurado el acceso RSP, se debe garantizar que el sistema clonado o restaurado tenga una configuración RSP diferente activa.

Debe desactivar o desinstalar el RSP antes de clonar o realizar una copia de seguridad del sistema original.

Si se utiliza un certificado para conectarse a RSP en más de un sistema, el certificado se revocará y ninguno de los sistemas OpenScape podrá conectarse al servicio RSP.

Requisitos previos

- Acceso a Internet para el sistema de comunicación o el proxy HTTP en la LAN de clientes.
- Activar el firewall en la LAN de clientes para registradores:
  - https://188.64.18.51
  - https://188.64.17.51
- Activar el firewall en la LAN de clientes para VPN:
  - https://188.64.18.50
  - https://188.64.17.50
- En la configuración de Internet hay que introducir el router estándar.

Nota: Si el sistema está en modo DTAG durante el arranque del sistema y tiene acceso a Internet sin haber instalado y configurado RSP.serviceplugin, un script instalará, configurará y activará automáticamente RSP.serviceplugin con el Id. de socio y la contraseña de DTAG (el nombre del dispositivo será la dirección MAC del sistema). El script se llamará periódicamente cada 10 minutos (por ejemplo, si no hay acceso a Internet después de la instalación inicial del sistema). El script no activará automáticamente RSP.serviceplugin si el usuario lo ha desactivado de forma manual.

25.16.1.1 Cómo instalar, configurar y registrar el plugin RSP.servicelink

El asistente **Registro / Configuración** permite instalar, configurar y registrar el plugin RSP.servicelink para el acceso remoto al sistema de comunicación mediante RSP.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Acceso remoto**.
3) Haga clic en **Registro / Configuración**.
4) Si el plugin RSP.servicelink todavía no está instalado, haga clic en **Instalar** y, a continuación, en **OK y Continuar**.
5) Si el plugin RSP.servicelink ya está instalado, haga clic en **OK & Continuar**.
6) Si en la red de clientes no se utiliza ningún servidor proxy, haga clic en **OK&Continuar**, porque no es necesario configurar los **Parámetros Proxy**. Omita los dos pasos siguientes.
7) Si en la red de clientes se utiliza un servidor proxy, hay que seleccionar el ajuste de los **Parámetros Proxy** en función de la red de clientes:
   - Si en la red de clientes hay un proxy con protocolo HTTP, active la casilla de verificación **Utilizar pila HTTP proxy**. En el campo **HTTP Proxy Host**, indique el nombre de host, y en el campo **HTTP Proxy Port** indique el número de puerto del servidor de proxy. Si es necesario, en el campo **Nombre de usuario** indique el nombre de usuario, y en el campo **Contraseña** indique la contraseña para la autenticación del servidor de proxy.
   - Si en la red de clientes hay un proxy con el protocolo SOCKS, active la casilla de verificación**Utilizar pila SOCKS proxy**. En el campo **SOCKS Proxy Host**, indique el nombre de host, y en el campo **SOCKS Proxy Port** indique el número de puerto del servidor de proxy. Si es necesario, en el campo **Nombre de usuario** indique el nombre de usuario, y en

el campo **Contraseña** indique la contraseña para la autenticación del servidor de proxy.

Consejo: El tipo y la configuración del servidor de proxy determina si es necesaria o no la autenticación.

8) Haga clic en **OK & Continuar**.
9) Si en necesario, en el campo **Partner ID** modifique el Partner ID predefinido.
10) En el campo **Contraseña** introduzca su contraseña.
11) Introduzca el nombre del dispositivo. Puede encontrar el dispositivo con el nombre del dispositivo en el SIRA Equipment Explorer (EqE). La dirección MAC de OpenScape Business es la entrada predeterminada.
12) Haga clic en **Salir**.

En la columna **RSP.servicelink**, en la fila **Connection Status** (Estado de conexión) se indica si el registro se ha realizado correctamente. Si el registro no ha sido correcto, pueden aparecer los mensajes de error siguientes:

- MAC already registered:

  Solución: borrar el dispositivo (sistema de comunicación OpenScape Business) del SIRA Equipment Explorer y registrarlo de nuevo con el asistente **Registro / Configuración**.

  Nota: Mediante el nombre del dispositivo o la dirección MAC, encontrará el dispositivo en el SIRA Equipment Explorer. Puede encontrar el nombre del dispositivo o la dirección MAC del sistema de comunicación OpenScape Business en el **Centro de servicios**, en **Acceso remoto**.

- Error de configuración:

  Solución: en el asistente **Registro / Configuración**, introduzca de nuevo el Partner ID y la contraseña y finalice el asistente correctamente.

- Credenciales erróneas:

  Solución: en el asistente **Registro / Configuración**, introduzca de nuevo el Partner ID y la contraseña y finalice el asistente correctamente.

25.16.1.2 Cómo activar el plugin RSP.servicelink

El asistente **Activación / Desactivación** permite activar el plugin RSP.servicelink para el acceso remoto al sistema de comunicación mediante RSP.

Requisitos previos

Hay disponible una configuración de DNS operativa.

Hay disponible un router estándar para acceder a Internet o, como alternativa, un servidor proxy en la red de cliente.

El plugin RSP.servicelink está desactivado.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Acceso remoto**.
3) En la columna **RSP.servicelink**, haga clic en **Habilitar / Deshabilitar**.
4) Haga clic en **Activar**.

25.16.1.3 Cómo desactivar el plugin RSP.servicelink

El asistente **Activación / Desactivación** permite activar el plugin RSP.servicelink para el acceso remoto al sistema de comunicación.

Requisitos previos

El plugin RSP.servicelink está activado.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Acceso remoto**.
3) Haga clic en **Activar/Desactivar** en la columna **RSP.servicelink**.
4) Haga clic en **Desactivar**.

25.16.1.4 Cómo restablecer el plugin de servicio RSP

Con el asistente **Habilitar / Deshabilitar** puede restablecer el plugin de servicio RSP. Con ello se borra toda la configuración RSP y se desactiva el plugin de servicio RSP.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Acceso remoto**.
3) En la columna **RSP.servicelink**, haga clic en **Habilitar / Deshabilitar**.
4) Haga clic en **Restablecer a valores predeterminados** y a continuación en **OK**.
5) En la columna **RSP.servicelink**, haga clic en **Habilitar / Deshabilitar**.
6) Haga clic en **Desactivar**.

7) Elimine el dispositivo (=sistema de comunicación OpenScape Business) en el servidor SIRA.

Nota: Mediante la dirección MAC, encontrará el dispositivo en el servidor SIRA. Puede encontrar la dirección MAC del sistema de comunicación OpenScape Business en el **Centro de servicios**, en **Inventario**.

25.16.1.5 Cómo configurar un PIN para activar y desactivar el plugin RSP.servicelink

El PIN permite activar y desactivar el plugin RSP.servicelink mediante un teléfono del sistema.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Acceso remoto**.
3) En el campo **PIN**, introduzca el PIN de cuatro dígitos deseado.
4) Haga clic en **Guardar** y a continuación en **Aceptar**.

Pasos siguientes

Para activar el plugin de servicio primario con un teléfono del sistema, hay que introducir el código correspondiente (código estándar = *996) y, a continuación, el PIN de cuatro dígitos.

Para desactivar el plugin de servicio con un teléfono del sistema, hay que introducir el código correspondiente (código estándar = #996) y, a continuación, el PIN de cuatro dígitos.

25.16.2 Acceso remoto

Con el Acceso remoto, se puede permitir el acceso remoto a los sistemas de comunicación OpenScape Business X por conexión Internet a técnicos de servicio autorizados. Esto permite, por ejemplo, compatibilidad con la activación de tareas administrativas o con la búsqueda de errores.

Para permitir el acceso remoto al sistema de comunicación hay que activarlo antes. El siguiente método de acceso es posible:

Acceso remoto por Internet

Consejo: El acceso remoto por Internet supone un mayor riesgo para la seguridad.

Para el acceso telefónico por Internet, el técnico de servicios necesita un puerto especial (**Número puerto**) para acceder al sistema de comunicación. De forma

predeterminada, está registrado el número de puerto 10099. Si se utiliza un router externo, hay que configurar en él un desvío de puerto para este número de puerto.

El número de puerto solo se puede bloquear por un cortafuegos (si lo hay) del PC del técnico de servicio. Por ello, la selección del número de puerto debe ser coordinada con el técnico.

Las aplicaciones de UC Booster (p.ej. UC Suite, OpenDirectory Service, Gate View) no se pueden administrar con este acceso remoto.

Para desactivar el acceso remoto al sistema de comunicación, hay que desactivar la función.

Nota: Para impedir el acceso no autorizado al sistema de comunicación, una vez finalizada la administración remota hay que volver a desactivar el acceso remoto.

25.16.2.1 Cómo activar el acceso remoto por RDSI

Con el asistente **Acceso remoto** puede permitir el acceso de técnicos de servicio autorizados al sistema de comunicación a través de una conexión RDSI.

Requisitos previos

OpenScape Business X cuenta con una conexión de línea urbana RDSI.

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Acceso remoto**.
3) Haga clic en **Acceso remoto** para iniciar el asistente **Acceso remoto**.
4) Active la opción **Acceso remoto: act.**, para activar el acceso remoto.
5) Active el campo de opción **Acceso remoto a través de: RDSI**, para activar el acceso remoto por RDSI.
6) En el campo **Número de teléfono**, indique el número de teléfono por el que se ha de realizar el acceso remoto.
7) En el campo **Número de acceso telefónico**, indique el número de marcación directa por el que se ha de realizar el acceso remoto.
8) Haga clic en **OK & Continuar** y, a continuación, en **Salir**.

25.16.2.2 Cómo configurar un PC con Microsoft Windows Vista para el acceso remoto a través de RDSI

Requisitos previos

El PC cuenta con una tarjeta RDSI y con una conexión de línea urbana RDSI.

Hay que acceder con un sistema de comunicación OpenScape Business X3/X5/X8 con conexión de centralita. Se dispone del código de red local y del número de teléfono del sistema del sistema de comunicación.

Se ha activado el acceso remoto a través de RDSI. Se dispone del número de acceso telefónico del sistema de comunicación.

Se dispone del nombre de usuario y de la contraseña para acceder al sistema de comunicación.

Consejo: Esta descripción se refiere a un PC con el sistema operativo Microsoft Windows Vista. El proceso es similar para el sistema operativo Microsoft Windows XP.

Paso a paso

1) En el **menú Inicio** de Windows Vista, haga clic en **Conectar a**. Se abre la ventana **Conectarse a una red**.
2) Haga clic en **Configurar una conexión o red**.
3) Haga clic en la opción de conexión **Conectarse a un área de trabajo** y, a continuación, haga clic en **Continuar**.
4) Haga clic en **Llamar directamente**.
5) En el campo **Número de teléfono**, indique el código urbano (por ejemplo `0`), el código de red local (por ejemplo `089`), el número de teléfono del sistema (por ejemplo `12345678`) y el número de acceso telefónico (por ejemplo `666`).

   La entrada completa del ejemplo citado es: `008912345678666`
6) En el campo **Nombre de conexión**, indique un nombre para la conexión.
7) Active la casilla de verificación **No conectarse ahora; configurar para conectarse más tarde**.
8) Haga clic en **Continuar**.
9) En el campo **Nombre de usuario**, indique el nombre de usuario para acceder al sistema de comunicación.
10) En el campo **Contraseña**, indique la contraseña para acceder al sistema de comunicación.

    Nota: Como datos estándar para acceder al sistema de comunicación se utilizan el nombre de usuario estándar y la contraseña estándar para el acceso de sistema mediante la herramienta de servicio Manager E.

    ---
11) Haga clic en **Crear**.
12) Haga clic en **Conectarse ahora**.

De esta forma se puede acceder de forma remota al sistema de comunicación.

Consejo: Para desactivar la conexión, haga clic en **Inicio** > **Conectar a**. Haga clic en la designación definida en el paso 6 (**nombre de destino**) y, a continuación, haga clic en **Desconectar**.

La conexión se puede activar haciendo clic en la denominación definida en el paso 6 (**nombre de destino**) y, a continuación, en **Conectar**.

25.16.2.3 Cómo configurar un PC con Microsoft Windows 7 para el acceso remoto a través de RDSI

Requisitos previos

El PC cuenta con una tarjeta RDSI y con una conexión de línea urbana RDSI.

Hay que acceder con un sistema de comunicación OpenScape Business X3/X5/X8 con conexión de centralita. Se dispone del código de red local y del número de teléfono del sistema del sistema de comunicación.

Se ha activado el acceso remoto a través de RDSI. Se dispone del número de acceso telefónico del sistema de comunicación.

Se dispone del nombre de usuario y de la contraseña para acceder al sistema de comunicación.

Consejo: Esta descripción se refiere a un PC con el sistema operativo Microsoft Windows 7.

Paso a paso

1) En el **menú Inicio** de Windows 7 haga clic en **Panel de control**.
2) Haga clic en **Redes e Internet**.
3) Haga clic en **Centro de redes y recursos compartidos**.
4) Haga clic en **Configurar una conexión o red**.
5) Haga clic en la opción de conexión **Conectarse a un área de trabajo** y, a continuación, haga clic en **Continuar**.
6) Haga clic en **Llamar directamente**.
7) En el campo **Número de teléfono**, indique el código urbano (por ejemplo `0`), el código de red local (por ejemplo `089`), el número de teléfono del sistema (por ejemplo `12345678`) y el número de acceso telefónico (por ejemplo `666`).

   La entrada completa del ejemplo citado es: `008912345678666`
8) En el campo **Nombre de conexión**, indique un nombre para la conexión.
9) Active la casilla de verificación **No conectarse ahora; configurar para conectarse más tarde**.
10) Haga clic en **Continuar**.
11) En el campo **Nombre de usuario**, indique el nombre de usuario para acceder al sistema de comunicación.
12) En el campo **Contraseña**, indique la contraseña para acceder al sistema de comunicación.

Nota: Como datos estándar para acceder al sistema de comunicación se utilizan el nombre de usuario estándar y la contraseña estándar para el acceso de sistema mediante la herramienta de servicio Manager E.

13) Haga clic en **Crear**.
14) Haga clic en **Conectarse ahora**. Por último, aparece el mensaje `Se ha establecido la conexión`.
15) Haga clic en **Cerrar**.

De esta forma se puede acceder de forma remota al sistema de comunicación.

Consejo: Para desactivar la conexión, en la barra de herramientas haga clic en el símbolo **Red**. Haga clic en la designación definida en el paso 8 (**nombre de destino**) y, a continuación, haga clic en **Desconectar**.

La conexión se puede activar haciendo clic en la designación definida en el paso 8 (**nombre de destino**) y, a continuación, en **Conectar**.

25.16.2.4 Cómo activar el acceso remoto a través de acceso a Internet con dirección IP fija

Con el asistente **Acceso remoto** puede permitir el acceso de técnicos de servicio autorizados al sistema de comunicación a través de una conexión de Internet.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Tiene el número de puerto por el que el técnico de servicio puede acceder vía Internet al sistema de comunicación. Este número de puerto solo se puede bloquear por un cortafuegos (si lo hay) del PC del técnico de servicio.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Acceso remoto**.
3) Haga clic en **Acceso remoto** para iniciar el asistente **Acceso remoto**.
4) Active la opción **Acceso remoto: act.**, para activar el acceso remoto.
5) Active el campo de opción **Acceso remoto a través de: Internet**, para activar el acceso remoto por Internet.
6) En el campo **Número puerto** indique el número de puerto por el que se ha de realizar el acceso remoto.

   De forma predeterminada, está registrado el número de puerto 10099.
7) Haga clic en **OK & Continuar**. Se muestra el mensaje `Se ha activado el acceso remoto...`. Este mensaje incluye el URLque permite acceder de forma remota al sistema de comunicación por navegador Web.
8) Haga clic en **Salir**.

25.16.2.5 Cómo activar el acceso remoto a través de acceso a Internet sin dirección IP fija

Con el asistente **Acceso remoto** puede permitir el acceso de técnicos de servicio autorizados al sistema de comunicación a través de una conexión de Internet.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Tiene el número de puerto por el que el técnico de servicio puede acceder vía Internet al sistema de comunicación. Este número de puerto solo se puede bloquear por un cortafuegos (si lo hay) del PC del técnico de servicio.

Hay una cuenta DynDNS.

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Acceso remoto**.
3) Haga clic en **Acceso remoto** para iniciar el asistente **Acceso remoto**.
4) Active la opción **Acceso remoto: act.**, para activar el acceso remoto.
5) Active el campo de opción **Acceso remoto a través de: Internet**, para activar el acceso remoto por Internet.
6) En el campo **Número puerto** indique el número de puerto por el que se ha de realizar el acceso remoto.

   De forma predeterminada, está registrado el número de puerto 10099.
7) Haga clic en **OK & Continuar**, para aplicar las entradas. Se abre la ventana **Configurar cuenta DynDNS**.
8) En el campo **Nombre de usuario** indique el nombre de usuario de su cuenta DynDNS de su proveedor, si no aparece ya en pantalla.
9) En el campo **Contraseña** y en el campo **Repetir contraseña**, indique la contraseña de la cuenta DynDNS de su proveedor, si esta información no aparece ya en pantalla.
10) En el campo **Nombre host**, introduzca el nombre de host sin nombre de dominio indicado por su proveedor DynDNS (por ejemplo, `mihost`), si no aparece ya en pantalla.
11) En la lista desplegable **Nombre dominio**, introduzca su proveedor DynDNS (por ejemplo, `dyndns.org`), si no aparece ya en pantalla. De esta forma, su nombre de dominio completo será, por ejemplo, `mihost.dyndns.org`.
12) Haga clic en **Prueba de conexión**. Se abre la ventana **Comprobar acceso DynDNS**.
13) Haga clic en **Aceptar**. Se transmiten al proveedor los datos de acceso DynDNS. El proceso dura unos 10 segundos.
14) Si la prueba ha sido correcta, se muestra el mensaje `Se ha activado el acceso remoto...`. Este mensaje incluye el URLque permite acceder de forma remota al sistema de comunicación por navegador Web. Haga clic en **Salir**.
15) Si la comprobación no ha terminado correctamente, haga clic en **Aceptar**. En la ventana que se abrirá a continuación, **Acceso DynDNS**, recibirá

indicaciones sobre las posibles causas del error. Haga clic en **Aceptar**. Se abre la ventana **Configurar cuenta DynDNS**. Compruebe y corrija, si es necesario, los datos de acceso indicados (pasos 8 a 11). Siga el procedimiento descrito en el paso 12.

25.16.2.6 Cómo desactivar el acceso remoto

Con el asistente **Acceso remoto** puede desactivar el acceso remoto.

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **Advanced** (Avanzado)).

Paso a paso

1) En la barra de navegación, haga clic en **Centro de servicios**.
2) En el árbol de navegación, haga clic en **Acceso remoto**.
3) Haga clic en **Acceso remoto** para iniciar el asistente **Acceso remoto**. Se muestra si el acceso remoto está activado por Internet y/o por RDSI.
4) Active el campo de opción **Acceso remoto: desact.**, para desactivar un acceso remoto.
5) Seleccione qué opción del acceso remoto desea desactivar:
   - Si desea desactivar el acceso remoto a través de Internet, active la opción **Acceso remoto a través de: Internet**.
   - Si desea desactivar el acceso remoto a través de RDSI, active la opción **Acceso remoto a través de RDSI**.
6) Haga clic en **OK & Continuar**.
7) Si también desea desactivar la segunda opción de acceso remoto, haga clic en **Volver**. Repita los pasos del 4 al 6.
8) Haga clic en **Salir**.

25.16.3 Usuario online

El Usuario online permite el control, la comprobación y la supervisión remotos de los teléfonos OpenStage mediante un equipo Windows. El comportamiento de un teléfono OpenStage se ilustra a través del Usuario online en el PC.

Para la comunicación con un teléfono OpenStage se requiere que el software del teléfono cuente con una clave dongle.

Para acceder a un teléfono OpenStage se requieren los siguientes datos sobre el Usuario online:

- Tipo de teléfono OpenStage
- Dirección IP del teléfono OpenStage
- Contraseña de administrador del teléfono OpenStage

Para obtener información sobre el uso del Usuario online, consulte la siguiente documentación: *OpenStage HUSIM Phone Tester User Guide* (en inglés). A través del portal de Intranet se puede acceder a documentación técnica de productos `http://apps.g-dms.com:8081/techdoc/search_en.htm`.

La herramienta de servicio Manager E también ofrece usuarios online para el control, la supervisión y la comprobación remotos de los teléfonos OpenStage.

Nota: La dirección IP de gateway notificada por el Usuario online es la misma que la dirección IP del sistema. La dirección IP de gateway no es la dirección IP de la ruta estándar.

25.16.3.1 Cómo iniciar el Usuario online

Requisitos previos

Ha iniciado sesión en la Gestión basada en Web (WBM) con el perfil **Experto**.

Paso a paso

1) En la barra de navegación, haga clic en **Modo Experto**.
2) En el árbol de navegación, haga clic en **Mantenimiento** > **Usuario online**. Se muestra la ventana de registro del Usuario online.
3) En la lista desplegable **Model** (Modelo) seleccione el modelo del teléfono OpenStage deseado.
4) En el campo **Phone IP** (IP del teléfono) introduzca la dirección IP del teléfono OpenStage deseado.
5) En el campo **Password** (Contraseña) introduzca la contraseña del administrador del teléfono OpenStage deseado. De forma predeterminada, la contraseña de administrador es `123456`.
6) En la lista desplegable **Protocolo**, seleccione el protocolo de transporte deseado.
7) Elija una de estas opciones para la versión de protocolo de Internet (IPv):
   - Si desea utilizar IP 4, active la opción **IPv4**.
   - Si desea utilizar IP 6, active la opción **IPv6**.
8) En la lista desplegable **Number of Key modules** (Número de módulos de teclas), seleccione el número de aparatos auxiliares.
9) Haga clic en **Aceptar** para iniciar el acceso al teléfono OpenStage deseado.

Consejo: Puede obtener información sobre el manejo del Usuario online en la guía *OpenStage HUSIM Phone Tester User Guide*, que puede consultar en la dirección `http://apps.g-dms.com:8081/techdoc/search_en.htm` (en inglés).

26 Migración

Los sistemas OpenScape Business V1, V2 y los sistemas HiPath 3000 se pueden migrar/actualizar a openScape Business V3.

Los siguientes escenarios de migración/actualización son compatibles con el software OpenScape Business V3.

Nota: Es vital eliminar los usuarios activos de Unify Phone antes de, por ejemplo, migraciones de sistema, para evitar discrepancias críticas entre la base de datos de OpenScape Business y la base de datos de la nube. Encontrará más información en el Libro blanco de Unify Phone en la wiki de expertos de Unify.

Nota: Véase también Cómo eliminar o eliminar usuarios de Unify Phone en la página 1224.

Sistema OpenScape Business X, incluidos UC Booster Card o Booster Server

- Actualización de software de OpenScape Business X V2 a V3 con «placa base V2»
- Migración de hardware/software de OpenScape Business X V2 a V3 con «placa base V3»
- Migración de hardware/software de OpenScape Business X V1 a V3 con «placa base V3»
- Migración de hardware/software de OpenScape Business X V3 con «placa base V2» a V3 con «placa base V3»

Sistema OpenScape Business S

- Actualización de software de OpenScape Business S V2 a V3

Red OpenScape Business

- Migración/actualización de una red OpenScape Business de V2 a V3

HiPath 3000, incluido OpenScape Office HX

- Migración de hardware de HiPath 3000, incluido OpenScape Office HX

HiPath 500

- Migración de hardware de HiPath 500 a OpenScape Business X1 V3

Las licencias existentes se pueden transferir completa o parcialmente, según el sistema de origen. Lo mismo aplica para el uso continuo de módulos periféricos y terminales conectados.

La compatibilidad de software existente para los sistemas OpenScape Business no se modificará después de la migración.

Para simplificar la migración/actualización para el uso continuo de las licencias existentes, en contraposición con una transferencia de licencias "offline", conecte el sistema OpenScape Business al servidor central de licencias de Unify y utilice la función **CLS Connect**.

En esta sección, se utilizan los siguientes términos:

Migración	en caso de cambio de hardware y software
Actualización	en caso de cambio estrictamente de software
Placa base V2	término utilizado para la familia de la placa base introducida con OpenScape Business.
Placa base V3	término utilizado para la familia de la placa base que se ha introducido con el software V3.

Nota: Un requisito previo para todos los escenarios de migración con el fin de actualizar de una placa base V2 a un sistema de placa base V3, es que el administrador tiene que cargar el conjunto de copias de seguridad a través del dispositivo HTTPS. Otros dispositivos como discos duros, FTP o unidades de red no son compatibles y fallarán en el proceso de migración.

Nota: Existen dos rutas de migración válidas en función de la versión de software del sistema OSBiz. Utilice un conjunto de copia de seguridad de un sistema de hardware V2 en el último enlace V2R7, o use el mismo enlace de software V3 en ambos sistemas de placa base V2 y V3 para asegurar la consistencia en la base de datos.

Nota: Si se va a sustituir un sistema OpenScape Office V3 MX/LX por un sistema OpenScape Business, este último debe pedirse como un sistema nuevo.

26.1 Actualización de software para sistemas OpenScape Business X

Básicamente, una actualización de software de los sistemas OpenScape Business X implica el reemplazo de algunos componentes de software.

Antes de actualizar el software de un sistema OpenScape Business X, debe determinar la configuración del sistema actual y los componentes de hardware/software y de licencia que van a reemplazarse, si corresponde.

Tabla 31: Actualización de software de OpenScape Business X - Lista de comprobación de hardware/software

Componentes	Reemplazado por
Componentes de hardware	
Componentes de software	
Software de sistemas V2 en la tarjeta SDHC	Software del sistema V3 (imagen en el Software Download Server)

Componentes	Reemplazado por
VPN en Wan con punto de terminación en el sistema	VPN con punto de terminación en router externo
XMPP	Sin solución sucesora
myPortal Smart	myPortal @work
Componentes de licencia	
Licencias en archivo de licencia	Transferencia de las licencias a un nuevo archivo de licencia

26.1.1 Actualización de software de OpenScape Business X V2 a OpenScape Business X V3

Al actualizar el software de un modelo OpenScape Business X de la versión de software V2 a V3, solo se reemplaza el software del sistema. Se conservan la placa base V2 y cualquier UC Booster Card o Booster Server. Las licencias y la configuración de cliente existentes se mantienen. La compatibilidad de software existente se mantiene sin cambios después de la migración.

Antes de la actualización de software de la versión V2 a V3, debe configurar, de no existir, un acceso permanente al servidor de licencias de Unify (a través de Internet) en el sistema y activar la función **CLS Connect**. De esta manera, se simplifica la transferencia de licencias y se acorta el tiempo de migración de manera considerable.

Requisitos previos

Para la actualización de software y la transferencia de la configuración de cliente existente, el sistema debe operar con la última versión de software V2R7 publicada antes de la actualización. De ser necesario, actualice el sistema a la última versión de software. Para ello el sistema debe tener un estado válido de compatibilidad de software.

Para la actualización del software del sistema de V2 a V3, según si se utiliza o no CLS Connect, se requiere el siguiente elemento:

- Licencia OpenScape Business V3 SW Upgrade (solo cuando no se utiliza **CLS Connect**)

Condiciones y restricciones de límites funcionales

Durante el transcurso de la migración, las licencias existentes se pueden transferir completamente de la placa base V2 existente a la placa base V3. La transferencia de licencia sin la activación de la función CLS Connect requiere la licencia «SW Upgrade», un tratamiento mucho más complejo y un gasto de tiempo mayor que si se utiliza la función CLS Connect.

La configuración de cliente y los datos de cliente se transfieren automáticamente de la versión de software V2 a V3 durante el proceso de actualización de software.

Los pasos técnicos principales de la actualización de software se describen en los siguientes capítulos. Para conservar las licencias existentes, en relación al tratamiento, se debe distinguir entre:

- Actualización de software con licencia permanente con y sin CLS Connect

- Actualización de software con licencia PayGo

26.1.1.1 Actualización de software de sistemas con licencia permanente con CLS Connect

Siga estos pasos de actualización en orden.

Paso a paso

1) Preparar el sistema OpenScape Business
   a) Actualice el sistema existente a la versión de software V2R7.
   b) Configure el acceso al servidor central de licencias (CLS) de Unify en el sistema y compruebe la conexión.
   c) Active **CLS Connect** en el sistema.

2) Actualizar el software
   a) Actualice el software V3 mediante OpenScape Business Assistant.
   b) La configuración del sistema se transfiere automáticamente a V3.
   c) Las licencias existentes se transfieren después de la actualización a V3.

3) Generación automática del archivo de licencia mediante el servidor central de licencias

   Después de reiniciar el sistema, el sistema transfiere la información al CLS de que las licencias existentes operan con la versión de software 3.

26.1.1.2 Actualización de software de sistemas con licencia permanente sin CLS Connect

Siga estos pasos de actualización en orden.

Paso a paso

1) Preparar el sistema OpenScape Business
   a) Actualice el sistema existente a la versión de software V2R7.

2) Crear el "archivo de licencia de upgrade" para el sistema V2 en el servidor central de licencias (CLS)
   a) Active la "Licencia de upgrade de software" para el sistema existente.
   b) Genere un nuevo archivo de licencia para la dirección MAC de la placa base V2.
   c) Descargue el archivo de licencia del CLS.

3) Importar y activar el archivo de licencia en el sistema OpenScape Business V2.

4) Actualizar el software
   a) Actualice el software V3 mediante OpenScape Business Assistant.
   b) La configuración del sistema se transfiere automáticamente a V3.
   c) Las licencias existentes en el sistema se transfieren a V3.

5) Reiniciar el sistema después de la actualización de software

26.1.1.3 Actualización de software de sistemas con licencia PayGo

Siga estos pasos de actualización en orden.

Paso a paso

1) Preparar el sistema OpenScape Business
   a) Actualice el sistema existente a la versión de software V2R7.
2) Regenerar el archivo de licencia en el servidor central de licencias (CLS)
   a) Regenere un nuevo archivo de licencia para la dirección MAC de la placa base V2.
   b) Descargue el archivo de licencia del CLS.
3) Importar y activar el nuevo archivo de licencia en el sistema OpenScape Business V2.
4) Actualización de software de OpenScape Business
   a) Actualice el software a V3 mediante OpenScape Business Assistant.
   b) La configuración del sistema se transfiere automáticamente a V3.
   c) El sistema está listo para operar después del reinicio.

26.2 Actualización de software de UC Booster Server a OpenScape Business X V3

La actualización de software de un UC Booster Server V2 a la versión V3 se puede realizar en un paso.

Una actualización de software de un UC Booster Server V1 a la versión V3 se debe realizar en dos pasos. Primero, actualice de V1 a V2R7, luego, de V2R7 a V3.

26.2.1 Cómo actualizar UC Business Booster Server v2 a v3

La actualización del software del servidor UC Booster de V2 a V3 solo es necesaria para los sistemas OpenScape Business X con una placa base V2. Los sistemas OpenScape Business X con placas base V3 ya no requieren un servidor UC Booster. En este caso, se requiere la versión V2.7 del software en el UC Booster Server para migrar la configuración del cliente y las licencias a la placa base V3.

Requisitos previos

- El sistema operativo Linux debe comprobarse y actualizarse si es necesario (consulte la *nota técnica de la versión del software del sistema OpenScape Business V3*)
- Antes de la actualización UC Booster Server funciona con la última versión de software publicada V2R7. Si es necesario, actualice el sistema a la última versión del software.
- En primer lugar, actualice el sistema OpenScape Business X al que está conectado el UC Booster Server a la versión V3 del software, incluidas las licencias, de acuerdo con la descripción en Actualización de software de OpenScape Business X V2 a OpenScape Business X V3 en la página 1403
- UC Booster Server SW Image V3

Antes de una actualización del software del UC Booster Server, determine la configuración actual del sistema y los componentes de hardware/software y licencia que pueden necesitar ser reemplazados.

Tabla 32: Migración de OpenScape Business S - Lista de comprobación de hardware/software

Componentes	Reemplazado por
Componentes de hardware	
PC servidor	La reutilización es posible. Los requisitos de hardware deben comprobarse para las extensiones de OpenScape Business S.[9]
Componentes de software	
Sistema operativo SLES 12 o SLES 15	La reutilización es posible. De forma eventual se puede requerir una actualización al último paquete de servicio. [10]
XMPP	Sin solución sucesora
myPortal Smart	myPortal @work
Componentes de licencia	
Licencias en el archivo de licencia (forma parte del archivo de licencia de OpenScape Business X)	Transferencia de las licencias a un nuevo archivo de licencia
Aplicación CSTA (a través de la tarjeta/servidor UC Booster)	Licencia CSTA para conectar soluciones externas (no necesaria para UC Suite, TAPI 170 y TAPI 120)

A continuación se describe la actualización del software OpenScape Business mientras se mantiene el sistema operativo SLES.

9 El hardware del PC servidor existente se puede utilizar cuando la configuración del sistema de UC Booster Server permanece sin cambios después de la actualización del software. Si se planean expansiones tras la actualización del software, es posible que sea necesario adaptar los requisitos de hardware de acuerdo con las especificaciones de la *Guía de instalación de OpenScape Business S, capítulo Requisitos previos*.

10 El sistema operativo SLES instalado en el PC servidor se puede adoptar en caso de una actualización del software del UC Booster Server. Sin embargo, debe actualizarse al último paquete de servicio publicado antes de la actualización del software.

Si Novell ha interrumpido el soporte de software para la versión de SLES utilizada, se debe informar al cliente y, si es necesario, se debe comercializar una actualización de SLES.

Es posible que la actualización de SLES deba realizarse en varios pasos para hacerse cargo de las instalaciones previas de OpenScape Business S, incluida la configuración y los datos del cliente. Una clave de actualización de SLES existente sigue siendo válida con una actualización de SLES. Sin embargo, es posible que tenga que darse de baja en Novell antes de la actualización de SLES y, a continuación, volver a registrarse en el nuevo sistema.

Paso a paso

1) Actualice el sistema OpenScape Business X a V3.

   Ver Actualización de software de OpenScape Business X V2 a OpenScape Business X V3 en la página 1403 para obtener más detalles.

2) Actualice el software del servidor UC Booster a V3

   Utilice la función de actualización dentro del OpenScape Business Assistant del servidor UC Booster para actualizar el SW V2R7 a la versión V3 (véase Actualización del sistema de comunicación en la página 1277).

3) Realizar una copia de seguridad de los datos después de la actualización del software

   Realice una copia de seguridad de sus datos V3 (consulte Almacenamiento inmediato en la página 1269)

26.3 Migración de hardware/software de los sistemas OpenScape Business X a V3

Al migrar los sistemas OpenScape Business X, se reemplazan los componentes tanto de hardware y software como de licencia.

Antes de migrar un sistema OpenBusiness X, determine la configuración del sistema actual y el hardware/software, así como los componentes de licencia que se van a reemplazar.

Nota: La placa OCCLA con sistema V3 puede tener hasta 60 (16) canales MEB. La migración a la nueva placa está restaurando la configuración OCC existente. Si desea aprovechar los canales MEB adicionales, debe reconfigurar su sistema utilizando los asistentes/páginas WBM correspondientes.

Los módulos que están presentes en la ranura 10 de los sistemas de pared OpenScape Business X5 no se pueden utilizar junto con placas base V3. Estos módulos deben ser reemplazados por módulos/soluciones sucesores.

Tabla 33: Migración de OpenScape Business X - Lista de comprobación de hardware/software

Componente	Reemplazado por
Componentes de hardware	
«Placa base V2» existente	Placa base V3 (básica o avanzada, según la configuración)
UC Booster Card/server (con UC Suite)	M.2 SSD adicional
módulo CMA	módulo CMAe
Módulo EXMR para dispositivos de anuncios externos	Placa base V3 (toma de entrada de sonido en la placa frontal)
Interfaces S0 en la placa base V2	Terminal S0 de la tarjeta periférica S0

Componente	Reemplazado por
Tarjetas X5W para la ranura 10 • SLCN16 • SLA16N • SLA24N	Reemplazado por: • Conexión directa Cordless • SLAV16 • SLAV16 SLAV8
Teléfonos optiPoint 500	Teléfonos OpenScape Deskphone CP
Teléfonos optiPoint 400	
Componentes de software	
Software del sistema V2 en la tarjeta SDHC	Software del sistema V3 (Imagen en el Software Download Server)
VPN en Wan con punto de terminación en el sistema	VPN con punto de terminación en router externo
XMPP	Sin solución sucesora
myPortal Smart	myPortal @work
Componentes de licencia	
Licencias en archivo de licencia	Transferencia de las licencias a un nuevo archivo de licencia
Aplicaciones CSTA externas (hasta ahora sin licencia, porque están conectadas a la tarjeta UC Booster/ servidor HW)	Licencia CSTA independiente para conectar soluciones externas (no necesaria para UC Suite, TAPI 170 y TAPI 120)

26.3.1 Migración de OpenScape Business X V2 a OpenScape Business X V3

Al migrar un modelo OpenScape Business X de la versión V2 a la V3, se reemplazan la placa base y el software del sistema. Las licencias existentes y la configuración del cliente se pueden transferir. El soporte de software existente se mantiene sin cambios después de la migración.

Antes de la migración, si aún no existe, configure un acceso permanente al servidor de licencias Unify (a través de Internet) en el sistema y active la función "CLS Connect". Esto simplifica la transferencia de licencias y reduce considerablemente el tiempo de migración. El cliente debe ser informado sobre el acceso requerido desde el Sistema OpenScape Business al CLS.

Requisitos previos

El sistema funciona con la última versión de software publicada, V2R7, antes de la actualización. Cuando sea necesario, actualice el sistema a la última versión del software. Para ello, el sistema debe tener un estado de soporte de software válido.

Para la migración de V2 a V3, dependiendo de si se utilizan CLS Connect, UC Suite o aplicaciones CSTA externas, se requieren los siguientes elementos:

- Placa base V3
- V3 SW en almacenamiento de datos M.2 SATA SSD

- M.2 SSD Almacenamiento masivo de datos de 256 GB (opcional con la aplicación UC Suite)
- Licencia de migración de hardware OpenScape Business V3 (si no se utiliza CLS Connect)
- Licencia OpenScape Business CSTA (opcional)

Condiciones y restricciones de límites funcionales

Las licencias existentes se pueden transferir completamente de la placa base V2 existente a la placa base V3 durante la migración. La transferencia de licencia sin activar la función CLS Connect requiere la licencia "HW Migration" y un proceso mucho más complejo y que consume mucho más tiempo que el uso de la función CLS Connect.

La configuración y los datos del cliente se migran de la versión V2 a la V3 del software mediante un proceso de copia de seguridad y restauración.

Los principales pasos técnicos de la migración se describen en los siguientes temas. Para conservar las licencias existentes, se establece una distinción en cuanto al manejo entre:

- Actualización de software para licencias permanentes con y sin CLS Connect
- Actualización de software con licencia de pago por uso

Nota: Durante la migración de la placa base V2 a la placa base V3, los puertos EVM adicionales no se incluyen adicionalmente en el grupo de búsqueda SmartVM. Esto requiere configuración manual, durante la cual también se debe realizar la restricción COS.

Nota: Al realizar una migración de hardware desde un sistema V2 configurado con una dirección IP DSP no predeterminada a un sistema V3, la dirección IP DSP se restablecerá al valor predeterminado. Tras la migración, el administrador debe reconfigurar manualmente la dirección IP del DSP y también la dirección IP del FPGA según las necesidades específicas del cliente.

26.3.1.1 Cómo migrar con CLS Connect a los sistemas con licencia permanente V3

Siga estos pasos de migración en orden.

Paso a paso

1) Preparar el sistema OpenScape Business
   a) Actualice el sistema existente a la versión de software V2R7.
   b) Configure el acceso al servidor central de licencias (CLS) en el sistema y compruebe la conexión.
   c) Active CLS Connect en el sistema.

2) Generar el archivo de licencia en el servidor central de licencias (CLS)
   a) Transfiera las licencias existentes de la dirección MAC de la placa base V2 a la dirección MAC de la placa base V3 mediante la función **Regenerar**
   b) Genere un nuevo archivo de licencia para la dirección MAC de la placa base V3.

3) Realice una copia de seguridad de la configuración del sistema V2 y los datos de cliente.

4) Reemplazar las placas base
   a) Apague el sistema y desconecte las fuentes de alimentación.
   b) Utilice un dispositivo de almacenamiento V3 y, si es necesario, el almacenamiento masivo de datos opcional en la placa base V3.
   c) Retire la tarjeta OCCB Voice Channel Booster de la placa base V2 e insértela en la placa base V3.
   d) Reemplace la placa base V2 por la placa base V3 en el sistema.
   e) Vuelva a conectar las fuentes de alimentación.

      El sistema arranca automáticamente.

5) Establecer los parámetros básicos del sistema en la Gestión basada en Web (WBM) después del arranque
   a) Establezca la fecha y hora del sistema.
   b) Establezca el paquete de aplicación.

      UC Smart para el sistema sin UC Smart o con UC Smart

      UC Suite para los sistemas con UC Suite

6) Restaurar la configuración del sistema
   a) Restaure la copia de seguridad con la función de restauración.
   b) Importe el archivo de licencia recién creado.

26.3.1.2 Cómo migrar sin CLS Connect a los sistemas con licencia permanente V3

Siga estos pasos de migración en orden.

Paso a paso

1) Preparar el sistema OpenScape Business
   a) Actualice el sistema existente a la versión de software V2R7.

2) Cree el "archivo de licencia de migración" para el sistema V2 en el servidor central de licencias (CLS)
   a) Active la "Licencia HW Migration" para el sistema existente.
   b) Genere un nuevo archivo de licencia para la dirección MAC de la placa base V2.

      Para ello, registre la dirección MAC de la placa base V3.
   c) Descargue el archivo de licencia del CLS.

3) Importe el archivo de licencia en el sistema OpenScape Business V2.

4) Anotar el **Código de confirmación** que se muestra en OpenScape Business Assistant

5) Generar un nuevo archivo de licencia para la placa base V3 en el servidor central de licencias (CLS)

a) Cree un nuevo archivo de licencia para la dirección MAC de la placa base V3 en el CLS; para ello, regenere la dirección MAC de la placa base V2 y el código de confirmación que se anotó anteriormente.

b) Busque el sistema OpenScape Business con la dirección MAC de la placa base V3 en el CLS.

c) Introduzca y active el Código de confirmación para desbloquear el sistema OpenScape Business.

d) Regenere el archivo de licencia

e) Descargue el archivo de licencia recién generado del CLS.

6) Realice una copia de seguridad de la configuración del sistema V2 y los datos de cliente.

7) Reemplazar las placas base

a) Apague el sistema y desconecte las fuentes de alimentación.

a) Utilice un dispositivo de almacenamiento V3 y, si es necesario, el almacenamiento masivo de datos opcional en la placa base V3.

b) Retire la tarjeta OCCB Voice Channel Booster de la placa base V2 e insértela en la placa base V3.

c) Reemplace la placa base V2 por la placa base V3 en el sistema.

b) Vuelva a conectar las fuentes de alimentación.

El sistema arranca automáticamente.

8) Establezca los parámetros básicos del sistema en la Gestión basada en Web (WBM) después del arranque

a) Establezca la fecha y hora del sistema.

b) Establezca el paquete de aplicación.

UC Smart para el sistema sin UC Smart o con UC Smart

UC Suite para los sistemas con UC Suite

9) Restaurar la configuración del sistema

a) Restaure la copia de seguridad con la función de restauración.

10) Importe manualmente el nuevo archivo de licencia en el sistema V3 después del arranque del sistema.

26.3.1.3 Cómo migrar a los sistemas con licencia PayGo V3

Siga estos pasos de migración en orden.

Paso a paso

1) Preparar el sistema OpenScape Business

a) Actualice el sistema existente a la versión de software V2R7.

2) Realice una copia de seguridad de la configuración del sistema V2 y los datos de cliente.

3) Regenerar el archivo de licencia en el servidor central de licencias (CLS)
   a) Regenere un nuevo archivo de licencia para la dirección MAC de la placa base V3.

      Transfiera las licencias existentes de la dirección MAC de la placa base V2 a la dirección MAC de la placa base V3.
   b) Descargue el nuevo archivo de licencia del CLS.

4) Reemplazar las placas base
   a) Apague el sistema y desconecte las fuentes de alimentación.
   b) Utilice un dispositivo de almacenamiento V3 y, si es necesario, el almacenamiento masivo de datos opcional en la placa base V3.
   c) Retire la tarjeta OCCB Voice Channel Booster de la placa base V2 e insértela en la placa base V3.
   d) Reemplace la placa base V2 por la placa base V3 en el sistema.
   e) Vuelva a conectar las fuentes de alimentación.

      El sistema arranca automáticamente.

5) Establecer los parámetros básicos del sistema en la Gestión basada en Web (WBM) después del arranque
   a) Establezca la fecha y hora del sistema.
   b) Establezca el paquete de aplicación.

      UC Smart para el sistema sin UC Smart o con UC Smart

      UC Suite para los sistemas con UC Suite

6) Restaurar la configuración del sistema
   a) Restaure la copia de seguridad con la función de restauración.

7) Importar manualmente el nuevo archivo de licencia en el sistema V3 y activarlo

26.4 Migración de un sistema OpenScape Business X V3 de placa base V2 a placa base V3

En este escenario, la placa base V2 existente del sistema OpenScape Business y cualquier hardware de UC Booster que pueda estar presente se reemplazan con una placa base V3. El sistema se actualizó anteriormente a la versión de software V3; por ejemplo, durante el transcurso de la compatibilidad de software.

Las licencias y la configuración de cliente existentes se pueden transferir. El servicio de compatibilidad de software existente se mantiene sin cambios después de la migración.

De existir una UC Booster Card o un UC Booster Server, ya no son necesarios en relación con la placa base V3. Un almacenamiento masivo de datos adicional se utiliza en la placa base V3 para este propósito.

En Tabla 33: Migración de OpenScape Business X - Lista de comprobación de hardware/software en la página 1407, puede encontrar información sobre qué componentes se sustituyen mediante el uso de la placa base V3 o se retiran sin sustitución. Se requiere una licencia CSTA para una conexión existente de aplicaciones CSTA externas. Esto no aplica para la conexión de OpenScape TAPI 170 o TAPI 120.

Requisitos previos

El sistema debe operarse con la última versión de software V2R7 publicada antes de la actualización. De ser necesario, actualice el sistema a la última versión de software. Para ello el sistema debe tener un estado válido de compatibilidad de software.

Para la migración, se requieren los siguientes elementos, según se utilicen CLS Connect, UC Suite o las aplicaciones CSTA externas:

- Placa base V3
- Software V3 en almacenamiento de datos M.2 SATA SSD
- Almacenamiento masivo de datos M.2 SSD de 256 GB (opcional con la aplicación UC Suite)
- Licencia OpenScape Business V3 HW Migration (opcional)
- Licencia OpenScape Business CSTA (opcional)

Condiciones y restricciones de límites funcionales

Durante el transcurso de la migración, las licencias existentes se pueden transferir completamente de la placa base V2 existente a la placa base V3. La transferencia de licencia sin la activación de la función CLS Connect requiere la licencia "HW Migration", un tratamiento mucho más complejo y un gasto de tiempo mayor que si se utiliza la función CLS Connect.

La configuración de cliente y los datos de cliente se transfieren mediante el proceso de copia de seguridad / restauración.

Los pasos técnicos principales de la migración se describen en los siguientes temas. Para conservar las licencias existentes, en relación al tratamiento, se debe distinguir entre:

- Actualización de software con licencia permanente con y sin CLS Connect
- Actualización de software con licencia PayGo

Nota: Durante la migración de la placa base V2 a la V3, los puertos EVM adicionales no se incluyen adicionalmente en el grupo de búsqueda de SmartVM. Esto requiere una configuración manual, en el curso de la cual también se debe realizar la restricción COS.

La conversión de un KDS de la misma versión de software a un tipo de sistema diferente no es compatible con Manager E. Si desea utilizar solo los datos del KDS puede intentar los siguientes pasos:

- Realice una migración completa del sistema de placa base V2 a placa base V3.
- Descargue el KDS del sistema de placa base V3 con Manager E y guárdelo localmente.
- Vuelva a cargar el sistema de la placa base V3.
- Cargue el KDS del sistema de placa base V3 almacenado previamente en su sistema de placa base V3.

El sistema de placa base V3 utilizará la configuración de la base de datos KDS y podrá continuar con la configuración manual de UC.

Nota: No es posible migrar el KDS del sistema de placa base V2 al sistema de placa base V3, ya que la base de datos de

la placa base V2 no es compatible con la base de datos de la placa base V3.

26.4.1 Cómo migrar con CLS Connect a los sistemas con licencia permanente de placa base V3

Siga estos pasos de migración en orden.

Paso a paso

1) Preparar el sistema OpenScape Business
   a) Configure el acceso al servidor central de licencias (CLS) en el sistema y compruebe la conexión.
   b) Active CLS Connect en el sistema.

2) Generar el archivo de licencia en el servidor central de licencias (CLS)
   a) Transfiera las licencias existentes de la dirección MAC de la placa base V2 a la dirección MAC de la placa base V3 mediante la función **Regenerar**
   b) Genere un nuevo archivo de licencia para la dirección MAC de la placa base V3.

3) Realizar una copia de seguridad de la configuración del sistema V3 y los datos de cliente

4) De ser necesario, crear una copia de seguridad de la configuración de Booster Server

5) Reemplazar las placas base
   a) Apague el sistema y desconecte las fuentes de alimentación.
   b) Utilice un dispositivo de almacenamiento V3 y, si es necesario, el almacenamiento masivo de datos opcional en la placa base V3.
   c) Retire la tarjeta OCCB Voice Channel Booster de la placa base V2 e insértela en la placa base V3.
   d) Reemplace la placa base V2 por la placa base V3 en el sistema.
   e) Vuelva a conectar las fuentes de alimentación.

      El sistema arranca automáticamente.

6) Establecer los parámetros básicos del sistema en la Gestión basada en Web (WBM) después del arranque
   a) Establezca la fecha y hora del sistema.
   b) Establezca el paquete de aplicación.

      UC Smart para el sistema sin UC Smart o con UC Smart

      UC Suite para los sistemas con UC Suite

7) Restaurar la configuración del sistema
   a) Importe el archivo de licencia recién creado.
   b) Restaure la copia de seguridad del sistema y, de ser necesario, la copia de seguridad del Booster Server con la función de restauración.

26.4.2 Cómo migrar sin CLS Connect a los sistemas con licencia permanente de placa base V3

Siga estos pasos de migración en orden.

Paso a paso

1) Crear el "archivo de licencia de migración" para la placa base V2 existente en el servidor central de licencias (CLS)
   a) Active la "Licencia HW Migration" para el sistema existente.
   b) Genere un nuevo archivo de licencia para la dirección MAC de la placa base V2.

      Para ello, se debe registrar la dirección MAC de la placa base V3.
   c) Descargue el archivo de licencia del CLS.

2) Importar el archivo de licencia en el sistema OpenScape Business con la placa base V2.

3) Anotar el **Código de confirmación** que se muestra en OpenScape Business Assistant

4) Generar un nuevo archivo de licencia para la placa base V3 en el servidor central de licencias (CLS)
   a) Cree un nuevo archivo de licencia para la dirección MAC de la placa base V3 en el CLS; para ello, regenere la dirección MAC de la placa base V2 y el código de confirmación que se anotó anteriormente.

      a) Busque el sistema OpenScape Business con la dirección MAC de la placa base V3 en el CLS.
      b) Introduzca y active el Código de confirmación para desbloquear el sistema OpenScape Business.
      c) Regenere el archivo de licencia
   b) Descargue el archivo de licencia recién generado del CLS.

5) Realizar una copia de seguridad de la configuración del sistema y los datos de cliente

6) Reemplazar las placas base
   a) Apague el sistema y desconecte las fuentes de alimentación.
   b) Utilice un dispositivo de almacenamiento V3 y, si es necesario, el almacenamiento masivo de datos opcional en la placa base V3.
   c) Retire la tarjeta OCCB Voice Channel Booster de la placa base V2 e insértela en la placa base V3.
   d) Reemplace la placa base V2 por la placa base V3 en el sistema.
   e) Vuelva a conectar las fuentes de alimentación.

      El sistema arranca automáticamente.

7) Establecer los parámetros básicos del sistema en la Gestión basada en Web (WBM) después del arranque
   a) Establezca la fecha y hora del sistema.
   b) Establezca el paquete de aplicación.

      UC Smart para el sistema sin UC Smart o con UC Smart

      UC Suite para los sistemas con UC Suite

8) Restaurar la configuración del sistema después del arranque del sistema
   a) Restaure la copia de seguridad con la función de restauración.

9) Importar manualmente el nuevo archivo de licencia en el sistema V3 después del arranque del sistema.

26.4.3 Cómo migrar a los sistemas con licencia PayGo de placa base V3

Siga estos pasos de migración en orden.

Paso a paso

1) Realizar una copia de seguridad de la configuración del sistema y los datos de cliente

2) Regenerar el archivo de licencia en el servidor central de licencias (CLS)

a) Regenere un nuevo archivo de licencia para la dirección MAC de la placa base V3.

Transfiera las licencias existentes de la dirección MAC de la placa base V2 a la dirección MAC de la placa base V3.

b) Descargue el nuevo archivo de licencia del CLS.

3) Reemplazar las placas base

a) Apague el sistema y desconecte las fuentes de alimentación.

b) Utilice un dispositivo de almacenamiento V3 y, si es necesario, el almacenamiento masivo de datos opcional en la placa base V3.

c) Retire la tarjeta OCCB Voice Channel Booster de la placa base V2 e insértela en la placa base V3.

d) Reemplace la placa base V2 por la placa base V3 en el sistema.

e) Vuelva a conectar las fuentes de alimentación.

El sistema arranca automáticamente.

4) Establecer los parámetros básicos del sistema en la Gestión basada en Web (WBM) después del arranque

a) Establezca la fecha y hora del sistema.

b) Establezca el paquete de aplicación.

UC Smart para el sistema sin UC Smart o con UC Smart

UC Suite para los sistemas con UC Suite

5) Restaurar la configuración del sistema después del arranque del sistema

a) Restaure la copia de seguridad con la función de restauración.

6) Importar manualmente el nuevo archivo de licencia en el sistema V3 y activarlo

26.5 Actualización de software de OpenScape Business S

Antes de la actualización de software del sistema OpenScape Business S, determine la configuración del sistema actual y los componentes de hardware/software y de licencia que posiblemente necesiten reemplazo.

Tabla 34: Migración de OpenScape Business S - Lista de comprobación de hardware/software

Componentes	Reemplazado por
Componentes de hardware	

Componentes	Reemplazado por
PC de servidor	La reutilización es posible. Deben comprobarse los requisitos de hardware para las extensiones de OpenScape Business S.[11]
Teléfonos optiPoint 400	Teléfonos OpenScape Deskphone CP
Componentes de software	
Sistema operativo SLES12	La reutilización es posible. Con el tiempo, se requerirá una actualización al service pack más reciente[12]
Software del sistema V2 en la tarjeta SDHC	Software del sistema V3 (Imagen en el Software Download Server)
XMPP	Sin solución sucesora
myPortal Smart	myPortal @work
Componentes de licencia	
Licencias en archivo de licencia	Transferencia de las licencias a un nuevo archivo de licencia
Aplicación CSTA (mediante UC Booster Card/Server)	Aplicación CSTA (mediante UC Booster Card/Server)

26.5.1 Actualización de software de OpenScape Business S V2 a OpenScape Business S V3

Al actualizar un modelo OpenScape Business S de la versión de software V2 a V3, solo se reemplaza el software del sistema.

Las licencias y la configuración de cliente existentes se transfieren. La compatibilidad de software existente se mantiene sin cambios después de la migración.

---

11 El hardware del PC de servidor existente se puede utilizar si la configuración del sistema UC Booster Server no se modifica después de la actualización de software. Si se planifican ampliaciones después de la actualización de software, es posible que los requisitos de hardware deban adaptarse según las especificaciones en *Instrucciones de instalación de OpenScape Business S, capítulo Requisitos previos*.

12 El sistema operativo SLES instalado en el PC de servidor se puede adoptar en caso de una actualización de software de OpenScape Business S / UC Booster Server. Sin embargo, debe actualizarse al último service pack publicado antes de la actualización de software.

Si Novell ha retirado la compatibilidad de software para la versión SLES utilizada, se debe informar al cliente y, de ser necesario, se debe adquirir una actualización de SLES.

Es posible que la actualización de SLES deba realizarse en varios pasos para aplicar las instalaciones de OpenScape Business S, incluidos la configuración de cliente y los datos de cliente. Una clave de actualización existente de SLES conserva su validez con una actualización de SLES. Sin embargo, es posible que se deba anular el registro de esta con Novell antes de la actualización de SLES y, luego, volver a registrarla para el nuevo sistema.

Lo siguiente describe la actualización de software de OpenScape Business conservando el sistema operativo SLES.

En este caso, no se requiere el pedido de elementos por separado para la actualización de software del sistema de V2 a V3.

Recuerde que la versión de software V3 ya no es compatible con determinadas funciones y componentes de hardware. En Tabla 34: Migración de OpenScape Business S - Lista de comprobación de hardware/software en la página 1416, encontrará información sobre qué componentes se sustituyen en la versión V3 o qué componentes se retiran sin sustitución. Depende de la ampliación del sistema del cliente.

Requisitos previos

El sistema debe operarse con la última versión de software V2R7 publicada antes de la actualización. De ser necesario, actualice el sistema a la última versión de software. Para ello el sistema debe tener un estado válido de compatibilidad de software.

Antes de la actualización de software de la versión V2 a V3, configure un acceso permanente al servidor de licencias de Unify (a través de Internet) en el sistema y active la función **CLS Connect**.

Condiciones y restricciones de límites funcionales

Las licencias existentes solo se pueden transferir durante el transcurso de la actualización de software si la función CLS Connect está activada.

La configuración de cliente y los datos de cliente se transfieren automáticamente de la versión de software V2 a V3 durante el proceso de actualización de software.

Los pasos técnicos principales de la migración se describen en los siguientes capítulos. Para conservar las licencias existentes, en relación al tratamiento, se debe distinguir entre:

- Actualización de software con licencia permanente con y sin CLS Connect
- Actualización de software con licencia PayGo

Tratamiento técnico de la actualización

Los pasos técnicos principales de la actualización se describen a continuación. Se distingue entre

- Actualización con licencia permanente y CLS Connect
- Actualización con licencia PayGo.

26.5.1.1 Cómo actualizar con CLS Connect a los sistemas con licencia permanente V3

Siga los siguientes pasos de migración:

Paso a paso

1) Preparar el sistema OpenScape Business V2
   a) Actualice el sistema existente a la versión de software V2R7.
   b) Configure el acceso al servidor central de licencias (CLS) en el sistema y compruebe la conexión.
   c) Active CLS Connect en el sistema V2.

2) Preparar el sistema operativo SLES

   Actualice el sistema operativo al último service pack publicado para la versión de SLES utilizada en relación con OpenScape Business S.

3) Actualizar el software de OpenScape Business
   a) Ejecute la actualización del software a V3 mediante OpenScape Business Assistant.
   b) La configuración del sistema se transfiere automáticamente a V3.
   c) Las licencias existentes se transfieren a V3.

4) El archivo de licencia se genera automáticamente mediante el servidor central de licencias (CLS)
   a) Después de reiniciar el sistema, el sistema transfiere la información de que las licencias existentes operan con la versión de software 3.
   b) El servidor de licencias genera automáticamente un nuevo archivo de licencia con la información de la versión V3 y lo transfiere de vuelta al sistema.

26.5.1.2 Cómo actualizar a sistemas con licencia PayGo V3

Siga los siguientes pasos de migración:

Paso a paso

1) Preparar el sistema OpenScape Business
   a) Actualice el sistema existente a la versión de software V2R7.

2) Preparar el sistema operativo SLES

   Actualice el sistema operativo al último service pack publicado para la versión de SLES utilizada en relación con OpenScape Business S.

3) Regenerar el archivo de licencia en el servidor central de licencias (CLS)
   a) Regenere un nuevo archivo de licencia para el sistema V2.
   b) Descargue el nuevo archivo de licencia del CLS.

4) Importar y activar el nuevo archivo de licencia en el sistema OpenScape Business V2.

5) Actualizar el software de OpenScape Business
   a) Ejecute la actualización del software a V3 mediante OpenScape Business Assistant.
   b) La configuración del sistema se transfiere automáticamente a V3.
   c) El sistema está listo para operar después del reinicio.

26.5.2 Actualización de software de OpenScape Business S V2 a OpenScape Business S V3

Siga los siguientes pasos de migración para actualizar un sistema OpenScape Business S V1 a un sistema OpenScape Business S V2.

Requisitos previos

Antes de la migración, compruebe si las características de hardware y software del servidor Linux son suficientes para OpenScape Business S V2. En algunos casos basta con actualizar el servidor Linux (p.ej., con más memoria de

trabajo disponible). El sistema operativo Linux SLES de 64 bits que se ha publicado para OpenScape Business V2 es un requisito previo. Para el paso de actualización a la versión de software V3 de OpenScape Business, se requiere la versión de SLES de 64 bits que se ha publicado para V3.

Si se requiere un nuevo servidor Linux, después de la instalación de Linux hay que instalar el software de comunicación OpenScape Business V1 S. A continuación, se puede transferir una copia de seguridad de datos de V1 y puede continuar con el paso 1 de la migración.

Condiciones y restricciones de límites funcionales

Cuando el sistema se ha actualizado de OpenScape Business V1 a OpenScape Business V2, no se pueden activar ni desactivar ITSP en el asistente de Telefonía Internet hasta que se restablezca el LCR. Los ITSP ya configurados en OpenScape Business V1 también seguirán funcionando en OpenScape Business V3 sin restablecer el LCR. El ITSP ya activado se puede editar, pero no se puede desactivar. Para hacer cambios de activación/desactivación en el asistente, restablezca el LCR. Esto es así para reflejar los cambios necesarios para el aumento de ITSP de 4 a 8. Para restablecer el LCR, vaya a **Modo Experto** > **LCR** > **Flags LCR** y haga clic en el flag **Restablecer datos LCR**.

Procedimiento de actualización

Siga los siguientes pasos de actualización:

1) **Actualice el software OpenScape Business V1**

   Mediante la Gestión basada den Web (WBM), actualice el software OpenScape Business V1 a la versión V1R3.3 o superior (Véase Actualización del sistema de comunicación en la página 1277).
2) **Cargue el archivo de licencia de OpenScape Business V2**

   Cargue el archivo de licencia de OpenScape Business V2 en el sistema OpenScape Business V1 y active las licencias (véase Activación de licencia (Standalone) en la página 318).

   Se puede seguir utilizando la licencia para las actualizaciones gratuitas de SLES.
3) **Cargue el software OS Biz V2 actual**

   Mediante la Gestión basada den Web (WBM), actualice el software OpenScape Business V2 en el sistema de comunicación. En el proceso, los datos de la versión V1 se convierten automáticamente en datos de V3 (véase Actualización del sistema de comunicación en la página 1277).
4) **Realizar un almacenamiento de datos**

   Realice una copia de seguridad de datos de la versión V2 (Véase Almacenamiento inmediato en la página 1269).

26.6 Migración/actualización de una red OpenScape Business V2 a V3

Al migrar o actualizar una red OpenScape Business a V3, todos los nodos en la red deben actualizarse a la versión de software V3. Para las funciones de interconexión, es irrelevante si la versión de software V3 se opera en un sistema OpenScape Business X en la red con una placa base V2 o con una placa base V3.

Actualice cada nodo de OpenScape Business de la red individualmente. Los componentes requeridos para una actualización se determinarán según cada nodo en función de los sistemas individuales de acuerdo a las descripciones en los capítulos Actualización de software para sistemas OpenScape Business X en la página 1402, Actualización de software de UC Booster Server a OpenScape Business X V3 en la página 1405, Migración de hardware/software de los sistemas OpenScape Business X a V3 en la página 1407 o Migración de un sistema OpenScape Business X V3 de placa base V2 a placa base V3 en la página 1412.

Las licencias para los nodos en la red V2 se pueden transferir a los sistemas V3 mediante el servidor central de licencias. Hay diferentes procedimientos para los sistemas con o sin la función **CLS Connect**. El procedimiento de activación de licencia «Pago por uso» no es compatible en la red OpenScape Business.

La transferencia de licencias en una red es significativamente más simple con **CLS Connect** que sin esta función.

Importante: Actualice los nodos en una red según el orden descrito para cada escenario. Es fundamental que todos los nodos esclavos estén en funcionamiento con la versión de software V3 antes de que el nodo maestro pueda migrarse o actualizarse a la versión de software V3.

En el transcurso de la actualización de red, operará una red heterogénea con software V2 y V3 durante un período de transición. Durante este tiempo, no se puede garantizar toda la funcionalidad de la gama de prestaciones de la red. En algunos escenarios, los sistemas actualizados/migrados operarán en un modo de emergencia solo hasta que el nodo maestro actualice el archivo de licencia.

Las redes OpenScape Business se pueden ejecutar en diferentes combinaciones respecto al uso de los sistemas OpenScape Business X y S, y las licencias de los sistemas en la red. Los pasos más importantes para la migración o actualización de una red OpenScape Business y su orden se muestran mediante combinaciones típicas.

En la descripción siempre se supone que existe un archivo de licencia de red para la red en el servidor central de licencias, mediante el cual el nodo maestro proporciona la información de licencia a todos los nodos esclavos.

- **Red compuesta por sistemas OpenScape Business X únicamente**
  - Escenario 1: Migración de hardware solo en el nodo maestro; actualización de software en todos los nodos esclavos
  - Escenario 2: Actualización de software en todos los nodos de OpenScape Business X de la red

- **Red compuesta por los sistemas OpenScape Business S y OpenScape Business X**
  - Escenario 3: OpenScape Business S es el nodo maestro y los sistemas OpenScape Business X son los nodos esclavos
    - Escenario 3a: Actualización de software en todos los nodos de OpenScape Business de la red
    - Escenario 3b: Actualización de software en el nodo maestro OpenScape Business S; migración de todos los nodos esclavos

26.6.1 Escenario 1: Migración de hardware de nodo maestro; actualización de software de nodos esclavos

Al migrar la red, se debe distinguir entre la función **CLS Connect** y el procedimiento de transferencia de licencia.

26.6.1.1 Migración/actualización con CLS Connect en el nodo maestro

Requisitos previos

- Todos los nodos en la red deben operarse con la última versión de software V2R7.x publicada.
- En el servidor central de licencias (CLS), debe haber un archivo de licencia de red central para el nodo maestro de la red.
- La función **CLS Connect** debe estar activada en el nodo maestro. CLS Connect no tiene que activarse en los nodos esclavos.

Paso a paso

1) Actualizar todos los nodos esclavos a la versión de software V3 (para obtener más información, véase Actualización de software para sistemas OpenScape Business X en la página 1402 o Actualización de software de UC Booster Server a OpenScape Business X V3 en la página 1405)

a) Importe el software V3 mediante OpenScape Business Assistant (WBM) y actualice el sistema.

b) Se conserva la configuración y la información de licencia.

El sistema no está operativo después del arranque, debido al archivo de licencia no válido.

2) Generar un nuevo archivo de licencia de red en el servidor de licencias

a) Regenere el archivo de licencia de red del nodo maestro para la dirección MAC de la placa base V3.

b) Descargue el nuevo archivo de licencia de red del CLS.

3) Migrar el nodo maestro a la placa base V3 (para obtener más información, véase Migración de hardware/software de los sistemas OpenScape Business X a V3 en la página 1407)
   a) Realice una copia de seguridad de la configuración del sistema mediante WBM.
   b) Reemplace la placa base.
   c) Establezca la fecha/hora y el paquete de aplicación mediante WBM.
   d) Importe y active el nuevo archivo de licencia de red mediante WBM.
   e) Restaure la configuración del sistema mediante WBM.

   En este caso, el archivo de licencia no se sobrescribe.
4) El nodo maestro transfiere automáticamente la información de la nueva licencia a los nodos esclavos.

Nota: Esta transmisión de licencias a los nodos esclavos puede llevar hasta 15 minutos.

26.6.1.2 Migración/actualización sin CLS Connect en el nodo maestro

Requisitos previos

- Todos los nodos en la red deben operarse con la última versión de software V2R7.x publicada.
- En el servidor central de licencias (CLS), debe haber un archivo de licencia de red central para el nodo maestro de la red.
- Disponible: licencia de migración de hardware para el nodo maestro.
- Disponible: licencias de upgrade de software para cada nodo esclavo.

Paso a paso

1) Generar un nuevo archivo de licencia de red en el servidor de licencias
   a) Divida el archivo de red en archivos de licencia individuales en el CLS.
   b) Genere un archivo de licencia para el nodo maestro.

      Active la licencia de migración de hardware para el nodo maestro.
   c) Genere un archivo de licencia para los nodos esclavos.

      Active la licencia de upgrade del software para cada nodo esclavo individual.
   d) Combine los archivos de licencia de los nodos individuales en un nuevo archivo de licencia de red.
   e) Descargue el nuevo archivo de licencia de red del CLS.
2) Actualizar los nodos esclavos a V3 (para obtener más información, véase Actualización de software para sistemas OpenScape Business X en la página 1402 o Actualización de software de UC Booster Server a OpenScape Business X V3 en la página 1405)
   a) Importe el software V3 mediante OpenScape Business Assistant (WBM) y actualice el sistema.
   b) La configuración y la información de licencia se transfieren automáticamente.

   El sistema no está operativo después del arranque, debido al archivo de licencia no válido.

3) Migrar el nodo maestro a V3 (para obtener más información, véase Migración de hardware/software de los sistemas OpenScape Business X a V3 en la página 1407)
   a) Realice una copia de seguridad de la configuración del sistema mediante WBM.
   b) Cambie la placa base.
   c) Establezca la fecha/hora y el paquete de aplicación mediante WBM.
   d) Importe y active el nuevo archivo de licencia de red mediante WBM.
   e) Restaure la configuración del sistema mediante WBM (en este caso, el archivo licencia no se sobrescribe).
4) El nodo maestro transfiere automáticamente la información de la nueva licencia a los nodos esclavos.

Nota: Esta transmisión de licencias a los nodos esclavos puede llevar hasta 15 minutos.

26.6.2 Escenario 2: Actualización de software de todos los sistemas en la red a V3

Al actualizar el software de red, el uso o no de la función **CLS Connect** define el procedimiento que se va a seguir para transferir la licencia.

26.6.2.1 Actualización de software con CLS Connect en el nodo maestro

Requisitos previos

- Todos los nodos en la red deben operarse con la última versión de software V2R7.x publicada.
- En el servidor central de licencias (CLS), debe haber un archivo de licencia de red central para el nodo maestro de la red.
- La función **CLS Connect** debe estar activada en el nodo maestro. CLS Connect no tiene que activarse en los nodos esclavos.

Paso a paso

1) Migrar todos los nodos esclavos a la versión de software V3 (para obtener más información, véase Actualización de software para sistemas OpenScape Business X en la página 1402 o Actualización de software de UC Booster Server a OpenScape Business X V3 en la página 1405)
   a) Importe el software V3 mediante OpenScape Business Assistant (WBM) y actualice el sistema.
   b) Se conserva la configuración y la información de licencia.

   El sistema no está operativo después del arranque, debido al archivo de licencia no válido.
2) Actualizar el nodo maestro a V3 (para obtener más información, véase Actualización de software para sistemas OpenScape Business X en la página 1402 o Actualización de software de UC Booster Server a OpenScape Business X V3 en la página 1405
   a) Importe el software V3 mediante OpenScape Business Assistant (WBM) y actualice el sistema.

b) Se conserva la configuración y la información de licencia.
c) Reinicie el sistema.

3) Los siguientes pasos son automáticos (no se requiere intervención manual)
a) El nodo maestro notifica al CLS después del arranque sobre la versión de software 3.
b) El CLS genera un nuevo archivo de licencia de red.
c) El CLS transfiere el nuevo archivo de licencia de red al nodo maestro.
d) El nodo maestro transmite automáticamente la información de la nueva licencia a los nodos esclavos.

Nota: Esta transmisión de licencias a los nodos esclavos puede llevar hasta 15 minutos.

26.6.2.2 Actualización de software sin CLS Connect en el nodo maestro

Requisitos previos

- Todos los nodos en la red deben operarse con la última versión de software V2R7.x publicada.
- En el servidor central de licencias (CLS), debe haber un archivo de licencia de red central para el nodo maestro de la red.
- Disponible: licencias de upgrade de software para cada nodo

Paso a paso

1) Generar nuevos archivos de licencia de red en el servidor de licencias
a) Divida el archivo de red en archivos de licencia individuales en el CLS.
b) Genere un archivo de licencia para el nodo maestro.
Active la licencia de upgrade de software para el nodo maestro.
c) Genere un archivo de licencia para los nodos esclavos.
Active la licencia de upgrade del software para cada nodo esclavo individual.
d) Combine los archivos de licencia de los nodos individuales en un nuevo archivo de licencia de red.
e) Descargue el nuevo archivo de licencia de red del CLS.

2) Migrar todos los nodos esclavos a V3 (para obtener más información, véase Actualización de software para sistemas OpenScape Business X en la página 1402 o Actualización de software de UC Booster Server a OpenScape Business X V3 en la página 1405)
a) Importe el software V3 mediante OpenScape Business Assistant (WBM) y actualice el sistema.
b) Se conserva la configuración y la información de licencia.
c) El sistema no está listo para operar después del arranque, debido al archivo de licencia no válido.
El sistema no está operativo después del arranque, debido al archivo de licencia no válido.

3) Actualizar el nodo maestro a V3 (para obtener más información, véase Actualización de software para sistemas OpenScape Business X en

la página 1402 o Actualización de software de UC Booster Server a OpenScape Business X V3 en la página 1405

a) Importe el software V3 mediante OpenScape Business Assistant (WBM) y actualice el sistema.
b) Se conserva la configuración y la información de licencia.
c) Importe el archivo de licencia de red en el nodo maestro y actívelo.

4) El nodo maestro transfiere automáticamente la información de la nueva licencia a los nodos esclavos.

Nota: Esta transmisión de licencias a los nodos esclavos puede llevar hasta 15 minutos.

26.6.3 Escenario 3a: Actualización de software de todos los nodos

En este escenario, el nodo maestro es un sistema OpenScape Business S, y los nodos esclavos son sistemas OpenScape Business X.

Este escenario es idéntico a Escenario 2: Actualización de software de todos los sistemas en la red a V3 en la página 1424

26.6.4 Escenario 3b: Actualización de software en el nodo maestro; migración de hardware de los nodos esclavos.

En este escenario, los nodos esclavos se migran a la placa base V3 y a la versión de software V3 mediante un reemplazo de hardware/software. En el sistema maestro OpenScape Business S, el software se actualiza de V2 a V3. Para la actualización de hardware/software de la red, el uso de la función CLS Connect define el procedimiento de transferencia de licencias.

26.6.4.1 Migración/actualización con CLS Connect en el nodo maestro

Requisitos previos

- Todos los nodos en la red deben operarse con la última versión de software V2R7.x publicada.
- En el servidor central de licencias (CLS), debe haber un archivo de licencia de red central para el nodo maestro de la red.
- La función **CLS Connect** debe estar activada en el nodo maestro. CLS Connect no tiene que activarse en los nodos esclavos.
- Disponible: placas base V3, incluido el software V3.

Paso a paso

1) Migrar todos los nodos esclavos a la placa base V3 (para obtener más información, véase Migración de hardware/software de los sistemas OpenScape Business X a V3 en la página 1407)

a) Realice una copia de seguridad de la configuración del sistema mediante WBM.

b) Reemplace las placas base.

c) Establezca la fecha/hora y el paquete de aplicación mediante WBM.

d) Restaure la configuración del sistema mediante WBM.

El sistema no está operativo después del arranque, debido al archivo de licencia no válido.

2) Actualizar el nodo maestro a V3 (para obtener más información, véase Actualización de software para sistemas OpenScape Business X en la página 1402 o Actualización de software de UC Booster Server a OpenScape Business X V3 en la página 1405

a) Importe el software V3 mediante OpenScape Business Assistant (WBM) y actualice el sistema.

b) Se conserva la configuración y la información de licencia.

c) Reinicie el sistema.

3) Los siguientes pasos son automáticos (no se requiere intervención manual)

a) El nodo maestro notifica al CLS después del arranque sobre la versión de software 3.

b) El CLS genera un nuevo archivo de licencia de red.

c) El CLS transfiere el nuevo archivo de licencia de red al nodo maestro.

d) El nodo maestro transmite automáticamente la información de la nueva licencia a los nodos esclavos.

Nota: Esta transmisión de licencias a los nodos esclavos puede llevar hasta 15 minutos.

26.6.4.2 Migración/actualización sin CLS Connect en el nodo maestro

Requisitos previos

- Todos los nodos en la red deben operarse con la última versión de software V2R7.x publicada.
- En el servidor central de licencias (CLS), debe haber un archivo de licencia de red central para el nodo maestro de la red.
- Disponible: licencia de upgrade de software para el nodo maestro.
- Disponible: licencias de migración de hardware para cada nodo esclavo.
- Disponible: placas base V3, incluido el software V3.

Paso a paso

1) Generar un nuevo archivo de licencia de red en el servidor de licencias
   a) Divida el archivo de red en archivos de licencia individuales en el CLS.
   b) Genere un archivo de licencia para el nodo maestro.
      Active la licencia de upgrade de software para el nodo maestro.
   c) Genere un archivo de licencia para los nodos esclavos.
      Active la licencia de migración de hardware para cada nodo esclavo.
   d) Combine los archivos de licencia de los nodos individuales en un nuevo archivo de licencia de red.
   e) Descargue el nuevo archivo de licencia de red del CLS.

2) Migrar todos los nodos esclavos a la placa base V3 (para obtener más información, véase Migración de hardware/software de los sistemas OpenScape Business X a V3 en la página 1407)
   a) Realice una copia de seguridad de la configuración del sistema mediante WBM.
   b) Reemplace las placas base.
   c) Establezca la fecha/hora y el paquete de aplicación mediante WBM.
   d) Restaure la configuración del sistema mediante WBM.

   El sistema no está operativo después del arranque, debido al archivo de licencia no válido.

3) Actualizar el nodo maestro a V3 (para obtener más información, véase Actualización de software para sistemas OpenScape Business X en la página 1402 o Actualización de software de UC Booster Server a OpenScape Business X V3 en la página 1405)
   a) Importe el software V3 mediante OpenScape Business Assistant (WBM) y actualice el sistema.
   b) Se conserva la configuración y la información de licencia.
   c) Importe el archivo de licencia de red en el nodo maestro y actívelo.

4) El nodo maestro transfiere automáticamente la información de la nueva licencia a los nodos esclavos.

Nota: Esta transmisión de licencias a los nodos esclavos puede llevar hasta 15 minutos.

26.7 Migración de HiPath 3000 a OpenScape Business V3

Se describe la migración técnica de sistemas independientes HiPath 3000 / HiPath 500 V9 e interredes HiPath 3000 a OpenScape Business V3 con placas base V3.

Al migrar de sistemas HiPath 3000 a OpenScape Business X V3 con placas base V3, según la configuración de hardware, se puede transferir parte del equipo de hardware del sistema y los terminales / clientes conectados.

Antes de migrar un HiPath 3000, la configuración del sistema actual y el hardware / software, así como los componentes de licencia que se van a reemplazar, de existir, deben determinarse mediante comprobaciones posteriores.

Comprobaciones generales

- **Comprobación de compatibilidad de funciones**

  Infórmese sobre qué funciones ya no son compatibles o han cambiado respecto a HiPath 3000 V9. El capítulo Prestaciones e interfaces modificadas/descartadas de HiPath 3000 en la página 1452 enumera las funciones de HiPath 3000 que ya no son compatibles en OpenScape Business o que se han reemplazado por funciones más nuevas.
- **Comprobación de versión de software**

  El sistema debe operarse en la versión de software V9 antes de la migración. Los sistemas con una versión de software anteriores a V9 deben actualizarse a la versión de software V9 y ponerse en servicio antes de la migración.
- **Comprobación de puesta a tierra de protección**

  ¡Para todos los sistemas de comunicación OpenScape Business X, es obligatoria la puesta a tierra de protección mediante un conductor de puesta a tierra adicional!

Comprobación de compatibilidad del hardware

Por motivos técnicos, algunos módulos y terminales no se pueden utilizar en los sistemas OpenScape Business X. Al migrar de HiPath 3000 a OpenScape Business V3, estos módulos y terminales deben quitarse. Si es necesario, utilice en su lugar los tipos de sucesores respectivos. La lista de los módulos que ya no son compatibles y sus sucesores se puede encontrar en la *documentación de servicio de OpenScape Business X3/X5/X8*, en la sección *Componentes de hardware no compatibles*.

- **Fuente de alimentación**

  OpenScape Business 33xx / 35xx se puede operar con la fuente de alimentación UPSC-D / DR o OCPSM. Las demás fuentes de alimentación PSU deben reemplazarse con OCPSM. Están disponibles los kits de actualización de la PSU adecuados.
- **Componentes periféricos**

  Compruebe si el hardware existente se sigue pudiendo utilizar. Si es necesario, los módulos y terminales que ya no sean compatibles deben retirarse y reemplazarse por sus sucesores.
- **Comprobación de backplane**

  En los sistemas HiPath 3550, la placa base V3 ya no puede acceder al slot 10 del backplane. Los módulos periféricos existentes que utilizan este slot no pueden operarse en OpenScape Business.
- **Comprobación de dispositivo telefónico**

  Los sistemas OpenScape Business V3 con placas base V3 admiten dispositivos analógicos, RDSI, SIP y OpenStage u OpenScape Deskphone IP / CP. Los dispositivos Optiset E, Optipoint 4xx y Optipoint 5xx deben reemplazarse.
- **Comprobación de carcasa**

  En los sistemas HiPath 33xx/35xx migrados, es posible que las tapas de las carcasas deban reemplazarse y, de ser necesario, deben instalarse unidades de ventiladores.

  Están disponibles los artículos de entrega correspondientes.

Otras comprobaciones

- **Plan de números de llamada para sistemas interconectados**

  Con las interconexiones de voz puras se puede implementar una numeración abierta o cerrada. Si se usa UC Suite, es necesaria una numeración cerrada (funciones UC a nivel de red).

26.7.1 Migración de HiPath 33xx, 35xx, 3800 a OpenScape Business X3/X5/X8 V3

Al migrar un sistema HiPath 33xx, 35xx, 3800 a OpenScape Business X V3, se reemplazan la placa base, los grupos periféricos y los terminales determinados, así como el software del sistema. Las licencias existentes se pueden migrar con una licencia de upgrade. La configuración del sistema puede transferirse. Después de la migración, el sistema OpenScape Business V3 tiene una compatibilidad de software de 3 años.

Para la migración de HiPath 3000 V9 a OpenScape Business V3, en principio se requieren los siguientes elementos:

- Placa base V3
- Software V3 en almacenamiento de datos SSD
- M2 SSD Almacenamiento masivo de datos de 256 GB (opcional con la aplicación UC Suite)
- OpenScape Business Upgrade HiPath 3000 V9 (migración de licencia), o
- OpenScape Business Upgrade HiPath 3000 V8 (migración de licencia), o
- OpenScape Business Upgrade HiPath 3000 V7 (migración de licencia)
- Licencia OpenScape Business CSTA (opcional)

De ser necesario, también deben solicitarse componentes de hardware y licencias adicionales. Depende de la configuración del sistema del cliente.

En *Documentación de servicio de OpenScape Business X3/X5/X8* en la sección *Componentes de hardware no compatibles* encontrará información sobre qué componentes se sustituyen en la versión V3 o se descontinuan sin sustitución. Recuerde que se requiere una licencia CSTA para una conexión existente de aplicaciones CSTA externas. Esto no aplica para la conexión de OpenScape Business TAPI 170 o TAPI 120.

Requisitos previos

Todos los componentes de hardware/software se deben revisar para determinar su reusabilidad.

Disponible: todos los componentes nuevos de hardware / software.

Se debe solicitar una la licencia de upgrade para actualizar HiPath 3000 V7, V8 o V9 a OpenScape Business V3 y el LAC de la licencia de upgrade debe estar disponible para abrir la nueva licencia en el servidor de licencia.

El sistema se debe actualizar a la versión de software V9 más reciente para la migración de software técnica y la transferencia de la configuración de cliente existente.

Se debe utilizar la versión de Manager E más reciente.

Determinación de las licencias OpenScape Business durante la migración

Las licencias existentes en los sistemas HiPath 3000 se pueden transferir al sistema OpenScape Business V3 si se activa la licencia «OpenScape Business Upgrade HiPath 3000 (V7, V8 o V9)» en el servidor central de licencias. Durante la transferencia de licencias, se crea un nuevo archivo de licencia para el sistema OpenScape Business V3 con las siguientes licencias.

Tabla 35: Migración de licencias de HiPath 3000

Licencia HP 3000	Licencia OpenScape Business	Observaciones
	Licencia básica	Recién creada, incl. 3 años de compatibilidad de software
	Licencia OpenDirectory Base	Recién creada
	Licencia Web Collaboration Connector	Recién creada
	Licencia TDM User	Número calculado a partir de la configuración del sistema[13]
IP-Subscriber (ComScendo)	Licencia IP User	Transferencia 1:1 desde el archivo de licencia HP 3000
	Licencia TDM User	Calculado a partir de la configuración del sistema[13]
Canales S2M	Licencias de líneas IP/ S2M/TI	Transferencia 1:1 desde el archivo de licencia HP 3000
Mobility Entry	Licencias Mobility User	Transferencia 1:1 desde el archivo de licencia HP 3000

Determinación de las licencias TDM User en el archivo de licencia

Durante la conversión técnica de la configuración del sistema HiPath 3000, el número de extensiones TDM lo determina la herramienta Manager E y se escribe en un "archivo (XML) de inventario".

El número de licencias TDM User se determina según estas reglas:

- 1 licencia TDM User por puerto UP0 activo: teléfono operativo (maestro/ esclavo), número de teléfono disponible
- 1 licencia TDM User por teléfono DECT registrado: número de teléfono disponible
- 1 licencia TDM User por puerto a/b activo (número de teléfono) para los módulos conectados

[13] Determinado en el transcurso de la descripción técnica de la conversión ver más abajo.

- 1 licencia TDM User por puerto S0 activo (número de teléfono MSN) para los módulos activos

La migración de licencia TDM User se realiza sin conexión en el CLS mediante el archivo XML de inventario.

El servidor central de licencias comprueba si existe un archivo de licencia para la dirección MAC de la placa base de HiPath 3000.

Si un archivo de licencia está disponible, la migración de licencia se realiza en función de este archivo de licencia y de la información del "archivo de inventario".

Si no está disponible ningún archivo de licencia, la actualización de OpenScape Business se realiza en función de la información del "archivo (XML) de inventario".

Según la licencia de upgrade (V7, V8 o V9) disponible, el siguiente porcentaje de los usuarios TDM determinados se aplica en OpenScape Business.

- Actualización de HiPath 3000 V4 o una versión anterior a OpenScape Business V3:

  No se calculan usuarios TDM para licencias de actualización de OpenScape Business más económicas/gratuitas
- Actualización de HiPath 3000 V5, V6 o V7 a OpenScape Business V3:

  El 70% de los usuarios de TDM solicitan licencias de actualización de OpenScape Business más económicas o gratuitas
- Actualización de HiPath 3000 V8 a OpenScape Business V3:

  El 80% de los usuarios de TDM solicitan licencias de actualización de OpenScape Business más económicas o gratuitas
- Actualización de HiPath 3000 V9 OpenScape Business V3:

  El 100% de los usuarios de TDM están calculados para obtener licencias de actualización de OpenScape Business más económicas o gratuitas.

Condiciones y restricciones de límites funcionales

- La migración de licencia solo se puede realizar a V3. Manager E no admite una migración de licencia a V2.
- La migración de licencia de un sistema (placa base) HiPath 3000 solo se puede realizar una vez, y la placa base se bloquea para acciones posteriores en el CLS después de la migración.
- Para migrar las líneas S2M y las extensiones Comscendo, debe estar disponible un archivo de licencia HiPath 3000 en el servidor central de licencias.
- Las licencias TDM User generadas durante la migración no se pueden transferir a otros sistemas o a una cuenta de CLS.
- Las licencias de usuario (User) y las licencias UC orientadas a usuario se asignan de forma fija a las extensiones en OpenScape Business. Recuerde que para los usuarios myAgent y myAttendant, está disponible el número suficiente de licencias. En OpenScape Business, los cambios de los estados de presencia de otros usuarios mediante usuarios de myAgent están vinculados a la licencia de myAttendant. Deben solicitarse por separado.
- La prestación Usuario Deskshare (IP-Moblity) necesita licencia en OpenScape Business, y no en HiPath 3000. Las licencias IP User adicionales deben estar disponibles y deben asignarse a "Usuarios

Deskshare" en el cuadro de diálogo de registro de licencias OpenScape Business Assistant.

- No se realiza ninguna migración de licencia para los siguientes productos y funciones:
  - Canales B HG1500: no hay módulo, las funciones están integradas en la nueva placa base.
  - optiClient Attendant V8: no funciona en OpenScape Business.

    Sucesor: OpenScape Business Attendant
  - optiClient BLF V1/V2: no funciona en OpenScape Business.

    Sucesor: OpenScape Business BLF
  - HiPath TAPI 120/170 V2: no funciona en OpenScape Business.

    Sucesor: OpenScape Business TAPI 120/170
  - Entry VoiceMail: no hay módulo, las funciones están integradas en la nueva placa base.

    Sucesor: Smart Voicemail
  - Web Services Communications Clients de myPortal entry en el Plug PC.
  - Extensiones base: ya no se requieren licencias para extensiones base.
  - Línea urbana ITSP: hay que comprar licencias para usar canales ITSP para la telefonía Internet en OpenScape Business.
  - Para línea urbana S0, línea urbana analógica y línea urbana CAS no se requieren licencias.
  - Para interconexiones y conexión de sistemas externos mediante líneas cruzadas hay que comprar una licencia de redes (Networking) por cada nodo de OpenScape Business.

Tratamiento técnico

Siga estos pasos de migración en orden:

1) **Descargue la memoria de datos de cliente (KDS) de HiPath 3000 desde el sistema**

   Con la última versión del Manager E, descargue la KDS actual de HiPath 3000 desde el sistema HiPath 3000.
2) **Anote la configuración de HG1500 (opcional)**

   Si hay insertados uno o varios módulos HG1500, anote los ajustes de HG1500 modificados respecto a los ajustes estándar mediante la Gestión basada en Web (WBM) del HG1500:

   - Enrutamiento IP
   - Encaminamiento PSTN
   - Firewall IP
   - Firewall de MAC
   - Cortafuegos de aplicaciones
   - IP-Accounting
   - Mapping IP
   - SNMP
3) **Convierta la memoria de datos de cliente (KDS) de HiPath 3000**

   Con la última versión de Manager E, convierta la KDS actual de HiPath 3000 a la KDS de OpenScape Business V3.

4) **Sustituya el hardware**

   Sustituya la placa base de HiPath 3000 por la nueva placa base de OpenScape Business V3. Retire también todos los módulos HG1500 y todos los módulos y los submódulos que ya no sean compatibles. Hay que conectar a tierra todos los sistemas de comunicación OpenScape Business con un conductor de protección de tierra adicional.

5) **Realice la instalación inicial**

   Configure el sistema de comunicación mediante la Gestión basada en Web (WBM) con el asistente **Instalación inicial**. Tome en consideración también los ajustes de HG1500 que ha anotado antes.

6) **Cargue la memoria de datos de cliente (KDS) convertida**

   Cargue la KDS convertida en el sistema OpenScape Business V2 mediante la última versión de Manager E. A continuación, El sistema OpenScape Business se reinicia automáticamente.

7) **Genere un nuevo archivo de licencia en el CLS**

   Genere un nuevo archivo de licencia en el CLS con el LAC de la licencia de upgrade, el archivo de configuración (archivo XML) y el ID de bloqueo de OpenScape Business.

8) **Active y asigne licencias**

   Registre la licencia del sistema de comunicación OpenScape Business en un plazo de 30 días mediante el archivo de licencia.

9) **Restablecer entradas LCR**

   En caso necesario, se pueden restablecer las entradas LCR configuradas en el sistema HiPath 3000 (por ejemplo, planes de marcación, tablas de ruta o reglas de marcación) con las entradas estándares de OpenScape Business. Este ajuste se encuentra en la Gestión basada en Web (WBM), en el asistente **Configuración básica**.

26.7.1.1 Cómo cargar la memoria de datos de cliente (KDS) desde HiPath 3000

Requisitos previos

Hay disponible un sistema de comunicación HiPath 3000 (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 o HiPath 3800).

Todos los teléfonos están conectados y activos.

La última versión de Manager E está instalada en el PC de administración.

El PC de administración está conectado con el sistema de comunicación HiPath 3000.

Paso a paso

1) En el PC de administración, inicie sesión en Manager E.
2) En la barra de menús, haga clic en **Archivo** > **Transferir**.
3) Haga clic en la pestaña **Comunicación**.
4) En el área **Acceso**, active la opción correspondiente al tipo de conexión del PC de administración con el sistema de comunicación.
5) Active la opción **Leer/escribir KDS** y haga clic en **Sistema** > **PC**.
6) Haga clic en **Aceptar**. La memoria de datos de cliente (KDS) se transfiere desde HiPath 3000 al Manager E.

7) Una vez concluida correctamente la transferencia, haga clic en **Aceptar** y, a continuación, en **Cerrar**.
8) En la barra de menús, haga clic en **Archivo** > **Guardar KDS como** y guarde la memoria de datos de cliente (KDS) en un directorio del PC de administración.

Pasos siguientes

Cómo consultar los ajustes de configuración de HG1500 en la página 1435

26.7.1.2 Cómo consultar los ajustes de configuración de HG1500

Requisitos previos

Hay insertados uno o varios módulos HG1500.

Ha iniciado sesión en 3000 Manager E.

Paso a paso

1) En la vista de sistemas de Manager E, haga clic en la entrada del HG1500. Se abre la Gestión basada en Web (WBM) del HG1500.
2) Anote los ajustes que ha modificado respecto a los valores estándar. Los ajustes del HG1500 no se aplican al convertir la memoria de datos de cliente (KDS) y hay que configurarlos de nuevo en la puesta en servicio inicial de OpenScape Business en la Gestión basada en Web (WBM).

Pasos siguientes

Cómo convertir la memoria de datos de cliente (KDS) de HiPath 3000 en la página 1435

26.7.1.3 Cómo convertir la memoria de datos de cliente (KDS) de HiPath 3000

Requisitos previos

Hay disponible un sistema de comunicación HiPath 3000 (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 o HiPath 3800).

El PC de administración está conectado con el sistema de comunicación HiPath 3000.

Paso a paso

1) En la barra de menús, haga clic en **Archivo** > **Convertir KDS**.
2) Seleccione la memoria de datos de cliente (KDS) almacenado previamente en el PC de administración y haga clic en **Aceptar**.
3) Como datos de cliente introduzca su **Nombre** y su **Número de contrato** y haga clic en **Continuar**.
4) En **Versión** seleccione la entrada **OpenScape Business V2** y haga clic en **Continuar**.
5) Confirme los avisos de módulos no compatibles pulsando **Aceptar**.
6) Haga clic en **Sí** para confirmar la indicación que le informa sobre el número de usuarios TDM que va a realizar la migración y continúe con esta.

   El número de usuarios TDM que van a migrar se calcula automáticamente.

7) Confirme la indicación de los módulos insertados con **Continuar**.
8) En la barra de menús, haga clic en **Archivo** > **Guardar KDS como** y guarde la memoria de datos de cliente (KDS) con otro nombre en un directorio del PC de administración que usted elija.
9) Cierre el Manager E.

Pasos siguientes

Cómo sustituir el hardware de HiPath 3300/3500 en la página 1436 o

Cómo sustituir el hardware de HiPath 3350/3550 en la página 1437 o

Cómo sustituir el hardware con el HiPath 3800 en la página 1438

26.7.1.4 Cómo sustituir el hardware de HiPath 3300/3500

Requisitos previos

Sistema de comunicación HiPath 3000 en servicio para el modo rack (HiPath 3300 o HiPath 3500).

Placa base (OCCMRA o OCCMRB) de OpenScape Business V3.

Atención:

Descarga eléctrica al tocar los cables con tensión

Asegúrese de que hay disponible un conductor de protección de tierra adicional con el diámetro mínimo requerido para el sistema de comunicación (véase Documentación de servicio, Montaje del hardware).

Paso a paso

1) Apague el HiPath 3000 y, a continuación, desconecte la toma de red.
2) Retire todos los conectores de la placa base (extensiones analógicas, líneas RDSI, etc.).
3) Suelte los dos tornillos de sujeción de la placa frontal de la placa base.
4) Con dos llaves de módulo (C39165-A7027-C26), suelte la placa base de la placa trasera.
5) Extraiga cuidadosamente con las dos manos la placa base HiPath 300 en horizontal del soporte para módulos y colóquela sobre una superficie plana, con toma de tierra y conductora.
6) Si los hay, retire los módulo HG1500 de la carcasa. Los slots HG1500 que han quedado libre se pueden utilizar para módulos adicionales.
7) Extraiga de la carcasa los módulos que ya no sean compatibles (si los hay). Los slots que han quedado libres se pueden utilizar para módulos adicionales.
8) Retire todos los submódulos conectados con la placa base del HiPath 3000 y conéctelos en la placa base del OpenScape Business V3 (si es necesario y hay compatibilidad).
9) Inserte la tarjeta M.2 SATA SSD con el software del sistema y M.2 NVMe SDD opcional en la placa base V3.
10) Inserte los módulos opcionales, p. ej., OCCBH o OCCBL.

11) Deslice cuidadosamente con las dos manos la placa base OCCMRA u OCCMRB en horizontal para insertarla en el slot del soporte para módulos donde estaba antes la placa base HiPath 3000.
12) Inserte los módulos opcionales, p. ej., STRBR para placa base V3.
13) Enchufe de nuevo todos los conectores en la placa base (extensiones analógicas, líneas RDSI, etc.).

Nota: Si se utilizan más de 2 puertos a/b analógicos en HiPath 3300 o 3500, en OpenScape Business se requieren 1 o 2 cables adaptadores en Y. Se pueden conectar hasta 4 puertos a/b con las 2 tomas RJ11 físicas. Por motivos de espacio, la nueva placa base solo tiene 2 tomas RJ11 con las que hay que conectar 4 extensiones a/b.

14) Conecte el sistema de comunicación correctamente con el conductor de protección de tierra.
15) Enchufe de nuevo la toma de red y arranque el sistema.

Pasos siguientes

Cómo ejecutar la la instalación inicial en la página 1439

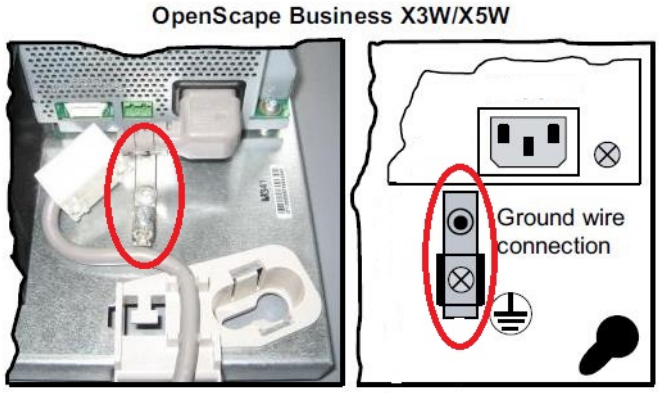
26.7.1.5 Cómo sustituir el hardware de HiPath 3350/3550

Requisitos previos

Sistema de comunicación HiPath 3000 operativo para montaje mural (HiPath 3350 o HiPath 3550).

Placa base (OCCMA o OCCMB) de OpenScape Business.

En caso de una migración de HiPath 3350/3550 a OpenScape Business X3W/X5W, el terminal de puesta a tierra de protección tiene que instalarse como se muestra en la imagen a continuación. A continuación, el conductor de puesta a tierra de protección debe conectarse según se describe en las Instrucciones de instalación de OpenScape Business V2, OpenScape Business X3/X5/X8.



Atención:

Descarga eléctrica al tocar los cables con tensión

Asegúrese de que hay disponible un conductor de protección de tierra adicional con el diámetro mínimo requerido para el sistema de comunicación (véase Documentación de servicio, Montaje del hardware).

Paso a paso

1) Apague el HiPath 3000 y, a continuación, desconecte la toma de red.
2) Abra los cierres de la carcasa y retírela.
3) Retire la cubierta.
4) Retire todos los conectores insertables (conectores EDGE) de la placa base (extensiones analógicas, líneas RDSI, etc.).
5) Retire la sujeción del módulo.
6) Extraiga cuidadosamente la placa base HiPath del soporte para módulos y colóquela sobre una superficie plana, con toma de tierra y conductora.
7) Si los hay, retire los módulo HG1500 de la carcasa. Los slots HG1500 que han quedado libre se pueden utilizar para módulos adicionales.
8) Extraiga de la carcasa los módulos que ya no sean compatibles (si los hay). Los slots que han quedado libres se pueden utilizar para módulos adicionales.
9) Retire todos los submódulos conectados con la placa base del HiPath 3000 y conéctelos en la placa base del OpenScape Business (si es necesario y hay compatibilidad).
10) Inserte la tarjeta M.2 SATA SSD con el software del sistema y M.2 NVMe SSD opcional en la placa base V3.
11) Inserte los módulos opcionales, p. ej., OCCBH o OCCBL.
12) Con cuidado, conecte la placa base OCCMA o OCCMB de OpenScape Business en la misma ranura donde antes estaba conectada la placa base de HiPath 3000.
13) Inserte los módulos opcionales, p. ej., STRBR para placa base V3.
14) Enchufe de nuevo todos los conectores insertables (conectores EDGE) en la placa base (extensiones analógicas, líneas RDSI, etc.). Tenga en cuenta que primero hay que pasar los conectores de las líneas RDSI por el orificio de la nueva sujeción de módulo.
15) Coloque la nueva sujeción de módulo.
16) Conecte el sistema de comunicación correctamente con el conductor de protección de tierra.
17) Coloque la carcasa y ciérrela.
18) Enchufe de nuevo la toma de red y arranque el sistema.

Pasos siguientes

Cómo ejecutar la la instalación inicial en la página 1439

26.7.1.6 Cómo sustituir el hardware con el HiPath 3800

Requisitos previos

Hay en uso un sistema de comunicación HiPath 3800.

Placa base OCCLA de OpenScape Business.

Atención:

Descarga eléctrica al tocar los cables con tensión

Asegúrese de que hay disponible un conductor de protección de tierra adicional con el diámetro mínimo requerido para el sistema de comunicación (véase Documentación de servicio, Montaje del hardware).

Paso a paso

1) Apague el HiPath 3000 y, a continuación, desconecte la toma de red.
2) Retire todos los conectores de la placa base.
3) Extraiga cuidadosamente la placa base HiPath 3000 del soporte para módulos y colóquela sobre una superficie plana, con toma de tierra y conductora.
4) En su caso, extraiga los módulos HG1500 que pudiera haber del soporte para módulos. Los slots HG1500 que han quedado libre se pueden utilizar para módulos adicionales.
5) Si los hay, extraiga los módulos que ya no sean compatibles del soporte para módulos. Los slots que han quedado libres se pueden utilizar para módulos adicionales.
6) Retire todos los submódulos conectados con la placa base del HiPath 3000 y conéctelos en la placa base del OpenScape Business (si es necesario y hay compatibilidad).
7) Inserte la tarjeta M.2 SATA SSD con el software del sistema y M.2 NVMe SDD opcional en la placa base V3.
8) Inserte los módulos opcionales, p. ej., OCCBH o OCCBL.
9) Con cuidado, conecte la placa base OCCLA de OpenScape Business en la misma ranura donde antes estaba conectada la placa base de HiPath 3000.
10) Vuelva a enchufar todos los conectores en la placa base.
11) Conecte el sistema de comunicación correctamente con el conductor de protección de tierra.
12) Enchufe de nuevo la toma de red y arranque el sistema.

Pasos siguientes

Cómo ejecutar la la instalación inicial en la página 1439

26.7.1.7 Cómo ejecutar la la instalación inicial

La instalación inicial del sistema de comunicación se describe en Integración en la LAN de clientes).

La instalación inicial incluye la configuración de la dirección IP del sistema, los ajustes de DHCP y los ajustes de país y hora.

Si el sistema HiPath 3000 tuviera también instalado un HG 1500, en la instalación inicial habría que haber usado la dirección IP del HG 1500 como dirección IP del sistema OpenScape Business.

Una vez finalizada la instalación inicial, el sistema de comunicación se reinicia.

Pasos siguientes

Cómo cargar la memoria de datos de cliente (KDS) convertida en el nuevo sistema en la página 1440

26.7.1.8 Cómo cargar la memoria de datos de cliente (KDS) convertida en el nuevo sistema

Requisitos previos

Se ha sustituido el hardware.

El PC de administración está conectado con el sistema de comunicación OpenScape Business (mediante la interfaz LAN).

El PC de administración está configurado de forma que pueda recibir la dirección IP y la máscara de red del servidor DHCP de OpenScape Business.

Paso a paso

1) En el PC de administración, inicie sesión en Manager E.
2) En la barra de menús, haga clic en **Archivo** > **Abrir KDS**.
3) Desplácese hasta la ubicación de la memoria de datos de cliente (KDS) de OpenScape Business convertida y haga clic en **Aceptar**.
4) Confirme la advertencia con **Aceptar**.
5) En la barra de menús, haga clic en **Archivo** > **Transferir**.
6) Haga clic en la pestaña **Comunicación**.
7) En el área **Acceso**, active la opción **IP - HiPath** y en el campo Dirección IP introduzca la dirección IP del sistema de comunicación OpenScape Business. Estándar: `192.168.1.2`.
8) Active el campo de opción **Seguridad**.
9) Haga clic en **Cambiar contraseña**.
10) Introduzca la contraseña antigua y la nueva y confirme las entradas con **Aceptar**.
11) Active la opción **Leer/escribir KDS**.
12) Active las casillas de verificación **Tasas de llamada** y **Hardware** y haga clic en **PC** > **Sistema**.
13) Haga clic en **Aceptar**. La memoria de datos de cliente (KDS) se transfiere desde el Manager E al sistema.
14) Una vez concluida correctamente la transferencia de la memoria de datos de cliente (KDS), haga clic en **Aceptar** y, a continuación, en **Cerrar**.
15) Cierre el Manager E. El sistema se reinicia automáticamente.

Pasos siguientes

Cómo generar un nuevo archivo de licencia en la página 1440

26.7.1.9 Cómo generar un nuevo archivo de licencia

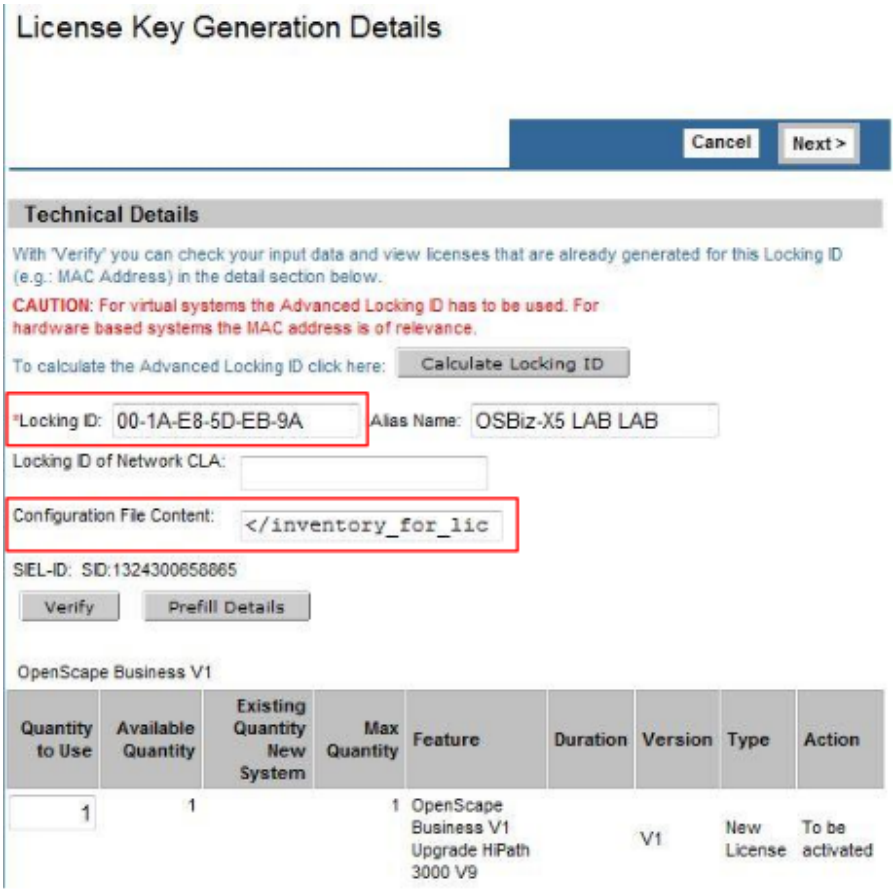
Requisitos previos

Se tiene el LAC de la licencia de upgrade.

Están disponibles los datos de registro del cliente.

Paso a paso

1) Inicie sesión en la Gestión basada en Web (WBM) con el perfil **Avanzado**.
2) En la barra de navegación, haga clic en **Administración de licencias**.
3) Anote el ID de bloqueo de OpenScape Business que aparece por encima de la tabla.
4) En el árbol de navegación, haga clic en **Registro**.
5) Introduzca sus datos y haga clic en **OK & Siguiente**.
6) Haga clic en **Exportar datos**. Se genera un archivo de comunicación (archivo XML) con los datos de registro y la información de inventario, incluyendo el número de extensiones TDM conectadas.
7) Guarde el archivo de configuración en el directorio que usted elija.
8) Inicie sesión en el CLS con su nombre de usuario y la contraseña.
9) En el grupo de menús, haga clic en **Licencia** > **Generar clave de licencia**.
10) En **LAC**, introduzca el LAC de la licencia de upgrade y haga clic en **Generar clave**.
11) Marque la prestación **OpenScape Business V2 Update HiPath 3000** y haga clic de nuevo en **Generar clave**.



12) En el campo **ID de bloqueo**, introduzca el ID de bloqueo de OpenScape Business.

13) Abra el archivo de configuración con un editor de texto (p.ej. Notepad) y copie todo el contenido del archivo de configuración en el campo **Contenido del archivo de configuración**.
14) Haga clic en **Siguiente** y siga las indicaciones para generar un nuevo archivo de licencia.

Nota: El procedimiento de migración de licencia en el CLS solo se puede realizar una vez. ¡Por ello, tenga cuidado de introducir los datos correctos!

15) Guarde el nuevo archivo de licencia en el directorio que usted elija.

Pasos siguientes

Cómo activar el archivo de licencia sin conexión en la página 1442

26.7.1.10 Cómo activar el archivo de licencia sin conexión

La activación de licencias sin conexión se describe en el capítulo Cómo activar licencias sin conexión (Standalone).

Pasos siguientes

Cómo asignar licencias en la página 1442

26.7.1.11 Cómo asignar licencias

La asignación de licencias se describe en Asignación de licencias (independiente) en la página 321.

26.7.1.12 Cómo restablecer las entradas LCR

La instalación básica del sistema de comunicación se describe en Configuración básica en la página 159).

La configuración básica incluye la configuración del número de teléfono del sistema, de las extensiones y el acceso a Internet y la telefonía Internet.

En el asistente **Configuración básica**, en la ventana **Funciones centrales para extensiones**, encontrará un botón de selección adicional para **Borrar los datos LCR configurados e inicializar el LCR con datos predeterminados**. Este campo de opción solo aparece si previamente se ha cargado en el sistema una memoria de datos de cliente (KDS) convertible. Si se activa el campo de opción, las entradas LCR configuradas en el sistema HiPath 3000 se borran y se sustituyen por las entradas estándares del sistema OpenScape Business.

Conceptos relacionados

Datos de extensión en la página 163

26.7.2 Migración de un sistema HiPath 3000 con OpenScape Office V3 HX a OpenScape Business V3 con placa base V3

No se requiere un servidor externo al migrar los sistemas HiPath 3000 con un servidor de OpenScape Office HX conectado. Su función la asume la placa base V3 correspondiente del sistema OpenScape Business X.

El sistema HiPath 3000 se migra según lo descrito en Migración de HiPath 33xx, 35xx, 3800 a OpenScape Business X3/X5/X8 V3 en la página 1430.

Las licencias OpenScape Office HX forman parte del archivo de licencia HiPath 3000. Por lo tanto, también se transfieren a las licencias OpenScape Business durante el transcurso de la migración de licencia HiPath 3000.

Requisitos

Para migrar las licencias OpenScape Business HX, debe estar disponible un archivo de licencia HiPath 3000 en el servidor central de licencias.

Para las licencias HiPath 3000, la migración de licencia se realiza según lo descrito en Tabla 35: Migración de licencias de HiPath 3000 en la página 1431. Lo siguiente aplica para la migración de licencia OpenScape Office HX:

Tabla 36: Migración de licencia OpenScape Office HX

Licencia OpenScape Office HX	Licencia OpenScape Business	Observaciones
Por cada licencia básica	1 licencia AutoAttendant	
Por cada OpenScape Office Standard User:	1 UC User 1 Voicemail User 1 Fax User	Aplica para las licencias Standard User en las licencias básicas HX 5/10, así como para las licencias individuales Single User
Licencia OpenScape Office HX Voicemail	500 Voicemail User	
myPortal for Outlook	Usuario groupware	Número conforme al archivo de licencia
myAttendant	myAttendant	Número conforme al archivo de licencia
myAgent	myAgent User	Número conforme al archivo de licencia
Contact Center Fax	Contact Center Fax User	Número conforme al archivo de licencia
Contact Center E-Mail	Contact Center E-Mail User	Número conforme al archivo de licencia
myReports	myReports	Número conforme al archivo de licencia
Application Launcher	Application Launcher	Número conforme al archivo de licencia

Licencia OpenScape Office HX	Licencia OpenScape Business	Observaciones
OpenDirectory Connector	OpenDirectory Connector	Número conforme al archivo de licencia

Condiciones y restricciones de límites funcionales

La migración de licencia solo se puede realizar a V3. Manager E no admite una migración de licencia a V2.

La migración de licencia solo se puede realizar una vez.

Las licencias de usuario (User) y las licencias UC orientadas a usuario se asignan de forma fija a los usuarios en OpenScape Business. Recuerde que para los usuarios myAgent y myAttendant, está disponible el número suficiente de licencias.

En OpenScape Business, los cambios de los estados de presencia de otros usuarios mediante usuarios de myAgent están vinculados a la licencia de myAttendant. Deben solicitarse por separado.

No es posible transferir anuncios, imágenes, buzones de voz, fax, diario, datos de Contact Center, configuración de extensión, perfiles, directorio externo y planes horarios de OpenScape Office HX a OpenScape Business V3 con placa base V3.

26.7.3 Migración de un sistema HiPath 3000 con OpenScape Office V3 HX a OpenScape Business V3 con UC Booster Server

La migración debe realizarse en dos pasos. En el primer paso, los sistemas se migran a V2. En el paso posterior, los sistemas se migran a V3.

Este escenario de migración solo debe realizarse en caso de que los datos de cliente en el servidor de OpenScape Office HX deban conservarse. La migración es un proceso largo y debe configurarse un nuevo UC Booster Server. La migración finaliza en un sistema OpenScape Business X V3 con placa base V2 y un UC Booster Server V3 conectado.

Debe considerarse de manera alternativa una migración conforme a Migración de un sistema HiPath 3000 con OpenScape Office V3 HX a OpenScape Business V3 con placa base V3 en la página 1443 si deben conservarse los datos de cliente en el servidor de HX.

Paso 1 Migración de un sistema HiPath 3000 con OpenScape Office V3 HX a OpenScape Business V2

En este paso, se migra HiPath 3000 a OpenScape Business V2 y se asignan las funciones de UC de OpenScape Office V3 HX a un OpenScape Business UC Booster Server V2.

El UC Booster Server debe instalarse desde cero en uns nueva base de hardware y software. Las licencias y datos de cliente pueden transferirse de OpenScape Office V3 HX a UC Booster Server si este se configuró antes con la versión de software 1R2.2 de OpenScape Business; se transfieren solo en este caso la configuración de UC y los datos de usuario siguientes:

- Anuncios

- Imágenes
- Buzón de voz
- Faxes
- Diario
- Datos de Contact Center
- Configuración de usuario
- Perfil de usuario
- Directorio externo
- Planes horarios

Los siguientes datos de usuario y de configuración de UC **no** se aplican y hay que configurarlos de nuevo en el UC Booster Server:

- Web-Services (p.ej. XMPP, Web Collaboration, Mobility)
- Open Directory Service

Después de la transferencia de licencias y datos de cliente, el software de UC Booster Server debe actualizarse a la versión de software V1R3.3 y, a continuación, debe actualizarse nuevamente a la versión de software V2R7 más reciente.

Siga estos pasos en orden para realizar la migración/actualización:

1) **Anote los ID de los agentes** (solo si se utiliza el Contact Center)

   Anote la asignación de los ID de agente a las extensiones de la UC Suite ya que esta asignación no se migra. La asignación debe configurarse de nuevo en la Gestión basada en Web (WBM) del sistema de comunicación OpenScape Business con el asistente **UCD**.
2) **Actualizar OpenScape Office V3 HX**

   Si todavía no lo ha hecho, actualice el OpenScape Office V3 HX al software V3 R3FR6.
3) **Crear un conjunto de copias de seguridad de OpenScape Office V3 HX**

   Mediante la Gestión basada en Web (WBM) de OpenScape Office V3 HX cree un conjunto de copias de seguridad en un soporte externo.

   Puede consultar información más precisa en la ayuda en línea del OpenScape Office Assistant.
4) **Actualizar HiPath 3000**

   Para actualizar de HiPath 3000 a OpenScape Business V1, siga los pasos de migración detallados para un sistema independiente (véase Migración de HiPath 33xx, 35xx, 3800 a OpenScape Business X3/X5/X8 V3 en la página 1430). Al hacer la libración de licencias en el servidor de licencias, las licencias de OpenScape Office V3 HX se transfieren a OpenScape Business. El archivo licencia incluye datos de licencia de OpenScape Business X3/X5/X8 y de la UC Suite.
5) **Configurar el UC Booster Server e integrarlo en la Lan de clientes**

   En el nuevo PC de servidor (servidor Linux) se instala el sistema operativo Linux SLES de 64 bits y, a continuación, el software de comunicación (versión V1 R2.2). Para obtener información detallada, véanse las *instrucciones de instalación del servidor Linux de OpenScape Business*.
6) **Activar UC Booster**

   Active la funcionalidad de UC Booster en la Gestión basada en Web (WBM) del sistema de comunicación OpenScape Business (**Configuración básica** > **Instalación inicial** > **Paquete con UC Suite en OpenScape**

Business UC Booster-Server) y registre la dirección IP del nuevo PC de servidor (si es posible, la misma dirección IP que el PC de servidor anterior). Compruebe que la UC Suite está activa en el UC Booster Server.

Puede consultar información más precisa en el capítulo "Instalación inicial de OpenScape Business X3/X5/X8", en Cómo establecer la solución UC en la página 157.

7) **Configurar UC Booster**

En la Gestión basada en Web (WBM) del UC Booster Server hay que indicar la dirección IP del sistema de comunicación.

Puede consultar información más precisa en el capítulo "Instalación inicial de OpenScape Business UC Booster" en Comunicar la dirección IP del sistema de comunicación en la página 292.

8) **Convertir un conjunto de copias de seguridad de OpenScape Office V3 HX**

El conjunto de copias de seguridad de OpenScape Office V3 HX guardado en el soporte externo se tiene que convertir en un conjunto de copias de seguridad OpenScape Business V1 mediante un script Linux. Para ello se requieren conocimientos sobre Linux. A continuación hay que cargar el conjunto de copias de seguridad en el UC Booster Server mediante la Gestión basada en Web (WBM). Después están disponibles los datos de usuario y de configuración de UC señalados anteriormente.

Puede obtener información más detallada en este capítulo, en Cómo convertir un conjunto de copias de seguridad de OpenScape Office V3 HX en la página 1446.

9) **Actualizar el software UC Booster Server a V2**

En primer lugar, actualice el UC Booster Server a la versión V1 R3.3 y, a continuación, al software OpenScape Business V2 más reciente.

26.7.3.1 Cómo convertir un conjunto de copias de seguridad de OpenScape Office V3 HX

Requisitos previos

El OpenScape Business UC Booster Server está operativo.

El conjunto de copias de seguridad de OpenScape Office V3 HX está en un soporte externo.

Paso a paso

1) Copie el conjunto de copias de seguridad de OpenScape Office V3 HX desde el soporte externo en el PC de servidor (servidor de Linux), en este directorio:

```
/mnt/persistent/apollo/
```

2) Abra un terminal el PC de servidor o conéctese mediante un shell SSH con el PC de servidor. Necesita derechos root.
3) Cambie al directorio de copia de seguridad mediante este comando:

```
cd /mnt/persistent/backup/
```

4) Active el script de conversión de esta forma:

```
/opt/symappl/services/backup/script/migrate.sh /mnt/
persistent/apollo/<nombre del conjunto de copias de
seguridad>
```

```
/opt/symappl/services/backup/script/migrate.sh /mnt/
persistent/apollo/BackupSet_130913-0400007.tar
```

5) Una vez ejecutado el script de conversión, se puede utilizar el conjunto de copias de seguridad convertido para la restauración.

26.7.4 Migración de una red HiPath 3000 a una red OpenScape Business

Para actualizar una red HiPath 3000 a una red OpenScape Business, hay que realizar los pasos de migración señalados a continuación.

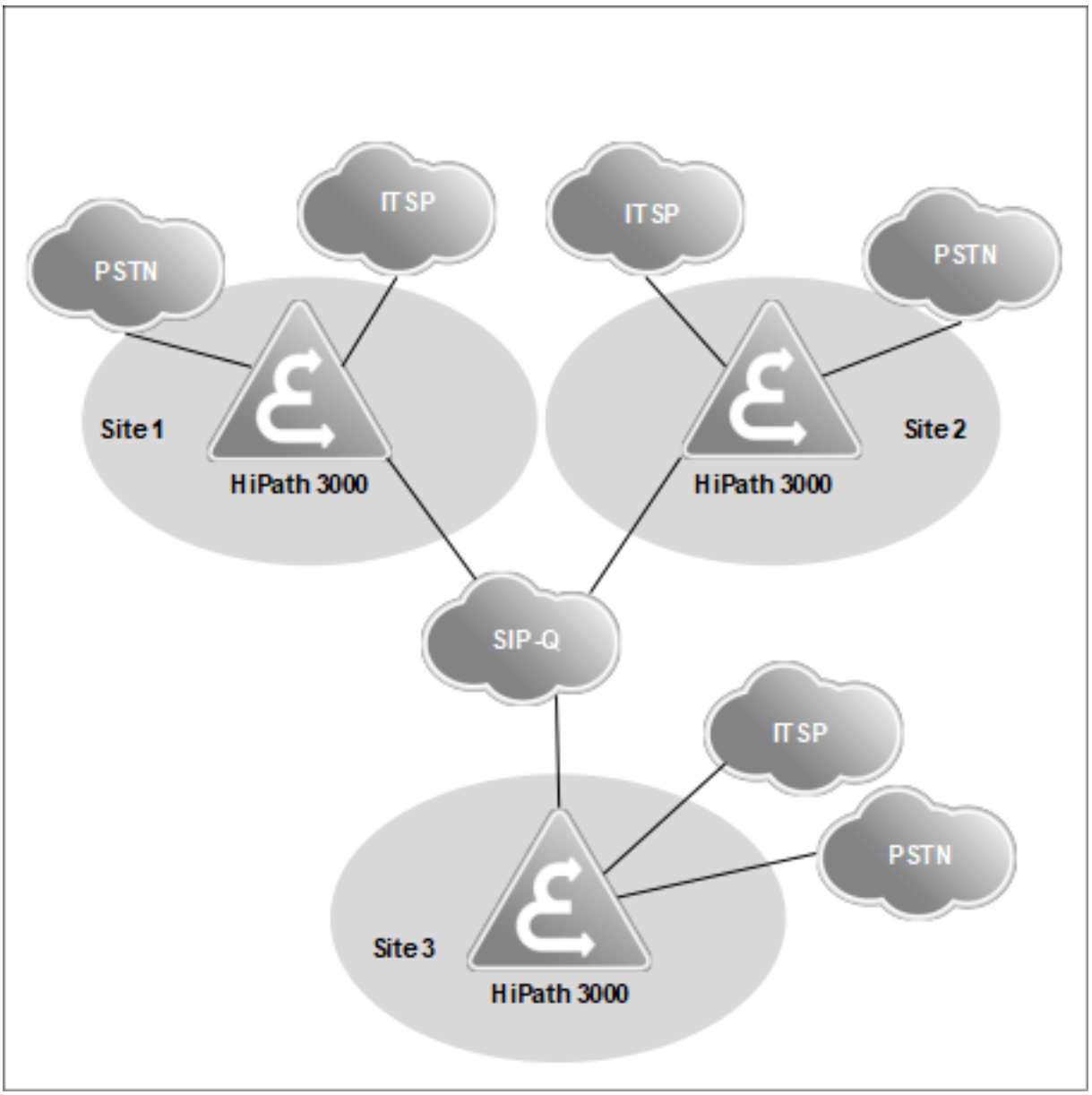


Figura 18: Interred HiPath 3000 V9

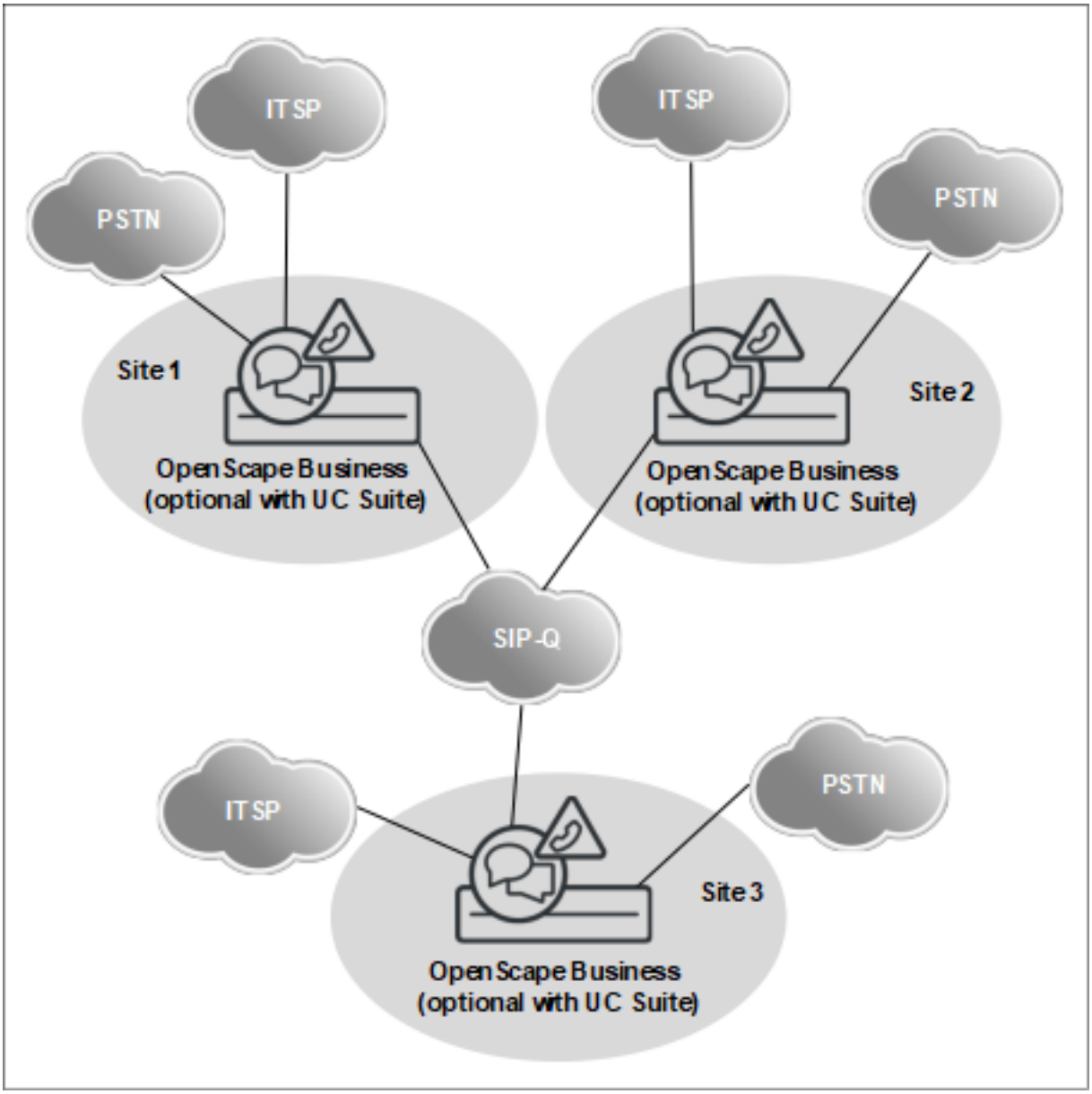


Figura 19: Interred OpenScape Business

Pasos de migración

Siga estos pasos en orden:

1) Actualizar HiPath 3000

Todos los sistemas HiPath 3000 de la interred deben actualizarse por separado, según los pasos de migración detallados para un sistema independiente (véase 1.7.1).

2) **Ajustar la configuración**

   Después hay que ajustar estos parámetros de configuración mediante el Modo Experto de la Gestión basada en Web (WBM):

   - Entradas LCR
   - Sistema de buzón de voz (línea colectiva, código para acceder por marcación al buzón de voz)
   - Anuncios

3) **Realizar el registro de licencia**

   Después de actualizar todos los sistemas, los distintos archivos de licencia se reunen en una sola licencia a nivel de red en el CLS.

26.7.5 Migración de una interred HiPath 3000 V9 con HiPath 5000 RSM

Una red HiPath 3000/5000 con un único archivo de licencia de red común se puede dividir en sistemas independientes con archivos de licencia independientes mediante el servidor central de licencias (CLS). Ahora cada sistema independiente puede migrar a OpenScape Business y registrar una licencia individual.

Si es necesario, los sistemas OpenScape Business se pueden combinar en un grupo de redes en el CLS, con un único archivo de licencia de red, después de la migración.

El abanico de funciones de HiPath 5000 RSM está integrado en OpenScape Business, por lo que en la interred OpenScape Business no se requiere HiPath 5000 RSM.

Para interconectar los sistemas OpenScape Business, las licencias de red de OpenScape Business deben estar disponibles adicionalmente por cada nodo.

Para telefonía Internet y líneas T1, se requieren licencias de línea adicionales.

Se deben seguir los pasos de migración detallados a continuación.

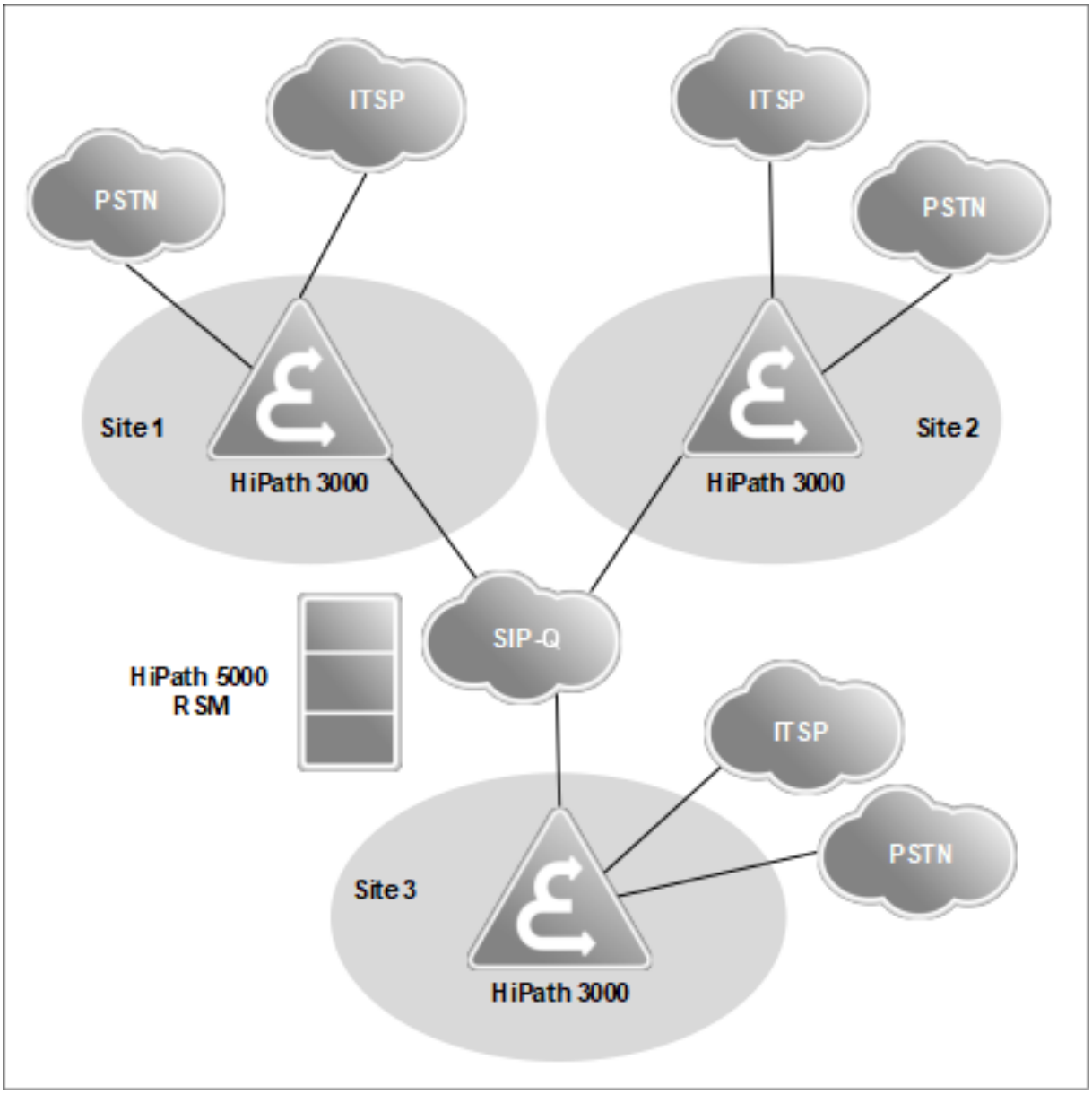


Figura 20: Interred HiPath 3000 V9

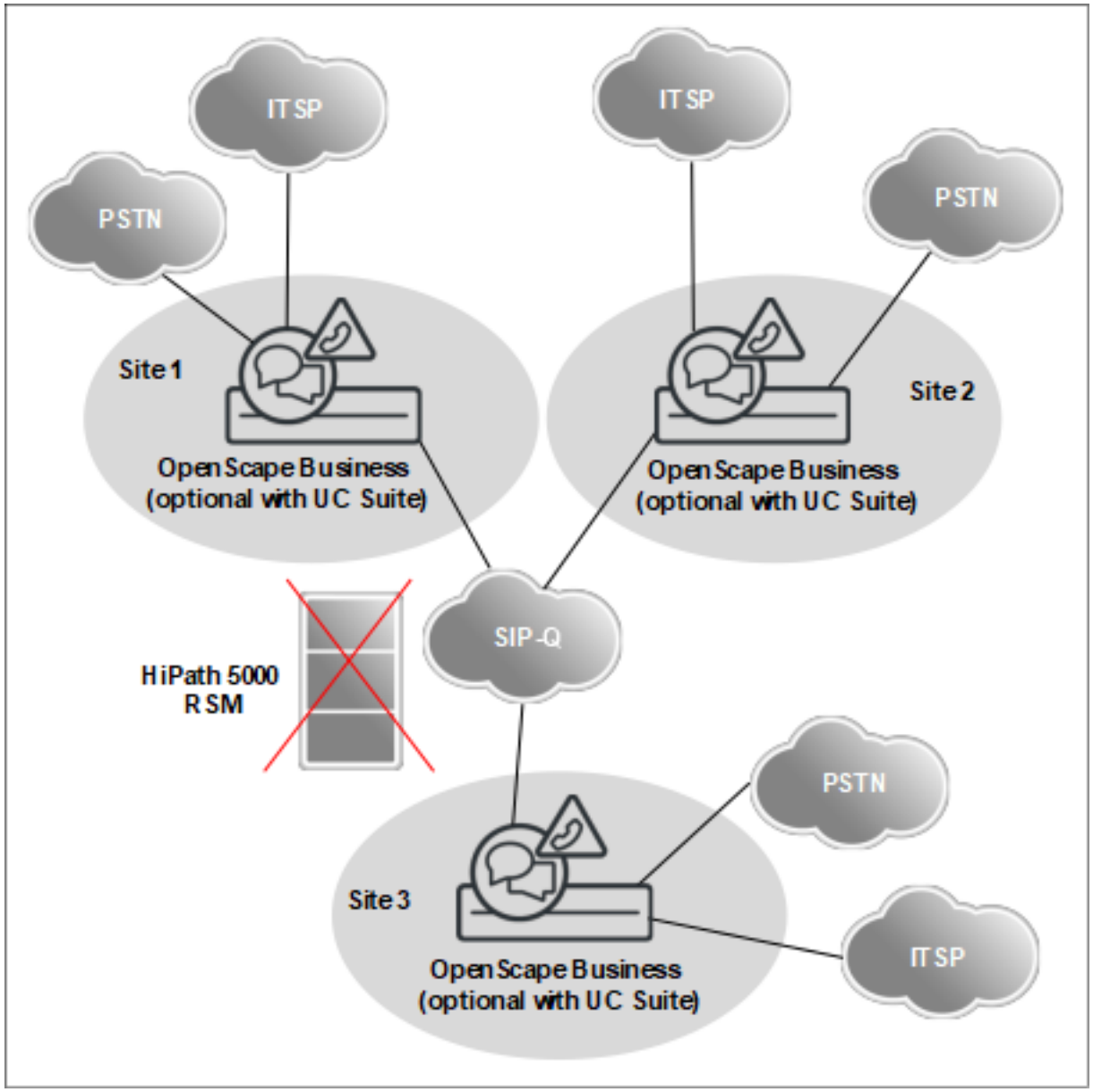


Figura 21: Interred OpenScape Business

Pasos de migración

Siga estos pasos en orden:

1) Dividir el archivo de licencia a nivel de red

Una interred HiPath 3000 con HiPath 5000 RSM solo utiliza el registro de licencia a nivel de red. En primer lugar, hay que dividir el archivo de licencia de red en el CLS en distintos archivos de licencia y asignar a los ID de bloqueos (direcciones MAC) de los sistemas HiPath 3000 V9 antes de comenzar con la migración a OpenScape Business propiamente dicha.

- En primer lugar, asigne las licencias de la interred HiPath 5000 RSM a los ID de bloqueo correspondientes de los nodos HiPath 3000. Recomendación: Cree una lista Excel con la asignación de las licencias a los ID de bloqueo de los sistemas HiPath 3000.

- Contacte con la hot-line de licencias para hacer la división de licencias de acuerdo con la lista Excel.
- Cargue las licencias individuales de los sistemas HiPath 3000 para que el CLS haga el control. No es necesario activar las licencias, es decir, transferirlas a los sistemas HiPath 3000.

2) Retirar HiPath 5000 RSM

Antes de actualizar la versión de los sistemas HiPath 3000 se desconecta HiPath 5000 RSM.

3) Actualizar HiPath 3000

Todos los sistemas HiPath 3000 de la interred deben actualizarse por separado, según los pasos de migración detallados para un sistema independiente. Véase 1.7.1

4) Ajustar la configuración

Después hay que ajustar estos parámetros de configuración en los sistemas OpenScape Business mediante el Modo Experto de la Gestión basada en Web (WBM):

- Entradas LCR
- Sistema de buzón de voz (línea colectiva, código para acceder por marcación al buzón de voz)
- Anuncios

5) Realizar el registro de licencia

Después de actualizar todos los sistemas, los distintos archivos de licencia de OpenScape Business se reunen en una sola licencia a nivel de red en el CLS.

Nota: Si se hace una extensión a nivel de red con funcionalidad de UC, hay que cambiar de numeración abierta a cerrada para adaptar los números internos. Hay que desactivar la numeración abierta; además, hay que eliminar el número de nodo y añadirlo luego como prefijo (por ejemplo, el número interno extendido 87100 en lugar de 100 y 88100 en lugar de 100).

Diferencias:

- La selección de participantes en su propio nodo se realiza con el número interno extendido.

- El número interno y el número de marcación directa pueden ser diferentes en caso necesario, pero no hay que cambiar los números de marcación directa.

26.7.6 Prestaciones e interfaces modificadas/descartadas de HiPath 3000

Algunas prestaciones e interfaces de HiPath 3000 se han adaptado y ampliado para OpenScape Business.

Sustitución de tarjetas MMC

Por motivos técnicos, la tarjeta SDHC / M.2 SATA SSD no se puede sustituir si el sistema está encendido (lo que en el HiPath 3000 se denomina Speed-Update). Además, la tarjeta SDHC / M.2 SATA SSD de un sistema A con

licencia registrada no se puede utilizar en otro sistema B, ya que el registro de licencia está vinculado con el ID de bloqueo de la placa base A. Si la tarjeta SDHC / M.2 SATA SSD se debe utilizar en el sistema B, primero debe inicializarse con el software nuevo mediante Card Manager.

Canales DSP / canales B de HG1500

Ya no se necesita el módulo HG1500. La funcionalidad DSP está integrada en OpenScape Business en la placa base V3 y disponible mediante las tarjetas Voice Channel Booster opcionales.

Determine cuántos canales DSP se necesitan. Los canales DSP son necesarios para implementar transferencias de red de telefonía TDM a VoIP. OpenScape Business tiene 8 canales DSP integrados en la placa base V3. Para ampliar los canales DSP, se puede utilizar el módulo DSP OCCB1/OCCBL (hasta 40 canales) o el módulo DSP OCCB3/OCCBH (hasta 120 canales).

entry Web Services

entry Web Services ya no son compatibles. El modelo sucesor de myPortal entry se denomina myPortal @work y ofrece un conjunto de funciones ampliado. myPortal for Mobile es sustituido por myPortal to go (Web Edition). Para utilizar myPortal to go (Web Edition) ya no se necesita el Plug PC.

Entry VoiceMail

El módulo Entry VoiceMail se descarta en OpenScape Business: la función está integrada como Smart Voicemail en la placa base de OpenScape Business. Los usuarios de Smart Voicemail deben contar con licencia.

Buzón de voz externo

Si en HiPath 3000 se usa un buzón de voz externo, como Xpressions, después de la conversión de la memoria de datos de cliente (KDS), los 10 puertos EVM del Manager E se deben cambiar de **Phonemail** a **Estándar**.

Ampliación de las funciones SIP

Estas prestaciones son adicionales respecto al HiPath 3000 V9:

- Call completed elsewhere
- Message Waiting Indication for Voicemail
- Calling Name Presentation (CNIP)
- Distinctive Ringing (internal/external calls)
- 3rd Party Call Control
- Call Forwarding busy/no reply/unconditional (handset controlled)

Tronqueo SIP

Para conectar servidores SIP externos (por ejemplo, OpenScape Alarm Server, HiPath 4000, OpenScape Voice o UC Suite) en OpenScape Business hay disponibles rutas SIP nativo/SIP-Q adicionales (con HiPath 3000 solo una). Para ello, además de las rutas clásicas de línea urbana, interconexión e ITSP, hay previstas interfaces de tronqueo SIP-Q nativas independientes (lo que se denomina "SIP-Interconnection") para aplicaciones SIP certificadas.

Véase Interconexión de OpenScape Business

LCR

Las tablas de rutas 1 a 15 son para las entradas predeterminadas o para la configuración mediante asistentes. Al hacer una migración, las entradas presentes en HiPath 3000 no se pasan a estas tablas de rutas. Es imprescindible un tratamiento posterior de las tablas de rutas.

Ocupación automática de ruta

Puede estar activa la función "LCR" o la función "Ocupación automática de ruta (marcación simplificada)". Por ello, al hacer una migración, "LCR" se activa automáticamente y "Ocupación automática de ruta (marcación simplificada)" se desactiva. Si desea desactivar LCR y activar "Ocupación automática de ruta" (marcación simplificada), primero hay que ejecutar el asistente "Instalación básica" y, a continuación, definir los flags con el Manager E (no para OpenScape Business X1, porque no permite la administración mediante Manager E).

Nota: Las aplicaciones CSTA no admiten la marcación simplificada.

VoIP over PPP vía RDSI

Ya no se admiten las conexiones de voz encaminadas a través de línea con un ancho de banda reducido

Compatibilidad de G.723

Los códecs G.723 ya no son compatibles.

Babyphone (Vigilancia de habitación)

La prestación "Babyphone (Vigilancia de habitación)" ya no es compatible. Como la función "Supervisión CSTA" siempre está activa (los teléfonos del sistema se pueden supervisar desde una aplicación, como myAgent o myPortal), la función "Vigilancia de habitación" no se puede activar en ese teléfono del sistema. Durante la conversión de la memoria de datos de cliente (KDS), se borra con el Manager E el código para activar la Vigilancia de habitación.

Número de extensiones base y teléfono DECT en OpenScape Business X3

El número de extensiones base en OpenScape Business X3 se ha ampliado respecto a HiPath 33XX, de 3 a 7. El número de teléfonos DECT en OpenScape Business X3 se ha ampliado respecto a HiPath 33XX, de 16 a 32.

BS4 de HiPath 3000

Ya no se requieren licencias para extensiones base en OpenScape Business.

SSDP basado en el Plug PC

SSDP está integrado en OpenScape Business. Ya no se requiere el Plug PC.

Interfaz de Accounting

Las interfaces de datos de Accounting han cambiado respecto a HiPath 3000.

Aplicaciones V24

Ya no se admiten aplicaciones V24.

Aplicaciones CSTA

En OpenScape Business V·3, se requiere una placa base V3 o UC Booster Card/Server en combinación con una placa base V2 para conectar las aplicaciones CSTA. En una interred, una placa base V3 / UC Booster Card/ Server debe existir solo en el nodo maestro. Las aplicaciones deben ser compatibles con el protocolo CSTAv3. Se han implementado cambios en el protocolo CSTA respecto al HiPath 3000. Por ello, es posible que las aplicaciones CSTA de HiPath 3000 V9 no sean compatibles con los sistemas OpenScape Business. El protocolo CSTAv2 ya no se admite.

En el software V3, se requiere una licencia CSTA para el uso de la interfaz CSTA, a excepción de lo siguiente:

- Conexiones de CSTA en general con UC Booster Card
- Conexiones de CSTA en general con OpenScape Business TAPI 120 o TAPI 170

La interfaz de OpenScape Business CSTA se ha modificado respecto a la interfaz HiPath 3000 CSTA como sigue.

- La conexión con la interfaz CSTA es la misma para el nodo esclavo de OpenScape Business independiente e interconectado. La CSTA del nodo maestro en una red proporciona una funcionalidad mejorada. Se realiza exclusivamente mediante LAN. Las interfaces RS-232(V.24) y S0 ya no son compatibles.
- En OpenScape Business no se requieren componentes de hardware y software adicionales, como CSTA Service Provider (CSP), el módulo HG 1500 o el sistema HiPath 5000 RSM. En lugar de hardware de UC Booster, se requieren placas base V3.
- La interfaz CSTA está sujeta a licencia, con la excepción de las conexiones con UC Booster Card y TAPI 120/170.
- Para la conexión de aplicaciones externas se pueden utilizar 4 enlaces CSTA como máximo. En el estado de suministro, 3 de las 4 interfaces CSTA están preconfiguradas para el uso de aplicaciones internas de OpenScape Business. De forma opcional, también se pueden utilizar para la conexión de aplicaciones externas.
- Se ha mejorado la protección de las interfaces CSTA frente al uso indebido. Se ha modificado el mecanismo de acceso.
- La supervisión MULAP mediante CSTA solo es posible si se ha definido un punto de supervisión en el número MULAP. No se pueden supervisar miembros MULAP individuales. Si, no obstante, una aplicación CSTA desea supervisar miembros MULAP individuales, OpenScape Business no transmite eventos de CSTA a la aplicación. Esto también se aplica a miembros MULAP que formen parte de una línea colectiva.
- Se han ampliado las funciones CSTA disponibles. En el manual de interfaz de OpenScape Business CSTA encontrará información más detallada.
- La versión de protocolo CSTA Phase II ya no es compatible.
- Las aplicaciones CSTA que se operen en OpenScape Business se deben probar y autorizar en relación con OpenScape Business.

Aplicaciones HiPath TAPI 120/170 V2

Con HiPath TAPI 120/170 V2 no se pueden transferir y aplicar las licencias existentes. Hay que comprar nuevas licencias. HiPaht TAPI 120/170 V2 debe desinstalarse y hay que volver a instalar y configurar OpenScape Business TAPI 120/170 V1.

Las licencias TAPI se pueden configurar en OpenScape Business en base a usuarios, por lo que ya no es necesario hacer el registro de licencias TAPI en el dispositivo TAPI. Desde el primer usuario TAPI es necesario hacer el registro de licencia (así, TAPI120 tampoco queda exento del uso de licencias para los primeros 6 usuarios). El CMD (CSTA Message Dispatcher) está integrado en OpenScape Business. De esta forma, ya no se necesita un servidor Windows independiente para el CMD. Es posible conectarse a aplicaciones TAPI externas para OpenScape Business y OpenScape Business S. OpenScape Business requiere una placa base V3 o UC Booster / Server. En una interred debe haber al menos un OpenScape Business S o al menos el nodo maestro debe contar con una placa base V3 / UC Booster Card / Server.

OpenScape Business TAPI 120/170 V2 V1 se ha modificado respecto a HiPath TAPI 120/170 V2 como sigue.

- El acceso al sistema se realiza exclusivamente a través de LAN Ethernet. Las interfaces RS-232 y S0 ya no son compatibles.
- Nueva licencia TAPI común "por usuario" para TAPI 120 TSP y TAPI 170 TSP.
- Las licencias están vinculadas con el ID de bloqueo de OpenScape Business.
- Las licencias de HiPath TAPI 120 TSP o HiPath TAPI 170 TSP existentes no son compatibles con el nuevo mecanismo de registro de licencias.
- No hay retrocompatibilidad con HiPath 3000 V8 o V9
- Para TAPI 170 TSP:
  - El acceso al sistema se hace de forma predeterminada a través del puerto 8800.
  - Es obligatorio configurar la información de inicio de sesión CSTA en el cuadro de diálogo de configuración.
  - Compatibilidad multinodo en la red a través del CSP del nodo maestro central.
- Para TAPI 120 TSP:
  - El acceso al sistema se hace de forma predeterminada a través del puerto 8900.
  - Compatibilidad de nodo único, también con integración en el nodo maestro de una red.

Otras aplicaciones externas

Las posteriores aplicaciones conectadas de forma externa a HiPath 3000 ya no pueden operarse en OpenScape Business.

Aplicación de HiPath 3000	Aplicación sucesora para OpenScape Business	Observaciones
optiClient Attendant	OpenScape Business Attendant	Nueva aplicación No es posible la transferencia de licencias
optiClient BLF V1/V2	OpenScape Business Attendant (OpenScape Business BLF)	Nueva aplicación No es posible la transferencia de licencias
HiPath TAPI 120/170	OpenScape Business TAPI 120/170	Nueva aplicación No es posible la transferencia de licencias
Communication Clients de Entry WEB Services en el Plug PC	Solución UC integrada	Nueva aplicación No es posible la transferencia de licencias
myPortal for Mobile	myPortal to go	Nueva aplicación No es posible la transferencia de licencias

Prestaciones modificadas/descartadas de HiPath 5000 RSM

HiPath 5000 RSM ya no es compatible. Las funciones de HiPath 5000 RSM se han integrado en OpenScape Business. Esto significa que ya no se requiere un servidor independiente.

Tabla 37: Diferencias entre HiPath 5000 RSM y OpenScape Business V3

Prestación	HiPath 5000 RSM	OpenScape Business
Registro de licencia a nivel de red, asignación de licencias a los distintos nodos	Todas las licencias del sistema de la red se reunen en una licencia a nivel de red en el CLS.	Todas las licencias del sistema de la red se reunen en una licencia a nivel de red en el CLS.
Administración a nivel de red	DB-Feature Server: Todos los nodos de la red se reúnen en una memoria de datos de cliente (KDS) de red por medio del Manager E. La numeración se sincroniza en la red.	Mediante OpenScape Business Assistant (Gestión basada en Web, WBM), todos los nodos de la red se registran con un asistente de red. La gestión de números de teléfono se sincroniza a nivel de red (numeración cerrada).

Prestación	HiPath 5000 RSM	OpenScape Business
Integración en nodos o aplicaciones externos	Conexión SIP-Q de hasta 4 nodos externos	Hasta 10 rutas de interconexión SIP con hasta 2 SIP-Q, 10 SIP nativo u 8 ITSP
Resillience / Survivability	User-Survivability para teléfonos HFA con numeración cerrada	User-Survivability para teléfonos HFA con numeración cerrada (cambiar de OpenScape Business S <-> OpenScape Business X3/X5/X8)
Copia de seguridad / Restauración	A nivel de red	Local
Función de inventario	A nivel de red	Local
Gestor de presencia	Función a nivel de red con aprovisionamiento de 5000 RSM	Función a nivel de red con aprovisionamiento de un CSP multinodo basado en la tarjeta OpenScape Business UC Booster Card, el servidor OpenScape Business UC Booster Server u OpenScape Business S. Requisitos previos: numeración cerrada.
TAPI 170 en el sistema independiente	TAPI 170 en el sistema independiente se ejecuta en un PC con Windows con registro de licencia propio (archivo de licencia independiente para el TAPI 170).	TAPI 170 en el sistema independiente se ejecuta en un PC con Windows. La consulta de licencia y el suministro de la base de datos TAPI 170 se hacen desde la base de datos SQL de OpenScape Business. La conexión TAPI 170 se realiza mediante el CSP del sistema (la tarjeta OpenScape Business UC Booster Card, el servidor OpenScape Business UC Server Booster u OpenScape Business S)

Prestación	HiPath 5000 RSM	OpenScape Business
TAPI 170 en la interred	TAPI 170 operativo en el 5000 RSM con registro de licencia propio (archivo de licencia independiente para TAPI 170). La base de datos TAPI 170 se obtiene del DB Feature Server del 5000 RSM.	Como en el sistema independiente, pero la conexión del TAPI 170 se realiza en el CSP multinodo del nodo maestro (es decir, a nivel de red). Requisitos previos: numeración cerrada.

Redes mixtas

No se admiten interredes mixtas de OpenScape Business y OpenScape Office.

26.8 Migración en OpenScape Business V3

Aquí se describen las distintas opciones de migración dentro de sistemas OpenScape Business X V3 con placas base V2.

Nota: ¡Estos escenarios son obsoletos (no válidos) para sistemas OpenScape Business X V3 con placas base V3!

Aumento del número de usuarios UC Smart

Existen las opciones siguientes:

- Migración de **OpenScape Business X** (UC Smart) a **OpenScape Business X** con **UC Booster Card** (UC Smart)

  Conveniente para 50 - 150 usuarios UC Smart. Se aplican todos los datos de configuración y de usuario. Al hacer una reducción de versión o downgrade no se aplica ningún dato. Se requieren licencias de usuario UC adicionales para los nuevos usuarios UC Smart. OpenScape Business X1 no se puede ampliar con la UC Booster Card.
- Migración de **OpenScape Business X** (UC Smart) a **OpenScape Business X** con **UC Booster Server** (UC Smart)

  Conveniente para 50 - 500 usuarios UC Smart. Se aplican todos los datos de configuración y de usuario. Al hacer una reducción de versión o downgrade no se aplica ningún dato. Se requieren licencias de usuario UC adicionales para los nuevos usuarios UC Smart.
- Migración de **OpenScape Business X** con **UC Booster Card** (UC Smart) a **OpenScape Business X** con **UC Booster Server** (UC Smart)

  Conveniente para 150 - 500 usuarios UC Smart. Se aplican todos los datos de configuración y de usuario. Al hacer una reducción de versión o downgrade no se aplica ningún dato. Se requieren licencias de usuario UC adicionales para los nuevos usuarios UC Smart.

Upgrade de UC Smart a UC Suite

Existen las opciones siguientes:

- Migración de **OpenScape Business X** (UC Smart) a **OpenScape Business X** con **UC Booster Card** (UC Suite)

  No se aplican los datos de configuración y de usuario. Para los clientes UC Smart existentes se requiere una licencia de actualización de versión (upgrade) a clientes UC Suite. El cambio de la solución de UC a la UC Suite se realiza en la Gestión basada den Web (WBM) con el asistente **Instalación inicial**.
- Migración de **OpenScape Business X** (UC Smart) a **OpenScape Business X** con **UC Booster Server** (UC Suite)

  No se aplican los datos de configuración y de usuario. Para los clientes UC Smart existentes se requiere una licencia de actualización de versión (upgrade) a clientes UC Suite. El cambio de la solución de UC a la UC Suite se realiza en la Gestión basada den Web (WBM) con el asistente **Instalación inicial**.
- Migración de **OpenScape Business X** con **UC Booster Card** (UC Smart) a **OpenScape Business X** con **UC Booster Server** (UC Suite)

  No se aplican los datos de configuración y de usuario. Para los clientes UC Smart existentes se requiere una licencia de actualización de versión (upgrade) a clientes UC Suite. El cambio de la solución de UC a la UC Suite se realiza en la Gestión basada den Web (WBM) con el asistente **Instalación inicial**.
- Migración en **OpenScape Business S** de UC Smart a UC Suite

  No se aplican los datos de configuración y de usuario. Para los clientes UC Smart existentes se requiere una licencia de actualización de versión (upgrade) a clientes UC Suite. El cambio de la solución de UC a la UC Suite se realiza en la Gestión basada den Web (WBM) con el asistente **Instalación inicial**.
- Migración en **OpenScape Business UC Booster Server** de UC Smart a UC Suite

  No se aplican los datos de configuración y de usuario. Para los clientes UC Smart existentes se requiere una licencia de actualización de versión (upgrade) a clientes UC Suite. El cambio de la solución de UC a la UC Suite se realiza en la Gestión basada den Web (WBM) con el asistente **Instalación inicial**.

Aumento del número de usuarios UC Suite

Existen las opciones siguientes:

- Migración de **OpenScape Business X** con **UC Booster Card** (UC Suite) a **OpenScape Business X** con **UC Booster Server** (UC Suite)

  Conveniente para 150 - 500 usuarios UC Suite. Se aplican todos los datos de configuración y de usuario. Al hacer una reducción de versión o downgrade no se aplica ningún dato. Para los nuevos usuarios UC Suite se requieren licencias UC Suite User o licencias Groupware User adicionales.

26.9 Migración de módulos de hardware

Las siguientes acciones de migración de hardware son posibles en el caso de los sistemas OpenScape Business X8:

- Sustitución de SLMO24N con SLMU

- Sustitución de SLMO8N con SLMU
- Sustitución de SLCN con SLMUC (SLMU + CMAe)

26.9.1 Sustitución de SLMO24N con SLMU

Se admite un simple intercambio de tarjetas. Se puede quitar la SLMO24N del sistema y conectar la nueva SLMU. Todos los puertos configurados se mantienen sin cambios. No es necesario apagar el sistema.

26.9.2 Sustitución de SLM8N con SLMU

Como la tarjeta SLMU tiene más puertos que la SLMO8, la administración debe eliminar la tarjeta SLMO8. Para eliminar la tarjeta del sistema, se debe utilizar el usuario online con el siguiente cuadro de diálogo:

```
Administración del sistema 29- 4 - 1
```

y cambie el tipo de tarjeta a SLMUC.

Nota:

Si los usuarios están configurados para UC Suite, se crean con la configuración predeterminada. Todos los datos anteriores (por ejemplo, correo de voz, fax, configuración de usuario) se pierden.

Nota:

Si se intercambia la SLMO8 con la tarjeta SLMU sin eliminar la tarjeta mediante el procedimiento descrito, los 16 puertos adicionales de la tarjeta SLMU podrían perderse porque no se podrían configurar. Esto sucederá si ya hay otra tarjeta en funcionamiento que utilice el rango de puertos de estos 16 puertos. Si hay una sola SLMO8 en el sistema, reemplazada por una tarjeta SLMU, todos los puertos estarán disponibles.

26.9.3 Sustitución de SLCN con SLMUC (SLMU + CMAe)

Como la tarjeta SLMU tiene más puertos que la SLCN, la administración debe eliminar la SLCN antes de que la SLMUC entre en servicio en esa ranura. El proceso para retirar la tarjeta es el siguiente:

1) **Anule el registro de todos los auriculares CMI de la extensión base**
2) **Retire la tarjeta del sistema**
3) **Retire la tarjeta SLCN por usuario online con el cuadro de diálogo:**

   ```
   Administración del sistema 29- 4 - 1
   ```

   y cambie el tipo de tarjeta a SLMUC.
4) **Instale la tarjeta SLMUC**
5) **Configure el auricular utilizado**

6) Registre los auriculares CMI

Todos los teléfonos DECT afectados (máximo 128) deben estar conectados para el nuevo registro.

Nota:

Cuando se sustituye una tarjeta SLCN por una SLMUC, también se necesita una tapa ciega para la SLMUC en lugar de la cubierta de plástico que se usa para la SLCN.

Nota:

Si los usuarios están configurados para UC Suite, se crean con la configuración predeterminada. Todos los datos anteriores (por ejemplo, correo de voz, fax, configuración de usuario) se pierden.

26.10 Migración de OpenScape Business X1 V2 a OpenScape Business X1W V3

Al migrar un modelo OpenScape Business X1, es necesario sustituir todo el sistema.

Se pueden adquirir las licencias existentes. La configuración del cliente no puede retomarse y debe restaurarse manualmente tras la migración. El soporte de software existente continuará sin cambios tras la migración o se adoptará una nueva fecha de soporte de software para la placa base V3 si ésta es válida más allá del 31/12/2026.

Antes de la migración, debe configurarse en el sistema el acceso permanente al servidor de licencias de Unify (a través de Internet), si no se dispone ya de él, y debe activarse la función "CLS Connect". De esta manera, se simplifica la transferencia de licencias y se acorta el tiempo de migración de manera considerable. Se debe informar al cliente sobre el acceso requerido del sistema OpenScape Business al CLS.

Elementos de pedido obligatorios

Para la migración del modelo X1 a X1W con placa base V3, son necesarios los siguientes elementos de pedido en función de si se utiliza CLS Connect, UC Suite o aplicaciones CSTA externas:

- Sistema X1W
- Software V3 en almacenamiento de datos M.2 SATA SSD
- Almacenamiento masivo de datos M.2 SSD de 256 GB (opcional con la aplicación UC Suite)
- Actualización de OpenScape Business para licencia OS Biz X1 (siempre es necesaria)
- Licencia OpenScape Business CSTA (opcional)

Condiciones límite funcionales

Las licencias existentes pueden transferirse completamente del Sistema X1 existente al Sistema X1W con placa base V3 en el curso de la migración. La transferencia de licencias sin la activación de la función CLS Connect requiere

la licencia "Migración", un tratamiento mucho más complejo y un gasto de tiempo mayor que si se utiliza la función CLS Connect.

Los sistemas X1 con CLS Connect activo no pueden actualizarse a sistemas X1W con placa base V3 mediante la función "Regeneración". La licencia "Actualización de OpenScape Business a OS Biz X1" debe estar siempre activada, pero no es necesario introducir ningún código de confirmación durante el proceso de actualización.

No se admite la actualización del sistema OpenScape Business X1 PAYGO a los sistemas OpenScape Business X1W PAYGO.

En caso de que en el sistema funcionen clientes OpenScape Personal Edition y se disponga de las licencias correspondientes, estas deberán regenerarse siempre manualmente en el servidor central de licencias para el nuevo ID de bloqueo (dirección MAC) de la placa base V3, independientemente de si se utiliza CLS Connect o no.

La configuración del cliente no puede retomarse y debe restaurarse manualmente tras la migración.

Gestión técnica de la migración

Los pasos técnicos principales de la migración se describen a continuación. Se distingue entre

- Migración con licencia permanente
  - Migración con la función CLS Connect activada y conexión al servidor central de licencias
  - Migración sin la función CLS Connect y sin conexión al servidor central de licencias

Encontrará más información sobre la gestión técnica de la migración en el manual de OpenScape Business Administrations.

26.10.1 Cómo migrar con CLS Connect a los sistemas con licencia permanente X1W V3

Paso a paso

1) Genere archivos de licencia en el Servidor Central de Licencias (CLS).
   a) Active la licencia "Actualización de OpenScape Business a OS Biz X1" en el sistema X1 con placa base V2. Durante el proceso de activación proporcione la dirección MAC de la placa base V3.
   b) Genere un nuevo archivo de licencia para la dirección MAC de la placa base V3 del sistema X1W. Este archivo de licencia incluye el soporte ampliado de software.
   c) Transferencia de las posibles licencias Personal Edition existentes de la dirección MAC de la placa base V2 a la dirección MAC de la placa base V3 mediante la función "Regenerar" y generación de un nuevo archivo de licencia para las licencias Personal Edition.

2) Preparar el sistema OpenScape Business
   a) Actualice el sistema existente a la versión de software V2R7.
   b) Configure el acceso al servidor central de licencias (CLS) en el sistema y compruebe la conexión.
   c) Active CLS Connect en el sistema. Si no se ha hecho ya, el soporte de software se ampliará de nuevo durante 3 meses.

3) Intercambio del Sistema X1
   a) Apague el Sistema X1 y desconecte las fuentes de alimentación.
   b) Utilice un dispositivo de almacenamiento V3 y, si es necesario, el almacenamiento masivo de datos opcional en Sistema X1W.
   c) Retire la tarjeta OCCB Voice Channel Booster de la placa base V2 y/o CMAe e insértela en la placa base X1W V3.
   d) Sustituya el sistema X1 por el sistema X1W.
   e) Conecte el cable de tierra al sistema X1W.
   f) Conecte el teléfono, la línea urbana, la LAN y, si procede, el USB al sistema X1 W.
   g) Conecte de nuevo las fuentes de alimentación, el sistema arranca automáticamente.

4) Establezca los parámetros básicos del sistema en el WBM tras el inicio.
   a) Establezca la fecha y hora del sistema.
   b) Establezca el paquete de aplicación.
      - UC Smart para el sistema sin UC Smart o con UC Smart
      - UC Suite para los sistemas con UC Suite
   c) Restaure la configuración del sistema.
      - Configuración manual del X1W.
      - Importe el archivo de licencia recién creado.

26.10.2 Cómo migrar con CLS Connect a los sistemas sin licencia permanente X1W V3

Paso a paso

1) Prepare el sistema OpenScape Business.
   a) Actualice el sistema existente a la versión de software V2R7.

2) Cree el archivo de licencia de migración para el sistema X1 con placa base V2 en el servidor central de licencias (CLS).
   a) Activación de la "Licencia de migración X1" para el sistema existente.
   b) Genere un nuevo archivo de licencia para la dirección MAC de la placa base V2. Para ello, debe introducirse la dirección MAC del sistema X1W en el CLS.
   c) Descargue el archivo de licencia del CLS. Este archivo de licencia incluye el soporte ampliado de software.

3) Importe el archivo de licencia en el Sistema OpenScape Business X1 con la placa base V2.

4) Observe el "Código de confirmación" que aparece en OpenScape Business Assistant.

5) Genere un nuevo archivo de licencia para el sistema X1W con placa base V3 en el servidor central de licencias (CLS).

a) Cree un nuevo archivo de licencia para la dirección MAC del sistema X1W con placa base V3 en el CLS regenerando la dirección MAC del X1 con placa base V2 y el código de confirmación anotado anteriormente.

- Busque el sistema OpenScape Business con la dirección MAC del sistema X1W con placa base V3 en el CLS.
- Introduzca y active el Código de confirmación para desbloquear el sistema OpenScape Business.
- Regenere el archivo de licencia.

b) Descargue el archivo de licencia recién generado del CLS.

6) Cambio de placa base

a) Apague el sistema y desconecte las fuentes de alimentación.

b) Utilice un dispositivo de almacenamiento V3 y, si es necesario, el almacenamiento masivo de datos opcional en el Sistema X1W con la placa base V3.

c) Retire la tarjeta CMAe y/o la tarjeta OCCB Voice Channel Booster de la placa base V2 y conéctela al X1W con placa base V3.

d) Sustituya la placa base del Sistema X1 con V2 por la placa base del Sistema X1W con V3.

e) Conecte el cable de tierra al sistema X1W.

f) Conecte el teléfono, la línea urbana, la LAN y, si procede, el USB al sistema X1 W.

g) Vuelva a conectar la fuente de alimentación y el sistema se iniciará automáticamente.

7) Establezca los parámetros básicos del sistema en el WBM tras el inicio.

a) Establezca la fecha y hora del sistema.

b) Establezca el paquete de aplicación.

- UC Smart para el sistema sin UC Smart o con UC Smart
- UC Suite para los sistemas con UC Suite

c) Restaure la configuración del sistema.

- Configuración manual del X1W

d) Importación manual del nuevo archivo de licencia en el sistema V3 tras el arranque del sistema.

27 Límites de ampliación y capacidades

Los límites de ampliación y capacidades se basan en valores máximos condicionados por el sistema de un solo sistema. Los valores máximos de un sistema en una red pueden ser diferentes.

27.1 Valores máximos para extensiones

- Los datos de los sistemas con placas base OCC V2 se pueden encontrar en Tabla 38: Nivel de ampliación de extensiones/usuarios con placas base OCCx en la página 1466
- Los datos de los sistemas con placas base OCC V3 se pueden encontrar en Tabla 39: Estaciones/usuarios de nivel de expansión con placas base OCCSB/R, OCCMA/B u OCCLA en la página 1467
- Los datos de los sistemas OpenScape Business S Server se pueden encontrar en Tabla 40: Nivel de ampliación de extensiones/usuarios con OpenScape Business S en la página 1468

Tabla 38: Nivel de ampliación de extensiones/usuarios con placas base OCCx

Extensiones	X1	X3W/R	X5W/R	X8
Máximo de extensiones				
Núm. máx. extensiones[15]	30	500	500	500
Extensiones IP				
Sistema extensiones IP (HFA)	20[16]	500	500	500
Extensiones IP (SIP)	20[16]	500	500	500
Extensiones TDM				
Núm. máx. de extensiones TDM[17] [21]	30	384	384	384
Extensiones analógicas (TDM)	4	20	67	384
Extensiones maestras U_{P0} (TDM)[21]	8	24	56	384
Extensiones esclavas U_{P0} (TDM) (incl. a/b y adaptadores S0)	8	24	56	116
Extensiones RDSI S0 (TDM)	2	36	52	128
Extensiones DECT-CMI (TDM)	16	64	64	250
Usuario Mobility				
Núm. máx. de usuarios Mobility[18]	30	150	150	150
Usuarios Mobility Entry	20	150	150	150
Usuarios myPortal to go[19]	30	150	150	150
Usuarios Skype for Business	30	150	150	150

Extensiones	X1	X3W/R	X5W/R	X8
Otros usuarios				
Usuarios RAS	2	500	500	500
Extensiones virtuales configurables	30	250	250	250

Nota: Por cada configuración del sistema hay que comprobar si la salida de potencia nominal del suministro de corriente propio del sistema es suficiente o si se requiere una fuente de alimentación externa adicional (véase *OpenScape Business, Documentación de servicio - Consumo de un sistema de comunicación*).

Tabla 39: Estaciones/usuarios de nivel de expansión con placas base OCCSB/R, OCCMA/B u OCCLA

Extensiones	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Máximo de extensiones								
Núm. máx. extensiones[15]	30	30	500	500	500	500	500	500
Extensiones IP								
Sistema extensiones IP (HFA)	500	500	500	500	500	500	500	500
Extensiones IP (SIP)	500	500	500	500	500	500	500	500
Extensiones TDM								
Núm. máx. de extensiones TDM[17] [21]	384	384	384	384	384	384	384	384

14 Los valores están escalonados según la configuración de UC Booster: Booster Server / Booster Card / sin UC Booster

15 Total de: extensiones IP (HFA), IP (SIP), analógicas, maestras/esclavas UP0, DECT (CMI), RDSI S0, Mobility y Deskshare

16 Total de usuario IP y usuario Deskshare (limitación mediante configuración)

17 Total de: extensiones analógicas, UP0, DECT (CMI) y RDSI S0

18 Total de: participantes Mobility Entry, myPortal to go, Skype for Business

19 El número de conexiones simultáneas de VoIP de las extensiones depende de:

1) los canales DSP disponibles en el sistema para llamadas de gateway (transiciones IP/TDM).

2) Los canales proxy RTP internos disponibles en el sistema para las llamadas a través de VOIP por Internet.

20 El número de conexiones simultáneas según los canales DSP disponibles en el sistema para llamadas de gateway (transiciones IP/TDM).

21 En función de los tipos de teléfonos y del consumo de línea total del sistema de comunicación

Extensiones	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Extensiones analógicas (TDM)	4	4	20	20	67	67	384	384
Extensiones maestro/esclavo U_{P0} (TDM)[21]	8	8	24	24	56	56	384 maestro 116 esclavo	384 maestro 116 esclavo
Extensiones RDSI S0 (TDM)	0	0	32	32	48	48	128	128
Extensiones DECT-CMI (TDM)	16	16	64	64	64	64	250	250
Usuario Mobility								
Núm. máx. de usuarios Mobility[18]	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500 [22]	150/ 500[22]	500	500
Usuarios Mobility Entry	150	20	150	150	150	150	150	150
Usuarios myPortal to go[19]	150/ 500[22]	30	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500[22]	500	500
usuarios de myPortal for Teams[19]	150/ 500[22]	30	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500[22]	500	500
Usuarios Skype for Business	150/ 500[22]	30	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500[22]	500	500

Tabla 40: Nivel de ampliación de extensiones/usuarios con OpenScape Business S

Extensiones	Servidor básico (S)	Servidor estándar (S)	Servidor avanzado (S)
Máximo de extensiones			
Núm. máx. extensiones	50	500	1500
Extensiones IP			
Sistema extensiones IP (HFA)	50	500	1500
Extensiones IP (SIP)	50	500	500
Usuario Mobility			
Núm. máx. de usuarios Mobility	50	250	500
Usuarios Mobility Entry	50	150	150
Usuarios myPortal to go	50	250	500

22 Los valores están escalonados según la versión del módulo: básica o avanzada

Extensiones	Servidor básico (S)	Servidor estándar (S)	Servidor avanzado (S)
usuarios de myPortal for Teams	50	250	500
Usuarios Skype for Business	50	250	500

27.2 Valores máximos para líneas

- Los canales de todos los tipos de líneas (líneas urbanas, cruzadas, de interconexión, etc.) en las placas base OCC V2 se pueden encontrar en Tabla 41: Nivel de ampliación de canales de líneas con placas base OCCx en la página 1469.
- Los canales de todos los tipos de líneas (líneas urbanas, cruzadas, de interconexión, etc.) en las placas base OCC V3 se pueden encontrar en Tabla 42: Canales de línea de nivel de expansión con placas base OCCSB/R, OCCMA/B u OCCLA en la página 1470
- Los canales de todos los tipos de líneas (líneas urbanas, cruzadas, de interconexión, etc.) en OpenScape Business S se pueden encontrar en Tabla 43: Nivel de ampliación de canales de líneas con OpenScape Business S en la página 1471

Tabla 41: Nivel de ampliación de canales de líneas con placas base OCCx

	X1	X3W/R	X5W/R	X8
Máximo de canales de líneas				
Número máx. de canales de líneas[23]	250	250	250	250
Canales de líneas para la conexión de proveedor de servicios de telefonía, interconexión y equipo externo				
Canales troncales SIP (ITSP)	30	60[24]	60[24]	60[24]
Canales SIPQ (interconexión)	100	100	100	100
Canales RDSI S_0 (BRI)	4	20	52	128
Canales RDSI S_{2M} (PRI)	-	30	30	80
Canales RDSI CAS (PRI)	-	30	30	180
Canales analógicos (a/b)	-	X3R: 8 X3W: 16	X5R: 24 X5W: 48	120
Canales de líneas para fines internos				
Canales MEB para anuncios grabados internos[25]	0	16	16	16
Canales de línea urbana para UC Suite[26]	0	60 / 30 / 0[27]	60 / 30 / 0[27]	60 / 30 / 0[27]

[23] Total de canales de línea SIP, líneas ITSP, SIPQ, TDM y canales de línea urbana MEB sin (canales MEB para anuncios grabados).

Tabla 42: Canales de línea de nivel de expansión con placas base OCCSB/R, OCCMA/B u OCCLA

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Máximo de canales de líneas								
Número máx. de canales de líneas[23]	250	250	250	250	250	250	250	250
Canales de líneas para la conexión de proveedor de servicios de telefonía, interconexión y equipo externo								
Canales troncales SIP (ITSP)	60/ 120[28]	60/ 120[28]	60/ 120[28]	60/ 120[28]	60/ 120[28]	60/ 120[28]	120	120
Canales SIPQ (interconexión)	100	100	100	100	100	100	100	100
Canales RDSI S_0 (BRI)	-	-	16	16	48	48	128	128
Canales RDSI S_{2M} (PRI)	-	-	30	30	30	30	180	120
Canales RDSI CAS (PRI)	-	-	30	30	30	30	180	120
Canales analógicos (a/b)	-	-	X3R: 8 X3W: 16	X3R: 8 X3W: 16	X5R: 24 X5W: 48	X5R: 24 X5W: 48	120	120
Canales de líneas para fines internos								
Canales MEB para anuncios grabados internos[25]	16	46	16	16	16	16	16	16
Canales de línea urbana para UC Suite[26]	0	30/60[28]	0	30/60[28]	0	30/60[28]	0	60

24 En interconexión con OpenScape Business S como gateway ITSP, también son posibles más de 60 canales

25 El sistema asigna dinámicamente los canales MEB para anuncios grabados internos del sistema. Siempre se incluyen en el número máximo de canales de líneas.

26 Para sistemas con UC Suite, los canales MEB se generan dinámicamente para: Buzón de voz, AutoAttendant, Fax, conexiones de Call Me, anuncios grabados y llamadas en conferencia. Solo cuentan para el número máximo de canales de líneas en sistemas UC Suite.

27 Los valores están escalonados según la configuración de UC Booster: Booster Server / Booster Card / sin UC Booster

28 Los valores están escalonados según la versión del módulo: básica o avanzada

Tabla 43: Nivel de ampliación de canales de líneas con OpenScape Business S

	Servidor básico (S)	Servidor estándar (S)	Servidor avanzado (S)
Máximo de canales de líneas			
Número máx. de canales de líneas[23]	250	250	250
Canales de líneas para la conexión de proveedor de servicios de telefonía, interconexión y equipo externo			
Canales de línea SIP	180	180	180
Canales SIPQ (interconexión)	100	100	100
Canales de líneas para fines internos			
Canales MEB para anuncios grabados internos[25]	16	16	16
Canales de línea urbana para UC Suite[26]	60	60	60

27.3 Valores máximos de los recursos

Tabla 44: Nivel de ampliación de otras funciones/recursos

	X1		X3		X5		X8	Servidor (S)
	Rack	Mural	Rack	Mural	Rack	Mural	OCCL/ OCCLA	
Recursos del sistema								
Canales DSP								
DSP G.711 sin cifrado	8	8	128/ 48/ 8[34]	128/ 48/ 8[34]	128/ 48/ 8[34]	128/ 48/ 8[34]	128/ 48/ 8[34]	n/d
DSP G.711 + G.729 sin cifrado	8	8	104/ 40/ 8[34]	104/ 40/ 8[34]	104/ 40/ 8[34]	104/ 40/ 8[34]	104/ 40/ 8[34]	n/d
DSP G.711 con cifrado	6	6	102/ 38/ 6[34]	102/ 38/ 6[34]	102/ 38/ 6[34]	102/ 38/ 6[34]	102/ 38/ 6[34]	n/d
DSP G.711 + G.729 con cifrado	6	6	81/ 31/ 6[34]	81/ 31/ 6[34]	81/ 31/ 6[34]	81/ 31/ 6[34]	81/ 31/ 6[34]	n/d
DSP Fax T.38 (para gateway RDSI)[32]	3	3	12/ 6/ 3[34]	12/ 6/ 3[34]	12/ 6/ 3[34]	12/ 6/ 3[34]	12/ 6/ 3[34]	n/d

	X1		X3		X5		X8	Servidor (S)
	Rack	**Mural**	**Rack**	**Mural**	**Rack**	**Mural**	**OCCL/ OCCLA**	
DSP Fax T.38 (Para Fax de UC Suite)[33]	-	-	8/ 6/ 0[34]	8/ 6/ 0[34]	8/ 6/ 0[34]	8/ 6/ 0[34]	8/ 6/ 0[34]	n/d
Canales proxy RTP								
Canales proxy RTP	30	30	60	60	60	60	60	180
Canales de líneas MEB								
Canales de líneas MEB en total	**0**	**0**	**76/ 46/ 0[30]**	**76/ 46/ 0[30]**	**76/ 46/ 0[30]**	**76/ 46/ 0[30]**	**76/ 46/ 0[30]**	**76**
Canales de líneas MEB para anuncios grabados	0	0	16/ 16/ 0[30]	16/ 16/ 0[30]	16/ 16/ 0[30]	16/ 16/ 0[30]	16/ 16/ 0[30]	16
Canales de líneas MEB para UC Suite	-	-	60/ 30/ 0[30]	60/ 30/ 0[30]	60/ 30/ 0[30]	60/ 30/ 0[30]	60/ 30/ 0[30]	60
Música en espera (MOH) y PPP								
Fuentes MOH [29] (G.711a, G.711u, G.729ab, G.729a)	4	4	4	4	4	4	4	32
Canales PPP	8	8	8	8	8	8	8	n/d
Anuncios								
Número de equipos de anuncios grabados por sistema	16	16	16	16	16	16	16	16
Equipos de anuncios grabados mediante a/b	16	16	16	16	16	16	16	n/d
Anuncios grabados mediante Smart VM	6	6	6	6	6	6	6	6

29 Máximo de 16 conexiones simultáneas por fuente MOH

	X1		X3		X5		X8	Servidor (S)
	Rack	Mural	Rack	Mural	Rack	Mural	OCCL/ OCCLA	
Anuncios grabados mediante UC Suite	16	16	16	16	16	16	16	16
Anuncio grabado antes de contestar (sistema, no UC Suite)								
Número de llamantes a los que se les puede reproducir un anuncio grabado de forma simultánea.	24	24	24	24	24	24	24	24
Receptor MF								
Receptor MF	16	16	16	16	16	16	16	Por conversación mediante ITSP

27.3.1 Detalles sobre el uso de canales DSP

Dentro de OpenScape Business, los «canales DSP» se utilizan para la conversión (transcodificación) de flujos de datos. En principio, esto es necesario si hay una transición de IP a TDM o viceversa para los datos de voz o si se requiere un cifrado de los datos de voz. Detalladamente:

- Conexión de voz entre el teléfono IP y la RDSI o línea analógica (troncal).
- Conexión de voz mediante línea IP SIP/ITSP y teléfonos internos UP0/E, a/b o RDSI.
- Conexión de voz desde la línea IP o el suscriptor IP a una conferencia interna. En este caso, se requiere un canal de puerta de enlace para cada cliente de línea/IP que participe en una conferencia.
- Conexiones desde teléfonos UP0/E, a/b o RDSI o líneas RDSI/analógicas a anuncios de UC Suite, buzón de voz, fax o conferencias.

30 Los valores están escalonados según la configuración de UC Booster: Booster Server / Booster Card / sin UC Booster

31 El valor depende de UC Suite: Sistema con UC Suite / Sistema sin UC Suite

32 Los valores aplican para OpenScape Business como gateway RDSI. G.711 a T38 o a la inversa sin Fax de UC Suite

33 Por norma general, UC Suite puede procesar hasta 8 conexiones de fax simultáneas. OpenScape Business X3/X5/X8 como gateway RDSI puede procesar de 3 a 12 faxes simultáneos en función del módulo DSP. Ambos parámetros en combinación determinan el número de conexiones de fax T.38 o G.711 simultáneas.

34 Los valores están escalonados según la configuración de Voice Channel Booster: con OCCBH u OCCB3/ con OCCBL u OCCB1/solo placa base

- Conexiones de voz cifradas entre terminales y conexiones de voz cifradas a través de líneas ITSP. Este no es el caso de la familia de placas base V3, desde OpenScape Business V3R4 en adelante.
- Las conexiones a la música en espera interna requieren un canal DSP por códec MoH configurado.

Para las siguientes conexiones, no se necesita ningún canal DSP:

- Conexión entre usuarios IP internos sin cifrado (carga útil directa).
- Conexión entre ITSP y el suscriptor IP sin cifrado.

Los canales DSP se crean por un procesador de señal, que está integrado en la placa base OCCL u OCCLA respectiva en los modelos X1, X3, X5 y X8.

Dependiendo del tipo de transcodificación, un procesador de señal puede manejar más o menos canales DSP simultáneamente. Se admite la siguiente codificación (códecs).

- **Para conexiones de voz**
  - Conversión de IP (G.711) a TDM con G.711 o viceversa.
  - Conversión de IP (G.711) a TDM con G.711 o viceversa con cifrado (SPE).
  - Conversión de IP (G.729) a TDM con G.711 o viceversa.
  - Conversión de IP (G.729) a TDM con G.711 o viceversa con cifrado (SPE).
- **Para conexiones de fax**
  - Conversión de T.38 a G.711 cuando se utiliza OpenScape Business como puerta de enlace RDSI.
  - Conversión de fax G.711 a fax T.38 o viceversa cuando se utiliza la función de fax UC-Suite.

Si la capacidad del procesador de señal integrado en la placa base no es suficiente para realizar el número requerido de canales DSP, se pueden ampliar utilizando las tarjetas «Voice Channel Booster» disponibles opcionalmente OCCBL u OCCBH.

En la Tabla 11 se muestra el número máximo de canales DSP disponibles en función de la codificación. Tenga en cuenta que cada fila representa el número máximo de canales DSP similares, pero el sistema los asigna dinámicamente durante el funcionamiento. El número de canales DSP ocupados actualmente durante el funcionamiento se puede determinar a través de OpenScape Business Assistant (WBM). Encontrará más notas sobre cómo determinar el número requerido de canales DSP en el manual de administración.

27.3.2 Información detallada sobre el uso de los canales proxy RTP

OpenScape Business utiliza un "proxy RTP" interno para todas las conexiones de VoIP a través de Internet. El proxy ofrece un grupo de canales RTP que se asignan a las conexiones de VoIP a través de Internet de la siguiente manera:

- 1 canal proxy RTP por cada llamada ITSP
- 1 canal proxy RTP por llamada de Unify Phone
- 1 canal proxy RTP por cada sistema Equipo @Home en una llamada
- 1 canal proxy RTP por cada Equipo SIP @Home en una llamada
- 1 canal proxy RTP por cada VoIP de myPortal to go @Home en una llamada

- 1 canal proxy RTP por cada VoIP de myPortal @work @Home en una llamada

Se encuentra disponible un número diferente de canales proxy RTP en los distintos modelos de OpenScape Business. Véase Tabla 44: Nivel de ampliación de otras funciones/recursos en la página 1471.

Ejemplos

- Una llamada de voz saliente externa de una extensión del sistema IP interna mediante una línea ITSP requiere un canal proxy RTP.
- Una llamada de voz externa del cliente myPortal to go VoIP mediante WiFi (campus) interna a una extensión en la red pública a través de una línea ITSP requiere un canal proxy RTP. Esto se utiliza para la conexión mediante ITSP a la extensión llamada en la red pública.
- Una llamada de voz externa del cliente myPortal to go VoIP mediante WiFi pública a una extensión en la red pública a través de una línea ITSP requiere dos canales proxy RTP. Un canal proxy RTP es necesario para conectar el cliente VoIP a OpenScape Business y otro para la conexión mediante ITSP a la extensión llamada en la red pública.
- Una llamada de voz externa que llega mediante ITSP a un cliente de VoIP de myPortal @work en la sede central requiere dos canales proxy RTP. Un canal proxy RTP es necesario para la conexión de ITSP al sistema OpenScape Business y otro para la conexión de OpenScape Business a través de Internet al cliente de VoIP de myPortal @work en la sede central.

27.4 Valores máximos para prestaciones

Los valores máximos aquí descritos se basan principalmente en las capacidades de software de OpenScape Business.

27.4.1 Conexión al proveedor de servicios

	X1W/R		X3W/R		X5W/R		X8W/R		Servidor (S)
	V2	V3	V2	V3	V2	V3	V2	V3	
Conexión ITSP (Proveedor de servicios de telefonía por Internet)									
Canales de línea SIP	30	120	60	120	60	120	60	120	180
ITSP activos simultáneamente	8	8	8	8	8	8	8	8	8
Rutas									
Rutas	16	16	16	16	16	16	16	16	16
Rutas de desbordamiento por ruta	1	1	1	1	1	1	1	1	1

27.4.2 Extensiones

	X1W/R	X3W/R	X5W/R	X8	Servidor (S)
Número de teléfono de la extensión/Número de marcación directa					
Cifras por número de teléfono de extensión/Número de marcación directa	16 (estándar = 3)	16 (estándar = 3)	16 (estándar = 3)	16 (estándar = 3)	16 (estándar = 3)

27.4.3 Niveles de ampliación de UC Smart

- Los niveles de ampliación con placas base OCC V2 se pueden encontrar en Tabla 45: Nivel de ampliación de UC Smart con placas base OCCx en la página 1476
- Los niveles de ampliación con placas base OCC V3 se pueden encontrar en Tabla 46: Nivel de ampliación de UC Smart con placas base OCCSB/R, OCCMA/B u OCCLA en la página 1477
- Los niveles de ampliación con sistemas OpenScape Business S Server se pueden encontrar en Tabla 47: Nivel de ampliación de UC Smart con OpenScape Business S en la página 1479

Tabla 45: Nivel de ampliación de UC Smart con placas base OCCx

	X1	X3W/R	X5W/R	X8
Máximo de usuarios de UC Smart				
Número máx. de usuarios (cuentas) de UC Smart	30	250/ 150/ 50[35]	250/ 150/ 50[35]	250/ 150/ 50[35]
Clientes de UC Smart				
Número de clientes de UC activos simultáneamente[36]	30	500/ 300/ 150[35]	500/ 300/ 150[35]	500/ 300/ 150[35]
myPortal @work	30	250/ 150/ 50[35]	250/ 150/ 50[35]	250/ 150/ 50[35]
myPortal @work Llamadas paralelas de VoIP a otros usuarios llamados[37]	20	30	30	30
myPortal to go[37]	30	150/ 150/ 50[35]	150/ 150/ 50[35]	150/ 150/ 50[35]
DeskPhone CP 400/600/600E/ 700/700X/710 (Modo UC)	30	250/ 150/ 50[35]	250/ 150/ 50[35]	250/ 150/ 50[35]
OpenScape Business Attendant	8	8	8	8
Estado de presencia				
Estado por usuario	9	9	9	9
Anuncios grabados de buzón de voz por estado de presencia	1	1	1	1

	X1	X3W/R	X5W/R	X8
Favoritos				
Favoritos por usuario	100	100	100	100
Grupos de Favoritos por usuario	10	10	10	10
Diario de llamadas				
Registros del diario de llamadas por usuario	100	100	100	100
Conferencia gestionada de UC Smart (mediante cliente de UC)				
Número de conferencias gestionadas	5	5	5	5
Número de usuarios por conferencia gestionada	16	16	16	16
Canales para conferencias gestionadas	30	30	30	30

Tabla 46: Nivel de ampliación de UC Smart con placas base OCCSB/R, OCCMA/B u OCCLA

	X1W/R		X3W/R		X5		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Máximo de usuarios de UC Smart								
Número máx. de usuarios (cuentas) de UC Smart	150	150	150/ 500[39]	150/ 500[39]	150/ 500[39]	150/ 500[39]	500	500
Clientes de UC Smart								
Número de clientes de UC activos simultáneamente[36]	150	150	150/ 500[39]	300/1000	150/ 500[39]	300/ 1000[39]	1000	1000
myPortal @work	150	150	150/ 250[39]	150/ 250[39]	150/ 250[39]	150/ 250[39]	250	250

35 Los valores están escalonados según la configuración de UC Booster: Booster Server / Booster Card / sin UC Booster

36 Total de: myPortal @work, myPortal to go, CP 400/600/600E/700/700X/710 modo UC, Application Launcher, Business Attendant, TAPI 120 (WSI), clientes WSI de terceros (Contexto: varios clientes con la misma cuenta de UC Smart pueden iniciar sesión en el sistema)

37 El número de conexiones simultáneas de VoIP de las extensiones depende de:

1) los canales DSP disponibles en el sistema para llamadas de gateway (transiciones IP/TDM).

2) Los canales proxy RTP internos disponibles en el sistema para las llamadas a través de VOIP por Internet.

38 El número de conexiones simultáneas según los canales DSP disponibles en el sistema para llamadas de gateway (transiciones IP/TDM).

	X1W/R		X3W/R		X5		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
myPortal @work Llamadas paralelas de VoIP a otros usuarios llamados[37]	150	150	30/ 70[39]	30/ 70[39]	30/ 70[39]	30/ 70[39]	70	70
myPortal to go[37]	150	150	150/ 500[39]	150/ 500[39]	150/ 500[39]	150/ 500[39]	500	500
myPortal for Teams	150	150	150/ 500[39]	150/ 500[39]	150/ 500[39]	150/ 500[39]	500	500
DeskPhone CP 400/600/600E/ 700/700X/710 (Modo UC)	150	150	150/ 500[39]	150/ 500[39]	150/ 500[39]	150/ 500[39]	500	500
OpenScape Business Attendant	8	8	8	8	8	8	8	8
Estado de presencia								
Estado por usuario	9	9	9	9	9	9	9	9
Anuncios grabados de buzón de voz por estado de presencia	1	1	1	1	1	1	1	1
Favoritos								
Favoritos por usuario	100	100	100	100	100	100	100	100
Grupos de Favoritos por usuario	10	10	10	10	10	10	10	10
Diario de llamadas								
Registros del diario de llamadas por usuario	100	100	100	100	100	100	100	100
Conferencia gestionada de UC Smart (mediante cliente de UC)								
Número de conferencias gestionadas	5	5	5	5	5	5	5	5
Número de usuarios por conferencia gestionada	16	16	16	16	16	16	16	16
Canales para conferencias gestionadas	30	30	30	30	30	30	30	30

[39] Los valores están escalonados según la versión del módulo: básica o avanzada

Tabla 47: Nivel de ampliación de UC Smart con OpenScape Business S

	Servidor básico (S)	Servidor estándar (S)	Servidor avanzado (S)
Máximo de usuarios de UC Smart			
Número máx. de usuarios (cuentas) de UC Smart	50	500	1500
Clientes de UC Smart			
Número de clientes de UC activos simultáneamente[36]	50	500	1500
myPortal @work	50	250	500
myPortal to go[37]	50	250	500
myPortal for Teams	50	250	500
DeskPhone CP 400/600/600E/ 700/700X/710 (Modo UC)	50	250	500
OpenScape Business Attendant	8	8	8
Estado de presencia			
Estado por usuario	9	9	9
Anuncios grabados de buzón de voz por estado de presencia	1	1	1
Favoritos			
Favoritos por usuario	100	100	100
Grupos de Favoritos por usuario	10	10	10
Diario de llamadas			
Registros del diario de llamadas por usuario	100	100	100
Conferencia gestionada de UC Smart (mediante cliente de UC)			
Número de conferencias gestionadas	10	10	10
Número de usuarios por conferencia gestionada	16	16	16
Canales para conferencias gestionadas	30	30	30

27.4.4 Niveles de ampliación de Smart Voicemail

- Los niveles de ampliación con placas base OCC V2 se pueden encontrar en Tabla 48: Nivel de ampliación de Smart Voicemail con placas base OCCx en la página 1480
- Los niveles de ampliación con placas base OCC V3 se pueden encontrar en Tabla 49: Nivel de ampliación de Smart Voicemail con placas base OCCSB/ R, OCCMA/B u OCCLA en la página 1480

- Los niveles de ampliación con sistemas OpenScape Business S Server se pueden encontrar en Tabla 50: Nivel de ampliación de Smart Voicemail con OpenScape Business S en la página 1481

Tabla 48: Nivel de ampliación de Smart Voicemail con placas base OCCx

	X1	X3W/R	X5W/R	X8	Servidor (S)
Smart Voicemail					
Buzones de voz de Smart Voicemail	30	320	320	320	1500
Mensajes por buzón de voz	100	100	100	100	100
Tiempo de grabación por llamada (minutos)	2	2	2	2	2
Capacidad de grabación total en horas	32	32	32	32	32
Conexiones de buzón de voz simultáneas (canales)	10	10	10	10	60
Anuncios	16	16	16	16	16
Puestos de operadora automáticos de la empresa	100	100	100	100	100
Puestos de operadora automáticos de la empresa (activos simultáneamente)	6	6	6	6	6

Tabla 49: Nivel de ampliación de Smart Voicemail con placas base OCCSB/R, OCCMA/B u OCCLA

	X1W/R		X3W/R	X5W/R		X8		
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Smart Voicemail								
Buzones de voz de Smart Voicemail	320	320	320/ 500[40]	320/ 500[40]	320/ 500[40]	320/ 500[40]	500	500
Mensajes por buzón de voz	100	100	100	100	100	100	100	100
Tiempo de grabación por llamada (minutos)	2	4	4	4	4	4	4	4
Capacidad de grabación total en horas	32	64	32	64	32	64	32	64
Conexiones de buzón de voz simultáneas (canales)	30	30	30	30	30	30	30	30
Anuncios	16	16	16	16	16	16	16	16

	X1W/R		X3W/R	X5W/R		X8		
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Puestos de operadora automáticos de la empresa	100	100	100	100	100	100	100	100
Puestos de operadora automáticos de la empresa (activos simultáneamente)	6	6	6	6	6	6	6	6

Tabla 50: Nivel de ampliación de Smart Voicemail con OpenScape Business S

	Servidor básico (S)	Servidor estándar (S)	Servidor avanzado (S)
Smart Voicemail			
Buzones de voz de Smart Voicemail	1500	1500	1500
Mensajes por buzón de voz	100	100	100
Tiempo de grabación por llamada (minutos)	4	4	4
Capacidad de grabación total en horas	64	64	64
Conexiones de buzón de voz simultáneas (canales)	60	60	60
Anuncios	16	16	16
Puestos de operadora automáticos de la empresa	100	100	100
Puestos de operadora automáticos de la empresa (activos simultáneamente)	6	6	6

27.4.5 Niveles de ampliación de UC Suite

- Los niveles de ampliación con placas base OCC V2 se pueden encontrar en Tabla 51: Nivel de ampliación de UC Suite con placas base V2 en la página 1482
- Los niveles de ampliación con placas base OCC V3 se pueden encontrar en Tabla 52: Nivel de ampliación de UC Suite con placas base OCCSB, OCCMA/B u OCCLA en la página 1485
- Los niveles de ampliación con sistemas OpenScape Business S Server se pueden encontrar en Tabla 53: Nivel de ampliación de UC Suite con OpenScape Business S en la página 1488

[40] Los valores están escalonados según la versión del módulo: básica o avanzada

Tabla 51: Nivel de ampliación de UC Suite con placas base V2

	X1	X3W/R	X5W/R	X8	Servidor (S)
Máximo de usuarios de UC Suite					
Número máx. de usuarios (cuentas) de UC Suite	-	250/ 150/ 0[41]	250/ 150/ 0[41]	250/ 150/ 0[41]	1500
Clientes de UC Suite					
Número de clientes de UC activos simultáneamente[42]	-	500/ 150/ 0[41]	500/ 150/ 0[41]	500/ 150/ 0[41]	1500
myPortal for Desktop	-	500/ 150/ 0[41]	500/ 150/ 0[41]	500/ 150/ 0[41]	1500
myPortal for Outlook	-	500/ 150/ 0[41]	500/ 150/ 0[41]	500/ 150/ 0[41]	1500
myAgent (activos simultáneamente)	-	64	64	64	64
myAgent (configurables)	-	192	192	192	192
myReports	-	1	1	1	1
myAttendant	-	20	20	20	20
myPortal @work	-	250/ 150/ 0[41]	250/ 150/ 0[41]	250/ 150/ 0[41]	250
myPortal @work Llamadas paralelas de VoIP a otros usuarios llamados[44]	-	30	30	30	60
myPortal to go[44]	-	150/ 150/ 0[41]	150/ 150/ 0[41]	150/ 150/ 0[41]	250
Deskphone 400/600/600E/700/700X/710	-	250/ 150/ 0[41]	250/ 150/ 0[41]	250/ 150/ 0[41]	250
OpenScape Business Attendant	-	8	8	8	8
Estado de presencia					
Estado por extensión de UC Suite	-	9	9	9	9
Anuncios grabados de buzón de voz por estado de presencia	-	1	1	1	1
Diario de llamadas (myPortal for Desktop y myPortal for Outlook)					
Tiempo de archivado en los clientes de UC (días)	-	30 estándar = 30	30 estándar = 30	30 estándar = 30	30 estándar = 30
Tiempo de archivado en el sistema de comunicación	-	365 estándar = 30	365 estándar = 30	365 estándar = 30	365 estándar = 30
Registros del diario de llamadas[46]	-	Sin restricciones[46]	Sin restricciones[46]	Sin restricciones[46]	Sin restricciones[46]

	X1	X3W/R	X5W/R	X8	Servidor (S)
Registros del diario de llamadas myPortal for Desktop con GUI moderna	-	100 después del reinicio > 100 durante el funcionamiento	100 después del reinicio > 100 durante el funcionamiento	100 después del reinicio > 100 durante el funcionamiento	100 después del reinicio > 100 durante el funcionamiento
Buzón de voz de UC Suite					
Buzones de voz	-	500/ 500/ 0[45]	500/ 500/ 0[45]	500/ 500/ 0[45]	1500
Grupos de buzón de voz	-	20/ 20/ 0	20/ 20/ 0	20/ 20/ 0	20
Mensajes por buzón de voz[46]	-	n/d	n/d	n/d	n/d
Duración de grabación por llamada (minutos)	-	15	15	15	15
Duración de la grabación que puede transferirse por correo electrónico (minutos)[47]	-	~10	~10	~10	~10
Capacidad de grabación total (en horas)[46]	-	n/d	n/d	n/d	n/d
Conexiones simultáneas con el buzón de voz (canales MEB)	-	30	30	30	60
AutoAttendant de UC Suite					
Puesto de operadora automático personal	-	20/ 20/ 0[41]	20/ 20/ 0[41]	20/ 20/ 0[41]	20
Puesto de operadora automático de la empresa	-	1/ 1/ 0[41]	1/ 1/ 0[41]	1/ 1/ 0[41]	1
Chat entre varios usuarios (Mensajería instantánea)					
Interlocutores de comunicación internos	-	sin restricciones	sin restricciones	sin restricciones	sin restricciones
Interlocutor externo (XMPP)	-	-	-	-	-
Anuncios grabados por usuario de UC Suite					
Anuncios de bienvenida	-	1/ 1/ 0[41]	1/ 1/ 0[41]	1/ 1/ 0[41]	1
Anuncio grabado relativo a presencia	-	1/ 1/ 0[41]	1/ 1/ 0[41]	1/ 1/ 0[41]	1
Anuncio grabado para el puesto de operadora automático personal	-	1/ 1/ 0[41]	1/ 1/ 0[41]	1/ 1/ 0[41]	1
Grabación de llamada de UC Suite					
Duración de la grabación por llamada/conferencia	-	Limitada por la duración de la llamada	Limitada por la duración de la llamada	Limitada por la duración de la llamada	Limitada por la duración de la llamada
Fax de UC Suite					

	X1	X3W/R	X5W/R	X8	Servidor (S)
Buzones de fax	-	500/ 150/ 0[41]	500/ 150/ 0[41]	500/ 150/ 0[41]	1500
Grupos de buzón de fax	-	60/ 60/ 0[41]	60/ 60/ 0[41]	60/ 60/ 0[41]	60
Extensiones por grupo de buzón de fax	-	10/ 10/ 0[41]	10/ 10/ 0[41]	10/ 10/ 0[41]	10
Extensión del fax en páginas	-	500/ 500/ 0[41]	500/ 500/ 0[41]	500/ 500/ 0[41]	500
Faxes T.38 simultáneos	-	8/ 3/ 0[41]	8/ 3/ 0[41]	8/ 3/ 0[41]	8
Destinatarios de fax de serie	-	sin restricciones	sin restricciones	sin restricciones	sin restricciones
Conferencias de UC Suite					
Conferencias simultáneas de UC Suite	-	5/ 5/ 0[41]	5/ 5/ 0[41]	5/ 5/ 0[41]	10
Participantes por conferencia de UC Suite	-	16/ 16/ 0[41]	16/ 16/ 0[41]	16/ 16/ 0[41]	16
Participantes externos por conferencia de UC Suite	-	15/ 15/ 0[41]	15/ 15/ 0[41]	15/ 15/ 0[41]	15
Número máx. de canales para conferencias de UC Suite	-	30/ 30/ 0[41]	30/ 30/ 0[41]	30/ 30/ 0[41]	60
Número de canales reservados para conferencias Ad Hoc y Meet Me de UC Suite	-	20/ 20/ 0[41]	20/ 20/ 0[41]	20/ 20/ 0[41]	60
Conexión de base de datos externa (LDAP)					
Conexiones de base de datos externa del servidor UC	-	10/ 10/ 0[41]	10/ 10/ 0[41]	10/ 10/ 0[41]	10

41 Los valores están escalonados según la configuración de UC Booster: Booster Server / Booster Card / sin UC Booster

42 Total de: myPortal for Desktop, myPortal for Outlook, myAttendant, myAgent, myReports, myPortal @work, myPortal to go, myPortal for Teams, CP 400/600/600E/700/700X/710 UC modo UC (Contexto: varios clientes con la misma cuenta de UC Suite pueden iniciar sesión en el sistema)

43 El valor más bajo aplica para sistemas con UC Suite Contact Center

44 El número de conexiones simultáneas de VoIP de las extensiones depende de

1) los canales DSP disponibles en el sistema para llamadas de gateway (transiciones IP/TDM).

2) Los canales proxy RTP internos disponibles en el sistema para las llamadas a través de VOIP por Internet.

45 La UC Booster Card admite un máximo de 500 buzones de voz, independientemente del límite del cliente de UC Suite (150 usuarios).

46 El valor depende de la capacidad de memoria disponible del hardware/SSD. No se implementa una limitación relacionada con la extensión.

1) Buzón de voz/grabaciones: Un minuto de grabación utiliza alrededor de 1 MB de memoria

2) Fax: Un fax normal (2 páginas DIN A4) corresponde aprox. a 48 KB de memoria

Tabla 52: Nivel de ampliación de UC Suite con placas base OCCSB, OCCMA/B u OCCLA

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Máximo de usuarios de UC Suite						
Número máx. de usuarios (cuentas) de UC Suite	-	50/ 500[48] 300 en caso de Contact Center	-	50/ 500[48]	-	500 300 en caso de Contact Center
Clientes de UC Suite						
Número de clientes de UC activos simultáneamente[42]	-	100/ 1000[48] 600 en caso de Contact Center	-	100/ 1000[48] 600 en caso de Contact Center	-	1000 600 en caso de Contact Center
myPortal for Desktop	-	50/ 500[48] 300 en caso de Contact Center	-	50/ 500[48] 300 en caso de Contact Center	-	500 300 en caso de Contact Center
myPortal for Outlook	-	50/ 500[48] 300 en caso de Contact Center	-	50/ 500[48] 300 en caso de Contact Center	-	500 300 en caso de Contact Center
myAgent (activos simultáneamente)	-	0/ 64[48]	-	0/ 64[48]	-	64
myAgent (configurables)	-	0/ 192[48]	-	0/ 192[48]	-	192
myReports	-	0/ 1[48]	-	0/ 1[48]	-	1
myAttendant	-	4/ 20[48]	-	4/ 20[48]	-	20
myPortal @work	-	50/ 250[48] 300 en caso de Contact Center	-	50/ 250[48] 300 en caso de Contact Center	-	250 300 en caso de Contact Center
myPortal @work Llamadas paralelas de VoIP a otros usuarios llamados[44]	-	30/ 70[48]	-	30/ 70[48]	-	69

Ejemplo: El volumen de memoria de la partición para grabar anuncios de voz, mensajes de voz, grabaciones de voz y faxes es de 20 GB para un disco duro de 160 GB. Esto se corresponde con una duración total de grabaciones de 20 000 minutos.

47 En el caso de grabaciones más largas, la grabación se divide y se envía en varios archivos.

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
myPortal to go[44]	-	50/ 500[48] 300 en caso de Contact Center	-	50/ 500[48] 300 en caso de Contact Center	-	500 300 en caso de Contact Center
myPortal para Teams	-	50/ 500[48] 300 en caso de Contact Center	-	50/ 500[48] 300 en caso de Contact Center	-	500 300 en caso de Contact Center
DeskPhone CP 400/600/600E/ 700/700X/710	-	50/ 500[48] 300 en caso de Contact Center	-	50/ 500[48] 300 en caso de Contact Center	-	500 300 en caso de Contact Center
OpenScape Business Attendant	-	8	-	8	-	8
Estado de presencia						
Estado por extensión de UC Suite	-	9	-	9	-	9
Anuncios grabados de buzón de voz por estado de presencia	-	1	-	1	-	1
Diario de llamadas (myPortal for Desktop y myPortal for Outlook)						
Tiempo de archivado en los clientes de UC (días)	-	30 estándar = 30	-	30 estándar = 30	-	30 estándar = 30
Tiempo de archivado en el sistema de comunicación	-	365 estándar = 30	-	365 estándar = 30	-	365 estándar = 30
Registros del diario de llamadas[46]	-	Sin restricciones[46]	-	Sin restricciones[46]	-	Sin restricciones[46]
Registros del diario de llamadas myPortal for Desktop con GUI moderna	-	100 después del reinicio > 100 durante el funcionamiento	-	100 después del reinicio > 100 durante el funcionamiento	-	100 después del reinicio > 100 durante el funcionamiento
Buzón de voz de UC Suite						
Buzones de voz	-	50/ 500[48]	-	50/ 500[48]	-	500
Grupos de buzón de voz	-	32	-	32	-	32
Mensajes por buzón de voz[46]	-	n/d	-	n/d	-	n/d
Duración de grabación por llamada (minutos)	-	15	-	15	-	15

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Duración de la grabación que puede transferirse por correo electrónico (minutos)[47]	-	~10	-	~10	-	~10
Capacidad de grabación total (en horas)[46]	-	n/d	-	n/d	-	n/d
Conexiones simultáneas con el buzón de voz (canales MEB)	-	30/ 60[48]	-	30/ 60[48]	-	60
AutoAttendant de UC Suite						
Puesto de operadora automático personal	-	20	-	20	-	20
Puesto de operadora automático de la empresa	-	1	-	1	-	1
Chat entre varios usuarios (Mensajería instantánea)						
Interlocutores de comunicación internos	-	sin restricciones	-	sin restricciones	-	sin restricciones
Anuncios grabados por usuario de UC Suite						
Anuncios de bienvenida	-	1	-	1	-	1
Anuncio grabado relativo a presencia	-	1	-	1	-	1
Anuncio grabado para el puesto de operadora automático personal	-	1	-	1	-	1
Grabación de llamada de UC Suite						
Duración de la grabación por llamada/ conferencia	-	Limitada por la duración de la llamada	-	Limitada por la duración de la llamada	-	Limitada por la duración de la llamada
Fax de UC Suite						
Buzones de fax	-	50/ 500[48]	-	50/ 500[48]	-	500
Grupos de buzón de fax	-	60	-	60	-	60
Extensiones por grupo de buzón de fax	-	10	-	10	-	10
Extensión del fax en páginas	-	500	-	500	-	500
Faxes T.38 simultáneos	-	3/ 8[48]	-	3/ 8[48]	-	8
Destinatarios de fax de serie	-	sin restricciones	-	sin restricciones	-	sin restricciones
Conferencias de UC Suite						

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Conferencias simultáneas de UC Suite	-	5	-	5	-	5
Participantes por conferencia de UC Suite	-	16	-	16	-	16
Participantes externos por conferencia de UC Suite	-	15	-	15	-	15
Número máx. de canales para conferencias de UC Suite	-	30	-	30	-	30
Número de canales reservados para conferencias Ad Hoc y Meet Me de UC Suite	-	20	-	20	-	20
Conexión de base de datos externa (LDAP)						
Conexiones de base de datos externa del servidor UC	-	10	-	10	-	10

Tabla 53: Nivel de ampliación de UC Suite con OpenScape Business S

	Servidor básico (S)	Servidor estándar (S)	Servidor avanzado (S)
Máximo de usuarios de UC Suite			
Número máx. de usuarios (cuentas) de UC Suite	150	500	1500
Clientes de UC Suite			
Número de clientes de UC activos simultáneamente[42]	150	500	1500
myPortal for Desktop	50	500	1500
myPortal for Outlook	50	500	1500
myAgent (activos simultáneamente)	0	64	64
myAgent (configurables)	0	192	192
myReports	1	1	1
myAttendant	20	20	20

[48] Los valores están escalonados según la versión del módulo: básica o avanzada

	Servidor básico (S)	Servidor estándar (S)	Servidor avanzado (S)
myPortal @work	50	250	500
myPortal @work Llamadas paralelas de VoIP a otros usuarios llamados[44]	30	60	60
myPortal to go[44]	50	250	500
myPortal para Teams	50	250	500
DeskPhone CP 400/600/600E/ 700/700X/710	50	250	500
OpenScape Business Attendant	8	8	8
Estado de presencia			
Estado por extensión de UC Suite	9	9	9
Anuncios grabados de buzón de voz por estado de presencia	1	1	1
Diario de llamadas (myPortal for Desktop y myPortal for Outlook)			
Tiempo de archivado en los clientes de UC (días)	30 estándar = 30	30 estándar = 30	30 estándar = 30
Tiempo de archivado en el sistema de comunicación	365 estándar = 30	365 estándar = 30	365 estándar = 30
Registros del diario de llamadas[46]	Sin restricciones[46]	Sin restricciones[46]	Sin restricciones[46]
Registros del diario de llamadas myPortal for Desktop con GUI moderna	100 después del reinicio > 100 durante el funcionamiento	100 después del reinicio > 100 durante el funcionamiento	100 después del reinicio > 100 durante el funcionamiento
Buzón de voz de UC Suite			
Buzones de voz	150	500	1500
Grupos de buzón de voz	32	32	32
Mensajes por buzón de voz[46]	n/d	n/d	n/d
Duración de grabación por llamada (minutos)	15	15	15
Duración de la grabación que puede transferirse por correo electrónico (minutos)[47]	~10	~10	~10
Capacidad de grabación total (en horas)[46]	n/d	n/d	n/d
Conexiones simultáneas con el buzón de voz (canales MEB)	60	60	60

	Servidor básico (S)	Servidor estándar (S)	Servidor avanzado (S)
AutoAttendant de UC Suite			
Puesto de operadora automático personal	20	20	20
Puesto de operadora automático de la empresa	1	1	1
Chat entre varios usuarios (Mensajería instantánea)			
Interlocutores de comunicación internos	sin restricciones	sin restricciones	sin restricciones
Anuncios grabados por usuario de UC Suite			
Anuncios de bienvenida	1	1	1
Anuncio grabado relativo a presencia	1	1	1
Anuncio grabado para el puesto de operadora automático personal	1	1	1
Grabación de llamada de UC Suite			
Duración de la grabación por llamada/ conferencia	Limitada por la duración de la llamada	Limitada por la duración de la llamada	Limitada por la duración de la llamada
Fax de UC Suite			
Buzones de fax	1500	1500	1500
Grupos de buzón de fax	60	60	60
Extensiones por grupo de buzón de fax	10	10	10
Extensión del fax en páginas	500	500	500
Faxes T.38 simultáneos	8	8	8
Destinatarios de fax de serie	sin restricciones	sin restricciones	sin restricciones
Conferencias de UC Suite			
Conferencias simultáneas de UC Suite	10	10	10
Participantes por conferencia de UC Suite	16	16	16
Participantes externos por conferencia de UC Suite	15	15	15
Número máx. de canales para conferencias de UC Suite	60	60	60
Número de canales reservados para conferencias Ad Hoc y Meet Me de UC Suite	60	60	60
Conexión de base de datos externa (LDAP)			
Conexiones de base de datos externa del servidor UC	10	10	10

27.4.6 Funciones del teléfono

	X1W/R	X3W/R	X5W/R	X8W/R	Servidor (S)
Lista de llamantes para teléfonos del sistema (HFA)					
Listas de llamantes por sistema	650	650	650	650	1300
Lisas de llamantes por extensión del sistema	1	1	1	1	1
Registros por lista de llamantes	10	10	10	10	10
Cifras guardadas por entrada más código de ocupación	25 + (6)	25 + (6)	25 + (6)	25 + (6)	25 + (6)
Teclas de llamada directa (teclas DSS)					
Aparatos auxiliares por sistema de comunicación	250	250	250	250	250
Aparatos auxiliares por teléfono	2	2	2	2	2
Teclas por OpenStage Key Module	12	12	12	12	12
Teclas por OpenStage Key Module 15	18	18	18	18	18
Paneles de lámparas de ocupado (BLF) por sistema de comunicación	12	25	25	25	25
Teclas por panel de lámparas de ocupado	90	90	90	90	90
Marcación abreviada individual (KWI)					
Entradas en el pool de marcación abreviada individual por sistema de comunicación	2000	2000	2000	2000	2000
Entradas por extensión	10	10	10	10	10
Cifras por entrada (más código de ocupación)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Marcación abreviada central (KWZ)					
Entradas en el pool de marcación abreviada individual por sistema de comunicación	8000	8000	8000	8000	8000
Número de caracteres del nombre	16	16	16	16	16
Cifras por entrada (más código de ocupación)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)

	X1W/R	X3W/R	X5W/R	X8W/R	Servidor (S)
Rellamada					
Entradas por OpenStage 20/ 20E/ 20G/ 40/ 40G	3	3	3	3	3
Entradas por OpenStage 15	10	10	10	10	10
Entradas por OpenStage 60/ 60G/ 80/ 80G	30	30	30	30	30
Entradas por teléfono sin pantalla	1	1	1	1	1
Cifras guardadas por entrada	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Aviso de llamada/Tonos de llamada en espera					
Llamantes en espera por teléfono	16				
Aparcamiento					
Posiciones de aparcamiento por sistema	10				
Llamadas de devolución de llamada					
Entradas de devolución de llamada por teléfono	5				
Mensajes por ausencia/Mensajes de texto					
Mensajes por ausencia por sistema	250	250	250	250	250
Mensajes de texto por sistema	150	150	150	150	150
Mensajes por ausencia configurables + Mensajes de texto por sistema	10 + 10	10 + 10	10 + 10	10 + 10	10 + 10
Número de caracteres de un mensaje por ausencia/ mensaje de texto configurable	24	24	24	24	24
Mensajes por ausencia/ Mensajes de texto recibidos por teléfono con pantalla	5	5	5	5	5
Mensajes por ausencia recibidos/Mensajes de texto por teléfono sin pantalla	1	1	1	1	1
Timbre adicional act.					
Exts.con señal.timbre	5				
Desvío de llamadas (AUL)					
Destinos de desvío por teléfono	4	4	4	4	4

	X1W/R	X3W/R	X5W/R	X8W/R	Servidor (S)
Cifras por destino de desvío externo (más código de ocupación)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Destinos de desvío encadenados					5
Conferencias controladas por sistema					
Conferencias de sistema simultáneas por sistema	10	10	10	10	8
Extensiones por conferencia	8	8	8	8	8
Extensiones internas por conferencia	7	7	7	7	7
Canales de conferencia	32	32	32	32	20
Portero eléctrico/Abrepuertas					
Conexiones mediante interfaces a/b por sistema	4	4	4	4	-
Cifras por entrada de código	5	5	5	5	-
Reserva de línea					
Entradas simultáneas por sistema	32	32	32	32	-

Nota: Para todos los escenarios de desvío de llamadas anteriores, solo puede indicarse un destino de transferencia automática diferida por MSN. Se pueden transferir 10 MSN como máximo.

En caso de que ITSP o RDSI estén configurados con marcación directa, este número es 249.

27.4.7 Trabajar en equipo (Grupos)

- Se puede encontrar información sobre las placas base OCC V2 en Tabla 54: Datos para placas base V2 en la página 1493
- Se puede encontrar información sobre las placas base OCC V3 en Tabla 55: Datos para placas base V3 en la página 1495
- Se puede encontrar información sobre los sistemas OpenScape Business S Server en Tabla 56: Datos para OpenScape Business S en la página 1497

Tabla 54: Datos para placas base V2

	X1	X3W/R	X5W/R	X8
Grupos de telecaptura				
Grupos de telecaptura por sistema	32	32	32	32
Extensiones por grupo de telecaptura	32	32	32	32

	X1	X3W/R	X5W/R	X8
Timbre adicional (grupo configurable por el usuario)				
Número de extensiones en un grupo de timbre adicional	5	5	5	5
Llamadas de grupo, líneas colectivas, MULAP básicos				
Número total de llamadas de grupo, líneas colectivas, MULAP básicos, MULAP Jefe y grupos de buzón de voz por sistema de comunicación	800	800	800	800
Longitud de nombre de grupo	16	16	16	16
Número de grupos a los que se puede asignar un usuario	32	32	32	32
Extensiones por llamada de grupo, Línea colectiva, MULAP básico	20	20	20	20
MULAP Jefe, grupos Team, grupos Top y grupos de buzón de voz:				
Número total de MULAP Jefe, grupos Team y Top por	500	500	500	500
Extensiones por MULAP Jefe, Grupo Team, Grupo Top	10	10	10	10
Teclas MULAP por teléfono	10	10	10	10
Grupos de buzón de voz				
Número de grupos de buzón de voz	20	20	20	20
Extensiones por grupo de buzón de voz	20	20	20	20
Mensaje a grupo (Mensaje por voz)				
Mensajes simultáneos por sistema de comunicación	1	1	1	1
Destinatarios del mensaje	20	20	20	20
Grupos UCD				
Grupos UCD por sistema	60	60	60	60
Anuncios grabados por grupo UCD	7	7	7	7
Niveles de prioridad por grupo UCD	10	10	10	10
Llamadas en espera por grupo UCD (máx. de último grupo: 72)	30	30	30	30
Agentes UCD				
ID de agentes UCD por sistema de comunicación	330	330	330	330
Agentes activos simultáneamente por sistema de comunicación	64	64	64	64
Anuncios grabados de UCD				

	X1	X3W/R	X5W/R	X8
Llamantes por sistema de comunicación a los que se puede reproducir, de forma simultánea, un anuncio grabado	8	8	8	8

Tabla 55: Datos para placas base V3

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Grupos de telecaptura								
Grupos de telecaptura por sistema	64	64	64/128[49]	64/128[49]	64/128[49]	64/128[49]	128	128
Extensiones por grupo de telecaptura	32	32	32	32	32	32	32	32
Timbre adicional (grupo configurable por el usuario)								
Número de extensiones en un grupo de timbre adicional	5	5	5	5	5	5	5	5
Llamadas de grupo, líneas colectivas, MULAP básicos								
Número total de llamadas de grupo, líneas colectivas, MULAP básicos, MULAP Jefe y grupos de buzón de voz por sistema de comunicación	800	800	800	800	800	800	800	800
Longitud de nombre de grupo	16	16	16	16	16	16	16	16
Número de grupos a los que se puede asignar un usuario	32	32	32	32	32	32	32	32
Extensiones por llamada de grupo, Línea colectiva, MULAP básico	20	20	20/32[49]	20/32[49]	20/32[49]	20/32[49]	32	32
MULAP Jefe, grupos Team, grupos Top y grupos de buzón de voz:								
Número total de MULAP Jefe, grupos Team y Top por	500	500	500	500	500	500	500	500
Extensiones por MULAP Jefe, Grupo Team, Grupo Top	10	10	10	10	10	10	10	10

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Teclas MULAP por teléfono	10	10	10	10	10	10	10	10
Grupos de buzón de voz								
Número de grupos de buzón de voz	20	20	20	20	20	20	20	20
Extensiones por grupo de buzón de voz	20	20	20	20	20	20	20	20
Mensaje a grupo (Mensaje por voz)								
Mensajes simultáneos por sistema de comunicación	1	1	1	1	1	1	1	1
Destinatarios del mensaje	20	20	20/32[49]	20/32[49]	20/32[49]	20/32[49]	32	32
Grupos UCD								
Grupos UCD por sistema	60	60	60	60	60	60	60	60
Anuncios grabados por grupo UCD	7	7	7	7	7	7	7	7
Niveles de prioridad por grupo UCD	10	10	10	10	10	10	10	10
Llamadas en espera por grupo UCD (máx. de último grupo: 72)	30	30	30	30	30	30	30	30
Agentes UCD								
ID de agentes UCD por sistema de comunicación	330	330	330	330	330	330	330	330
Agentes activos simultáneamente por sistema de comunicación	64	64	64	64	64	64	64	64
Anuncios grabados de UCD								
Llamantes por sistema de comunicación a los que se puede reproducir, de forma simultánea, un anuncio grabado	8	8	8	8	8	8	8	8

Tabla 56: Datos para OpenScape Business S

	Servidor básico (S)	Servidor estándar (S)	Servidor avanzado (S)
Grupos de telecaptura			
Grupos de telecaptura por sistema	32	64	128
Extensiones por grupo de telecaptura	32	32	32
Timbre adicional (grupo configurable por el usuario)			
Número de extensiones en un grupo de timbre adicional	5	5	5
Llamadas de grupo, líneas colectivas, MULAP básicos			
Número total de llamadas de grupo, líneas colectivas, MULAP básicos, MULAP Jefe y grupos de buzón de voz por sistema de comunicación	800	800	800
Longitud de nombre de grupo	16	16	16
Número de grupos a los que se puede asignar un usuario	32	32	32
Extensiones por llamada de grupo, Línea colectiva, MULAP básico	32	32	32
MULAP Jefe, grupos Team, grupos Top y grupos de buzón de voz:			
Número total de MULAP Jefe, grupos Team y Top por	500	500	500
Extensiones por MULAP Jefe, Grupo Team, Grupo Top	10	10	10
Teclas MULAP por teléfono	10	10	10
Grupos de buzón de voz			
Número de grupos de buzón de voz	20	20	20
Extensiones por grupo de buzón de voz	20	20	20
Mensaje a grupo (Mensaje por voz)			
Mensajes simultáneos por sistema de comunicación	1	1	1
Destinatarios del mensaje	20	20	20
Grupos UCD			
Grupos UCD por sistema	60	60	60
Anuncios grabados por grupo UCD	7	7	7
Niveles de prioridad por grupo UCD	10	10	10
Llamadas en espera por grupo UCD (máx. de último grupo: 72)	30	30	30

[49] Los valores están escalonados según la versión del módulo: básica o avanzada

	Servidor básico (S)	Servidor estándar (S)	Servidor avanzado (S)
Agentes UCD			
ID de agentes UCD por sistema de comunicación	330	330	330
Agentes activos simultáneamente por sistema de comunicación	64	64	64
Anuncios grabados de UCD			
Llamantes por sistema de comunicación a los que se puede reproducir, de forma simultánea, un anuncio grabado	8	8	8

27.4.8 Encaminamiento de llamadas

	X1W/R	X3W/R	X5W/R	X8	Servidor (S)
Ruta más económica (LCR)					
Cifras marcadas	24	24	24	24	24
Cifras comprobadas	24	24	24	24	24
Plan de marcación (máx. 10 campos por plan)	1000	1000	1000	1000	1000
Tablas de rutas	254	254	254	254	254
Rutas por tabla de rutas	16	16	16	16	16
Reglas de marcación por dirección	254	254	254	254	254
Número de zonas horarias por día/semana	8	8	8	8	8
Cifras por regla de marcación	40	40	40	40	40
Servicio nocturno					
Extensiones autorizadas por sistema	5	5	5	5	5
Servicio de emergencia E911 (solo para EE. UU)					
Cifras por LIN (Location Identification Number)	16	16	16	16	16
Llamada de socorro/Hotline					
Destinos de hotline por sistema de comunicación	6	6	6	6	6
Grupos VBZ					
Grupos VBZ por sistema	64	64	64	64	64

Asistentes para placas base V2

	X1	X3W/R	X5W/R	X8	Servidor (S)
myAttendant					
myAttendant (UC Suite) por sistema	-	20	20	20	20
AutoAttendant (UC Smart)					
Company AutoAttendant	100	100	100	100	100
AutoAttendant (UC suite)					
Puesto de operadora automático	-	20/ 20/ 0[50]	20/ 20/ 0[50]	20/ 20/ 0[50]	20
OpenScape Business Attendant					
OpenScape Business Attendants por sistema	-	8	8	8	8

Asistentes para placas base V3

	X1W/R	X3W/R	X5W/R	X8	Servidor (S)
myAttendant					
myAttendant (UC Suite) por sistema	4	4/20[51]	4/20[51]	20	20
AutoAttendant (UC Smart)					
Company AutoAttendant	100	100	100	100	100
AutoAttendant (UC suite)					
Puesto de operadora automático	20	20/ 20/[51]	20/ 20[51]	20/ 20[51]	20
OpenScape Business Attendant					
OpenScape Business Attendants por sistema	8	8	8	8	8

27.4.9 Multimedia Contact Center

	X1W/R	X3W/R	X5W/R	X8	Servidor (S)
Colas de centro de contactos					
Colas de espera por sistema de comunicación	-	50	50	50	50
Resumen					

50 Los valores están escalonados según la configuración de UC Booster: Booster Server / Booster Card / sin UC Booster. Para las placas base V3, es válido el valor más alto.

51 Los valores están escalonados según la versión del módulo: básica o avanzada

	X1W/R	X3W/R	X5W/R	X8	Servidor (S)
Códigos de tratamiento posterior	-	sin restricciones	sin restricciones	sin restricciones	sin restricciones
Agentes					
Agentes (activos simultáneamente)	-	64	64	64	64
Agentes (configurables)	-	192	192	192	192
Informes de historial					
Clientes myReports activos simultáneamente por sistema	-	1	1	1	1

27.4.10 Límites de expansión de Mobility

Tabla 57: Datos para placas base OCC V2

	X1	X3W/R	X5W/R	X8
Puestos de trabajo por teletrabajador				
Puestos de trabajo de teletrabajador a través de VPN por sistema de comunicación	10	10	10	10
Extensiones Mobility				
Extensiones Mobility Entry por sistema	30	150	150	150
myPortal to go (UC Smart): extensiones por sistema	30	150/ 150/ 50[52]	150/ 150/ 50[52]	150/ 150/ 50[52]
myPortal to go (UC Suite): extensiones por sistema	-	150/ 150/ 0[52]	150/ 150/ 0[52]	150/ 150/ 0[52]

Tabla 58: Datos para placas base OCC V3

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Puestos de trabajo por teletrabajador								
Puestos de trabajo de teletrabajador a través de VPN por sistema de comunicación	10	10	10	10	10	10	10	10
Extensiones Mobility								

[52] Los valores están escalonados según la configuración de UC Booster: Booster Server / Booster Card / sin UC Booster

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Extensiones Mobility Entry por sistema	150/ 500[53]	150/ 500[53]	150	150/ 500[53]	150/ 500[53]	150/ 500[53]	500	500
myPortal to go (UC Smart): extensiones por sistema	150	150	150/ 500[53]	150/ 500[53]	150/ 500[53]	150/ 500[53]	500	500
myPortal to go (UC Suite): extensiones por sistema	-	50	-	50/ 500 300 en caso de Contact Center	-	50/ 500 300 en caso de Contact Center	-	500 300 en caso de Contact Center
myPortal for Teams (UC Smart): extensiones por sistema	150	150	150/ 500[53]	150/ 500[53]	150/ 500[53]	150/ 500[53]	500	500
myPortal for Teams (UC Suite): extensiones por sistema	-	50	-	50/ 500 300 en caso de Contact Center	-	50/ 500 300 en caso de Contact Center	-	500 300 en caso de Contact Center

Tabla 59: Datos para OpenScape Business S

	Servidor básico (S)	Servidor estándar (S)	Servidor avanzado (S)
Extensiones Mobility			
Extensiones Mobility Entry por sistema	50	150	150
myPortal to go (UC Smart): extensiones por sistema	50	250	500
myPortal to go (UC Suite): extensiones por sistema	50	250	500
myPortal for Teams (UC Smart): extensiones por sistema	50	250	500
myPortal for Teams (UC Suite): extensiones por sistema	50	250	500

27.4.11 Seguridad

	X1W/R	X3W/R	X5W/R	X8	Servidor (S)
Candado telefónico individual					

[53] Los valores están escalonados según la versión del módulo: básica o avanzada

	X1W/R	X3W/R	X5W/R	X8	Servidor (S)
Cifras por candado telefónico	5	5	5	5	5
Caracteres permitidos	0 - 9	0 - 9	0 - 9	0 - 9	0 - 9
Acceso a la red urbana					
Número de listas de números autorizados	6	6	6	6	6
Número de listas de números prohibidos	6	6	6	6	6
Lista de números autorizados corta (10 entradas con 32 dígitos cada una)	5	5	5	5	5
Lista de números autorizados larga (100 entradas con 32 dígitos cada una)	1	1	1	1	1
Lista de números prohibidos corta (10 entradas con 32 dígitos cada una)	5	5	5	5	5
Lista de números prohibidos larga (50 entradas con 32 dígitos cada una)	1	1	1	1	1
Clases de servicio					
Clases de servicio por sistema	15	15	15	15	15
Tamaño de la matriz; día y noche; número de líneas	30	30	30	30	30
Listas de números prohibidos y autorizados	15	15	15	15	15
Grupos utilizados cerrados (grupos VBZ)					
Grupos VBZ por sistema	16	64	64	64	64
Tamaño de la matriz; día y noche; número de líneas	30	30	30	30	30
Listas de números prohibidos y autorizados	15	15	15	15	15

27.4.12 Interconexión de OpenScape Business

Interconexión OpenScape Business X1W/R, OpenScape Business X3R/X3W, OpenScape Business X5R/X5W, OpenScape Business X8, OpenScape Business S: Se pueden solicitar límites de ampliación para interconexiones

fuera de lo indicado a través de autorizaciones específicas de proyecto. Consulte la versión de distribución actual.

	X1W/R	X3W/R	X5W/R	X8	Servidor (S)
Interconexión de OpenScape Business					
Sistemas de comunicación interconectados (nodos)	8/ 32[54]	8/ 32[54]	8/ 32[54]	8/ 32[54]	8/ 32[54]
Extensiones en la red	1000	1000	1000	1000	1000

27.4.13 Application Connectivity

Tabla 60: Datos para placas base OCC V2

	X1	X3W/R	X5W/R	X8
Interfaz CSTA				
Enlaces CSTA mediante CSP por sistema	-	4/ 4/ 0[55]	4/ 4/ 0[55]	4/ 4/ 0[55]
Puntos de supervisión para líneas urbanas o extensiones	-	1500	1500	1500
TAPI 170 Middleware Server	-	4	4	4
Clientes TAPI 120 (CSTA)	-	150/ 150/ 0[55]	150/ 150/ 0[55]	150/ 150/ 0[55]
Interfaz Web Services (WSI)				
WSI: total de clientes activos simultáneamente	30	500/ 300/ 150[55]	500/ 300/ 150[55]	500/ 300/ 150[55]
myPortal @work	30	250/ 150/ 50[55]	250/ 150/ 50[55]	250/ 150/ 50[55]
myPortal to go	30	150/ 150/ 50[55]	150/ 150/ 50[55]	150/ 150/ 50[55]
DeskPhone CP 400/600/600E/ 700/700X/710 con WSI	30	150/ 150/ 50[55]	150/ 150/ 50[55]	150/ 150/ 50[55]
OpenScape Business Attendant	0	8/ 8/ 8[55]	8/ 8/ 8[55]	8/ 8/ 8[55]
OpenScape Business BLF	0	150/ 150/ 50[55]	150/ 150/ 50[55]	150/ 150/ 50[55]
Application Launcher	30	250/ 150/ 50[55]	250/ 150/ 50[55]	250/ 150/ 50[55]
TAPI 120 (modo WSI)	30	0/ 0/ 30[55]	0/ 0/ 30[55]	0/ 0/ 30[55]
Aplicación externa	rest	rest	rest	rest

54 Los valores están escalonados según: Red con UC Suite / Red sin UC Suite

55 Los valores están escalonados según la configuración de UC Booster: Booster Server / Booster Card / sin UC Booster

Tabla 61: Datos para placas base OCC V3

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Interfaz CSTA								
Enlaces CSTA mediante CSP por sistema	-	-	4	4	4	4	4	4
Puntos de supervisión para líneas urbanas o extensiones	1650	1650	1650/ 3750[56]	1650/ 3750[56]	1650/ 3750[56]	1650/ 3750[56]	3750	3750
TAPI 170 Middleware Server	4	4	4	4	4	4	4	4
Clientes TAPI 120 (CSTA)	150	150	150/ 500[56]	150/ 500[56]	150/ 500[56]	150/ 500[56]	500	500
Interfaz Web Services (WSI)								
WSI: total de clientes activos simultáneamente	150	300	150/ 500[56]	300/ 1000[56]	150/ 500[56]	300/ 1000[56]	1000	1000
myPortal @work	150	150	150/ 250[56]	150/ 250[56]	150/ 250[56]	150/ 250[56]	250	250
myPortal to go	150	150	150/ 500[56]	150/ 500[56]	150/ 500[56]	150/ 500[56]	500	500
myPortal for Teams	150	150	150/ 500[56]	150/ 500[56]	150/ 500[56]	150/ 500[56]	500	500
DeskPhone CP 400/600/600E/ 700/700X/710 con WSI	150	150	150/ 500[56]	150/ 500[56]	150/ 500[56]	150/ 500[56]	500	500
OpenScape Business Attendant	8	8	8	8	8	8	8	8
OpenScape Business BLF	150	150	150	150	150	150	150	150
Application Launcher	150	150	150/ 500[56]	150/ 500[56]	150/ 500[56]	150/ 500[56]	500	500
TAPI 120 (modo WSI)	**Nota:** Retirado en placas base OCC V3. Admitido solo en V3 para placas base V2.							
Aplicación externa	rest	rest	rest	rest	rest	rest	rest	rest

Tabla 62: Datos para OpenScape Business S

	Servidor básico (S)	Servidor estándar (S)	Servidor avanzado (S)
Interfaz CSTA			
Enlaces CSTA mediante CSP por sistema	4	4	4
Puntos de supervisión para líneas urbanas o extensiones	3750	3750	3750
TAPI 170 Middleware Server	4	4	4
Clientes TAPI 120 (CSTA)	50	500	1500
Interfaz Web Services (WSI)			
WSI: total de clientes activos simultáneamente	150	500	1500
myPortal @work	50	250	500
myPortal to go	50	250	500
myPortal for Teams	50	250	500
DeskPhone CP 400/600/600E/ 700/700X/710 con WSI	50	250	500
OpenScape Business Attendant	8	8	8
Application Launcher	50	250	500
TAPI 120 (modo WSI)	0	0	0
Aplicación externa	rest	rest	rest

27.4.14 Accounting

	X1W/R	X3W/R	X5W/R	X8	Servidor (S)
Grabación central de detalles de llamada					
Entradas en la memoria temporal de datos de llamada por sistema	20000	20000	20000	20000	20000
Código de proyecto (PRO):					
Entradas de código de proyecto por sistema de comunicación	1000	1000	1000	1000	1000
Cifras comprobables por código de proyecto	11	11	11	11	11
Caracteres permitidos	0-9	0-9	0-9	0-9	0-9

[56] Los valores están escalonados según la versión del módulo: básica o avanzada

28 Modo Experto

El **Modo Experto** ofrece menús con funciones para la configuración y el mantenimiento del sistema.

28.1 Convenciones de representación para descripciones de parámetros

Las descripciones de los parámetros siguen la estructura del modo Experto de la Gestión basada en Web (WBM).

Entrada de menú	Cada entrada de menú del modo Experto tiene asignado un tema de ayuda que se puede consultar directamente (contextual) desde la Gestión basada en Web (WBM). El título del tema de ayuda indica la ruta de la ventana de la Gestión basada en Web (WBM). Ejemplo: **Ajustes básicos** > **Sistema** > **Flags del sistema**
Pestaña	Cada pestaña tiene asignada una tabla de parámetros propia en el tema de ayuda. Los mismos parámetros de distintas pestañas se describen en la misma tabla de parámetros. Por encima de cada tabla de parámetros encontrará un listado de las pestañas que les corresponden. Ejemplo: • **Añadir dirección IP estática** • **Editar dirección IP estática** • **Borrar dirección IP estática**
Área	Si las ventanas de la Gestión basada en Web (WBM) están estructuradas en áreas, esta misma estructura se reproducirá en la tabla de parámetros. La tabla de parámetros incluye un subencabezado para cada área, seguido de los parámetros de esa área.

Parámetros	Los parámetros se describen en una tabla de parámetros de dos columnas. La columna izquierda indica el parámetro. La columna derecha describe los parámetros. Los parámetros autoexplicativos, se designan, pero no se describen. Puede consultar el rango de valores y el valor estándar (predeterminado) al final de la descripción, si la hay.
Parámetro (opcional)	Los parámetros que no hace falta indicar aparecen indicados con la palabra clave opcional.
Entrada en la lista desplegable	Las entradas que no son autoexplicativas en las listas desplegables también aparecen como parámetros en la columna izquierda de la tabla de parámetros. La entrada se separa del nombre de la lista desplegable con dos puntos. Ejemplo: **Algoritmos de cifrado: AES**
Casilla de verificación/Campo de opción/Flag	La descripción de casillas de verificación/campos de opción/flags siempre se refiere al estado activado.

28.2 Mantenimiento

Las funciones para mantener el sistema de comunicación, por ejemplo, para cargar música en espera o actualizar imágenes de software, se agrupan en **Mantenimiento**.

28.2.1 Configuración

En **Configuración** se reunen funciones para, por ejemplo, cargar una música en espera (MoH) o para visualizar la configuración de hardware.

28.2.1.1 Configuración > Música en espera (MoH) > Cargar al gateway

Descripción de parámetros de las pestañas:

- **Cargar archivos de música en espera (MoH) vía HTTP**

Parámetros	Descripción
Cargar archivos de música en espera (MoH) vía HTTP	

Parámetros	Descripción
Archivo de MoH diurna	Seleccionar el archivo de MoH diurna en el sistema de archivos local. Formato de archivo: véase Nota en el WBM.
Archivo de MoH nocturna	Seleccionar el archivo de MoH nocturna en el sistema de archivos local. Formato de archivo: véase Nota en el WBM.
Cargar	Cargar los archivos de MoH seleccionados en el sistema (hay que reiniciar). Activación en Configuración, Telefonía central > Música en espera/Anuncios grabados.

Descripción de parámetros de las pestañas:

- **Cargar archivos de sonido a través de HTTP**

Parámetros	Descripción
Cargar archivos de sonido a través de HTTP	
Archivo de anuncio	Seleccionar del archivo WAV con el anuncio grabado en el sistema de archivo local. Formato de archivo: véase Nota en el WBM.
Archivos de sonido ya cargados	
Archivo Wave	Indicación de los archivos de anuncio grabado cargados en el sistema de comunicación
Eliminar	Borrar el archivo de anuncio
Cargar	Cargar el archivo de anuncio seleccionado en el sistema. Activación en Configuración, Telefonía central > Música en espera/Anuncios grabados.

28.2.1.2 Configuración > Anuncios > Cargar el Gateway

Descripción de parámetros de las pestañas:

- **Cargar archivos de audio mediante HTTP**

Parámetros	Descripción
Cargar archivos de audio mediante HTTP	
Archivo de anuncio	Seleccione el archivo WAV con el anuncio desde el sistema de archivos local. Formato de archivo: ver nota en WBM.
Archivos de audio ya subidos	
Archivo de Wave	Muestra los archivos de anuncios cargados en el sistema de comunicación
Eliminar	Elimina el archivo de anuncio

Parámetros	Descripción
Cargar	Carga el archivo de anuncio seleccionado en el sistema. Activación en Configuración, Telefonía Central> Música en espera/Anuncios.

28.2.1.3 Configuración > Configuración de puerto

Descripción de parámetros de la pestaña:

- **Exportar la configuración**

Parámetros	Descripción
Exportar la configuración	
Nombre archivo	Nombre del archivo exportado.
Acción	Exportación de un archivo XML comprimido (p. ej. para editar en Excel) con estos datos: nombre, número de teléfono de la extensión, número de marcación directa, tipo de extensión, licencias, grupos/líneas colectivas (no Team/Top), extensiones virtuales, líneas, grupos de líneas, buzón de voz, etc.

28.2.1.4 Configuración > SmartVM

Descripción de parámetros de las pestañas:

- **Descripción general**

Parámetros	Descripción
Idiomas Visualización de todos los idiomas en los que está disponible la guía de voz. Existe la siguiente convención de nombres: aabb aa = código de idioma de dos cifras bb = código de país de dos cifras El código de país (bb) por lo general es idéntico al código de idioma (aa)	
Información de buzón	
Número de llamada	Visualización del número de teléfono del buzón de voz.
Nombre	Visualización del nombre del buzón de voz.
Mensajes	Visualización del número de mensajes nuevos o de todos los mensajes.
Uso total de buzón	Visualización del uso de memoria, en porcentaje.

28.2.1.5 Configuración > SmartVM > Operaciones de buzón

Descripción de parámetros de las pestañas:

- **Ejecutar operaciones de buzón**

Parámetros	Descripción
Restablecer la configuración de todos los buzones (borrar todos los mensajes y anuncios grabados)	Si este flag está activado, se borran todos los saludos y los mensajes de todos los buzones de voz de SmartVM. Estándar: desactivado.
El índice	Visualización del índice del buzón de voz.
N.º llam.	Visualización del número de teléfono del buzón de voz.
Nombre	Visualización del nombre del buzón de voz.
Restablecer contraseñas	Si este flag está activado, la contraseña del buzón de voz se restablece al valor predeterminado `123456`. Cuando vuelva a utilizar el buzón de voz, el usuario debe modificar la contraseña. Estándar: desactivado.
Inicializar buzones	Si este flag está activado, se ejecutan las siguientes acciones para el buzón de voz seleccionado: Buzones voz estándar: – Se repone la contraseña – Se activa el flag **Grabaciones** – Eliminando mensajes – Se borran saludos – Control de saludos - manual – Saludo activo: Saludo 1 Buzones de voz AutoAttendant: – Se repone la contraseña – El flag **Interceptar después de anuncio** se desactiva – Se borran destinos de marcación abrev. – Se borran saludos – Control de saludos - manual – Saludo activo: Saludo 1 Estándar: desactivado.

28.2.1.6 Configuración > SmartVM > Operaciones en archivo

Descripción de parámetros de las pestañas:

- **Copia de seguridad**

Parámetros	Descripción
Copia de seguridad	

Parámetros	Descripción
Mensajes	Si este flag está activado, además de los saludos también se guardan los mensajes de los buzones de voz seleccionados. Estándar: desactivado.
Buzones disponibles	Lista de todos los buzones de voz existentes. En la lista de los buzones de voz con copia de seguridad se pueden incluir buzones de voz sueltos o todos lo buzones.
Buzones para copia de seguridad	Lista de los buzones de voz de los que se va a hacer copia de seguridad.
Botones	
Aplicar	Los saludos (y los mensajes si el flag **Mensajes** está activado) de los buzones de voz para copia de seguridad se guardan en un archivo de copia de seguridad (`*.tar`).

Descripción de parámetros de las pestañas:

- **Datos de anuncios grabados**

Parámetros	Descripción
Datos de anuncios grabados	
Selección de buzón	Selección del buzón de voz.
Anuncio grabado 1 (día)	Indicación del saludo que se está utilizando en ese momento. **Estándar**: no hay ningún saludo personalizado para la extensión.
Anuncio grabado 2 (noche)	Indicación del saludo que se está utilizando en ese momento. **Estándar**: no hay ningún saludo personalizado para la extensión.
Saludo 3	Indicación del saludo que se está utilizando en ese momento. **Estándar**: no hay ningún saludo personalizado para la extensión.
Saludo 4	Indicación del saludo que se está utilizando en ese momento. **Estándar**: no hay ningún saludo personalizado para la extensión.
Botones	
Examinar	Navegación hasta la ruta de almacenamiento del archivo de saludo.
Cargar	En el SmartVM se carga un saludo guardado previamente o un archivo Wave. El archivo wave a cargar tiene que tener el siguiente formato: PCM, 16 bit, 8khz, mono Al realizar la carga, el archivo wave seleccionado se convierte. Esto puede tardar bastante, dependiendo del tamaño del archivo wave.
Guardar	El saludo que se está utilizando en ese momento se guarda en el PC. Los saludos se guardan en formato binario en el PC (archivo vma) y, por ello, no se pueden reproducir ni modificar.
Eliminar	El saludo que se está utilizando en ese momento se borra del SmartVM.

Descripción de parámetros de las pestañas:

- **Recuperar**

Parámetros	Descripción
Recuperar	
Mensajes	Sobrescribe los saludos de los buzones de voz seleccionados y también los mensajes. Estándar: desactivado.
Intercalar	Si este flag está desactivado, solo se sobrescriben los saludos de los buzones de voz seleccionados que están en los datos de copia de seguridad. Si además está activado el flag **Mensajes**, también se añaden los mensajes recogidos en los datos de copia de seguridad. Los mensajes ya existentes no se pierden. Si este flag está activado, antes de la restauración se borran todos los saludos y los mensajes de los buzones de voz seleccionados en el SmartVM. Si se seleccionan buzones de voz que no están incluidos en los datos de copia de seguridad, también se borran. Los saludos incluidos en los datos de seguridad se transfieren. Si además está activado el flag **Mensajes**, también se transfieren los mensajes contenidos en los datos de copia de seguridad. Estándar: desactivado.
Buzones disponibles	Lista de todos los buzones de voz presentes en el archivo de copia de seguridad. En la lista de los buzones de voz para restauración se pueden incluir buzones de voz sueltos o todos los buzones.
Buzones para copia de seguridad	Lista de los buzones de voz de los que se va a hacer una restauración.
Botones	
Examinar	Navegación hasta la ruta de almacenamiento del archivo de copia de seguridad.
Cargar	Se muestran los buzones de voz incluidos en el archivo de copia de seguridad. Al hacer clic de nuevo en el botón se restablecen los saludos y los mensajes de los buzones de voz seleccionados.

28.2.1.7 Configuración > Marca

Descripción de parámetros de la pestaña:

- **Marca**

Parámetros	Descripción
Marca	Selección de la denominación de producto.

28.2.1.8 Configuración > Dirección IP del gateway

Descripción de parámetros de la pestaña:

- **Modificar dirección IP del gateway**

Parámetros	Descripción
Modificar dirección IP del gateway	
Dirección IP del gateway	Entrada de la dirección IP del sistema de comunicación, por ejemplo, 192.168.1.2

28.2.2 Imagen software

En **Imagen de software** se reunen las funciones para actualizar el software de gateway y las imágenes de teléfono.

28.2.2.1 Imagen de software > Software del sistema > Actualización a través de Internet

Descripción de parámetros de las pestañas:

- **Cargar imágenes de software de un servidor web**

Parámetros	Descripción
Ajustes servidor web	
URL imagen de software	Indicación y modificación de los enlaces del servidor de software, incl. ruta al archivo de imagen.
Nombre de usuario	Nombre de usuario para iniciar sesión en el servidor de software.
Contraseña	Contraseña para iniciar sesión en el servidor de software.
Información de la actualización de software	Activación de la consulta para comprobar si hay disponible una nueva versión de software en el servidor de software.
Hora de inicio	Hora de la consulta. Rango de valores: 00.00 - 24.00, valor estándar: 02,00
Utilizar proxy	Activación de proxy, si se utiliza un proxy.
Proxy HTTP	
Proxy HTTP	Entrada del enlace al servidor proxy.
Puerto proxy HTTP	Entrada del puerto del servidor proxy. Valor estándar: 80
Nombre de usuario	Nombre de usuario para iniciar sesión en el servidor proxy.
Contraseña	Contraseña para iniciar sesión en el servidor proxy.

Parámetros	Descripción
Utilizar ruta estática dedicada	Los clientes con una conexión WAN para troncales SIP sin volumen de datos de Internet, pueden utilizar la funcionalidad **Utilizar ruta estática dedicada** para realizar una actualización del software OSBiz a través de la interfaz LAN alternativa. La dirección IP dinámica del servidor de actualización se determina automáticamente y queda disponible como entrada de enrutamiento para este proceso. Para utilizar esta opción: • Activar el flag **Utilizar ruta estática dedicada**
Ruta estática dedicada para la actualización de software a través de la interfaz LAN	
Dirección IP de la puerta de enlace de la ruta	Configure la dirección IP de la pasarela por defecto de la interfaz LAN, a través de la cual es posible la conexión a Internet, como dirección IP de la pasarela de la ruta.
Última actualización de software en	Indicación de la última actualización de software realizada.
Botones	
Estándar	Restablece los valores modificados a los valores estándar.

28.2.2.2 Imagen software > Software del sistema > Actualización a través de Carga de archivo

Descripción de parámetros de las pestañas:

- **Cargar imágenes de software a través de Carga de archivo**

Parámetros	Descripción
Nombre archivo remoto (sist. archivos PC)	Navegación hasta la ubicación del archivo de imagen.
Limpie el espacio de almacenamiento antes de la transferencia	Cuando la actualización se ejecuta con este indicador activo, los registros, las trazas, las imágenes del software del teléfono y los volcados TCP se eliminan para liberar memoria de almacenamiento.
Activación de software	
Iniciar acción inmed. tras transmisión	El software se transmite inmediatamente al sistema de comunicación en segundo plano. Después de reiniciar dos veces, el software está actualizado.
Iniciar acción en	El software se transmite inmediatamente al sistema de comunicación en segundo plano. Una vez terminado el tiempo indicado, el software se activa. Indicación del tiempo en días, horas y minutos.
Iniciar acción el	El software se transmite inmediatamente al sistema de comunicación en segundo plano. El software se activa en el momento determinado. Indicación del momento, como fecha y hora.
Hora del sistema local	Indicación de la fecha y la hora del sistema.

Parámetros	Descripción
Versión de software de las imágenes de software del sistema utilizadas actualmente	Indicación de la versión de software del archivo de imagen actual.

28.2.2.3 Imagen software > Software del sistema > Actualización vía lápiz USB

Descripción de parámetros de las pestañas:

- **Cargar imágenes de software desde un lápiz USB**

Parámetros	Descripción
Lista de los archivos de imagen compatibles disponibles	
Versión	Indicación del número de versión de los archivos de imagen encontrados en el soporte USB.
Cargar	Marque el archivo de imagen del soporte USB que desea utilizar para la actualización de software.
Nombre de archivo	Indicación de los nombres de archivo de los archivos de imagen del soporte USB.
Tamaño de Imagen (MB)	Indicación del tamaño de archivo de los archivos de imagen del soporte USB.
Activación de software	
Iniciar acción inmed. tras transmisión	El software se transfiere inmediatamente al sistema de comunicación en segundo plano y se activa. Para la activación se interrumpe brevemente el funcionamiento del sistema.
Iniciar acción en	El software se transmite inmediatamente al sistema de comunicación en segundo plano. Una vez terminado el tiempo indicado, el software se activa. Indicación del tiempo en días, horas y minutos.
Iniciar acción el	El software se transmite inmediatamente al sistema de comunicación en segundo plano. El software se activa en el momento determinado. Entrada del momento, con fecha y hora.
Hora del sistema local	Indicación de la fecha y la hora del sistema.
Versión de software de las imágenes de software del sistema utilizadas actualmente	Indicación de la versión de software activa.

28.2.2.4 Imagen software > Imágenes de teléfono > Cargar

Descripción de parámetros de las pestañas:

- **Cargar imagen de software telefónico**

Parámetros	Descripción
Nombre archivo remoto (sist. archivos PC)	Selección del software telefónico (archivo de imagen)
Imágenes actualmente instaladas	
Eliminar	Las imágenes telefónicas se marcan para su borrado.
Nombre de archivo	Indicación del nombre de archivo de imagen.
Tipo disposit.	Indicación del tipo de teléfono del sistema al que pertenece el archivo de imagen.
Versión	Indicación de la versión del archivo de imagen.
Botones	
Cargar	La imagen de teléfono indicada se carga en el sistema de comunicación.
Eliminar	Las imágenes telefónicas marcadas se borran del sistema de comunicación.

28.2.2.5 Imagen software > Imágenes de teléfono > Distribuir

Descripción de parámetros de las pestañas:

- **Distribución del software telefónico**

Parámetros	Descripción
Imágenes actualmente instaladas	
Distribuir	Si la casilla de verificación está activada, el software telefónico se transfiere a todos los teléfonos del sistema que haya conectados y que sean del tipo de teléfono.
Nombre de archivo	Indicación del nombre de archivo de imagen.
Tipo disposit.	Indicación del tipo de teléfono del sistema al que pertenece el archivo de imagen.
Versión	Indicación de la versión del archivo de imagen.
Tipo	Tipo del teléfono del sistema.
Estándar	El software telefónico marcado como estándar se transfiere automáticamente a un teléfono del sistema de este tipo cuando inicia sesión por primera vez en el sistema.

28.2.2.6 Imagen de software > Imágenes de teléfono > Distribuir por dispositivo

Descripción de parámetros de las pestañas:

- **Distribución del software telefónico por terminal**

  Si el usuario es Usuario Deskshare, la casilla de verificación estará en gris y, por lo tanto, no puede distribuir un dispositivo a dicho usuario.

Parámetros	Descripción
Imágenes actualmente instaladas	
N° llam.	Número de teléfono del teléfono del sistema.
Tipo disposit.	Tipo del teléfono del sistema.
Dirección IP	Dirección IP del teléfono del sistema; enlace directo con la Gestión basada en Web (WBM) del teléfono del sistema.
Dirección MAC	Dirección MAC del teléfono del sistema.
Versión de software actual	Versión de software actual del teléfono del sistema.
Software distribuible	Selección de la imagen telefónica que se transferirá al teléfono del sistema.

28.2.2.7 Imagen software > Logotipos de imagen de teléfono > Cargar

Se puede cargar una imagen (p. ej., un logotipo de empresa) en el display de los teléfonos del sistema (OpenStage 40/60/80 o versiones específicas de la compañía telefónica) y hacer que aparezca en reposo (on-hook). Especificación del archivo de logotipo, véase Logotipos telefónicos.

Descripción de parámetros de las pestañas:

- **Carga del logotipo telefónico**

Parámetros	Descripción
Nombre archivo remoto (sist. archivos PC)	Selección del archivo con el logotipo telefónico.
Imágenes de logotipo instaladas en este momento	
Eliminar	Los archivos de logotipo telefónico se marcan para borrado.
Nombre archivo	Indicación del nombre de archivo del logotipo telefónico.
Botones	
Cargar	El archivo del logotipo telefónico indicado se carga en el sistema de comunicación.
Eliminar	Los archivos de logotipo telefónico se borran del sistema de comunicación.

28.2.2.8 Imagen software > Logotipos de imagen de teléfono > Distribuir

Se puede cargar una imagen (p. ej., un logotipo de empresa) en el display de los teléfonos del sistema (OpenStage 40/60/80 o versiones específicas de la compañía telefónica) y hacer que aparezca en reposo (on-hook). Especificación del archivo de logotipo, véase Logotipos telefónicos.

Descripción de parámetros de las pestañas:

- **Distribución del logotipo telefónico**

Parámetros	Descripción
Imágenes de logotipo instaladas en este momento	
Distribuir	Si la casilla de verificación está activada, el archivo de logotipo telefónico se transfiere a los teléfonos del sistema seleccionados.
Nombre archivo	Indicación del nombre de archivo del logotipo telefónico.
Distribuir a puntos de trabajo (workpoint) con el tipo de dispositivo seleccionado	Se selecciona si el logotipo de teléfono se transferirá a todos los teléfonos del sistema o solo a un tipo de teléfono del sistema determinado.

28.2.3 Inalámbrico (Cordless)

En **Cordless** se reúnen las funciones de todas las extensiones base configuradas.

28.2.3.1 Extensiones base > Cordless

Descripción de los parámetros de las pestañas:

- **Estado de extensión base**

Parámetros	Descripción
Datos de extensión base	
Frecuencia BS	Muestra las frecuencias de la extensión base seleccionada. Se pueden seleccionar hasta 10 canales de frecuencia diferentes al mismo tiempo (véase la tabla siguiente).
Extensión base	Número de la extensión base
Versión software	Versión de software de la extensión base.
Versión de hardware	Versión de hardware de la extensión base.
Estado	Estado del puerto correspondiente: Puerto activo Ninguna BS Bloqueado BS conectada BS conectada 1er puerto adicional al ... (N° del puerto matriz) 2do. puerto adicional al ... (N° del puerto matriz)
Sobrecarga	Cantidad de situaciones de sobrecarga que se hayan producido en el interfaz UP0/E.
Reinicio	Cantidad de veces que se ha rearrancado la extensión base.
L1/L2 Error	Número de errores L1/L2 que se han producido en la extensión base.

Parámetros	Descripción
Abnormal Release	Número de llamadas interrumpidas que han tenido lugar en la extensión base.
Calls per BS	Número de llamadas (tanto entrantes como salientes) realizadas a través de la extensión base.
Modo salto frecuencia	Los sistemas Cordless de la versión 2 siempre operan en ”Modo salto de frecuencia rápido” (Fast Hopping Mode), es decir, pueden utilizarse todos los pares de frecuencia y de intervalo de tiempo. De este modo, hay disponibles 120 canales dúplex. En el caso de estaciones base Slow Hopping, sólo puede utilizarse cada segundo par de frecuencia y de intervalo de tiempo. Por tanto, sólo hay disponibles 60 canales dúplex. Todos los sistemas Cordless de la versión 1 operan en ”Modo salto de frecuencia lento” (Slow Hopping Mode).
BHO Count OK	Número de handovers intracelda (handovers de portadora - BHO) que se han completado con éxito, es decir, que la transferencia de la frecuencia portadora y/o ventana de tiempo se ha finalizado satisfactoriamente. No compatible con Hicom cordless EM V2.1 y V2.2. El contador no se admite, pero la prestación del handover de portadora está disponible.
BHO Count not OK	Número de handovers intracelda (handovers de portadora - BHO) que no se han completado por fallo. No compatible con Hicom cordless EM V2.1 y V2.2. El contador no se admite, pero la prestación del handover de portadora está disponible.
Intra SLC Handover	Número de procedimientos de handover dentro del módulo SLC16. Este valor se contabiliza en la extensión base nueva.
Inter SLC Handover	Número de procedimientos de handover entre módulos SLC16. Este valor se contabiliza en la extensión base nueva.
En toda la SLC	
Lost Calls	Cantidad de llamadas que no han podido transmitirse por falta de recursos.
Sobrecarga SLMUC	Número de situaciones de sobrecarga en el módulo SLC. El número de elementos de pool libres en el módulo SLC está por debajo de un valor mínimo. Todas las conexiones entrantes se rechazarán por la IWU del SLC hasta que la situación de sobrecarga vuelva a la normalidad.
Itinerancia LR	La Itinerancia LR cuenta cada ocupación realizada en un teléfono inalámbrico con un PMID predeterminado y ubicación SLC modificada. Se trata del número de mensajes de consulta de ubicación (LR) que hayan indicado la existencia de itinerancia, (es decir, que se produce un cambio de la ubicación actual del teléfono móvil). El teléfono móvil realiza una consulta de ubicación (LR, Locate Request) cada vez que se activa. Si el teléfono móvil se desactiva y se activa en otra célula radiotelefónica, este contador no computa.
LR Async	LR Async computa cada ocupación realizada en un teléfono inalámbrico con un PMID predeterminado siempre que no se modifique la ubicación SLC. Se trata de la cantidad de mensajes de LR que han indicado la asincronía de capas (es decir, el lugar de ubicación actual del teléfono inalámbrico no se ha modificado). El cómputo siempre se realiza en el SLC doméstico y por ello sólo tendrá lugar si la conexión radiotelefónica llega realmente a producirse o si se admite CHO con PMID estándar. En las ocupaciones deben cumplirse adicionalmente los criterios para una actualización del lugar de ubicación, es decir, debe haberse obtenido un LOCATE-Request o deben haberse cumplido las medidas de seguridad, autenticación (y Ciphering) para el enlace.

Parámetros	Descripción
HDLC Error	Número de mensajes de error HDLC no críticos que se no hayan indicado al sistema de comunicación (desbordamiento, sin capacidad de proceso, error CRC).
CMI Version	Aquí se muestra la versión actual de Cordless.

Frecuencia (Channel)	DECT	Europa 1880 – 1900 MHz	Latinoamérica 1910 – 1930 MHz
10	9	1881,792 MHz	1911,16 MHz
9	8	1883,520 MHz	1912,896 MHz
8	7	1885,24 MHz	1914,624 MHz
7	6	1886,976 MHz	1916,352 MHz
6	5	1888,704 MHz	1918,080 MHz
5	4	1890,432 MHz	1919,80 MHz
4	3	1892,160 MHz	1921,536 MHz
3	2	1893,88 MHz	1923,264 MHz
2	1	1895,616 MHz	1924,992 MHz
1	0	1897,344 MHz	1926,720 MHz

28.2.4 Estado de puerto/módulos

Se puede mostrar el estado de todos los módulos. Además, los módulos y sus puertos se pueden liberar y bloquear.

28.2.4.1 Estado de puerto/módulos > Estado de módulos

Descripción de parámetros de las pestañas:

- **Estado de los módulos**

Parámetros	Descripción
Slot	Número de slot físico.
Módulo	Designación del módulo.
No insertado	Marcada con una cruz cuando el módulo no está insertado.
Defectuoso	Marcada con una cruz cuando el módulo es defectuoso (no está cargado). También es posible que no aparezca un módulo dañado o sin configurar.
Bloqueada	Marcada con una cruz cuando por lo menos un puerto de este módulo está bloqueado.
Libre	Marcada con una cruz cuando todos los puertos de este módulo están libres.

Parámetros	Descripción
Ocupado	Marcada con una cruz cuando por lo menos una extensión o una línea de este módulo ha contestado a una llamada, ha llamado o está manteniendo una comunicación telefónica.
Fuente temporiz.	Marcada con una cruz cuando el módulo envía el impulso de referencia.
Botones	
Inicio	Se empieza a actualizar la visualización. El estado se actualiza cada 3 segundos.
Detener	Se detiene la actualización de la visualización.

28.2.4.2 Estado de puerto/módulos > Fuera de servicio

Descripción de parámetros de las pestañas:

- **Puerto fuera de servicio**
- **Módulo Fuera de servicio**

Parámetros	Descripción
Acceso	Slot y puerto en el que está conectada la extensión o la línea.
N° llam.	El número de teléfono asignado al puerto.
Nombre	El nombre que corresponde a la extensión o línea de enlace.
Estado	Los puertos pueden encontrarse en estado **activo** o **inactivo** según si hay o no un terminal o una línea de enlace válidos conectados al puerto. Los puertos también pueden estar **En servicio** (ajuste estándar) o **Fuera de servicio por herramienta**, es decir, bloqueados a través de la opción **Bloquear módulos**. El estado **En servicio** no es lo mismo que **Activo**. Por ejemplo, un determinado puerto podría encontrarse: **activo**, **en servicio** o podría estar también **inactivo**, **en servicio**.
Botones	
Bloquear selección	Se bloquean los puertos marcados. Al bloquear puertos $U_{P0/E}$ se pone siempre fuera de servicio el puerto físico asociado. Ello tiene como consecuencia que al seleccionar un puerto maestro, el puerto esclavo asociado a éste también deja de funcionar.
Liberar selección	Se liberan los puertos marcados.
Bloquear módulos	Se bloquean los módulos marcados y sus puertos. Al bloquear teléfonos móviles individuales de un módulo Cordless (inalámbrico), se bloquea siempre el módulo entero y, con ello, todos los teléfonos móviles. Los teléfonos móviles individuales también se pueden bloquear modificando los PIN de los teléfonos móviles.
Liberar módulos	Se liberan los módulos marcados y sus puertos.

28.2.5 Traces

En **Traces** se reunen las funciones de seguimiento. El administrador puede iniciar y detener los seguimientos y modificar los ajustes de configuración.

28.2.5.1 Traces > Configuración de formato trace

A través de la Configuración de formato trace, se define qué datos de encabezado deberán incluirse en la salida Trace y el formato que deberán tener los datos Trace.

Descripción de parámetros de las pestañas:

- **Editar config. trace**

Parámetros	Descripción
Datos encabezam. contenidos en salida trace	
Ajustes globales formato de encabezam. trace	Si el flag está activado, se pueden activar o desactivar las funciones para los siguientes datos de encabezado (header). Valor estándar: Activado
ID subsist.	Si el flag está activado, el ID de subsistema se incluye en la salida trace. Valor estándar: Activado
Nombre tarea	Si el flag está activado, el nombre de tarea se incluye en la salida trace. Valor estándar: Activado
ID tarea	Si el flag está activado, el ID de tarea se incluye en la salida trace. Valor estándar: Activado
Hora	Si el flag está activado, la indicación de hora se incluye en la salida trace. Valor estándar: Activado
Nombre mód.	Si el flag está activado, el nombre de módulo se incluye en la salida trace. Valor estándar: Activado
N.º línea	Si el flag está activado, el número de línea se incluye en la salida trace. Valor estándar: Activado
Preparación de los datos trace (formateo)	
Formateo completo con expansión de parámetros (estándar)	Modo de salida estándar: se expanden todos los tipos de datos. Salida trace: normal (apto para el modo normal) Valor estándar: Activado
Restringido (tipos de mensajes binarios, especial para X-Tracer)	En el modo de salida restringido se emiten los tipos de datos en formato binario, es decir, tal y como están en el momento del trace. El formato binario es adecuado para el análisis con la herramienta X-Tracer. Salida trace: rápido (adecuado para cargas medias y altas) Valor estándar: Desactivado

Parámetros	Descripción
Restringido (solo expansión de tipos de datos elementales)	En este modo de salida, solo se expanden los tipos de datos básicos (p. ej., integer, short, long, string). Salida trace: muy rápido (adecuado para cargas altas) Valor estándar: Desactivado
Trace con rendimiento optimizado sin expansión de parámetros	En este modo de salida no se expande ningún tipo de datos. Por ello tampoco hay costos para el formato trace. Salida trace: extremadamente rápido (adecuado para cargas muy altas) Valor estándar: Desactivado

28.2.5.2 Traces > Interfaces de salida trace

Descripción de parámetros de las pestañas:

- **Editar interfaces de salida trace**

Parámetros	Descripción
Trace archivo	
Act. trace archivo	Si el flag está activado, los mensajes trace del sistema de comunicación se registran en un archivo de protocolo. Valor estándar: Activado
Cuota trace máxima (kbytes)	Indicación del tamaño máximo de la memoria trace en kByte
Directriz para manejar el cumplimiento de la cuota máxima	Se puede seleccionar qué sucederá cuando se alcance la cuota trace máxima.
Directriz para manejar el cumplimiento de la cuota máxima: Saltar (eliminar archivo trace más antiguo)	Al llegar a la cuota trace máxima se sobrescribe el archivo de protocolo trace más antiguo. Valor estándar: Activado
Directriz para manejar el cumplimiento de la cuota máxima: Detener temporalmente el archivo trace	Al llegar a la cuota trace máxima se detiene la salida del archivo trace. Valor estándar: Desactivado
Tiempo transcurrido entre la creación de nuevos archivos trace (s)	Indicación del tiempo (en segundos) después del cual se empieza a crear un nuevo archivo de protocolo trace.
Margen de tiempo durante el que están disponibles los archivos trace	Indicación del periodo de tiempo durante el que están disponibles los archivos de protocolo trace.
Trace vía LAN	

Parámetros	Descripción
Act. trace vía LAN	Los mensajes Trace se transfieren a través de la interfaz LAN. Valor estándar: Desactivado
Valor timer (s)	Indicación del tiempo (en segundos) tras el cual se empiezan a transmitir datos trace.

28.2.5.3 Traces > Protocolo trace

Descripción de parámetros de las pestañas:

- **Cargar vía HTTP**
- **Borrar protocolo trace**

Consejo: Si se borran datos de protocolo trace, la acción no se puede deshacer.

Parámetros	Descripción
Protocolo trace	
Todo el protocolo	Se descargan todos los archivos de protocolo trace disponibles.
Protocolo de hoy	Se descargan los archivos de protocolo trace del día en curso (desde las 00:00 horas).
Selección propia	Se descargan los archivos de protocolo trace del periodo seleccionado.

28.2.5.4 Traces > Loopback digital

Los loopbacks digitales solo se pueden configurar con Manager E.

Los loopbacks digitales se utilizan para comprobar los canales B de las interfaces S_0, S_{2M} y T1 de los módulos que pudiera haber. Los loopbacks digitales solo se tienen que activar si así lo solicita el proveedor de servicios.

Descripción de parámetros de las pestañas:

- **Editar Digital loopback**

28.2.5.5 Traces > Protocolo trace de cliente

Esta función permite iniciar la indicación de sucesos (trace de cliente). Los tipos de mensajes son, entre otros: Sistema, SIP, STUN y LDAP.

Descripción de parámetros de las pestañas:

- **Mostrar**
- **Cargar vía HTTP**
- **Borrar protocolo trace**

Parámetros	Descripción
Actualización autom.	Si el flag está activado, se realiza una actualización automática de la indicación del protocolo de trace de cliente. Valor estándar: Activado
Segundos hasta la próx. actualiz.	Tiempo en segundos tras el cual se actualizará el protocolo de trace de cliente.

28.2.5.6 Traces > Componente trace M5T

Esta función permite supervisar la pila SIP.

Solo hay que modificar la configuración si así lo solicita el soporte técnico responsable.

Descripción de parámetros de las pestañas:

- **Editar componentes trace M5T**
- **Iniciar/Detener componente trace**

Parámetros	Descripción
Nombre de paquete	Nombre del componente trace M5T
Nivel trace	Nivel de detalle del registro del componente trace M5T (nivel 0=nivel mínimo a nivel 9=nivel máximo) Valor estándar: 0
Trace act.	Si el flag está activado, se graban automáticamente los datos del componente trace M5T. Valor estándar: Desactivado
Bifurcación	Incremento de la activación

28.2.5.7 Traces > Secure Trace

Esta función permite registrar flujos de datos de señalización y de uso de VoIP cifrados.

Para registrar datos de conexión cifrados es necesaria la aceptación del cliente y solo se puede realizar previo acuerdo con el servicio de soporte técnico responsable. Información sobre el procedimiento, véase Traces (Secure Trace).

Nota: Si no se notifica a las extensiones previamente, la grabación de llamadas y de datos de conexión va en contra de la ley.

Descripción de parámetros de las pestañas:

- **Modificar frase de contraseña Secure Trace**
- **Importar archivo X.509 para Secure Trace**

Parámetros	Descripción
Cambiar frase de contraseña de activación Secure Trace	
Frase de contraseña actual	Contraseña (passphrase) actual para iniciar y detener el Secure Trace
Nueva frase de contraseña	Nueva contraseña (Passphrase) para iniciar y detener el Secure Trace Rango de valores: de 5 a 12 caracteres
Confirmar nueva frase de contraseña	Nueva contraseña (Passphrase) idéntica para iniciar y detener el Secure Trace Rango de valores: de 5 a 12 caracteres
Archivo de certificado (PEM o binario)	Selección del archivo X.509 que incluye el certificado que se va a importar en el sistema de comunicación. Después de seleccionar el archivo X.509 se puede mostrar la huella dactilar el certificado que se va a importar y, a continuación, se importa el certificado en el sistema de comunicación. ***INFO:*** El certificado se debería importar después de comprobar la huella dactilar.

28.2.5.8 Traces > Secure Trace > Certificado Secure Trace

Esta función permite visualizar el certificado Secure Trace importado.

Descripción de parámetros de las pestañas:

- **Mostrar certificado Secure Trace**

28.2.5.9 Traces > Secure Trace > Ajustes Secure Trace

Esta función sirve para consultar el estado y para iniciar/detener el Secure Trace.

Descripción de parámetros de las pestañas:

- **Estado Secure Trace**
- **Iniciar/detener Secure Trace**

Parámetros	Descripción
Estado actual Secure Trace	
Secure Trace está activo	Estado del Secure Trace
Hora de desactivación automática	Tiempo hasta que el Secure Trace se desactiva automáticamente.
Secure Trace para estos protocolos	Indicación de los protocolos para los que se genera el Secure Trace.
Parámetros de inicio	
Frase de contraseña de activación Secure Trace	Contraseña (Passphrase) para iniciar y detener el Secure Trace

Parámetros	Descripción
Duración de Secure Trace (min.)	Periodo de tiempo en minutos durante el que estará activo el Secure Trace. ***INFO:*** Es imprescindible introducir un valor.
Secure Trace para estos protocolos	
TC (TLS)	Si el flag está activado, Secure Trace considera el protocolo TC (TLS). Valor estándar: Desactivado
H.323 Core/HSA (TLS)	Si el flag está activado, Secure Trace considera el protocolo H.323 Core/HSA (TLS). Valor estándar: Desactivado
MMX (PEP)	Si el flag está activado, Secure Trace considera el protocolo MMX (PEP). Valor estándar: Desactivado
SIP Core/SSA (TLS)	Si el flag está activado, Secure Trace considera el protocolo SIP Core/SSA (TLS). Valor estándar: Desactivado
MSC (SRTP)	Si el flag está activado, Secure Trace considera el protocolo MSC (SRTP). Valor estándar: Desactivado

28.2.5.10 Traces > Trace pila H.323

Esta función permite hacer un seguimiento de problemas con los componentes que usan el protocolo H.323.

Solo hay que modificar la configuración si así lo solicita el soporte técnico responsable.

Descripción de parámetros de las pestañas:

- **Editar config. trace pila H.323**
- **Editar todos mód. H.323**
- **Cargar protocolo trace pila H.323 vía HTTP**
- **Borrar protocolo trace pila H.323**

Parámetros	Descripción
General	
Nivel trace	Nivel de detalle para el registro trace (nivel trace 0 = detalle más bajo a nivel trace 4 = nivel más alto) Valor estándar: 2
Trace consolas	
Act. trace consolas	Si el flag está activado, los mensajes de trace pila H.323 se emiten en la consola. Valor estándar: Desactivado
Trace archivo	

Parámetros	Descripción
Act. trace archivo	Si el flag está activado, los mensajes de trace pila H.323 se registran en un archivo de protocolo. Valor estándar: Desactivado
Tamaño máx. búfer trace (bytes)	Tamaño máx. búfer trace (bytes) (cantidad de datos almacenados en la memoria intermedia).
Tamaño máx. archivo trace (bytes)	Tamaño máximo del archivo de protocolo trace en bytes
Timer trace (s)	Tiempo en segundos tras el que se escribirán los datos Trace en el archivo de protocolo.
Nombre mód.	Nombre del módulo de Trace pila H.323
Trace act.	Si el flag está activado, el módulo trace pila H.323 está activo.

28.2.5.11 Traces > Supervisión de llamadas

Esta función permite iniciar y detener la supervisión de interfaces de línea y de extensión.

Descripción de parámetros de las pestañas:

- **Iniciar/Detener protocolo**
- **Mostrar**
- **Cargar vía HTTP**

Parámetros	Descripción
Puerto seleccionado	Interfaz de línea o de extensión para la que se va a iniciar o detener la supervisión de llamadas.
N°	Número consecutivo.
Hora	Hora del evento (event).
Callnumber/Access	Número de teléfono e interfaz física.

Parámetros	Descripción
Estado	Estado de la interfaz. Estos son los estados de interfaz posibles: • Idle (interfaz en reposo) • Call Initiated (interfaz operativa) • Overlap Sending (envío de dígitos externo) • Outgoing Call Proc (final de marcación) • Call Request (esperar a alerta) • Call Present (llamando a la interfaz) • Active (la interfaz está llamando) • Hold (interfaz retenida) • Disconnect Indication (solicitud para interrumpir una llamada activa) • Direct (interfaz en modo de mensaje directo) • Intrusion (activando intercalado) • Call Back A (devolución de llamada, extensión A) • Call Back B (devolución de llamada, extensión B) • Busy (interfaz ocupada) • Error (Error) • Disconnect PI (esperar a desconexión de PI (Progress Indicator)) • Sensor (El sensor ha enviado una señal.) • Conference Master (Maestro de conferencias) • Paging (buscador) • Help Dial (utilizando marcación asociada) • Remote (interfaz ocupada mediante servicio remoto o DISA) • ACD (distribución de llamadas) • Unknown State (estado desconocido)
Suceso	Suceso Estos son los eventos posibles: • Setup (interfaz de línea: ocupación entrante o saliente) • Setup Ackn (interfaz de línea: confirmación de ocupación) • Info (interfaz de línea: info (códigos de número de teléfono)) • Call Proc (interfaz de línea: final de marcación sin evaluar) • Progress (interfaz de línea: información adicional para el establecimiento de conexión) • Alert (interfaz de línea: final de marcación evaluado) • Connect (interfaz de línea: conexión de canal B) • Connect Ackn (interfaz de línea: confirmación de conexión de canal B) • Disconnect (interfaz de línea: orden de desconexión) • Release (interfaz de línea: confirmación de desconexión) • Release Compl (interfaz de línea: conexión interrumpida) • Monitor On (interfaz de línea/extensión: supervisión de llamadas iniciada) • Monitor Off (interfaz de línea/extensión: supervisión de llamadas detenida) • Off Hook (interfaz de extensión: auricular descolgado) • On Hook (interfaz de extensión: auricular colgado) • Digit (interfaz de extensión: marcando cifras)

Parámetros	Descripción
Actualización autom.	Si el flag está activado, se actualiza automáticamente la indicación de la supervisión de llamadas. Valor estándar: Activado
Segundos hasta la próx. actualiz.	Tiempo en segundos que debe transcurrir para actualizar la supervisión de llamadas.

28.2.5.12 Traces > Componente de licencia

Esta función permite supervisar el agente de licencia interno del sistema (CLA, Customer License Agent).

Solo hay que modificar la configuración si así lo solicita el soporte técnico responsable.

Descripción de parámetros de las pestañas:

- **Cambio del componente trace CLA**

Parámetros	Descripción
Nombre de paquete	Nombre del componente trace de licencia.
Nivel trace	Definición del nivel de detalle del registro del componente trace de licencia. Valor estándar: Estándar
Nivel trace: bajo	Nivel de detalle bajo para el registro trace.
Nivel trace: Estándar	Nivel de detalle medio para el registro trace.
Nivel trace: Todos	Nivel de detalle alto para el registro trace.
Nivel trace: desact.	Componente trace de licencia detenido.

28.2.5.13 Traces > Perfiles trace

Los perfiles trace incluyen componentes trace predeterminados para supervisar unidades funcionales completas del sistema de comunicación.

Descripción de parámetros de las pestañas:

- **Mostrar todos perfiles trace**
- **Añadir perfil trace (perfil vacío)**
- **Añadir perfil trace (con ajustes trace actuales)**
- **Detener todos perfiles trace**
- **Iniciar/Detener perfil trace**

Parámetros	Descripción
Nombre de perfil	Nombre del perfil trace
Iniciar perfil	Indica si se ha iniciado el perfil trace.

Parámetros	Descripción
Perfil protegido contra escrit.	Indica si el perfil trace está protegido contra escritura (todos los perfiles trace disponibles de forma predeterminada tienen acceso de solo lectura).
Componente trace	Nombre del componente trace
Incluido	Si el flag está activado, el componente trace se añade al nuevo perfil Trace. Valor estándar: Activado
Nivel	Nivel de detalle del registro de los componentes trace (nivel trace 0 = nivel de detalle mínimo a nivel trace 9 = nivel máximo)

28.2.5.14 Traces > Componentes trace

Con ayuda de los componentes trace se registra la información de estado y de proceso de los distintos componentes del sistema de comunicación.

Descripción de parámetros de las pestañas:

- **Mostrar todos componentes trace**
- **Mostrar componentes trace iniciados**
- **Mostrar componentes trace parados**
- **Editar componentes trace**
- **Detener todos los componentes trace**
- **Iniciar/Detener componente trace**
- **Ajustes estándar de trace**

Parámetros	Descripción
Nombre subsist.	Nombre del componente trace
Índice componentes trace	Número consecutivo
Nivel trace	Nivel de detalle para el registro trace (nivel trace 0 = detalle más bajo a nivel trace 9 = nivel más alto)
Trace act.	Si el marcador está activado, se registran los datos del componente trace.

28.2.5.15 Traces > TCP Dump

Un TCP Dump permite supervisar y evaluar el tráfico de datos en una interconexión IP. Para hacer el diagnóstico de los archivos TCP Dump se requiere una aplicación adecuada.

Descripción de parámetros de las pestañas:

- **Estado TCP Dump**

Parámetros	Descripción
Iniciar TCP Dump	Se inicia el TCP Dump
Parámetro de inicio	

Parámetros	Descripción
Nombre de interfaz	Interfaz en la que se hace una evaluación del tráfico de datos. Las interfaces disponibles se muestran en **Detalles de interfaz**. La entrada **any** hace una evaluación del tráfico de datos de todas las interfaces disponibles. Valor estándar: any
Tamaño de paquete	Tamaño de los paquetes de datos (en bytes) que se van a capturar. La entrada **0** significa: todos los paquetes se capturarán íntegramente. Rango de valores: 0 a 2000000000, valor estándar: 0
Criterios de fin	
Cantidad de paquetes	Número de paquetes de datos que, al ser alcanzado, finaliza el TCP Dump.
Tiempo hasta finalización (s)	Tiempo en segundo que, al ser alcanzado, finaliza el TCP Dump.
Terminar TCP Dump	Parada del TCP Dump
Borrar TCP Dump	Borrado de los archivos TCP Dump guardados en el sistema de comunicación
Actualización autom.	Si el flag está activado, se actualiza automáticamente el indicador de estado. Valor estándar: Activado

28.2.5.16 Traces > rpcap Daemon

Un daemon RPCAP (Remote Packet Capture) permite supervisar y evaluar el tráfico de datos en una interconexión IP. El daemon RPCAP permite el acceso remoto de aplicaciones externas a los paquetes TCP/IP de las interfaces LAN del sistema de comunicación. A menudo, los daemon RPCAP se utilizan para realizar seguimientos (Traces) a largo plazo, ya que los archivos Trace se almacenan en un PC y no en el sistema de comunicación.

Nota: Hay que seguir las indicaciones de seguridad recogidas en la pestaña.

Descripción de parámetros de las pestañas:

- **rpcap**

Parámetros	Descripción
Dirección con la que enlazar	
Dirección IP (numérica o con letras)	Dirección IP del host en el que se van a hacer las grabaciones. Valor estándar: 0.0.0.0
Puerto (seleccione uno libre)	Puerto del host en el que se van a hacer las grabaciones.

Parámetros	Descripción
Rastrear LAN interna	Si el flag está activado, se hace una grabación del tráfico de datos entre dos módulos mediante la interfaz eth9. Valor estándar: Desactivado
Identificación de cliente para permitir acceso	
Dirección IP (numérica o con letras)	Dirección IP del cliente remoto en el que se va a emitir el Trace. Valor estándar: 0.0.0.0

28.2.5.17 Rastros > Datos de colisiones del kernel

El servicio Kernel Crash Data se utiliza para recopilar automáticamente los datos de los accidentes del núcleo. Sólo está disponible en sistemas OSBiz X con placas base V3: OCCLA, OCCMA(R), OCCMB(R).

El servicio requiere un espacio de almacenamiento de 200 MB. Los discos afectados son:

- SSD SATA de 16 GB (si no se monta una SSD NVMe)
- + NVMe SSD

Se recomienda eliminar los rastros antes de iniciar el servicio, si se quiere liberar espacio de almacenamiento. Si no hay espacio suficiente, el servicio no recogerá los datos.

Descripción de parámetros de las pestañas:

- **Datos de colisión del núcleo**

Parámetros	Descripción
Servicio de Datos de Choque del Núcleo	Estado del servicio: Verde: El servicio está activado. GRIS El servicio está desactivado.
Inicio	Inicia el servicio Kernel Crash Data.
Detener	Detiene el servicio Kernel Crash Data.

Al iniciar o detener el Servicio de Datos de Colisión del Núcleo, se inicia automáticamente un reinicio del sistema. El servicio conserva el estado tras el reinicio del sistema.

Con el servicio activado, después de un reinicio del sistema con la razón WATCHDOG o KERNEL_OOPS, los datos de los fallos del kernel están disponibles en el espacio de almacenamiento de diagnóstico oso. Para recopilar los datos de fallos del núcleo, la casilla de verificación **del Protocolo CoreLog** debe estar seleccionada en **Centro de servicios** > **Diagnóstico** > **Rastreo** > **Registros de diagnóstico**.

Después de recoger los datos de la caída del kernel, el servicio debe ser desactivado manualmente.

28.2.5.18 Traces > Trace del servidor de medios

El Trace del servidor de medios se puede utilizar para registrar el proceso y la información de estado del componente Servidor de medios del sistema de comunicación.

Descripción de parámetros de las pestañas:

- **Editar el componente de trace del servidor de medios**

Parámetros	Descripción
Nombre de paquete	Nombre del componente trace Valor estándar: Servidor de medios
Nivel trace	Nivel de detalle del trace (Ninguno, No especificado, Predeterminado, Fatal, Error, Advertencia, Información, Inesperado, Depuración, Detallado, Muy detallado)
Estado del trace	Estado del trace: Verde: El trace está activado. Gris: El trace está desactivado.
Iniciar	Inicia el Trace del servidor de medios.
Detener	Detiene el Trace del servidor de medios.

28.2.6 Sucesos

En **Sucesos** se reunen las funciones para mostrar y controlar los sucesos ("events"). Aquí se incluyen, por ejemplo, la configuración de sucesos y la configuración de correo electrónico.

28.2.6.1 Sucesos > Config. sucesos

Descripción de parámetros de las pestañas:

- **Editar config. sucesos**

Parámetros	Descripción
Ajustes archivo sucesos	
Tamaño máx. búfer sucesos (bytes)	Indicación del tamaño máximo del búfer de sucesos en bytes
Tamaño máx. archivo sucesos (bytes)	Indicación del tamaño máximo del archivo de protocolo de sucesos en bytes
Timer sucesos (s)	Indicación del tiempo (en segundos) que debe transcurrir para crear un nuevo archivo de protocolo de sucesos.
Suceso vía LAN	

Parámetros	Descripción
Act. protocoliz. sucesos vía LAN	Si el flag está activado, se transfieren mensajes de protocolo de suceso mediante la interfaz LAN. Valor estándar: Desactivado
Valor timer (s)	Indicación del tiempo (en segundos) que debe transcurrir para transferir datos de protocolo de sucesos mediante la interfaz LAN.

28.2.6.2 Sucesos > Protocolo sucesos

Esta función sirve para descargar o borrar el archivo de protocolo de sucesos.

Descripción de parámetros de las pestañas:

- **Cargar vía HTTP**
- **Borrar protocolo de sucesos**

28.2.6.3 Sucesos > Correo electrónico

Descripción de parámetros de las pestañas:

- **Editar ajustes e-mail**

Parámetros	Descripción
Ajustes de correo electrónico	
Asunto	Texto que aparece en el campo de Asunto de los correos electrónicos.
Direcciones e-mail receptor	
Receptor 1	Dirección de correcto electrónico donde se enviará un correo electrónico al producirse un suceso.
Receptor 2	Dirección de correcto electrónico donde se enviará un correo electrónico al producirse un suceso.
Receptor 3	Dirección de correcto electrónico donde se enviará un correo electrónico al producirse un suceso.
Receptor 4	Dirección de correcto electrónico donde se enviará un correo electrónico al producirse un suceso.
Receptor 5	Dirección de correcto electrónico donde se enviará un correo electrónico al producirse un suceso.
Destinatario de notificaciones de emergencia	
Destinatario de emergencia	Dirección de correo electrónico de un responsable de seguridad *in situ* a quien se le enviará un correo electrónico al marcar un número de emergencias.

28.2.6.4 Sucesos > Tabla reacción

Los administradores pueden valerse de la tabla de reacción para definir las reacciones ante todos los eventos posibles por separado.

Descripción de parámetros de las pestañas:

- **Editar todos los sucesos**
- **Restaurar todos los sucesos a la configuración predeterminada.**
- **Editar suceso**
- **Iniciar/Detener perfil trace asignado**

Parámetros	Descripción
Nombre suceso	Nombre del suceso
Enviar trap SNMP	Si el flag está activado, al producirse el suceso se envía un trap SNMP.
Enviar email	Si el flag está activado, al producirse el suceso se envía un correo electrónico al destinatario especificado en **Editar ajustes e-mail**.
Perfil trace asignado	Perfil trace que se debe iniciar o detener al producirse el suceso.
Iniciar perfil trace	Si el flag está activado, al producirse el suceso se inicia el perfil trace seleccionado.
Parar perfil trace	Si el flag está activado, al producirse el suceso se detiene el perfil trace seleccionado.
Reiniciar gateway	Indica si al producirse el suceso se reiniciará el sistema de comunicación.
Reiniciar gateway: Sí	Al producirse el suceso se reinicia el sistema de comunicación.
Reiniciar gateway: no	Al producirse el suceso no se reinicia el sistema de comunicación.
Informar a OpenScape	Indica si al producirse el suceso se envía un mensaje al sistema de comunicación.
Informar a OpenScape: Sí	Al producirse el suceso se envía un mensaje al sistema de comunicación.
Informar a OpenScape: no	Al producirse el suceso no se envía ningún mensaje al sistema de comunicación.

28.2.6.5 Sucesos > Protocolos diagnóstico

Aquí se muestran los protocolos diagnóstico (archivos de protocolo) que se generan automáticamente en los estados de sistema críticos.

Descripción de parámetros de las pestañas:

- **Extraer protocolos diagnóstico**
- **Borrar protocolos diagnóstico**

Parámetros	Descripción
Nombre de archivo	Nombre del protocolo de diagnóstico que se guarda en el sistema de comunicación (archivo de protocolo)
Tamaño (en bytes)	Tamaño del protocolo de diagnóstico in bytes

Parámetros	Descripción
Modificado	Fecha de modificación del protocolo de diagnóstico
Permisos	Atributos del protocolo de diagnóstico: • r = Autorización de lectura (Read) • w = Autorización de escritura (Write)

28.2.6.6 Sucesos > Señalización de alarmas

Aquí se seleccionan las extensiones (teléfonos del sistema con display, UP0 y HFA) que recibirán una notificación cuando la temperatura del sistema supere los 55 grados Celsius. Ser superado 60 grados Celsius, se apagarán de forma controlada o se desconectarán los módulos responsables del sobrecalentamiento (p.ej. OCAB, SLAD8/16).

Descripción de parámetros de las pestañas:

- **Modificar la señalización de alarmas**

Parámetros	Descripción
Temperatura del puerto de señalización de alarmas	
Extensión 1	1.er destino (extensión con teléfono del sistema).
Extensión 2	2.do destino (extensión con teléfono del sistema).
Extensión 3	3.ro destino (extensión con teléfono del sistema).

28.2.7 Reiniciar / Volver a cargar

Aquí se puede activar un reinicio (Restart) o una recarga (Reload) de OpenScape Business. También se puede apagar (Shutdown) OpenScape Business X de forma controlada. Además, se puede activar un reinicio (Restart) de la aplicación de Comunicaciones Unificadas (UC Smart o UC Suite) o de la UC Booster Card (Tablero de aplicaciones OCAB). Para poder hacer un apagado controlado de OpenScape Business X con un teléfono del sistema se puede definir un PIN. Con las interconexiones se pueden sincronizar los sistemas de comunicación interconectados.

28.2.7.1 Reiniciar / Volver a cargar > Reiniciar / Volver a cargar

Parámetros	Descripción
Sistema	

Parámetros	Descripción
Reiniciar sistema	Reinicio (Restart) controlado de OpenScape Business: • OpenScape Business S y OpenScape Business X: Se realiza un reinicio (Restart) controlado del sistema de comunicación. Si OpenScape Business X3/X5/X8 equipa una tarjeta UC Booster Card (Tablero de aplicaciones OCAB), la aplicación de UC (UC Smart o UC Suite) se reinicia (Restart) de forma controlada. • OpenScape Business UC Booster Server (Servidor de aplicaciones): realiza un reinicio (Restart) controlado de la parte de OpenScape Business y de la aplicación de UC (UC Suite).
Recargar sistema	Recarga (Reload) de OpenScape Business: • OpenScape Business S y OpenScape Business X: Se realiza una recarga (Reload) del sistema de comunicación. Después de arrancar, el sistema de comunicación se encuentra en estado básico. Todos los ajustes específicos del cliente y del país se eliminan (Distintivo de país del sistema = Alemania). El sistema de comunicación tiene la dirección IP estándar 192.168.1.2 y el área de direcciones IP interna 192.168.3.xxx. Se mantiene el registro de licencia. • OpenScape Business UC Booster Server: Se realiza una recarga de la parte OpenScape Business. Después de la inicialización la parte OpenScape Business se encuentra en estado básico. Todos los ajustes específicos del cliente de la parte OpenScape Business (por ejemplo, el directorio de usuarios) se han borrado. Se mantiene el registro de licencia. El sistema operativo no se restablece.
Apagar sistema	Apagado controlado de OpenScape Business X: • OpenScape Business X3/X5: El sistema de comunicación solo se puede volver a poner en servicio extrayendo y volviendo a enchufar la toma de red. • OpenScape Business X8: El sistema de comunicación solo se puede volver a poner en servicio apagando y volviendo a encender todas las fuentes de alimentación LUNA2.
Habilitar/Deshabilitar apagado	Definición de un PIN para activar el Shutdown (el apagado controlado del sistema de comunicación) con un teléfono del sistema
Reiniciar tablero de aplicaciones	Reinicio (Restart) controlado del tablero de aplicaciones OCAB, incluyendo la aplicación de UC (UC Smart o UC Suite): Al reiniciar el tablero de aplicaciones OCAB, se interrumpen las conexiones con todas las aplicaciones activas (por ejemplo, myPortal for Desktop y myAttendant). Una vez finalizado el inicio, se restablecen todas las condiciones automáticamente.
Aplicaciones	
Sincronizar red	Sincronización de sistemas de comunicación interconectados: Después de modificar números de teléfono, números de marcación directa o nombres, con la sincronización los datos se actualizan en todos los sistemas interconectados.

Parámetros	Descripción
Reiniciar aplicación de UC	Reinicio (Restart) controlado de la aplicación de UC (UC Smart o UC Suite): Al reiniciar la aplicación de UC, se interrumpen las conexiones con todas las aplicaciones activas (por ejemplo, myPortal for Desktop y myAttendant). Una vez finalizado el inicio, se restablecen todas las condiciones automáticamente.

28.2.8 SNMP

En **SNMP** se reunen las funciones para configurar comunidades y capturas ("traps"). Las comunidades regulan los derechos de acceso a los datos SNMP. Si surgen problemas en el sistema se crean traps para informar de los errores y fallos de funcionamiento al administrador.

28.2.8.1 SNMP > Comunidades

Descripción de parámetros de las pestañas:

- **Mostrar comunidades**

Parámetros	Descripción
Dirección IP	Dirección IP del interlocutor SNMP. Con la dirección 127.0.0.1, se bloquea la comunicación con direcciones IP externas.
Comunidad	Identificación/contraseña de acceso que se utiliza para el usuario SNMP. ***INFO:*** Para mayor seguridad es recomendable no utilizar el valor estándar **public**.
Tipo	Selección del tipo.
Tipo: Comunidad lectura	Interlocutor con acceso SNMP de lectura.
Tipo: Comunidad lectura	Interlocutor con acceso SNMP de lectura y escritura.
Tipo: Comunidad trap	Interlocutor al que se envían los mensajes de error (traps).

28.2.8.2 SNMP > Comunidades > Comunidades lectura

Descripción de parámetros de las pestañas:

- **Mostrar comunidades lectura**
- **Añadir comunidad de lectura**

Parámetros	Descripción
Dirección IP	Dirección IP del interlocutor SNMP. Con la dirección 127.0.0.1, se bloquea la comunicación con direcciones IP externas.

Parámetros	Descripción
Comunidad	Identificación/contraseña de acceso que se utiliza para el usuario SNMP. ***INFO:*** Para mayor seguridad es recomendable no utilizar el valor estándar **public**.

28.2.8.3 SNMP > Comunidades > Comunidades escritura

Descripción de parámetros de las pestañas:

- **Mostrar comunidades escritura**
- **Añadir comunidad de escritura**

Parámetros	Descripción
Dirección IP	Dirección IP del interlocutor SNMP. Con la dirección 127.0.0.1, se bloquea la comunicación con direcciones IP externas.
Comunidad	Identificación/contraseña de acceso que se utiliza para el usuario SNMP. ***INFO:*** Para mayor seguridad es recomendable no utilizar el valor estándar **public**.

28.2.8.4 SNMP > Comunidades > Comunidades trap

Descripción de parámetros de las pestañas:

- **Mostrar comunidades trap**
- **Añadir comunidad trap**

Parámetros	Descripción
Dirección IP	Dirección IP del interlocutor SNMP. Con la dirección 127.0.0.1, se bloquea la comunicación con direcciones IP externas.
Comunidad	Identificación/contraseña de acceso que se utiliza para el usuario SNMP. ***INFO:*** Para mayor seguridad es recomendable no utilizar el valor estándar **public**.

28.2.8.5 SNMP > Traps

Descripción de parámetros de las pestañas:

- **Mostrar todas traps**
- **Mostrar todas traps críticas**

Parámetros	Descripción
VarBind1 (Severidad)	Clasificación del trap: • Crítico: (Critical) Mensaje de error. El error es causa de problemas. • Mayor: (Major) Mensaje de error. El error puede tener causar problemas. • Menor: (Minor) Mensaje de error. El error no causa problemas. • Aviso: (Warning) Mensaje sobre un procedimiento o estado posiblemente problemático. • Borrado: (Cleared) El mensaje de error se ha anulado (por ejemplo, el puerto vuelve a estar en servicio) • Información: (Information) Mensaje de estado puro, ningún mensaje de error
VarBind2 (Nombre)	Nombre de la trap
Nombre genérico	Designación general como, por ejemplo Enterprise Specific
Nombre específico	Tipo del trapTraps: • 1 = Software • 2 = Hardware
Empresa	(no se usa)
Hora	Momento del error
El índice	Número consecutivo

28.2.9 Protocolo admin.

A través de **Protocolo admin.**, el administrador puede modificar la configuración (p. ej. el idioma) del protocolo administrativo.

28.2.9.1 Protocolo admin. > Configuración

Descripción de parámetros de la pestaña:

- **Editar config.**

Parámetros	Descripción
Idioma protocolo admin.	Configuración del idioma deseado para el protocolo admin. El protocolo admin. ofrece una vista general de los cambios realizados en el sistema de comunicación. Idiomas posibles: Alemán, Inglés, Francés, Español, Italiano, Portugués, Holandés

28.2.9.2 Protocolo admin. > Datos protocolo admin.

Descripción de parámetros de la pestaña:

- **Cargar vía HTTP**

Parámetros	Descripción
Cargar vía HTTP	Guarda el registro de administración del sistema de comunicación. El protocolo de administración permite saber qué cambios se han hecho en el sistema de comunicación y quién hizo tales cambios. Se registran los inicios de sesión en el sistema de comunicación.

28.2.10 Acciones

En **Acciones** se reunen las funciones que ayudan al administrador en las tareas administrativas más frecuentes, por ejemplo, borrar datos de protocolo.

28.2.10.1 Acciones > Acciones manuales > Protocolos de diagnóstico

Descripción de parámetros de las pestañas:

- **Cargar datos vía HTTP**

Parámetros	Descripción
Protocolo trace	Si el flag está activado, se descargan archivos de protocolo de trace del sistema. Hay las siguientes opciones: • Todo el protocolo de trace: se descargan todos los archivos de protocolo de trace del sistema existentes. • Protocolo de hoy: se descargan los archivos de protocolo de trace del sistema del día de hoy (a partir de las 00:00 horas). • Selección propia: De: Desde: XXX: Hasta: YYY: se descargan los archivos de protocolo de trace del sistema del periodo seleccionado. Valor estándar: Activado, Todo el protocolo
Protocolo de sucesos	Si el flag está activado, se descargan archivos de protocolo con datos sobre acciones o sucesos del sistema de comunicación (Reset, Encendido/ Apagado, etc.). Valor estándar: Activado
Protocolo de administración	Si el flag está activado se descargan archivos de protocolo con datos sobre procesos de administración (intentos de inicio de sesión, etc.). Valor estándar: Activado
Protocolos de licencia	Si el flag está activado, se descargan archivos de protocolo con mensajes sobre componentes del sistema de comunicación que necesitan licencia. Valor estándar: Activado
Trace de cliente	Si el flag está activado se descargan archivos de protocolo con mensajes para el trace de cliente (inicio de sesión remoto, inicio de sesión ITSP, etc.). Los mensajes para el trace de cliente se muestran de forma más detallada que, por ejemplo, en el protocolo trace. Valor estándar: Activado

Parámetros	Descripción
Protocolo Framework	Si el flag está activado, se descargan archivos de protocolo con mensajes de la Gestión basada en Web (WBM). Valor estándar: Activado
Protocolo de diagnóstico	Si el flag está activado se descargan protocolos de diagnóstico del sistema de comunicación. Valor estándar: Activado
Protocolos de UC Suite	Si el flag está activado, se descargan archivos de protocolo con mensajes de la UC Suite (protocolos de UC Suite, CSP y MEB). Hay las siguientes opciones: • Todo el protocolo de trace: se descargan todos los archivos de protocolo existentes de UC Suite, CSP y MEB. • Protocolo de hoy: se descargan los archivos de protocolo de UC Suite, CSP y MEB del día de hoy (a partir de las 00:00 horas). • Selección propia: De: Desde: XXX: Hasta: YYY: se descargan los archivos de protocolo de UC Suite, CSP y MEB del periodo seleccionado. Todos los archivos de protocolo se agrupan en un archivo comprimido. Para los protocolos OpenScape Business se aplican las siguientes designaciones de archivo: archivos de protocolo de UC Suite = vs_aaaa_mm_dd.log, archivos de protocolo CSP = csptrace_aaaa_mm_dd.log, archivos de protocolo MEB = mebtrace_aaaa_mm_dd.log Valor estándar: Desactivado
Protocolos de aplicación	Si el flag está activado, se descargan archivos de protocolo con mensajes de la parte de aplicaciones del sistema de comunicación (por ejemplo, protocolos CSP). • Todo el protocolo de trace: Se descargan todos los archivos de protocolo disponibles • Protocolo de hoy: se descargan los archivos de protocolo del día en curso (desde las 00:00 horas). • Selección propia: De: Desde: XXX: Hasta: YYY: se descargan los archivos de protocolo del periodo seleccionado. Todos los archivos de protocolo se agrupan en un archivo comprimido. Valor estándar: Desactivado
Protocolos de diagnóstico del sistema	Si el flag está activado se descargan protocolos de diagnóstico del sistema de comunicación. Valor estándar: Activado
Protocolo PPP	Si el flag está activado, se descargan archivos de protocolo con mensajes para el protocolo Point-to-Point. Valor estándar: Activado
Protocolo CoreLog	Si el flag está activado, se descargan archivos de protocolo con información sobre el estado más reciente del sistema operativo. Los CoreLogs se generan por ejemplo al reiniciar. Valor estándar: Desactivado

28.2.10.2 Acciones > Acciones manuales > Mantenimiento DLI

Descripción de parámetros de las pestañas:

- **Mantenimiento de dispositivos DLI**

Parámetros	Descripción
Eliminar dispositivo	Seleccione el teléfono del sistema que desea borrar. Con esta acción, el teléfono del sistema se elimina de la base de datos DLI. **Nota:** Antes de realizar cualquier acción de Mantenimiento DLI (eliminar), primero debe asegurarse de que el dispositivo ya no se encuentra en uso.
N° llam.	Número de teléfono del teléfono del sistema.
Tipo disposit.	Tipo del teléfono del sistema.
Dirección IP	Dirección IP del teléfono del sistema; enlace directo con la Gestión basada en Web (WBM) del teléfono del sistema.
Dirección MAC	Dirección MAC del teléfono del sistema.
Versión de software actual	Versión de software actual del teléfono del sistema.

28.2.10.3 Acciones > Acciones automát. > Garbage Collection

Descripción de parámetros de las pestañas:

- **Modificar acción**
- **Iniciar/Detener acción**

Parámetros	Descripción
Acción activada	Si el flag está activado, se realiza regularmente una limpieza de memoria automática en el sistema de comunicación. Siempre que termina una limpieza de memoria, el sistema de comunicación se reinicia (Restart). Valor estándar: Desactivado
Inicio después de medianoche	Hora, después de media noche, en que se ejecutará la acción Garbage Collection. Ejemplo: En el campo **h** se ha introducido 3 y en el campo **min.** 30. Esto significa que la acción Garbage Collection se iniciará mañana a las 3:30 h. Valor estándar: 3:00 horas
Ejecutar acción los sig. días de la semana	La acción Garbage Collection se ejecutará los días de la semana seleccionados. Valor estándar: Activado

28.2.10.4 Acciones > Acciones automát. > Notificación DLS

Descripción de parámetros de las pestañas:

- **Modificar acción**
- **Iniciar/Detener acción**

Parámetros	Descripción
Acción activada	Si el flag está activado, al iniciar el sistema de comunicación se inicia el inicio de sesión automático en un servidor DLS externo. Valor estándar: Desactivado
Dirección IP	Dirección IP del servidor DLS externo Valor estándar: 0.0.0.0
Puerto	Puerto del servidor DLS externo Valor estándar: 10444
Nombre de usuario	Nombre de usuario para iniciar sesión en el servidor DLS externo
Contraseña	Contraseña para iniciar sesión en el servidor DLS externo

28.2.10.5 Acciones > Acciones automát. > Comprobación de mantenimiento SDHC

Descripción de parámetros de las pestañas

- Comprobación de mantenimiento SDHC

Parámetros	Descripción
Comprobación de mantenimiento SDHC	
Iniciar comprobación de mantenimiento	Permite comprobar al instante el estado de la tarjeta
Iniciar comprobación de mantenimiento el	Permite indicar un día, mes, año y hora para la verificación del estado de la tarjeta.
Archivo de protocolo Se muestra el resultado de las últimas comprobaciones de archivos.	
Estado / Acción recomendada Recomiende acciones para cada estado de tarjeta.	

28.2.11 Diagnóstico de plataforma

Permite hacer un diagnóstico de plataforma (solo para desarrollo).

28.2.12 Diagnóstico de aplicación

Permite realizar un diagnóstico de aplicación (solo para desarrollo).

28.2.12.1 Diagnóstico de aplicación > Configuración del desarrollador > Salida de consola trace

Permite realizar un diagnóstico de aplicación (solo para desarrollo).

28.2.12.2 Diagnóstico de aplicación > Configuración del desarrollador > Asumir permiso de escritura

Permite realizar un diagnóstico de aplicación (solo para desarrollo).

28.2.12.3 Diagnóstico de aplicación > Placa base

Solo hay que modificar la configuración si así lo solicita el soporte técnico responsable.

28.2.12.4 Diagnóstico de aplicación > Configuración del desarrollador > Perfiles de proveedor SIP

Descripción de Parámetros de las pestañas:

- Añadir perfiles de proveedor SIP
- Editar perfiles de proveedor SIP

Esta página está dirigida a los técnicos formados que realizan la certificación de un ITSP nuevo. Para obtener más información, consulte la documentación disponible en la wiki de Unify: http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#How_to_get_a_new_VoIP_provider_released.

28.2.13 Diagnóstico de IP

Permite realizar un diagnóstico de IP (solo para desarrollo).

28.2.13.1 Diagnóstico de IP > Placa base > Protocolo ARP

Esta función permite visualizar los datos del protocolo ARP (Address Resolution Protocol). La tabla de Mapping muestra la asignación de las direcciones de red a las direcciones MAC.

Descripción de parámetros de las pestañas:

- **Mostrar protocolo ARP**

Parámetros	Descripción
Dirección IP	Muestra las direcciones de red conectadas en ese momento en la placa base del sistema de comunicación.
Dirección MAC	Muestra la dirección física correspondiente de las direcciones de red conectadas

Parámetros	Descripción
Tipo	Muestra la asignación de las direcciones. Puede ser una dirección fija (estática) o dinámica.
Interfaz	Denominación interna de las interfaces LAN presentes (p. ej., eth0, eth1, eth2, eth3)

28.2.13.2 Diagnóstico de IP > Placa base > Solicitud ICMP > Ping

Esta función permite comprobar la conexión de red entre el sistema de comunicación y una dirección de destino cualquiera mediante el comando Ping (solicitud eco).

Descripción de parámetros de las pestañas:

- **Ejecutar ping**

Parámetros	Descripción
Parámetro ICMP	
Dir. destino	Dirección IP del destino cuya conexión de red con el sistema de comunicación se quiere comprobar mediante paquetes de solicitud eco. Valor estándar: 127.0.0.1
Cant. de solicit. eco por enviar	Número de paquetes de solicitud eco que se van a enviar para comprobar la conexión de red Valor estándar: 3

28.2.13.3 Diagnóstico de IP > Placa base > Solicitud ICMP > Traceroute

Esta función permite determinar, mediante solicitudes eco ICMP, a través de qué router se transfieren paquetes de datos hasta la dirección de destino consultada.

Descripción de parámetros de las pestañas:

- **Traceroute**

Parámetros	Descripción
Parámetro ICMP	
Dir. destino	Dirección IP del destino cuyo traceroute con el sistema de comunicación se comprueba mediante solicitudes eco ICMP. Valor estándar: 127.0.0.1
Byte TOS	Indicación de si se envían bytes TOS (Tipo de servicio). Los bytes TOS ofrecen información sobre la calidad de un servicio. Rango de valores: de 0 a 255, valor estándar: 0

28.2.14 Usuario online

Herramienta Web para el control remoto de teléfonos OpenStage.

28.2.14.1 Usuario online

Con el Usuario online se abre el Java Husim Phone Tester (jHPT). Se trata de una herramienta web para el control remoto de teléfonos OpenStage por Internet. Mediante una interfaz Web se controla un teléfono del sistema de forma que se transmiten las pulsaciones de teclas reales y la visualización del sistema de comunicación. Para jHPT hay documentación independiente que se puede descargar mediante la función de ayuda de la herramienta (aquí no se ofrecen más detalles de las páginas jHPT).

28.3 Telefonía

En **Telefonía** se reunen las funciones para la configuración de la telefonía, por ejemplo, para configurar extensiones o la Gestión de llamadas (CM, Call Management).

28.3.1 Ajustes básicos

En **Ajustes básicos** se reunen funciones como, por ejemplo, Flags del sistema, ajustes de directorios y destinos de marcación abreviada, DynDNS, calidad del servicio, Fecha y hora y Tasas de llamada.

28.3.1.1 Ajustes básicos > Sistema > Flags del sistema

Descripción de parámetros de las pestañas:

- **Editar flags del sistema**

Parámetros	Descripción
Interconectar en caso de DESV externo act	Si el flag está activado, las llamadas se interconectan inmediatamente en caso de desvío externo. La interconexión se realiza en todas las llamadas, ya sean externas o internas (líneas urbanas analógicas/RDSI). Si el desvío de llamadas se realiza a través de una línea urbana RDSI y el destino del desvío externo se encuentra en otra red (por ejemplo, la red GSM), el establecimiento de conexión de la línea urbana RDSI se señaliza con el indicador de progreso "Leaving ISDN". A partir de ese momento, el llamante está sujeto a costes de conexión. Valor estándar: Desactivado
Desvío tras HKZ permitido	Si el flag está activado, tras el desvío de llamadas externo siguen llamadas a través de líneas urbanas analógicas (HKZ). Valor estándar: Activado

Parámetros	Descripción
Transfer. autom. diferida tras desvío a dest. ext.	Si el flag está activado y no se puede acceder al destino del desvío externo, se produce una transferencia automática diferida al siguiente destino registrado en la lista de destinos. Valor estándar: Desactivado
Tono de conferencia	Si el flag está activado, cada 20 segundos, un tono especial avisa a los participantes en una conferencia de que están participando en ella. Valor estándar: Desactivado
Señal de advertencia para grupos de telecaptura	Si el flag está activado, los miembros de los grupos de telecaptura reciben una indicación visual (Display) si otro miembro del grupo tiene una llamada. Si la llamada no se acepta en cuatro ciclos de llamada (4x5 segundos), los demás miembros del grupo reciben también un tono de advertencia. Valor estándar: Activado
Elevar el volumen de voz para terminales optiPoint/ OpenStage	Si el flag está activado, en el caso de los teléfonos optiPoint y OpenStage, se conmuta a un plan de atenuación alternativo y, con ello, se consigue un mayor volumen de altavoces. Valor estándar: Desactivado
Permitido cambio de terminales	Si el flag está activado, los teléfonos del sistema cambiar de posición física (Relocate/Reasignación) sin tener que modificar la configuración lógica (número de teléfono, nombre, programación de teclas, etc.). Valor estándar: Desactivado
Más de 1 miembro de conferencia externo	Si el flag está activado, pueden participar varias extensiones externas en una conferencia. Valor estándar: Activado
Reserva de línea automática	Si el flag está activado, una extensión puede reservar una línea si no tiene disponible ninguna línea urbana libre. En cuanto la línea vuelve a estar libre, recibe una llamada recordatoria y, a continuación, puede establecer la conexión externa. Valor estándar: Desactivado
Rellamada con PKZ	Si el flag está activado, en las rellamadas se repite el número de teléfono y el código de proyecto (PRO/PKZ) introducido previamente. Valor estándar: Desactivado

Parámetros	Descripción
Ocupación automática de ruta	Cuando se activa este flag, al marcar un solo dígito en un teléfono del sistema, inmediatamente se activa una ocupación de línea y se marca el número de llamada requerido. No es necesario marcar el código de acceso. Para marcar una extensión interna, se debe utilizar uno de los procedimientos siguientes: • Presione la tecla Interno (Mute cambiará a Interno, si la marcación simple está activa) y marque el número de la extensión • o presione la tecla DSS correspondiente. Esta función solo está disponible si se ha configurado únicamente una ruta (véase Rutas). Si Entry, RDSI o los teléfonos a/b siguen conectados al sistema de comunicación, LCR con marcación automática no es posible.
Utilizar sólo números configurados para MSN	Si el flag está activado, en un Bus S0 los MSN (Multiple Subscriber Number) solo se pueden configurar para números de teléfono internos ya existentes (para impedir posibles fraudes de consumo). Valor estándar: Desactivado
Optimación de rutas	Si el flag está activado, en los sistemas de comunicación interconectados se realiza una optimización de rutas. El flag debe activarse en todos los sistemas de comunicación pertenecientes a una interconexión. Ejemplo de dos sistemas interconectados (sistema 1 y sistema 2): si se produce una llamada de la extensión A (sistema 1) a la extensión B (sistema 2) y, a continuación, se realiza un desvío de llamadas a la extensión C (sistema 1) se ocupan dos líneas. Mediante la optimación de rutas, la conexión de A a C se conmuta automáticamente a través de una única línea. Valor estándar: Activado
MF automático	Si el flag está activado, después de cada establecimiento de una llamada saliente realizado correctamente se conmuta de forma automática al modo Multifrecuencia (DTMF). De esta forma, por ejemplo, se permite la consulta remota de contestadores automáticos. Valor estándar: Activado
Búsqueda con comunicación bilateral	Si el flag está activado, la función de mensaje directo (Paging) permite establecer una conexión interna sin que la extensión llamada descuelgue el microteléfono. Al descolgar el microteléfono se pasa a una llamada bipartita normal. Valor estándar: Activado
Tono de la central	Si el flag está activado, las conexiones también se conmutan a la línea urbana o a un sistema de comunicación interconectado si el interlocutor no envía ningún tono de señal. Valor estándar: Desactivado
Bloqueo de llamadas a cobro revertido	Si el flag está activado, las llamadas a cobro revertido se inician automáticamente. Valor estándar: Desactivado

Parámetros	Descripción
Euroimpedancia	Si el flag está activado, se aplican los siguientes valores de impedancia en Europa: Interfaces a/b para la conexión de extensión analógica: impedancia de entrada = 270 ohmios + 750 ohmios || 150 nF, impedancia de equilibrio = 270 ohmios + 750 ohmios || 150 nF, umbral relativo A/D = 0 dBr, umbral relativo D/A = –7 - 7 dBr Interfaces a/b para la conexión urbana analógica: impedancia de entrada = 270 ohmios + 750 ohmios || 150 nF, impedancia de equilibrio = 270 ohmios + 750 ohmios || 150 nF, umbral relativo A/D = –6 - 6 dBr, umbral relativo D/A = –1 - 1 dBr Valor estándar: Desactivado
Diferentes anuncios de Phonemail día/noche	Si el flag está activado (y el sistema de comunicación tiene buzón de voz) se pueden activar diferentes anuncios grabados del buzón de voz para una extensión. Al hacerlo se transmiten diferentes números de teléfono para la extensión al buzón de voz. Con tal fin es necesario configurar para la extensión distintas transferencias automáticas diferidas para el servicio diurno y nocturno. Valor estándar: Desactivado
Indicar codigo International / national	Si el flag está activado, se define el formato de visualización de los números de marcación abreviada central (KWZ) en las llamadas entrantes para las que no hay memorizado un nombre en la memoria de marcación abreviada central. Cuando se produce una llamada entrante, en la pantalla del teléfono se muestra el número de teléfono completo (número de teléfono del sistema + marcación directa, con código de red local y prefijo del país, si está disponible). Ejemplo: el número de marcación abreviada central 06671234 se ha configurado sin nombre. Código de red local = 02302, número de teléfono del sistema = 667, número de marcación directa DID = 1234. En el caso de una llamada entrante desde 6671234, aparece el número 023026671234 en la pantalla. Valor estándar: Desactivado
Cambio de línea para llamada directa	Con este flag se define el comportamiento de una tecla de llamada directa, si hay una conexión de llamada activa en una línea MULAP. Relevante para Configuración de equipo / grupo Team, grupo Top/Jefe/Secretaria, MULAP básico, MULAP Jefe. Después de pulsar una tecla de llamada directa se realiza un cambio de línea. Se retiene la conversación y solo se puede retomar en ese teléfono. Valor estándar: desactivado (no para EE. UU., Canadá), activado (solo para EE. UU., Canadá)
Repetición de llamada automática	Si la extensión está ocupada se realiza una repetición de llamada automática. A través del parámetro de tiempo Tiempo para repetición de llamada automática se define el tiempo tras el que se activa la repetición de llamada. Valor estándar: Desactivado

Parámetros	Descripción
Número de llamada de nodo en caso de mensaje de voz	Si el flag está activado, en los sistemas de comunicación interconectados se define si el número de llamada de nodo se debe incluir en la identificación de un servidor de buzón de voz central o de varios servidores descentralizados. El número de llamada de nodo se debe incluir para la identificación del servidor o servidores de buzón de voz. Valor estándar: Desactivado
Telecaptura de llamadas después de llamada recordatoria	Si el flag está activado, las rellamadas y devoluciones de llamada también se señalizan en los demás miembros de un grupo de telecaptura y dichos miembros pueden aceptarlas. Valor estándar: Desactivado
CLIP ajustable	Si el flag está activado, en lugar del número de teléfono en sí, se transfiere el número introducido en Clip/Lin a la conexión externa llamada y dicho número se muestra en la pantalla. Si la entrada Clip/Lin está vacía, se transfiere el número de teléfono. Valor estándar: Activado
Lista de llamantes en la extensión de destino en caso de desvío MULAP	Si el flag está activado, en caso de desvío MULAP, las llamadas entrantes se registran en la lista de llamantes de la extensión de destino. Valor estándar: Desactivado
Transferencia de llamadas tras Deflect call / Transferencia paso individual	Si el flag está activado, si una extensión ha activado un desvío de llamadas a un destino interno (Deflect Call), la llamada se señaliza en este destino. Una vez finalizado el tiempo de transferencia de llamadas, la llamada se señaliza en el primer destino registrado en la lista de destinos de llamada y, a continuación, en el segundo destino registrado (si lo hay). Ejemplo: para la extensión A se ha realizado un Deflect Call a la extensión B. El primer destino registrado en la lista de destinos de llamadas de la extensión B es la extensión C y el segundo destino es la extensión D. La llamada se señaliza en la extensión C y, una vez finalizado el tiempo de transferencia de llamadas, se señaliza en la extensión D. Solo resulta conveniente activar este flag, si también se ha activado el flag Determinación del destino mediante lista de destinos llam. durante Deflect call. Para que este flag tenga efecto, las funciones de desvío tendrán lugar durante la llamada, Deflect call/Transferencia paso individual, y se aplica principalmente a las llamadas administradas mediante UC (Auto Attendant/ Grupos UCD) en las que se apliquen dichas funciones de desvío. Valor estándar: Activado

Parámetros	Descripción
Determinación del destino mediante lista de destinos llam. durante Deflect call	Si el flag está activado, si una extensión ha activado un desvío de llamadas a un destino interno (Deflect Call), las llamadas se señalizan en ese destino. Una vez finalizado el tiempo de transferencia de llamadas se señalizan también en otros destinos registrados en la lista de destinos de llamada. Ejemplo: para la extensión A se ha realizado un Deflect Call a la extensión B. El primer destino registrado en la lista de destinos de llamadas de la extensión B es la extensión C. Una vez finalizado el tiempo de transferencia de llamadas, se señaliza en la extensión C. Para que este flag tenga efecto, las funciones de desvío tendrán lugar durante la llamada, Deflect call/Transferencia paso individual, y se aplica principalmente a las llamadas administradas mediante UC (Auto Attendant/ Grupos UCD) en las que se apliquen dichas funciones de desvío. Valor estándar: Activado
Tono de aviso durante grabación de voz	Si el flag está activado, se aplica lo siguiente para OpenScape Business X: si la grabación de voz (Live Call Record) está activada durante una llamada y el flag está definido, se emite un tono de aviso. Valor estándar: Activado
Numeración E.164	Este flag se usa para activar o desactivar la red de la memoria de datos de cliente (KDS) de sistemas de varias ubicaciones o de clientes de todo el mundo. Se puede acceder a las extensiones desde un número de teléfono público (número E.164) en el formato nacional o internacional (por ejemplo, número de llamante para la llamada interna en formato RDSI), sin marcar antes un número de nodo. Cada extensión está representada por su número E.164, que se puede presentar de forma optimizada. Si el flag está activado, el número de llamada interna se transfiere en formato E.164. Si este flag está establecido, las extensiones SIP se registran con la versión larga del número de llamada E.164 (número de emplazamiento + número de llamada interna, por ejemplo 4923026673665). Valor estándar: Desactivado
Funcionalidad ampliada de teclas	Si el flag está habilitado, una vez que una tecla se define como "tecla Mayús", solo se pueden guardar números de teléfono sin soporte de LED en el segundo nivel de la tecla que ahora está disponible. Se puede programar cualquier función de tecla en el primer nivel de la tecla. La señalización LED está asociada solo con el primer nivel de la tecla. Valor estándar: Desactivado
Número de llamada en grupos de telecaptura / timbre adicional / desvío de llamada en caso de no contesta / caso de libre	Si el flag está activado, se define si el número de teléfono y el nombre de un llamante se mostrarán en todos los miembros de un grupo de telecaptura, en las extensiones conectadas (Timbre adicional) y en los destinos de desvío de llamada en caso de no contesta y en caso de libre. El número de teléfono y el nombre se muestran en la pantalla. Valor estándar: Activado

Parámetros	Descripción
Soporte SPE	Si el flag está activado, se admite la prestación de Cifrado de señalización y carga útil (SPE). Los flujos de datos de señalización y uso de VoIP procedentes del sistema de comunicación, dirigidos a él o intercambiados entre los teléfonos de sistema OpenStage se cifran. Valor estándar: Desactivado **Nota:** Si desea utilizar el Servicio en la nube Unify Video, debe desactivar el **Soporte SPE** para registrar la línea urbana, a menos que haya un certificado SPE importado en el sistema.
Tono resp. SPE	Si el flag está activado, si también está activado el flag del sistema Soporte SPE y se utiliza un teléfono OpenStage 15, 20, 20 E o 20 G, las extensiones indican que se está produciendo una conexión sin cifrar con un tono de aviso y una indicación en pantalla. Es necesario habilitar el parámetro de extensión Seguridad de Payload para utilizar SPE mediante una extensión. Si se utiliza un teléfono OpenStage 40, 40 G, 60, 60 G, 80 o 80 G no se emite ningún tono de aviso. El estado de la conexión (cifrada/sin cifrar) se muestra permanentemente en la pantalla. Valor estándar: Desactivado **Nota:** Si desea utilizar el Servicio en la nube Unify Video, debe desactivar el **Tono resp. SPE** para poder registrar la línea urbana, a menos que haya un certificado SPE importado en el sistema.
Tránsito de proveedor SIP a proveedor SIP	Si el flag está activado, se permiten las conexiones de línea de tránsito con conexiones de ITSP. Una conexión de línea de tránsito aparece si una llamada ocupa dos líneas del mismo sistema de comunicación. Ejemplo: se realiza una llamada externa a una extensión interna mediante un ITSP. A continuación, la extensión interna transfiere la llamada a través de un ITSP a un destino externo. De esta forma se establece conexión de líneas de tránsito dentro del sistema de comunicación. Durante la llamada hay ocupadas dos líneas. Se permiten las conexiones de líneas de tránsito resultantes. Valor estándar: Desactivado
Marcación de * y # en las interfaces de línea	Si el flag está activado, las prestaciones Centrex se pueden activar y desactivar mediante líneas IP y líneas urbanas RDSI. Distintos proveedores ofrecen prestaciones Centrex (Central Office Exchange) que se pueden activar y desactivar mediante códigos. Los códigos se deben introducir en estado de marcación (por ejemplo, después de introducir el código de línea). La entrada comienza siempre por * (asterisco) o # (almohadilla). A continuación, hay que introducir el código en sí (cifras del 0 al 9). La entrada finaliza con # (tecla de almohadilla). En el estado de conversación no se pueden activar ni desactivar prestaciones Centrex. Se pueden activar y desactivar prestaciones Centrex mediante líneas IP (ITSP) y líneas urbanas RDSI. Valor estándar: Desactivado

Parámetros	Descripción
Añadir código de ruta para MEX	Solo es válido para llamadas externas realizadas a través de la prestación ITSP "Mobile Extension (MEX)". Si el flag está activado, cuando se realizan llamadas salientes externas, el sistema añade automáticamente el código urbano al número de teléfono si este tiene más de 7 cifras, ya que lo interpreta como un número de teléfono externo. Si el número de teléfono tiene menos de 7 cifras, no se añade el código urbano, ya que el sistema lo interpreta como un número de teléfono interno. Si el flag está desactivado, el proveedor de servicios debe añadir el código urbano al número de teléfono en todas las llamadas salientes ternas. Valor estándar: Desactivado
Timbre CMI MWI	Si el flag está activado, el timbre de MWI (indicación de mensaje en espera) está desactivado para los teléfonos DECT (CMI: Cordless Multicell integration). Al recibir mensajes nuevos en el buzón de voz se emite un timbre de aviso. Valor estándar: Desactivado
Actualización automática de software de teléfonos Openstage	Si este flag está habilitado, cuando la versión de software de un teléfono TDM es más antigua que la versión de software del sistema, el software del teléfono se actualiza automáticamente. Valor estándar: Activado
Restringir conexiones de grupo de líneas indirectas según matriz VBZ	Si una empresa tiene sucursales en varias ciudades, cada sucursal puede tener una línea con el proveedor nacional de telecomunicaciones. Estas sucursales también se pueden conectar entre sí a través de líneas cruzadas privadas. Por motivos de legislación nacional, por ejemplo en la India, puede ser ilegal realizar la conexión siguiente: una extensión utiliza la línea cruzada privada para su sistema de comunicaciones con un sistema de comunicaciones privado de otra ciudad, y después un proveedor nacional de telecomunicaciones urbanas para acceder a un destino externo local. En este caso, para llamadas interurbanas se debe utilizar un proveedor nacional de telecomunicaciones urbanas. Este requisito se implementa de la siguiente manera: • Las conexiones entre líneas cruzadas privadas se pueden restringir mediante la configuración de la matriz de VBZ. • En el caso de líneas cruzadas privadas que requieren las funciones Transferencia automática diferida, Transferir y Conferencia, se incorporó el flag "Restringir las conexiones del haz de línea indirecto según la matriz VBZ". La activación o la desactivación de este flag tiene los efectos siguientes: – Activado: se restringen las llamadas interurbanas que utilizan líneas cruzadas privadas. – Desactivado: se permiten las llamadas interurbanas que utilizan líneas cruzadas privadas. Valor estándar: Desactivado
Numeración abierta	

Parámetros	Descripción
activo	Si se usa numeración abierta, una extensión se identifica por el número de llamada de nodo seguido de su número de llamada o número de marcación directa. De este modo, se puede asignar el mismo número de llamada a extensiones en diferentes nodos. En un sistema interconectado, este flag es siempre igual para todos los sistemas. Valor estándar: Desactivado
Número de llamada de nodo	En caso de numeración abierta, hay que introducir aquí el número de llamada de nodo. Solo se puede contactar una extensión desde otro nodo marcando el número de llamada de ese nodo seguido del número de llamada de extensión. Si la suma de cifras del número de llamada de nodo y del número de llamada de extensión es superior a 7 dígitos aparece el correspondiente mensaje de advertencia. Valor estándar: Desactivado
Permiso de tránsito	
Prestación tránsito	Si el flag está activado, se permiten las conexiones de tránsito vinculadas a determinadas prestaciones como, por ejemplo, desvío de llamadas externo, transferencia y aplicaciones DISA. No importa que se trate de conexiones de enlace directo o de línea urbana a línea urbana. Valor estándar: Activado
Marcación directa tránsito-enlace directo	Si el flag está activado, se permiten las conexiones de tránsito en la marcación directa con conexiones cruzadas (sistemas de comunicación interconectados). Valor estándar: Activado
Marcación directa tránsito-central	Si el flag está activado, se permiten las conexiones de tránsito en la marcación directa con conexiones entre líneas urbanas. Valor estándar: Desactivado
Interruptor especial	
no enviar CALL PROC	Este flag debe estar activado si el proveedor de servicios no ha recibido ningún mensaje RDSI (Call Proceeding) procedente del sistema de comunicación. Valor estándar: Desactivado
Ocupación de línea cíclica, autom.	Si el flag está activado, las llamadas salientes ocuparán cíclicamente nuevas líneas urbanas RDSI si el establecimiento de conexión falla (p.ej., en ausencia de confirmación ACK). Los números de línea o de ruta van subiendo. Valor estándar: Activado
Restricción de llamadas UC	
Restricción de llamadas UC	Si el flag está activado, con todas las llamadas UC iniciadas por el sistema (p.ej. mediante servicio CallMe) se comprueba antes de marcar si el usuario UC que solicita la llamada está autorizado. Si el usuario UC no está autorizado, no se realiza la llamada. Valor estándar: Desactivado

28.3.1.2 Ajustes básicos > Sistema > Parámetros de tiempo

En la tabla aparecen indicados todos los parámetros de tiempo que se pueden ajustar (columna **Descripción**). En las columnas **Base** y **Factor** se puede ajustar el valor del temporizador para el parámetro de tiempo correspondiente. Donde la hora es = Base x Factor. Si se registra el valor 255 en la columna **Factor**, este temporizador quedará sin efecto.

Descripción de parámetros de las pestañas:

- **Modificar parámetros de tiempo**

Parámetros	Descripción
NoFe Tiempo marc. posterior receptor códigos - tiempo conexión	Controla la duración de la conexión entre el receptor de códigos y las unidades de terminal Multifrecuencia y, por tanto, controla también la condición de preparado para marcar. Cuando expira este temporizador, el receptor de códigos queda liberado. Rango de valores: 5 - 15 s
Tiempo para la activación de prestaciones NoFe	Se activa si se pulsa la tecla de señalización de un terminal. Esta tecla sirve para distinguir si el abonado desea retirar una llamada de consulta retenida o si lo que desea es activar una función, por ejemplo, conferencia. Rango de valores: 2 - 4 s
Tiempo de bloqueo para nueva ocupación	Se activa en caso de circuitos de línea y, hasta que expira, no se permite ocupar de nuevo la línea en sentido saliente. Rango de valores: 0 - 5 s
Tiempo de retardo de devolución de llamada	Comienza cuando el terminal pasa a reposo. Una vez transcurrido el tiempo se comprueba si hay que realizar devolución de llamada automática. De este modo, la extensión tiene la oportunidad de realizar nuevas llamadas salientes. Rango de valores: 0 - 60 s
Duración de la devolución de la llamada	Si no se contesta la devolución de llamada automática durante el tiempo de este temporizador, se finaliza la llamada y se pospone la devolución de llamada. Rango de valores: 15 - 60 s
Tiempo de interceptación para llamada recordatoria	Cuando no se contesta una llamada recordatoria automática (de que ha habido una transferencia) en el transcurso de un tiempo determinado, la conexión se transfiere a la consola de operadora, siempre y cuando se haya seleccionado este criterio de interceptación. Rango de valores: 20 - 600 s
Duración de llamada para transf. antes de contestar	Si una llamada transferida antes de contestar (a una extensión ocupada) no se contesta dentro de este periodo de tiempo, la llamada recordatoria se produce en la extensión que ha transferido la llamada. Rango de valores: 30 - 600 s

Parámetros	Descripción
Fin de marcación en caso de marc. incompleta (solo en Austria)	Temporizador de supervisión para marcación directa. En caso de que no se realice una selección en el transcurso de un tiempo determinado, la marcación directa queda reconocida como incompleta o sin realización de llamada. (Solo aplicable en Austria). Rango de valores: 10 - 30 s
Tiempo fin de marcación (sin marcación)	En caso de que no se realice una selección en el transcurso de un tiempo determinado, se genera de forma automática un fin de marcación. Rango de valores: 5 - 15 s
Tiempo entre el 1.er y el 2.° anuncio grabado para Fax/ DuWa	Fax/N.° llam. marc. directa, marcación directa analógica, tiempo después de anuncio grabado. Valor estándar: 15 s
Tiempo para aparcar + transic. a retención	En el transcurso de un tiempo determinado debe tener lugar la reactivación de la llamada que se encuentre aparcada. Si durante este tiempo no se ha contestado esta llamada aparcada (recuperación), se lleva a cabo una llamada recordatoria automática dirigida a la extensión que hubiera aparcado la llamada. Mediante dicha llamada, la comunicación abandona el estado de retención y se transforma en llamada. Rango de valores: 60 - 255 s
Fin marcación en caso de marcación incompleta	Si no se prosigue la marcación en el transcurso de un tiempo determinado, se genera de forma automática un fin de marcación. Rango de valores: 10 - 20 s
Ext. AB Tiempo flash mínimo	Se establece un tiempo mínimo para el reconocimiento de la señal de flash, durante el que se deberá interrumpir el bucle de abonado. Valor estándar: 0 s
Tiempo flash NoFe máximo	Se establece un tiempo máximo para el reconocimiento de la señal de flash, durante el que se puede interrumpir el bucle. Valor estándar: 0 s
Tiempo para activación de llam. recordatoria en PO	Si una llamada recordatoria automática no se atiende en la consola de operadora en el transcurso de un tiempo determinado, se efectúa la liberación de la conexión. Rango de valores: 30 - 180 s
Tiempo previo contacto NSA	Tiempo de retención previo para el contacto normalmente abierto de diales de rueda (NSA). Sirve para evitar ruidos de marcación en los auriculares de aparatos DEC (antes del impulso). Valor estándar: 0 s
Tiempo posterior contacto NSA	Tiempo de retención posterior para el contacto normalmente abierto de diales de rueda (NSA). Sirve para evitar ruidos de marcación en los auriculares de aparatos DEC (después del impulso). Valor estándar: 0 s

Parámetros	Descripción
Tiempo supresión errores para llamada	Tiempo para ocultar los fallos de línea en la marcación DEC. Valor estándar: 0 s
Fin de marcación para marc. 1A	Indica el tiempo tras el que se marcará el último dígito con el procedimiento de marcación 1A. La salida de marcación de cada dígito tiene lugar después de que se haya introducido el dígito siguiente. El último dígito se marca tras expirar el temporizador o si la extensión lo ha señalado con el indicativo de fin de marcación (#). Rango de valores: 4 - 4,5 s
Tiempo posterior tarificación	Cuando se libera una línea de enlace, el sistema de comunicación puede analizar durante este periodo la información entrante sobre tarificación (impulsos de tarificación) en el caso de líneas analógicas. Durante este periodo, la línea de enlace queda bloqueada para la realización de llamadas salientes. Valor estándar: 0 s
Tiempo marc. intermedia para DEC	Pausa permitida entre dígitos con la marcación DEC. Valor estándar: 10 s
Tiempo supervisión tono marcación	Indica el tiempo de espera hasta que se dispone de tono de marcación al ocupar un tronqueo. En caso de que expire este temporizador, el sistema funciona teniendo en cuenta que ha ocurrido un fallo en la línea de enlace. Se marca esta línea de enlace como "en fallo". Valor estándar: 10 s
Tiempo pausa para DEC	La marcación DEC se realiza mediante secuencias de impulso-pausa, detección de pausas en líneas DEC. Valor estándar: 0 s
Tiempo impulso para DEC	La marcación DEC se realiza mediante secuencias de impulso-pausa. Detección de pausas en líneas DEC. Valor estándar: 0 s
Tiempo flash para PABX	Tiempo de interrupción en bucles de extensión, para activar las funciones de control (p. ej., Consulta) en la instalación. Valor estándar: 0 s
Tiempo flash para servicio centr. púb.	Tiempo de interrupción en bucles de extensión, para activar las funciones de control (p. ej., Consulta) en la línea analógica. Valor estándar: 0 s
Tiempo imp. mín. para NoFe DEC	La marcación DEC se realiza mediante secuencias de impulso-pausa. Detección de impulsos del teléfono DEC. Valor estándar: 0 s
Tiempo imp. máx. para NoFe DEC	La marcación DEC se realiza mediante secuencias de impulso-pausa. Detección de impulsos del teléfono DEC. Valor estándar: 80 ms

Parámetros	Descripción
Tiempo emisión para señales MF	Duración de las señales de marcación MF, valor específico del país. Valor estándar: 80 ms
Tiempo pausa entre señales MF	Pausa entre las señales de marcación MF, valor específico del país. Valor estándar: 80 ms
Temporizador retardo de MOH (música en espera)	Si así se ha configurado, en caso de que se produzca una retención en una conexión, se activa la señal de música en espera (MOH). El paso a música en espera (MOH) tiene lugar tras la finalización de este periodo, para garantizar que la activación de determinadas funciones, como conferencia, no se ve interferida por la activación de música en espera (MOH). Rango de valores: 1 - 5 s
Liberar si no se produce la marcación (solo para desarrollo)	Si se lleva a cabo la ocupación de una línea de enlace y en el transcurso de un tiempo determinado no se produce ninguna marcación, se libera la conexión. Valor estándar: 3 s
Pausa de tarificación min	Tiempo entre impulsos de tarificación (minutos). Valor estándar: 0 min.
Impulso tarificación min	Duración de los impulsos de tarificación (minutos). Valor estándar: 0 min.
NSA Tiempo impulso contest.	Contacto siempre abierto del dial de rueda (líneas DEC). Valor estándar: 0 s
NSA Tiempo impulso ocupación	Contacto siempre abierto del dial de rueda (líneas DEC). Valor estándar: 0 s
Liberar si no se produce marcación	Si se produce una ocupación de línea y en un intervalo de tiempo determinado no se ha producido marcación, la conexión se libera. A la extensión solicitante se le señaliza un tono de ocupado. Rango de valores: 5 - 30 s
DEC NoFe Tiempo marc. intermedia mín.	Tiempo entre dígitos de marcación en los teléfonos DEC. Valor estándar: 0 ms
MF NoFe Flash tiempo supr. Rebote	Impide que se detecten varias veces las pulsaciones de teclas flash. Valor estándar: 0 ms
MF Tiempo supresión	Tiempo de espera para evitar fallos en las marcaciones MF en líneas salientes. Valor estándar 100 ms
Tiempo supresión flash (véase ayuda)	Tiempo de espera tras flash en líneas analógicas. Valor estándar: 1 s

Parámetros	Descripción
Longitud de ciclo para nueva puesta en servicio	Tiempo para reiniciar líneas analógicas después de no detectar tonos de marcación. Valor estándar: 120 s
Longitud pausa marcación	Indica la duración de la pausa, que debe darse obligatoriamente entre dos dígitos, si se reconoce la señal de marca de pausa. Rango de valores: 1 - 5 s
Tiempo de exclusión de errores para llam. en servicio PABX	Tiempo para ocultar fallos de línea. Valor estándar: 0 s
Fin de marcación artificial	En la marcación externa, los dígitos recibidos después del fin de marcación artificial se interpretan como llamada de consulta. Rango de valores: 5 - 15 s
Tiempo para repetición de llamada automática	Tras expirar el temporizador se ejecuta en caso de que el usuario se encuentre ocupado con una repetición de llamada automática. Requisito para ello es la selección de la opción Repetición de llamada automática en Flags. Rango de valores: 10 - 650 s
Exclusión de errores para el primer cambio de polaridad (FRK/SPA)	Tiempo para ocultar fallos de línea. Valor estándar: 0 ms
Tiempo retardo anuncio antes de contestar	Permite definir el tiempo de retardo que ha de transcurrir para que conteste el equipo de anuncios grabados. Rango de valores: 1,5 - 30 s
Tiempo entre evaluación tono audible y marcación troncal de línea analógica	Determina el periodo transcurrido entre el reconocimiento del tono acústico y la marcación del primer dígito en líneas analógicas. Rango de valores: 0 - 2 s
La long. de pausa tras marcación de 2.° AKZ	Determina la duración de la pausa que se efectúa después de la marcación del 2.º código de ocupación de ruta o del número del código internacional. Transición al siguiente nudo de conmutación. Rango de valores: 1 - 5 s

Parámetros	Descripción
Tiempo hasta tono advertencia en enlaces de tránsito HKZ	Las conexiones de tránsito se supervisan en función del tipo de protocolo utilizado. Esto se lleva a cabo para evitar que pueda haber una conexión que no tuviera fin. Cuando por lo menos un tipo de circuito de conexión de esta conexión de tránsito dispone de un reconocimiento de liberación, no se suele realizar ninguna supervisión temporal (véanse las excepciones en la tabla que aparece abajo). En el tipo de circuito de conexión de línea analógica no se produce ningún reconocimiento de liberación. Sin embargo se dispone de una opción de hardware para la reposición silenciosa. De este modo puede llevarse a cabo un reconocimiento de liberación en las líneas analógicas. La tabla de supervisión de tráfico (válido para los tipos de tronqueo específicos de los EE. UU.) indica los tipos de tronqueo en los que se implementa una supervisión de temporizador. Se puede configurar la duración de la supervisión. Sin embargo, al emplear líneas urbanas analógicas con reposición silenciosa, debe observarse que hay números de llamada en los que, en determinadas circunstancias, no se reconoce la contestación de la llamada y, por lo tanto, tampoco se puede reconocer ninguna activación. Por norma general, estos números de teléfono son servicios de anuncios grabados. El operador del sistema de comunicación debe ser informado explícitamente de ello. Rango de valores: 120 s - 42 min
Tiempo desde tono de advertencia hasta activación...	En caso de supervisión de conexiones de tránsito, se genera un tono de advertencia después de la finalización del temporizador de supervisión. La conexión no se interrumpe de forma automática, sino que, antes de que la comunicación pueda finalizar, ha de transcurrir un periodo de tiempo determinado. Rango de valores: 10 - 650
Temporizador de activación para HKZ	Cualquier llamada de una línea analógica (HKZ) por medio de marcación directa (Duwa) se activa tras este espacio de tiempo, si no se realiza ninguna comunicación telefónica. Rango de valores: 30 s - 254 min
Tras retención se activa un tono de advertencia (Italia)	Después de transcurrido el periodo fijado por este temporizador, se activa un tono de advertencia que informa al abonado de que mantiene una llamada retenida. Rango de valores: 30 - 180 s
LCR: Fin de marcación artificial	Tiempo de espera entre el último dígito y el final de la marcación (marcación en bloque LCR). Valor estándar: 5 s
Supervisión de una llamada UCD en una línea analógica	Tiempo para activación de llamada de línea analógica en un grupo UCD si no se ha logrado establecer conexión. Rango de valores: 10 - 3810 s
Supervisión de transferencia antes de contestar a un grupo UCD (solo para desarrollo	Si se realiza la t transferencia antes de contestar de una comunicación a un grupo CD, el temporizador se activa. Si la llamada transferida no se responde, una vez agotado el plazo, se produce una llamada recordatoria. Rango de valores: 10 - 3810 s

Parámetros	Descripción
Temporizador de demora para PC-PO	Tiempo hasta que se envía el mensaje de actualización al puesto de operadora de PC (Business Attendant). Rango de valores: 300 ms
Intervalo de temporizador USBS	Basándose en el ETS 300 716, se puede utilizar el servicio USBS (User Signaling Bearer Service - Servicio portador de señalización de usuario) para el acceso a través de los puertos S0-Port, TA-S0, TA-RS232 y TA-API. Rango de valores: 1 - 60 s
Temporizador para Fraud Monitoring	Cuando finaliza el tiempo, en el display del puesto de operadora se señaliza la conexión de tránsito que esté activa; la cual, dado el caso, puede liberar líneas de forma individual. Ésta es una posibilidad de supervisar la duración de las conexiones de tránsito. Rango de valores: 0 - 650 s
Tono de ocupado especial, si la ext. de destino no contesta	Cuando finaliza este temporizador, el abonado que llama recibe un tono especial de ocupado. Rango de valores: 30 - 120 s
Tono de ocupado especial si la línea se ocupa sin marcar	En caso de que un abonado realice la ocupación de una línea saliente sin haber realizado la marcación, recibe un tono especial de ocupado una vez que ha finalizado el periodo fijado en este temporizador. Rango de valores: 20 - 60 s
Tiempo de llamada para transferencia antes de contestar a ext. ocupada	Cuando finaliza este temporizador, el abonado A, al que se ha transferido desde el abonado B hacia el abonado C que se encuentra ocupado, se vuelve a transferir de nuevo hacia el abonado B. Rango de valores: 15 - 180 s
Intervalo de señalización de errores	Con el tiempo de señalización de errores se determina un intervalo en un margen de valores de 1 min. hasta 15 min. Los decimales se redondean a minutos enteros, los valores inferiores a 1 min. o superiores a 15 min. se interpretan como 15 min. Tras expirar el intervalo, los errores de clase B registrados actualmente en el protocolo de eventos se transfieren cíclicamente al Centro de administración remota. Rango de valores: 60 - 900 s

28.3.1.3 Ajustes básicos > Sistema > Display

Descripción de parámetros de las pestañas:

- **Editar Display**

Parámetros	Descripción
Indicar nombre / n° llamada	Se puede configurar qué datos aparecerán en los displays de todos los teléfonos conectados durante las llamadas: Solo número de llamada, Nombre (si está disponible), o Nombre y n.º de llamada al mismo tiempo. Si un teléfono no admite alguno de estos ajustes, en lugar de la visualización simultánea del nombre y del número de teléfono se mostrará, por ejemplo, solo el número de teléfono. Los teléfonos OpenStage son compatibles con la visualización simultánea del nombre y del número de teléfono. Valor estándar: Nombre y n° de llamada
Nombre en pantalla/ Algoritmo	La compatibilidad del nombre completo se realiza con tres campos: uno para el nombre, otro para los apellidos y un tercero para el nombre de visualización. El campo "Nombre para mostrar" admite hasta 16 caracteres; los campos de nombre y apellidos admiten hasta 32 caracteres. Se puede utilizar una de estas opciones de algoritmo de nombre de visualización: • <apellido>, <nombre> • <apellido>, <inicial del nombre.\> • <nombre>, <apellido> • <inicial del nombre>, <apellido> • <apellido> Valor estándar: <apellido>, <nombre> **Importante:** Para usuarios MULAP, la opción **<nombre>, <apellido>** no está reconocida en UC Suite. Si se utiliza esta opción, el nombre y el apellido o apellidos de los usuarios de UC Suite aparecerán juntos en el campo del nombre dentro del directorio de usuarios de UC y el campo del apellido quedará vacío. Para este caso, utilice el valor predeterminado de la opción, que emplea la coma como separador.
Tranferencia antes de contestar	En la Transferencia antes de contestar se puede visualizar el número de llamada de la Extensión que transfiere la llamada o el número de llamada de la Extensión transferida. Una llamada transferida con Transferencia antes de contestar no puede ser rechazada por la extensión llamada. Si se selecciona Extensión transferida, antes de establecer la conexión y tras terminarla se visualiza en el display la extensión que transfiere. Si se selecciona Extensión que transfiere en el display se visualiza la extensión que transfiere mientras ésta esté conectada con la extensión receptora. Una vez que la extensión que transfiere envía la llamada y se establece la conexión, en el display se cambia el número de la extensión que transfiere por el de aquélla a la que se realiza la transferencia. Valor estándar: Extensión transferida

Parámetros	Descripción
Llamada recordatoria	Cuando se transfiere una llamada y posteriormente se realiza una llamada recordatoria, en la extensión receptora de la transferencia se puede mostrar bien el número de la extensión que transfiere o bien el número de la extensión que realiza la llamada recordatoria. La transferencia de una comunicación se visualiza en la extensión interna B. C recibe un tono de llamada hasta que B contesta o tras una llamada recordatoria de A. Aquí se puede configurar si en el display del destino de transmisión B se va a indicar la extensión A (Llamante) o la extensión C (Destino de transferencia). Si la extensión A acepta una llamada recordatoria, en el display de las dos extensiones aparece el mensaje no hay respuesta. Valor estándar: Destino de transferencia
Formato de fecha/hora	La fecha se puede mostrar con diferentes formatos. Valor estándar: Europa- Formato 24 horas
Lista de llamantes, modo	Si se activa Llamadas internas y externas o Solo llamadas externas, todas las llamadas no contestadas se almacenan en una lista, cuyo contenido podrá consultarse posteriormente mediante un procedimiento de sistema. Si se activa También llamadas atendidas, se registran en la lista de llamantes también las llamadas atendidas. Los números de llamada no se eliminan de la lista, ya se trate de llamadas entrantes o salientes. Cuando todas las posiciones de memoria de la lista de llamantes se encuentran ocupadas, al guardar el siguiente número de llamada se sobrescribe el registro más antiguo. Las comunicaciones no atendidas se visualizan de la forma habitual tal y como se describe en la prestación lista de llamantes. Las llamadas atendidas se visualizan igual que a través de la función de la lista de llamantes Guardar número de llamada. Si se transfiere una llamada entrante externa a través del AutoAttendant a una extensión interna y la extensión se encuentra ocupada en ese momento o tiene activado el desvío de llamadas, no se agregará ninguna entrada a la lista de llamadas. Valor estándar: Sólo llamadas externas
Supresión de indicación del n° de llamada	Si el flag está activado, se impide la indicación del número de llamada en la extensión RDSI, es decir, el interlocutor no obtiene ninguna indicación del número de llamada (la prestación debe estar activada también en la compañía telefónica). Hay escenarios de llamada en los que la oficina central restringe a un llamante a solo presentación. Si este flag está activo, el número de teléfono del llamante se muestra en la extensión llamada. Si el flag está desactivado, se muestra el texto Número desconocido. El flag depende de los ajustes de línea urbana de cada proveedor. Valor estándar: desactivado

Parámetros	Descripción
Listín telefónico interno	Las extensiones podrán acceder a un listín telefónico en línea que incluye los nombres y números de llamada de todas las extensiones internas. Los terminales con display específicos del sistema permiten visualizar todas las extensiones internas disponibles con nombre y número de llamada, realizar búsquedas específicas y, a continuación, llamar a la extensión deseada. Los terminales que disponen de teclado alfanumérico pueden utilizarlo para realizar la búsqueda de un determinado número. En la lista, seleccione la opción correspondiente: no: sin acceso al listín telefónico; internamente: acceso al listín telefónico interno (extensiones, grupos y destinos de marcación abreviada); LDAP: acceso a la información de listín del servidor LDAP. el acceso LDAP debe configurarse mediante LDAP; todos: los usuarios pueden optar entre acceder al listín telefónico interno o LDAP. Valor estándar: Interna
Agenda interna mediante Directorio Unificado	Si este flag está activado, el usuario puede buscar contactos en todos los directorios. Las solicitudes de búsqueda se manejan como solicitudes al directorio Unificado. Si el flag no está activado, las solicitudes de búsqueda se gestionan de forma local desde el sistema. Valor estándar: Activado
Interruptor	
Indicación duración de llamada	En las llamadas salientes externas no se muestra información de tarificación. En terminales UP0/E con display, se muestra la duración de la llamada actual. En las líneas analógicas, el momento inicial de registro de tiempos (5 segundos después de la finalización de la marcación) se determina mediante un temporizador, y en el caso de líneas urbanas analógicas, mediante CONNECT. En el caso de terminales S0, el sistema de comunicación no admite la indicación de la duración de la llamada. Valor estándar: desactivado
Indicación cubierta DTMF	Las entradas de código PIN se muestran de forma cifrada en los teléfonos del sistema con display. Valor estándar: activado
Indicación del display en el caso de mensajes informativos	Los mensajes informativos presentes se muestran en el display de los teléfonos del sistema. Valor estándar: activado
Transmitir número de llamada de forma transparente	En caso de desvío de llamadas o de transferencia automática diferida a una extensión externa, la extensión llamada visualizará el número de llamada de la extensión llamante. En un sistema interconectado, hay que ajustar esta opción en el nodo al que esté conectada la conexión urbana. Condición previa para que la prestación funcione es que se haya activado la función Clip No Screening en la línea urbana, dicha función debe abonarse. Este flag funciona en interacción con el flag Suprimir núm. llam. de extensión en Rutas. Valor estándar: desactivado

Parámetros	Descripción
SST con opción de transferencia (transferir número del llamante)	Si el flag está activado, cuando el usuario selecciona la opción de menú "¿Iniciar transferencia?" (con una llamada activa), la transferencia se ejecutará como Transferencia de un solo paso (y no como llamada de consulta). Si el usuario selecciona realizar primero una llamada de consulta (por ejemplo, con la opción "¿Consulta?") y luego transfiere la nueva llamada al interlocutor retenido, la transferencia se ejecutará como una transferencia ciega normal (o como una transferencia después de contestar). Si se produce una transferencia de un solo paso, el número llamante aparece en el destino externo al sonar el dispositivo móvil; por ejemplo, si el usuario llamado ve el número llamante y no el número del usuario que transfiere la llamada, un dispositivo del sistema transfiere la llamada. También debe activarse el flag “Transmitir número de llamada de forma transparente”. Valor estándar: desactivado **Nota:** Si la llamada se transfiere desde un dispositivo externo, el proveedor de red debe admitir y activar la función CLIP no ascensión. De lo contrario, se usará el DID estándar del sistema desde la línea urbana y la llamada se rechazará desde aquí.

28.3.1.4 Ajustes básicos > Sistema > DISA

Descripción de parámetros de las pestañas:

- **Editar DISA**

Parámetros	Descripción
DISA	
Marcación directa	Número de teléfono con el que se puede acceder a la función DISA desde el exterior. El número de teléfono puede ser diferente para el uso externo e interno.
Modo de seguridad	Para poder utilizar las funciones DISA la extensión debe introducir una clave. Mediante las opciones del Modo de seguridad se puede determinar si, una vez introducida la clave, la extensión debe esperar primero, o si debe introducir el carácter # (almohadilla). Valor estándar: Después de tiempo de espera
DISA interno	
Número de teléfono	DISA interno se refiere al uso en otro nodo interconectado por IP.
Mobility Callback	
Marcación directa	La autenticación mediante contraseña resulta innecesaria si una llamada reconocida como número de llamada Mobility se realiza desde el exterior al número de marcación directa Devolución de llamada Mobility. En este caso se activa directamente el tono de marcar interno. Para ello el terminal de la extensión externa debe transmitir su número de llamada. Este número de llamada se comprueba con la lista Mobility.

28.3.1.5 Configuración básica > Sistema > Interceptación/PO/Hot-line

Descripción de parámetros de las pestañas:

- **Editar Intercepción/Asistente/Línea directa**

Parámetros	Descripción
Puesto de interceptación	
Día/noche	Núm. de tel. de puesto de interceptación. El puesto de interceptación puede establecerse separadamente para el servicio diurno y el nocturno. Por otro lado, si se activa el servicio nocturno, existe la posibilidad de indicar cualquier destino que se desee (servicio nocturno variable).
Puesto de interceptación central	
Ruta	Índice de ruta para el puesto de interceptación central en los sistemas de comunicación interconectados
Número de llamada	Número de teléfono del puesto de interceptación central en los sistemas de comunicación interconectados
Interceptación al puesto interc.	
en caso de libre	La llamada sigue el procedimiento definido para llamadas entrantes. Si se ha alcanzado el final de la tabla, el sistema comprueba si se debe realizar interceptación por tiempo o no. Si así fuera, se llama al puesto de interceptación después de realizado el número de timbres de llamada determinado en Transferencia automática diferida. En una línea colectiva no se lleva a cabo la interceptación. La llamada se vuelve a transferir a la primera extensión, es decir, queda siempre dentro de la línea colectiva. Valor estándar: activado
en caso de ocupado	Si se ha activado En caso de ocupado se comprueba en primer lugar si se puede enviar un aviso de llamada en espera o no. Si no fuera posible avisar sobre la llamada en espera (bloqueo de aviso de llamada en espera o criterio de interceptación), la llamada sigue el procedimiento definido en Gestión de las llamadas (Call Management). Si no se puede enviar el aviso de llamada en espera a ninguna extensión, el sistema comprueba si se ha establecido si procede realizar interceptación o liberar la llamada (señalización B a la línea urbana). Cuando un teléfono analógico con rechazo de llamadas en espera se encuentra ocupado, se libera la llamada con independencia del tipo de línea de enlace de que se trate. En los casos de marcación directa con Multifrecuencia y líneas analógicas, la llamada siempre se intercepta. Valor estándar: desactivado
en caso de marcación errónea	Al marcar un número de llamada erróneo, el sistema comprueba si se debe llevar a cabo la interceptación. En el caso de marcación directa con Multifrecuencia, la llamada siempre se intercepta. Valor estándar: activado

Parámetros	Descripción
En incompleto	Si el número de llamada de la extensión marcado está incompleto, después de un periodo predefinido se llama al puesto de interceptación. El tiempo puede ajustarse en el campo Fin marcación en caso de marcación incompleta en Parámetros de tiempo. Valor estándar: activado
En rellamada sin respuesta	Si el abonado B no atiende una llamada externa después de una transferencia antes de contestar del abonado A al abonado B, y después de una llamada recordatoria al abonado A, tampoco se produce una contestación, una vez transcurrido el tiempo preajustado se llama al puesto de interceptación. El tiempo puede ajustarse en el campo Fin marcación en caso de marcación incompleta en Parámetros de tiempo. Si no se ha activado este flag, una vez transcurrido el tiempo ajustado se libera la llamada. Valor estándar: desactivado
Con llamada rechazada	Si una extensión interna rechaza la llamada con "Rechazar llamada entrante", la llamada sigue a la Gestión de llamadas (Call Management). Si no se puede enviar el aviso de llamada en espera a ninguna extensión, el sistema comprueba si se ha establecido si procede realizar interceptación o liberar la llamada (señalización B a la línea urbana). Valor estándar: activado
Intercepción de bloqueo telefónico	
Número de llamada	Si se ha activado el candado telefónico en una extensión y dicha extensión marca un código de un haz de líneas, la llamada se desvía automáticamente hacia el destino de interceptación que se haya introducido. Esto quiere decir que si el usuario marca un número que no disponga de autorización, la llamada se señalizará en la extensión designada. La función Interceptación en caso de candado telefónico se puede definir de forma individual para cada extensión a través de los flags de extensión.
Autorización de troncal conmutada	
Autorización de troncal conmutada	En este campo, debe configurar una estación con acceso troncal sin restricciones; de lo contrario, no será posible desviar la llamada a un destino externo.
Código del puesto de operadora	
Número de llamada Interno	Los equipos internos utilizan este número de teléfono para llegar hasta el puesto de interceptación. Rango de valores: Entrada gratuita de cualquier dígito, siempre que no esté ya utilizado en el plan de marcado.
Número de llamada externo	A través de este número de teléfono se puede llegar al puesto de interceptación mediante marcación directa o desde la red del sistema (CorNet-N o CorNet-NQ).
Hot-line	

Parámetros	Descripción
Tiempo llamada de socorro	Cuando un usuario descuelga el microteléfono, una vez transcurrido el tiempo de llamada de socorro se llama automáticamente a la hot-line, siempre que el usuario no marque ninguna cifra durante este lapso de tiempo. El tiempo llamada de socorro se especifica en segundos.
N.° llam. destino 1 a 6	A nivel de sistema se pueden registrar 6 destinos de hot-line; la selección se hace por cada extensión (véase Extensiones/Editar parámetros exten.)
Consola de operadora	
Llamadas en espera	En el campo Llamadas en espera se define el número máximo de llamadas que se pueden encontrar en la cola del puesto de operadora. En caso de que el número de extensiones que se encuentran en cola de espera del puesto de operadora alcance este valor, las llamadas subsiguientes se transfieren hacia un destino de desbordamiento configurable. Rango de valores: 1-15
Tiempo de espera	En el campo Tiempo de espera, se introducen los segundos que como máximo puede estar una llamada en cola de espera. Cuando las llamadas superan el periodo definido, se transfieren hacia un destino de desbordamiento definido en la Gestión de llamadas.
conmutación rápida	Cuando se activa este flag, la operadora puede responder una llamada y a continuación llevar a cabo su transferencia hacia un destino distinto, simplemente introduciendo el número de extensión que corresponda. Esta transferencia abreviada de llamadas solo se puede utilizar cuando el flag para todo el sistema **MF automático** está desactivado. Valor estándar: desactivado
conmutar línea libre	Las extensiones autorizadas (puesto de conmutación, PO) tienen la posibilidad de asignar una línea externa libre a una extensión interna que carece de autorización suficiente para las llamadas externas, con el fin de que la última pueda cursar exactamente una comunicación externa. Una vez transferida la línea libre a la extensión con autorización insuficiente se ejecuta un control de marcación con arreglo a una autorización de acceso a la red urbana adicional para líneas conmutadas. Solo si dicha autorización de acceso a la red urbana es suficiente, es decir, si la extensión marca p.ej. un número válido según la lista de números prohibidos o permitidos para líneas conmutadas, se autorizará la comunicación externa saliente. El usuario de la extensión debe marcar por sí mismo el código de ocupación en la línea conmutada. En el sistema de comunicación se puede configurar, a través de una extensión de referencia, un acceso a la línea urbana para líneas conmutadas por ruta. La extensión de referencia estándar es el primer puerto de extensión lógico o el puesto de operadora. La autorización estándar está ajustada a Acceso directo a la línea urbana para todas las rutas. Valor estándar: desactivado
Otros criterios	
Aviso de llamada en espera en caso de ocupado	Si está activado este flag, la prestación "Aviso de llamada en espera" esté activa para todo el conjunto de usuarios del sistema de comunicación. Valor estándar: activado

Parámetros	Descripción
Aviso de llamada en espera inmediato para llamadas de puesto de operadora	Solo relevante en sistemas interconectados CorNet. Si está activado este flag, solamente un PO llamante (sistema A) puede enviar un aviso de llamada en espera a la extensión B (sistema B). Todas las demás extensiones del sistema A no pueden enviar avisos de llamada en espera al sistema B. Para las extensiones dentro del sistema B, rige la condición Bloqueo de aviso de llamada en espera (véase Vista de extensión: Flags) para la respectiva extensión. Si no se ha activado este flag, todas las llamadas pueden enviar avisos de llamada en espera a las extensiones ocupadas de otros sistemas, si la extensión en cuestión no ha activado el bloqueo de aviso de llamada en espera. Este flag debe activarse si se desea conseguir que un PO llamante a una extensión ocupada pase inmediatamente al estado de espera y pueda emitir un aviso de llamada en espera. Si no está activado este flag, el PO obtiene el tono de ocupado y pasa al estado de espera tras pocos segundos. Valor estándar: desactivado
Excepción con llamadas de puesto de operadora	Si este flag está activado, el puesto de operadora está autorizado para la prestación "Intercalación". Con ello puede intercalarse en una llamada de una extensión interna. Valor estándar: activado

28.3.1.6 Ajustes básicos > Sistema > LDAP

Descripción de parámetros de las pestañas:

- **Editar LDAP**

Parámetros	Descripción
Acceso LDAP	
Dirección IP del servidor LDAP	Dirección IP del servidor LDAP, en el que se va a recopilar la información de listín.
Número de puerto de acceso LDAP	Número de puerto para el acceso LDAP. Valor estándar: 389
Nombre de usuario/clave	En Windows Server ADS no se puede realizar un acceso anónimo. En este caso, hay que introducir aquí el nombre de usuario y la contraseña de la conexión LDAP. Rango de valores: máx. 48 caracteres
Parámetros de servidor LDAP	
DN base	DN = Distinguished Name; base para la consulta de búsqueda en el servidor LDAP (ASCII, 100 caracteres), p. ej. ou=com, cn=unify, cn=de

Parámetros	Descripción
Búsqueda	Patrón para la búsqueda en el servidor LDAP. Como comodín para el nombre a buscar tiene que introducirse el carácter $. Tenga en cuenta que un patrón de búsqueda no puede comenzar con una expresión habitual. Rango de valores: ASCII, 50 caracteres Valor estándar: cn=$*
Atributo de resultado Nombre	El atributo de resultado Nombre admite los caracteres del conjunto de caracteres ISO-8859-1 con valores de código desde 0x20 hasta 0x80 (caracteres ASCII), así como los caracteres Ä, Å, Æ, Ñ, Õ, Ö, Ø, Ü, ß, ä, õ, ö, ü. La indicación de los caracteres depende del idioma ajustado y del terminal utilizado. Rango de valores: ASCII, 24 caracteres Valor estándar: cn
Atributo de resultado Nº llamada	El atributo de resultado Nº llamada puede devolver hasta 25 cifras de marcación (0...9, *, #) y hasta 6 caracteres de formateo (+,(), espacios en blanco, -). El número de llamada tiene que tener formato canónico (p. ej., +49 (89) 70070). Rango de valores: ASCII, 25 caracteres Valor estándar: telephoneNumber
Clasificación de resultados de búsqueda	Los resultados de la búsqueda se ordenan alfabéticamente, por nombre. Valor estándar: activado
Evaluación de números de teléfono LDAP	
Código de ocupación LDAP	El código de ocupación corresponde al código de ruta marcado. Valor estándar: 0 (código de ruta predeterminado de la primera ruta)
Prefijo de nº llamada LDAP	El prefijo indicado aquí se antepone al número de llamada encontrado. Rango de valores: ASCII, 5 caracteres

Nota: Para que se muestren los recursos LDAP, debe seleccionar la opción adecuada en **Ajustes básicos** > **Mostrar** > **Agenda interna** en el menú **Mostrar**. Para más información, consulte el capítulo 28.3.1.3 Ajustes básicos > Sistema > Display.

28.3.1.7 Ajustes básicos > Sistema > Textos

Descripción de parámetros de las pestañas:

- **Editar Textos**

Parámetros	Descripción
Restablecer los valores predeterminados	Los textos informativos y de respuesta se restablecen a los valores preestablecidos de un idioma determinado. La reposición se realiza seleccionando el idioma en la lista desplegable.
Textos informativos	Mensajes breves que una extensión puede enviar a otra. El sistema de comunicación incluye diez textos informativos por defecto. Todos los mensajes estándar pueden sobrescribe. En cada momento, solo se dispone de diez mensajes posibles. Las extensiones pueden acceder a estos textos informativos a través de la opción de menú ¿Enviar mensajes de información? del teléfono de sistema. Las extensiones que disponen de terminales con teclado alfanumérico tienen además la posibilidad de crear sus propios mensajes; no obstante, no pueden cambiar los mensajes predeterminados. Rango de valores: máx. 24 caracteres alfanuméricos
Textos de respuesta	Mensajes breves que la extensión puede enviar a un llamante en caso de ausencia. Hay diez textos predeterminados. Todos los mensajes estándar pueden sobrescribe. Las extensiones que disponen de terminales con teclado alfanumérico tienen además la posibilidad de crear sus propios mensajes; no obstante, no pueden cambiar los mensajes predeterminados. En la mayoría de los casos, las extensiones solo tienen que añadir alguna información adicional a los mensajes existentes. Los textos que contienen un guión ofrecen a la extensión la posibilidad de completar el mensaje o añadir un número o una fecha. Las extensiones pueden acceder a los textos de respuesta a través de la opción de menú ¿Activar mensaje de aviso? del teléfono de sistema. Rango de valores: máx. 24 caracteres alfanuméricos

28.3.1.8 Ajustes básicos > Sistema > Menús flexibles

Los menús flexibles permiten adaptar, de forma individualizada, las opciones de menú del Menú Servicio de los teléfonos de sistema. Si la casilla de verificación de la **Lista de prestaciones ocultas** está activada, no aparece esta opción de menú. Esta configuración se aplica a nivel de sistema a todos los teléfonos del sistema. Las funciones ocultas se pueden activar mediante códigos.

28.3.1.9 Ajustes básicos > Sistema > Destinos de marcación abreviada

Se pueden configurar o modificar de forma manual hasta 8000 entradas de listín. Los destinos de marcación abreviada son números de marcación directa centrales (RNGZ). Al hacer clic en un nombre de columna, las entradas se ordenan por esa columna.

Descripción de parámetros de las pestañas:

- **Cambiar Marcaciones abreviadas**

Parámetros	Descripción
Marc. abr.	Número marcado por la extensión. Los números de marcación abreviada deben tener cuatro dígitos (`0000-7999`, utilizar ceros iniciales).

Parámetros	Descripción
Número de teléfono	Número de teléfono de marcación del puesto de destino deseado, es decir, con código de línea o ruta (p. ej., 0, 9, 81 o 801). Rango de valores: máx. 31 cifras
Nombre	Nombre para el destino de marcación abreviada tal y como está memorizado en el listín telefónico interno y como aparece al marcar el destino correspondiente. Las llamadas entrantes (con CLIP) se comparan con los destinos de marcación abreviada memorizados y se muestran como nombre del destino de marcación abreviada, siempre y cuando se haya activado el parámetro Nombre o bien Nombre y Número. Rango de valores: máx. 16 caracteres
Buscar	Si en los campos de búsqueda **Marc. abr.**, **Número de teléfono** o **Nombre**, se introduce un término de búsqueda y, a continuación, se pulsa la tecla Intro, se muestran todos los resultados que incluyen el término de búsqueda. Si por ejemplo se escribe `521` como número de teléfono, aparecerían los resultados `+495213535` y `+498967521`. O por ejemplo, si se escribe `co` como nombre, aparecerían los resultados `Collins`, `Mcoin` y `Branco`. Si no hay nada en ningún campo de búsqueda y se pulsa la tecla Intro, aparecen todas las entradas.
Botones	
Aplicar	Añadir entradas existentes o modificar entradas existentes.
Deshacer	Restablecer cambios de entradas existentes (antes de aplicarlos).

Descripción de parámetros de las pestañas:

- **Importar/Exportar un archivo CSV/XML a través de HTTP**

Parámetros	Descripción
Importar archivo CSV/XML a través de HTTP	Los destinos de marcación abreviada se pueden importar mediante un archivo XML en formato UTF-8. Los números de marcación abreviada ya existentes se borran antes de la importación. Puede encontrar una plantilla XML para importar números de marcación abreviada en **Centro de servicios** > **Documentos** > **Plantillas CSV.**
Exportar un archivo xml a través de HTTP	Los destinos de marcación abreviada se pueden exportar como archivo XML en formato UTF-8. Siempre se exportan todos los registros de datos. **Nota:** Ya no se recomienda importar listas de marcación abreviada desde archivos CSV y solo se admite para clientes antiguos.

28.3.1.10 Ajustes básicos > Sistema > Códigos de servicio

Con el teléfono, se pueden activar y desactivar prestaciones mediante códigos de servicio. Los códigos de servicio estándar se pueden modificar, pero al hacerlo hay que garantizar que la asignación de los códigos sea coherente.

Además, se pueden modificar los dos códigos que sustituyen a los símbolos * (asterisco, valor estándar: 75) y # (almohadilla, valor estándar: 76) (sustituciones) en los teléfonos DEC y RDSI.

28.3.1.11 Ajustes básicos > Sistema > Contraseña de registro HFA

Descripción de parámetros de las pestañas:

- **Contraseña de registro HFA**

Parámetros	Descripción
Para que este parámetro se aplique es necesario que los teléfonos del sistema utilicen el DLI del sistema y que este pueda suministrar a los teléfonos del sistema los parámetros necesarios.	
Cambiar contraseña de registro HFA El administrador puede modificar la contraseña de registro HFA	
Aplicar autenticación para dispositivos HFA	En la lista desplegable, seleccione una de estas opciones: • **No** (valor predeterminado): no se aplica autenticación Si esta opción está seleccionada, los campos de contraseña están desactivados. Al hacer clic en el botón **Aplicar**, la autenticación se desactiva. • **Únicamente dispositivos que no sean Deskshare con DLI**: la contraseña se aplicará únicamente a los clientes del sistema que tienen DLI configurado. La contraseña se establecerá en la base de datos del sistema para esos dispositivos y será distribuida a los adecuados por DLI. • **Únicamente dispositivos Deskshare con DLI**: la contraseña se aplicará únicamente a los dispositivos Deskshare que tengan DLI configurado. La contraseña se establecerá en la base de datos del sistema para esos dispositivos y será distribuida a los adecuados por DLI. • **Todos los dispositivos que no sean Deskshare**: la contraseña se aplicará a todos los clientes del sistema. La contraseña se establecerá en la base de datos del sistema para todos esos dispositivos y será distribuida a los adecuados por DLI. Para los clientes del Sistema que no tengan configurado el DLI, se deberá introducir manualmente la contraseña a cada uno de ellos para poder entrar en servicio. • **Todos los dispositivos**: la contraseña se aplica a todos los dispositivos habilitados. La contraseña se establecerá en la base de datos del sistema para todos esos dispositivos y será distribuida a los adecuados por DLI. Para los dispositivos deskshare que no tengan configurado el DLI, se deberá introducir manualmente la contraseña a cada uno de ellos para que entren en servicio.

Parámetros	Descripción
Contraseña	La contraseña debe ser ingresada en este campo. La contraseña debe tener al menos 8 caracteres de longitud e incluir como mínimo un dígito o una letra.
Confirmar contraseña	La contraseña debe repetirse en este campo para fines de verificación.

28.3.1.12 Ajustes básicos > Gateway

Descripción de parámetros de las pestañas:

- **Editar propiedades gateway**

Parámetros	Descripción
General	
Nombre del cliente	Nombre libre del cliente, solo para información (opcional) Rango de valores: máx. 15 caracteres
Número de contrato	Secuencia de caracteres libre, para información(opcional) Rango de valores: Ilimitado
Nombre del sistema	Nombre libre del sistema de comunicación. Esta serie de caracteres se muestra en el display de todos los teléfonos del sistema. Rango de valores: máx. 24 caracteres
Emplazam. gateway	Serie de caracteres libre para indicar el lugar de montaje del sistema de comunicación. Esta información ayuda a los técnicos de servicio a encontrar el sistema de comunicación si es necesario acceder a él de forma física. (opcional) Rango de valores: Ilimitado
Dirección contacto	Secuencia de caracteres libre para indicar una persona de contacto con la que contactar en caso de problemas con el sistema de comunicación. (opcional) Rango de valores: Ilimitado
Distintivo país sistema	Selección del país en el que va a operar el sistema de comunicación; si se cambia el código de país del sistema el sistema se reinicia automáticamente.
Dirección IP del gateway	Indicación de la dirección IP del sistema de comunicación, por ejemplo, 192.168.1.2.
Másc. red gateway	Indicación de la máscara de red del sistema de comunicación, p. ej. 255.255.255.0.
Prefijo internacional	Indicación del prefijo para la marcación internacional, por ejemplo, 00 para Alemania o 011 para EE. UU.
Prefijo nacional	Indicación del prefijo para la marcación nacional, por ejemplo, 0.
Brand	Selección del producto adquirido (OpenScape Business u Octopus F X)

Parámetros	Descripción
Emplazam. gateway	
Prefijo del país	Indicación del prefijo del país, por ejemplo, 49 para Alemania o 1 para EE. UU.
Código de red local	Indicación del del código de red local, p. ej. 89 para Múnich.
Número de teléfono del sistema	Indicación del número de teléfono del sistema (número de encabezado, sin marcación directa), p. ej., 7007
Parámetros de red	
ID de nodo	Se debe asignar un ID de nodo exclusivo a cada nodo de un sistema interconectado. De esta forma es posible identificar exactamente cada nodo individual del sistema interconectado. Rango de valores: de 1 a 100
Tono de marcación interno	
Tono continuo	Este flag se activa si el tono de marcación interno no es una secuencia de tonos sino un tono continuo. El tono de marcación interno suena desde que se descuelga el auricular y hasta que se marque un número. Estándar: desactivado

28.3.1.13 Ajustes básicos > DynDNS > Servicio DynDNS

Descripción de parámetros de las pestañas:

- **Mostrar configuración DynDNS**
- **Editar configuración DynDNS**

Parámetros	Descripción
Activar DynDNS	A través del servicio DynDNS es posible acceder al gateway desde distintas ubicaciones sin necesidad de conocer la dirección IP del gateway. El servicio DynDNS se puede activar aquí.
Dominio definido por el usuario	La casilla de verificación se debe activar si el proveedor DynDNS no aparece en la lista **Nombre dominio**.
Nombre de usuario	Nombre de usuario de la cuenta DynDNS en el proveedor DynDNS. Esta cuenta DynDNS se puede configurar, por ejemplo, en la dirección de Internet `http://www.dyndns.org/account/create.html`.
Contraseña	Contraseña de la cuenta DynDNS en el proveedor DynDNS. Cuando se introduce la contraseña, los caracteres son sustituidos en pantalla por marcadores de posición, por motivos de seguridad.
Repetir contraseña	Repetición de la contraseña de la cuenta de usuario del servicio DynDNS. Cuando se introduce la contraseña, los caracteres son sustituidos en pantalla por marcadores de posición, por motivos de seguridad.
Hostname (Nombre host)	Indicación del nombre de host registrado con el proveedor DynDNS, sin el nombre de dominio, por ejemplo, myhost. El nombre completo de subdominio consta del nombre host y el nombre de dominio, p. ej. mihost.DynDNS.org.

Parámetros	Descripción
Nombre dominio	Selección del proveedor DynDNS en una lista (p.ej. dyndns.org) o entrada manual del proveedor DynDNS (si la casilla de verificación **Dominio definido por el usuario** está activada).

URL de actualización	Entrada de la URL de actualización de un proveedor DynDNS que no aparezca en la lista. La estructura de la URL depende del proveedor DynDNS. Además, hay que indicar parámetros específicos del cliente (en el ejemplo, marcados en *cursiva*).
	Ejemplo de una URL de actualización:
	`http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`
	Ejemplo de una URL de actualización con autenticación cifrada con Base64:
	`https://<b64><username>:<pass></b64>@members.dyndns.org/nic/update?hostname=<domain>&myip=<ipaddr>&wildcard=NOCHG&mx=NOCHG&backmx=NOCHG`
	<b64>...</b64> para parámetros codificados con Base64

Últ. actualiz.	Momento de la última actualización del servicio DynDNS.
Dirección IP en DynDNS	Dirección IP del proveedor DynDNS donde se pueden encaminar las consultas para el subdominio DynDNS configurado.
Dirección IP dinámica propia	Indicación de la dirección IP actual del sistema de comunicación asignada por el proveedor de servicios de Internet.
Act. comodín	Si se activa esta opción, las consultas del sub-subdominio como cualquiera.mihost.DynDNS.org se encaminan en mihost.DynDNS.org.
Mail Exchanger	Mail Exchanger (Registro MX) indica, dentro del DNS, a qué dirección IP o a qué nombre de dominio hay que enviar los correos electrónicos para el subdominio DynDNS configurado. Detrás del destino indicado debe haber un servidor de correo.
Backup MX	Si se activa esta opción, los correos electrónicos que no se pueden suministrar al Mail-Exchanger indicado (p. ej., porque no está disponible en ese momento) se almacenan de forma intermedia en el servicio DynDNS y se suministran cuando el Mail-Exchanger vuelve a estar disponible.
Utilizar HTTPS para actualiz.	Si se activa esta opción, para la actualización se elige una conexión HTTPs cifrada y segura.

28.3.1.14 Ajustes básicos > DynDNS > Tiempo actualiz. nombres DNS

Descripción de parámetros de las pestañas:

- **Editar tiempo actualiz.**

Parámetros	Descripción
Actualizar nombres DNS	Esta opción solo es válida para VPN. Una vez acabado el tiempo configurado en "Valor timer para actualiz. de nombres DNS", el componente VPN comprueba si los nombres DNS en uso de la configuración VPN se resuelven con nuevas direcciones IP (VPN con direcciones IP dinámicas). En tal caso, VPN se configura de nuevo con las nuevas direcciones IP.
Valor timer para actualiz. de nombres DNS	Número de segundos para el intervalo entre dos actualizaciones. Rango de valores: de 60 a 1800, valor estándar: 180

28.3.1.15 Ajustes básicos > Calidad del servicio

Con el tráfico de datos por IP, los paquetes IP que genera el propio sistema de comunicación se dividen en cinco grupos. En cuatro de los grupos se puede definir con qué punto de código se marcarán los paquetes. El tráfico de datos restante no se prioriza (marca 00).

Clase de prioridad	Valor ToS binario	Valor ToS hexadecimal
AF (Assured Forwarding)		
AF11	001-010-00	28
AF12	001-100-00	30
AF13	001-110-00	38
AF21	010-010-00	48
AF22	010-100-00	50
AF23	010-110-00	58
AF31	011-010-00	67
AF32	011-100-00	69
AF33	011-110-00	77
AF41	100-010-00	88
AF42	100-100-00	90
AF43	100-110-00	98
EF (Expedited Forwarding)		
EF	101-110-00	B8
Best Effort (BE)		
BE	000-000-00	00
CS (Class Selector)		
CS3	011-000-00	60
CS4	100-000-00	79
CS5	101-000-00	A0
CS6	110-000-00	C0
CS7	111-000-00	E0

Clase de prioridad	Valor ToS binario	Valor ToS hexadecimal
Entrada manual	xxx-xxx-00	0-63 (decimal)

Descripción de parámetros de las pestañas:

- **Editar calidad del servicio**

Parámetros	Descripción
Clase de prioridad para datos señalización	Señalización de llamadas para el establecimiento de conexión con H.323/SIP Valor estándar: AF31
Clase prioridad para payload fax/módem	Payload de datos, por ejemplo, para interconexión IP con fax o módem Valor estándar: EF
Clase de prioridad para control de red	Control de red, por ejemplo, traps SNMP Valor estándar: CS7
Clase de prioridad para payload voz	Payload de voz para la telefonía IP (Voz a través de IP) Valor estándar: EF

28.3.1.16 Ajustes básicos > Fecha y hora > Fecha y hora

Descripción de parámetros de las pestañas:

- **Ajustar fecha y hora**

Parámetros	Descripción
Fecha y hora	
Día	Selección del día.
Mes	Selección del mes.
Año	Indicación del año.
HOR:MM:SS	Indicación de la hora en formato de 24 horas.

28.3.1.17 Ajustes básicos > Fecha y hora > Ajustes zona horaria

Descripción de parámetros de las pestañas:

- **Editar ajustes zona horaria**

Parámetros	Descripción
Zona horaria	Zona horaria local en la que se encuentra el sistema

28.3.1.18 Ajustes básicos > Fecha y hora > Ajustes SNTP

Descripción de parámetros de las pestañas:

- **Editar ajustes**

Parámetros	Descripción
Cliente SNTP Entrada de los datos de acceso para un servidor de tiempo externo (SNTP) con sincronización a nivel de red del reloj del sistema.	
Estado administrativo del cliente SNTP	Activar o desactivar la conexión del sistema de comunicación con el servidor SNTP Valor estándar: bajo
Dirección IP/nombre DNS del servidor temp. externo	Dirección IP o nombre DNS del servidor SNTP. Valor estándar: 0.de.pool.ntp.org
Tiempo de interrogación para servidor de hora externo	Intervalo de tiempo para sincronizar la fecha y la hora con el servidor SNTP. Valor estándar: 4 horas.

28.3.1.19 Ajustes básicos > Administración de puertos

Los puertos representados permiten identificar los protocolos de red y los servicios de red correspondientes. Algunos de los puertos que utiliza el propio sistema de comunicación no se pueden modificar aquí. Esto permite adaptar la comunicación de red a cada red de cliente si los puertos ya están en uso en otro lugar. Si se han hecho cambios en la administración de puertos, por norma general, estas modificaciones deben hacerse en todos los componentes (teléfonos, sistemas, etc.), para garantizar las funciones.

Descripción de parámetros de las pestañas:

- **Editar ajustes globales del Administrador de puertos**

Parámetros	Descripción
Nombre protocolo	Servicio.
Número puerto	Número de puerto del servicio (configurable).
Tipo puerto	Se muestra el tipo de puerto a título informativo; Single: un solo puerto; Min: valor mínimo para un área de puertos.
Servicios	
CSP	CSTA Service Provider, puerto IP para todas las aplicaciones que se quieren conectar con el CSP. Valor estándar: 8800
HFA	Control de clientes HFA (puerto de servidor CorNet-TC). Valor estándar: 4060
HFA_EXT	Control de clientes HFA (puerto de servidor CorNet-TC) para Dispositivo de sistema@Casa. Valor estándar: 4062

Parámetros	Descripción
HFA_TLS	CorNet-TC mediante TLS. Valor estándar: 4061
HFA_TLS_EXT	CorNet-TC mediante TLS para Dispositivo de sistema@Casa. Valor estándar: 4063
MEB_SIP	MediaExtensionBridge, señalización de llamadas para tronqueo SIPQ. Valor estándar: 15060
RTP_MIN	Puertos RTP/RTCP y T.38 (MediaBasePort). Valor estándar: 29100
SIP	Señalización de llamada para terminales SIP y tronqueo basado en SIP. Valor estándar: 5060
SIP_EXT	Señalización de llamada para terminales SIP y tronqueo ITSP para dispositivo SIP@Casa. Valor estándar: 5070
SIPS	Señalización de llamadas segura para tronqueo SIPQ. Valor estándar: 5061
SIP_TLS_SUB	Señalización segura de llamada para extensiones SIP. Valor estándar: 5062
SIP_TLS_SUB_EXT	Señalización segura de llamada para extensiones SIP para Dispositivo SIP@Casa. Valor estándar: 5071
VSL_MULTISITE	Conexiones multisitio. Valor estándar: 8778

28.3.1.20 Ajustes básicos > Tasas de llamada > Tasas de llamada - Formato de salida

Descripción de parámetros de las pestañas:

- **Editar formato de salida**

Parámetros	Descripción
Formato del registro de datos de comunicación	
Formato de salida comprimido	Valor estándar: activado
Suprimir las últimas 4 cifras	Los últimos 4 números del campo de Número de teléfono se sustituyen por interrogantes para proteger la privacidad. Valor estándar: desactivado

Parámetros	Descripción
Protocolizar llamadas entrantes	Valor estándar: desactivado
Protoc. de la duración de llamada act.	Protocolización de la duración de la llamada en horas, minutos y segundos. Valor estándar: activado
Protocolo de llamada act.	Al recibir una llamada e inmediatamente después del comienzo de la llamada se crea un registro de datos de conexión, por ejemplo para transmitir información adicional sobre el llamante elaborada a partir de una evaluación del conjunto de datos basada en PC para una lista de llamantes. Valor estándar: desactivado
Salida de los MSN	Protocolización de los MSN utilizados (solo RDSI) Valor estándar: desactivado
Formato decimal	(no en EE. UU.) Formato de la indicación de importes. Se puede configurar según el país. En Alemania siempre se utiliza el formato decimal. Esta representación decimal significa que el factor se indica en céntimos. El factor indica por qué importe se multiplica una unidad de tarifa a fin de calcular el importe en la moneda correspondiente (p. ej., 0,06 euros en lugar de 6 céntimos). Valor estándar: activado
Reflejar Importes en vez de unidades	Se indican importes en lugar de unidades de tarifa (p. ej., 4,50 EUR en lugar de 75 unidades). Valor estándar: activado
Saliente sin conex.	Protocolización de las llamadas salientes no contestadas. Valor estándar: desactivado
Número de LCR saliente o número entrante marcado	Si este flag está activado, se añade un campo de número de teléfono adicional al registro de datos de llamada. Contiene: • para una llamada saliente: el número de teléfono LCR que se envió al intercambio tras la conversión mediante LCR o • para una llamada entrante: el número de teléfono interno de la extensión requerida, es decir, la primera extensión marcada. A continuación se genera un registro de llamadas, incluso si se realiza una llamada para una extensión ocupada. Este registro de llamadas tiene el mismo formato que el registro de datos creados para una extensión libre, excepto que la duración de la llamada se establece en "0". Valor estándar: desactivado
Grabación central de detalles de llamada	
Salida: ninguno	No se transmiten datos de conexión Valor estándar: HTTP
Salida: HTTPS	Transmisión de datos de conexión al Gestor de tasa de llamadas suministrado u otro software de contabilidad Valor estándar: HTTP

Parámetros	Descripción
Salida: Cliente TCP LAN	Transmisión de datos de conexión al servidor externo por TCP/IP Valor estándar: HTTP
Cliente TCP	Definición de la dirección IP y del número de puerto de un servidor de tarifas externo. Si se originan gastos de llamada, el sistema de comunicación inicia una conexión TCP/IP con el servidor de tarifas externo. Después de establecer la conexión, se transmiten los datos de tarifas, la conexión se mantiene y se transmiten los demás gastos que pudieran ocasionarse. Cada registro de datos se envía por separado.

28.3.1.21 Ajustes básicos > Tasas de llamada > Tasas de llamada - Factores

Descripción de parámetros de las pestañas:

- **Editar factores**

Parámetros	Descripción
Factor de tarificación por ruta	La información sobre tarifas se puede ofrecer en forma de unidades de tarificación (impulsos) o en forma de unidades monetarias (importes). Aunque ambos formatos son compatibles, en el display solo se muestran unidades monetarias. Al transmitir información en forma de unidades monetarias, se utiliza un factor de conversión. Estos factores se configuran por ruta y son válidos tanto para las llamadas de línea urbana como en la interred (entrantes y salientes).
Rutas	Indicación de las rutas presentes en el sistema
Factor	Este factor se utiliza para convertir unidades de tarificación en importes monetarios. Rango de valores: de 0 a 65534, valor estándar: 6
RDSI múltip.	Factor para convertir importes de recepción y envío en unidades de tarificación, y a la inversa. Solo para rutas con el protocolo QSIG. Rango de valores: de 1 a 65535, valor estándar: 6
Moneda	Denominación breve de la moneda, por ejemplo, EUR. Debe coincidir con el sistema de comunicación conectado. La configuración de la cadena de moneda no depende de la cadena de moneda para la visualización en los terminales. Aviso: El parámetro solo es relevante en rutas con el protocolo QSIG. Con otros protocolos el parámetro es irrelevante y hay que mantener el ajuste de configuración predeterminado (ajuste estándar). Rango de valores: máx. 3 caracteres.
Importe	En la columna Importe se determina si en la ruta se intercambiarán importes o unidades de tarificación. Si la opción está activada, se envía y recibe el importe (véase RDSI múltip.). Si no lo está, se envían y reciben unidades de tarificación. Debe coincidir con el sistema de comunicación conectado. Si en la ruta se intercambian impulsos de tarificación, la cadena de moneda debe dejarse en blanco. Aviso: El parámetro solo es relevante en rutas con el protocolo QSIG. Con otros protocolos el parámetro es irrelevante y hay que mantener el ajuste de configuración predeterminado (ajuste estándar).

Parámetros	Descripción
Información de tasación: Sin cargo	Por la ruta no se reciben tarifas, por ejemplo, líneas urbanas de EE. UU. El parámetro es irrelevante en rutas con el protocolo QSIG.
Información de tasación: Ínterin	Solo se reciben tasas de llamada durante la conexión, no en el establecimiento de la conexión.
Información de tasación: Final	Solo se reciben tasas de llamada al finalizar la conexión.
Información de tasación: Ínterin final	Se reciben tasas de llamada durante la conexión y al finalizar la conexión.
Moneda	Identificación de moneda para la indicación de tasas en los terminales.
Exactitud del cálculo	Debe configurarse de forma que la precisión del sistema de comunicación sea al menos igual a la de los importes enviados desde la línea urbana. Si los tres decimales posibles máximos no son suficientes, se redondea automáticamente. Hay que marcar "Mediante impulsos de tasación" en las rutas con el protocolo QSIG.

28.3.1.22 Ajustes básicos > Tasas de llamada > Tasas de llamada - Códigos de proyecto

Descripción de parámetros de las pestañas:

- **Modificar códigos de proyecto**

Parámetros	Descripción
Procedimiento de prueba	
Procedimiento de prueba: Ninguna prueba	Los códigos de proyecto introducidos no se comprueban. Esta opción no se puede introducir con rutas que tengan un procedimiento de entrada de datos obligatorio.
Procedimiento de prueba: Prueba de listas	Se comprueba la validez de los códigos de proyecto introducidos mediante las listas de códigos de proyecto.
Procedimiento de prueba: Prueba de cantidad de posiciones	Se comprueba el número de posiciones de los códigos de proyecto introducidos.
Cantidad de posiciones que deben ser comprobadas	Número de posiciones válido para los códigos de proyecto. Rango de valores: de 1 a 11, valor estándar: 5
Listas PKZ	
Lista	En la prueba de listas se pueden introducir como máximo 1000 códigos de proyecto.
Código de cuenta	Rango de valores: máx. 11 cifras

28.3.1.23 Ajustes básicos > Reproductor para mensajes de voz / anuncios

Descripción de parámetros de las pestañas:

- **Modificar el reproductor para mensajes de voz / anuncios**

Parámetros	Descripción
Buzón de voz	
Prefijo	Número de teléfono del buzón de voz.
Reproductor de anuncios	
Número de llamada	Número de teléfono del reproductor (Announcement Player).

28.3.1.24 Configuración básica > Implementación de parámetros del teléfono

Descripción de parámetros de las pestañas:

- **Editar la implementación de parámetros del teléfono**

Parámetros	Descripción
Implementación de parámetros del teléfono Para que este parámetro se aplique es necesario que los teléfonos del sistema utilicen el DLI del sistema y que este pueda suministrar a los teléfonos del sistema los parámetros necesarios. Los parámetros de los teléfonos del sistema se actualizan en cuanto un teléfono del sistema se reinicia o se conecta de nuevo con el sistema, o se reinicia el sistema. Los parámetros individuales se pueden configurar directamente en el teléfono del sistema o con la Gestión basada en Web (WBM) del teléfono del sistema. El DLI no sobrescribe los ajustes para el puerto PC Ethernet y para la priorización de códec si se han configurado directamente en el teléfono del sistema con la WBM del teléfono del sistema.	
activar la implementación de parámetros del teléfono	Si este marcador está activado, se podrán editar las siguientes opciones.
Distribuir SW a dispositivos @Home	Si este marcador está activado, se otorgan permisos de actualización de software a través de DLI para dispositivos HFA@Casa.
Configuración de parámetros del teléfono Los siguientes ajustes de teléfono se pueden modificar aquí.	
Puerto PC	Si este marcador está activado, se conecta el puerto PC Ethernet de todos los teléfonos del sistema activos. Estándar: desactivado

Parámetros	Descripción
Configuración de códec: "ancho de banda bajo preferido"	Si este marcador está activado, se aplica la siguiente priorización de códec a todos los teléfonos del sistema: G.729 - G.711 - G.722 Si este marcador está desactivado, se aplica la siguiente priorización de códec: G.722 - G.711 - G.729 **Nota:** CP100 no soporta G.722 Estándar: desactivado
Mostrar imágenes de llamante	Si este marcador está activado, en los teléfonos del sistema con pantalla a color grande se muestra la imagen del llamante al recibir llamadas entrantes, siempre que la imagen se haya cargado en el sistema mediante UC Smart o UC Suite. Estándar: desactivado
Aplicar la configuración de parámetros del teléfono	
Aplicar configuración de parámetros de teléfono a todos los teléfonos	Si este marcador está activado, se sobrescriben todos los ajustes administrados de forma local. Estándar: desactivado

Descripción de parámetros de las pestañas:

- **Información del dispositivo**

  Estos son los datos disponibles:

  Número de llamada, Display, Tipo de dispositivo, Dirección IP, Dirección MAC, Versión de software actual, Versión de hardware, Puerto PC, Configuración de códec.

Descripción de parámetros de las pestañas:

- **Cambiar contraseña de administrador**

  El administrador puede configurar la contraseña para acceder al WBM de un teléfono.

Parámetros	Descripción
Para que este parámetro se aplique es necesario que los teléfonos del sistema utilicen el DLI del sistema y que este pueda suministrar a los teléfonos del sistema los parámetros necesarios.	
Cambiar contraseña de administrador El administrador puede cambiar la contraseña predeterminada de forma centralizada para todos los dispositivos conectados a DLI.	
Contraseña	La contraseña debe ser ingresada en este campo. La contraseña debe tener como mínimo 6 caracteres.
Confirmar contraseña	La contraseña debe repetirse en este campo para fines de verificación.

Descripción de parámetros de las pestañas:

- **Configuración de marcación canónica**

  El administrador puede distribuir de forma masiva la configuración de marcado canónico a todos los dispositivos Desk Phone CP HFA que tengan DLI configurado.

  Tenga en cuenta que los valores de configuración de marcación canónica, configurados en WBM, siempre sobrescribirán la configuración local (teléfono).

Parámetros	Descripción
Configuración de marcación canónica	
Código local del país	Obligatorio: código interno para la ubicación del teléfono. Si no se establece, la conversión no se llevará a cabo. Longitud máxima: 5 caracteres.
Dígito del prefijo nacional	Necesario: dígito del prefijo troncal para marcar PSTN dentro del país local. Valor: Longitud máxima: 5 caracteres.
Código nacional local	Necesario: código de área PSTN para la ubicación del teléfono. Longitud máxima 6 caracteres.
Longitud mínima del número local	Necesario: longitud de los números del área local de PSTN. Rango: 0-50
Longitud máxima del número local	Opcional: longitud de los números del área local PSTN. Un valor de 0 significa que esta nueva regla no se aplicará. Rango: 0-50
Nodo de empresa local	Opcional: prefijo de código de red empresarial local para un teléfono como extensión. Longitud máxima 10 caracteres.
Código de acceso PSTN	Opcional: lista de dígitos para obtener acceso PSTN. Longitud máxima 10 caracteres.
Código de acceso internacional	Necesario: lista de códigos de acceso PSTN para la puerta de enlace internacional. Longitud máxima 5 caracteres.
Código de operador	Opcional: lista de números de extensiones para operadores. Longitud máxima 50 caracteres.
Números de emergencia	Opcional: lista de números que se utilizan para llamadas de emergencia. Longitud máxima 50 caracteres.
Dígitos iniciales de la extensión / Dígitos iniciales	Opcional: lista de dígitos iniciales para la extensión en la red empresarial local (definida por el nodo empresarial local). Longitud máxima 50 caracteres.
Esperar número de marcación	Opcional: booleano para indicar cuándo se conserva un dígito de prefijo nacional del código de acceso PSTN y no se convierte en el código de acceso internacional. Verdadero/Falso con el valor predeterminado como falso.
Marcación canónica	
Números internos	Lista desplegable con las siguientes opciones: Formulario de empresa local (predeterminado), Agregar siempre nodo, Usar números externos. Entero.
Números externos	Lista desplegable con las siguientes opciones: Formulario público local (predeterminado), formulario público nacional, formulario público internacional. Entero.
Código de acceso externo	Lista desplegable con las siguientes opciones: No requerido (predeterminado), para números externos. Entero.

Parámetros	Descripción
Código de gateway internacional	Lista desplegable con las siguientes opciones: Utilice el código nacional (predeterminado), déjelo como +. Entero.
Búsqueda de marcación canónica	
Código local 1-5	Opcional: un código de nodo local en la red empresarial. Longitud máxima 10 caracteres.
Código internacional 1-5	Opcional: el código internacional equivalente al código local. Longitud máxima 30 caracteres.

28.3.1.25 Ajustes básicos > Gestión de energía

Descripción de parámetros de las pestañas:

- **Activar/Desactivar la gestión de energía**

Parámetros	Descripción
Gestión de energía La gestión de energía solo se puede activar si las interfaces LAN del sistema están en el modo Ethernet-Link **Auto**. En el modo de ahorro de energía, las interfaces LAN del sistema de comunicación cambian automáticamente al modo dúplex completo de 100Mbit/s. Las interfaces LAN de la infraestructura conectada también deben estar en modo de detección automática.	
Activar/Desactivar la gestión de energía	Pone el sistema en modo de ahorro de energía.
Comienzo del modo de ahorro de energía	Momento inicial del modo de ahorro de energía.
Final del modo de ahorro de energía	Momento final del modo de ahorro de energía.
El ancho de banda IP se reduce a 100MBit/s FDX	Indicación de la tasa de datos en modo de ahorro de energía.

28.3.1.26 Instalación básica > Datos masivos

- Descripción de parámetros de las pestañas:

Parámetro	Descripción
Puerto	Número de puerto. Campo no editable.

Parámetro	Descripción
Validez	Existen dos tipos de validación: Prueba de consistencia de front-end y Prueba de consistencia de back-end. a. La **Prueba de consistencia de front-end** valida los datos presentados en los campos de la ventana Asistente de datos masivos, comprobando si presentan inconsistencias y conflictos. En el campo Validez aparece un indicador rojo bajo los números correspondientes. Al pasar el ratón sobre una ventana emergente se puede ver cuál es el conflicto exacto. La **Prueba de consistencia de back-end** valida los datos presentados en el Asistente de datos masivos comparándolos con datos que no se pueden ver pero que están presentes en la base de datos del sistema. Estos son: Grupo, MULAP, Contestador aut., Acceso nacional/internacional, números VSL, Códigos de ruta y Códigos de línea (como acceso de línea urbana).
N.º llam.	Número de teléfono interno de la extensión.
Marcación directa	Número de marcación directa de la extensión.
N.º Dual Mode	Número de teléfono móvil de la extensión.
N.º UC Mobile	Número de móvil personal del usuario de UC Smart o UC Suite. El número debe estar en formato canónico; p. ej., +49 89 7007 100. Este número se muestra en la vista **Mis detalles personales** del usuario, en el **Directorio de usuario**.
Dirección de correo electrónico	Dirección de correo electrónico de la extensión.
Mostrar	Nombre de la extensión (libre). De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización.
Nombre	Nombre de la extensión (libre).
Apellidos	Apellidos de la extensión (libre).
Tipo disposit.	El tipo de dispositivo asignado al usuario. Campo no editable.
Tipo	Tipo de la extensión.
Tipo: **Puerto sin terminal**	El número de teléfono todavía no tiene asignada ninguna extensión.
Tipo: **Cliente sist.**	Un cliente del sistema es una extensión IP que puede utilizar todas las prestaciones del sistema de comunicación mediante CorNet-IP (antes se lo denominaba cliente de sistema HFA)
Tipo: **Cliente SIP**	Un cliente SIP es una extensión IP que usa el protocolo SIP. A través de SIP solo puede utilizar un conjunto de prestaciones restringido del sistema de comunicación.
Tipo: **Usuario de Deskshare**	Un "Usuario Deskshare" es una extensión IP que puede iniciar sesión en otro teléfono del sistema IP (Mobile Login) y utilizarlo como si fuera el suyo propio (incl. número de teléfono).
Fax N.º llam	Si hay configurado un buzón de voz (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que indicar aquí el número de fax con el que la extensión puede recibir mensajes de fax de forma interna.

Parámetro	Descripción
N.º llam. marc. directa de fax	Si hay configurado un buzón de fax (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que introducir aquí el número de teléfono de fax con el que la extensión puede recibir mensajes de fax de forma externa.
Acceso	Indicación de la interfaz física con la que está conectado el terminal.
Clip/Lin	Cadena numérica que ve el usuario llamado al hacerse una llamada saliente externa. Esta cadena aparece en lugar del número de teléfono real (p. ej. para el servicio de emergencia E911 EE. UU.)
Estado	Muestra el estado del dispositivo. Activo o inactivo.

28.3.2 Seguridad

En **Seguridad** se reunen los ajustes importantes en materia de seguridad. Entre ellos se encuentran los ajustes de firewall, filtros, VPN y SSL.

28.3.2.1 Cortafuegos de aplicaciones > de seguridad

Descripción de parámetros de las pestañas:

- **Servicios de visualización**
- **Añadir servicio**
- **Eliminar todos los servicios**

Parámetros	Descripción
Cortafuegos de aplicaciones	El cortafuegos de aplicaciones se utiliza para restringir el acceso a servicios específicos como FTP o LDAP. Por defecto está deshabilitado y se puede habilitar definiendo las reglas adecuadas. Los siguientes servicios pueden ser bloqueados o restringidos a direcciones IP específicas o rangos de direcciones IP por el cortafuegos de aplicaciones: **Servicio / Puertos** HTTPS / 443 Postgres / 5432 LDAP / 389 Manager E / 7000 ssh (bloqueado por defecto) / 22 FTP / 21, 40000 - 40040 OBSERVER / El servicio OBSERVER, que ya no es compatible, permitía el acceso desde una aplicación OpenScape Observer. Solo los servicios enumerados se pueden bloquear a través de un menú de selección en el modo Experto. Las funciones telefónicas como SIP, HFA, etc., no se pueden bloquear mediante el cortafuegos de aplicaciones. Un servicio se puede seleccionar varias veces; cada vez se pueden especificar diferentes restricciones de IP. **Nota:** El cortafuegos de aplicaciones, cuando está habilitado, no bloquea los servicios de forma predeterminada hasta que se añade una regla para ello, momento en el que solo las direcciones IP incluidas en la regla pueden acceder a ese servicio específico. El cortafuegos de aplicaciones puede restringir el acceso a las funciones entre nodos cuando el sistema está conectado en red a otros sistemas OpenScape Business. Por ejemplo, la función de supervivencia requiere que el servicio POSTGRES funcione correctamente. Si se añade manualmente una regla para el servicio POSTGRES, añada las direcciones IP de los otros nodos de red de OpenScape Business a la regla POSTGRES para garantizar el funcionamiento correcto de la característica de supervivencia.
Nombre de la regla	Nombre de la regla
Regla activada	La regla está activada.
Límite inferior del rango de direcciones IP de origen	El límite inferior de las direcciones IP bloqueadas.
Límite superior del rango de direcciones IP de origen	El límite superior de las direcciones IP bloqueadas.

28.3.2.2 Seguridad > Deployment and Licensing Client (DLSC)

Para utilizar las funciones DLS, el sistema de comunicación debe permitir al DLS acceder a los datos de configuración. El sistema de comunicación funciona entonces como cliente de despliegue y licencias. El servidor DLS externo se configura en > Placa base > DHCP > Servidor DHCP > Ajustes globales.

Descripción de parámetros de las pestañas:

- **Configuración básica de DLSC**
- **DLSC de contacto**
- **Restablecer bootstrapping DLSC**

Parámetros	Descripción
Estado	
Comunicación segura con cliente DLS	Indica si la comunicación activa con el cliente DLS está activada o no (0) y en que grado
Cliente DLS	
Intervalo de tiempo para respuesta ContactMe	Valor estándar: 0
PIN necesario para bootstrapping DLS	Nivel de seguridad avanzado mediante entrada de PIN en ambas partes
PIN de bootstrap	Rango de valores: mín. 8 a máx. 32 caracteres
Servidor DLS	
Dirección IP del servidor DLS	Entrada de la dirección IP del servidor DLS externo.
Puerto del servidor DLS	Entrada de puerto del servidor DLS externo Valor estándar: 18443
Puerto seguro del servidor DLS	Indicación del número de puerto para una conexión segura

28.3.2.3 Seguridad > Deployment and Licensing Client (DLSC) > Certificado de cliente DLSC

Descripción de parámetros de las pestañas:

- **Información de certif.**

Parámetros	Descripción
Tipo certif.	Sirve para establecer un contacto inicial seguro entre el sistema de comunicación y el DLS
N° de serie del certificado	Indicación del número de serie establecido.

Parámetros	Descripción
N° de serie del certificado (hex.)	Indicación del número de serie especificado en formato hexadecimal.
Tipo algoritmo firma	Indicación del algoritmo de firma utilizado Rango de valores: sha256RSA, sha512RSA
Inicio de la vigencia del certif. (GMT)	Indicación del comienzo de la validez del certificado. La hora se interpreta como GMT (Greenwich Mean Time).
Fin de la vigencia del certif. (GMT)	Indicación del final de la validez del certificado. La hora se interpreta como GMT (Greenwich Mean Time).
Punto distribución CRL	Indicación de la URL opcional desde la que se distribuyen las listas de bloqueo de certificados (CRL)
Expedido por ent. emisora	Autoridad de certificación que ha firmado el certificado
País (C)	Código de país de dos cifras
Organización (O)	Nombre completo de la empresa legal
Unidad organizativa (OU)	La Unidad organizativa es la división de la compañía que solicita el certificado.
Nombre común (CN)	Nombre de dominio completo (FQDN)
Solicitante	Indicación de los datos del solicitante del certificado según las convenciones del estándar X.509 (p. ej., en el campo País (C) DE para Alemania)
País (C)	Código de país de dos cifras
Organización (O)	Nombre completo de la empresa legal
Unidad organizativa (OU)	La Unidad organizativa es la división de la compañía que solicita el certificado.
Nombre común (CN)	Nombre de dominio completo (FQDN)
Solicitante alternativo	Esta entrada adicional distingue entre el Formato del nombre DN (entradas como en Solicitante) y Otro formato (por ejemplo, entrada de una dirección IP). La máscara de entrada depende del formato elegido
Datos de la clave pública	Datos de clave pública del certificado utilizado para el cifrado
Longitud de la clave pública	Rango de valores: 1024, 1536, 2048
Clave pública	Cifrado mediante claves públicas, confirmadas por un tercero según el estándar X.509. Se garantiza una alta seguridad ya que la clave debe volver a definirse individualmente para el descifrado y solo la guarda el usuario.
Huella dactilar	La clave pública utilizada y la huella decimal se presentan en formato hexadecimal.

28.3.2.4 Seguridad > Deployment and Licensing Client (DLSC) > Certificado de entidad emisora DLSC

Descripción de parámetros de las pestañas:

- **Información de certif.**

Parámetros	Descripción
Tipo certif.	Sirve para establecer un contacto inicial seguro entre el sistema de comunicación y el DLS
N° de serie del certificado	Indicación del número de serie establecido.
N° de serie del certificado (hex.)	Indicación del número de serie especificado en formato hexadecimal.
Tipo algoritmo firma	Indicación del algoritmo de firma utilizado. Rango de valores: sha256RSA, sha512RSA
Inicio de la vigencia del certif. (GMT)	Indicación del comienzo de la validez del certificado. La hora se interpreta como GMT (Greenwich Mean Time).
Fin de la vigencia del certif. (GMT)	Indicación del final de la validez del certificado. La hora se interpreta como GMT (Greenwich Mean Time).
Punto distribución CRL	Indicación de la URL opcional desde la que se distribuyen las listas de bloqueo de certificados (CRL).
Expedido por ent. emisora	Autoridad de certificación que ha firmado el certificado
País (C)	Código de país de dos cifras
Organización (O)	Nombre completo de la empresa legal
Unidad organizativa (OU)	La Unidad organizativa es la división de la compañía que solicita el certificado.
Nombre común (CN)	Nombre de dominio completo (FQDN)
Solicitante	Indicación de los datos del solicitante del certificado según las convenciones del estándar X.509 (p. ej., en el campo País (C) DE para Alemania).
País (C)	Código de país de dos cifras
Organización (O)	Nombre completo de la empresa legal
Unidad organizativa (OU)	La Unidad organizativa es la división de la compañía que solicita el certificado.
Nombre común (CN)	Nombre de dominio completo (FQDN)
Solicitante alternativo	Esta entrada adicional distingue entre el Formato del nombre DN (entradas como en Solicitante) y Otro formato (por ejemplo, entrada de una dirección IP). La máscara de entrada depende del formato elegido.
Datos de la clave pública	Datos de clave pública del certificado utilizado para el cifrado
Longitud de la clave pública	Rango de valores: 1024, 1536, 2048
Clave pública	Cifrado mediante claves públicas, confirmadas por un tercero según el estándar X.509. Se garantiza una alta seguridad ya que la clave debe volver a definirse individualmente para el descifrado y solo la guarda el usuario.
Huella dactilar	La clave pública utilizada y la huella decimal se presentan en formato hexadecimal.

Parámetros	Descripción
Tipo certif.	Sirve para establecer un contacto inicial seguro entre el sistema de comunicación y el DLS

28.3.2.5 Seguridad > Cifrado de señalización y carga útil

Descripción de parámetros de las pestañas:

- **Editar ajustes de seguridad**

Parámetros	Descripción
Extensión mínima de la clave RSA	Extensión mínima de la clave RSA en los certificados. Cuanto mayor sea este valor, más segura será la clave Rango de valores: 512, 1024, 2048 Estándar: 1024
Validación de certificados	Activa o desactiva complemente la validación de certificados. No se recomienda desactivar esta validación. Valor estándar: Activado
Comprobar nombre del solicitante	Comprobando el nombre de solicitante del certificado de un gateway se pude comprobar su identidad. El nombre de solicitante incluye la dirección IP o el nombre DNS (DNS: Domain Name System) del gateway correspondiente Estándar: desactivado
Verificación de CRL	Las listas de bloqueo de certificados (CRL: Certificate Revocation List) permiten determinar si un certificado se ha bloqueado/revocado y por qué. Si una autoridad de certificación (CA: Certificate Authority) señala que un certificado no es válido, registra su número de serie en una lista. Durante la comprobación de certificados, esta lista se puede consultar por Internet en la autoridad de certificación Estándar: desactivado
Forzar remarcado seguro (RFC 5746)	Este procedimiento mejora la seguridad con e remarcado de los parámetros de cifrado de conexiones TLS. Solo se puede utilizar si se utiliza también en todos los servidores conectados. (OpenScape Business, OpenScape 4000 y OpenScape Voice admiten este procedimiento mejorado, pero no HiPath 3000). Estándar: desactivado
Intervalo máximo de remarcado (horas)	Este intervalo determina durante cuánto se puede utilizar una determinada clave para el cifrado de los datos de señalización y uso. Una vez terminado ese tiempo se establece una nueva clave Rango de valores: de 6 a 48 Estándar: 24

28.3.2.6 Seguridad > Cifrado de señalización y carga útil > Certificado SPE

Descripción de parámetros de la pestaña:

- **Importar certificado SPE y clave privada (archivo PKCS#12)**

Parámetros	Descripción
Clave de descifrado	Entrada de la contraseña utilizada al generar el archivo PKCS#12.
Archivo con certificado y clave privada (PEM o Formato PKCS#12)	Selección del archivo que incluye los datos de certificado que se van a importar.

28.3.2.7 Seguridad > Cifrado de señalización y carga útil > Certificados de entidad emisora SPE

Por ejemplo, un cliente de autoridad de certificación PKI (RA/CA) puede importar por separado hasta 16 certificados de entidad emisora de confianza.

Descripción de parámetros de la pestaña:

- **Importar certificado de entidad emisora seguro (archivo X.509) para SPE**

Parámetros	Descripción
Archivo con certificado (PEM o binario)	Selección del archivo PEM o binario que se va a importar.
Protocolo de punto de distribución CRL (CDP)	Selección de protocolo para las listas CRL (listas de revocación de certificados) Rango de valores: LDAP o HTTP
CDP (sin p. ej. ldap://)	Un CDP es una ampliación de certificado opcional. Los certificados recibidos se comprueban con la lista CRL configurada para el CDP.

28.3.2.8 Seguridad > VPN

Descripción de parámetros de las pestañas:

- **Mostrar información general**
- **Activar tablas VPN configuradas**
- **Activar / Desactivar IPsec**

Parámetros	Descripción
Algoritmos de cifrado	Algoritmos de cifrado utilizados Rango de valores: AES, 3DES
Algoritmos hash	Función hash estándar de criptología para calcular un valor de comprobación único (firma digital) Rango de valores: MD5, SHA1, SHA2
Algoritmos Public-Key	Procedimiento de cifrado asimétrico Rango de valores: RSA

Parámetros	Descripción
Grupos Diffie-Hellman	Procedimiento para sustituir claves Rango de valores: Grupo DH 2, Grupo DH 5
Botones	
Act. inmediat.	Aquí se pueden activar las tablas VPN. ¡Siga las indicaciones de aviso!
Activar/Desactivar IPsec	IPSec se puede activar o desactivar. ¡Siga las indicaciones de aviso!

28.3.2.9 Seguridad > VPN > Entidad emisora Lightweight

Descripción de parámetros de las pestañas:

- **Generar certificado de entidad emisora**

Parámetros	Descripción
Nombre del certif.	Nombre libre para el certificado que se va a generar
N° de serie del certificado	Entrada de un número de serie definido por Ud. El número de serie debe ser una cifra entera y positiva.
Tipo algoritmo firma	Selección del algoritmo de firma que se va a utilizar para este certificado Rango de valores: sha25RSA, sha512RSA
Longitud de la clave pública	Selección de una extensión de clave para el certificado Rango de valores: 2048
Inicio de la vigencia del certif. (GMT) Desde cuándo será válido el certificado. La hora se interpreta como GMT (Greenwich Mean Time).	
Fin de la vigencia del certif. (GMT) Hasta cuándo será válido el certificado. La hora se interpreta como GMT (Greenwich Mean Time).	
Solicitante Indicación de los datos para el solicitante del certificado según las convenciones del estándar X.509 (p. ej., en el campo País (C) DE para Alemania).	
Solicitante alternativo Esta entrada opcional distingue entre el formato del nombre DN (datos como en Solicitante) y otro formato (p. ej., entrada de una dirección IP). La máscara de entrada depende del formato elegido. Si se selecciona otro formato, se pueden configurar varias entradas SAN.	
Formato del nombre DN	También se suele proporcionar como RDN del nombre común en el campo Asunto del certificado principal.
Otro formato	Otros nombres, dados como un nombre general

Parámetros	Descripción
Nombre alternativo solicitante, extensión	Rango de valores: Nombre DNS, Dirección IP, Dirección e-mail, URI, Indicador universal de recursos, Otros
Solicitante alternativo	Esta entrada adicional distingue entre el Formato del nombre DN (entradas como en Solicitante) y Otro formato (por ejemplo, entrada de una dirección IP). La máscara de entrada depende del formato elegido. Si se selecciona otro formato, se pueden configurar varias entradas SAN.
Tipo de punto de distribución CRL	Rango de valores: Nombre DNS, Dirección IP, Dirección e-mail, URI, Indicador universal de recursos, Otros
Punto distribución CRL	Indicación de una URL desde la que se distribuyen listas de bloqueo de certificados (CRL).
Generar certificado	

28.3.2.10 Seguridad > VPN > Admin. certificados

Descripción de parámetros de las pestañas:

- **Mostrar certif. de archivo**

Parámetros	Descripción
Formato PKCS#12	Si el certificado está guardado en un archivo PKCS#12, hay que activar este campo.
Clave de descifrado	Si se ha activado el campo Formato PKCS#12, en este campo debe introducir la misma contraseña que se utilizó al generar el archivo.
Archivo con certificado	En este campo, introduzca la ruta y el nombre de archivo del certificado. Haga clic en Examinar si no conoce la ubicación archiva. Aparece un cuadro de diálogo de búsqueda.

28.3.2.11 Seguridad > VPN > Admin. certificados > Certif. de entidad emisora de confianza > Certificados activ.

Descripción de parámetros de la pestaña:

- **Importar certif. de entidad emisora de confianza (X.509)**

Parámetros	Descripción
Tipo certif.	Sirve para establecer un contacto inicial seguro entre el sistema de comunicación y el DLS
N° de serie del certificado	Indicación del número de serie establecido.
N° de serie del certificado (hex.)	Indicación del número de serie especificado en formato hexadecimal.
Tipo algoritmo firma	Indicación del algoritmo de firma utilizado Rango de valores: sha256RSA, sha512RSA

Parámetros	Descripción
Inicio de la vigencia del certif. (GMT)	Indicación del comienzo de la validez del certificado. La hora se interpreta como GMT (Greenwich Mean Time).
Fin de la vigencia del certif. (GMT)	Indicación del final de la validez del certificado. La hora se interpreta como GMT (Greenwich Mean Time).
Punto distribución CRL	Indicación de la URL opcional desde la que se distribuyen las listas de bloqueo de certificados (CRL)
Expedido por ent. emisora	Autoridad de certificación que ha firmado el certificado
País (C)	Código de país de dos cifras
Organización (O)	Nombre completo de la empresa legal
Unidad organizativa (OU)	La Unidad organizativa es la división de la compañía que solicita el certificado.
Nombre común (CN)	Nombre de dominio completo (FQDN)
Solicitante	Indicación de los datos del solicitante del certificado según las convenciones del estándar X.509 (p. ej., en el campo País (C) DE para Alemania)
País (C)	Código de país de dos cifras
Organización (O)	Nombre completo de la empresa legal
Unidad organizativa (OU)	La Unidad organizativa es la división de la compañía que solicita el certificado.
Nombre común (CN)	Nombre de dominio completo (FQDN)
Solicitante alternativo	Esta entrada adicional distingue entre el Formato del nombre DN (entradas como en Solicitante) y Otro formato (por ejemplo, entrada de una dirección IP). La máscara de entrada depende del formato elegido
Datos de la clave pública	Datos de clave pública del certificado utilizado para el cifrado
Longitud de la clave pública	Rango de valores: 1024, 1536, 2048
Clave pública	Cifrado mediante claves públicas, confirmadas por un tercero según el estándar X.509. Se garantiza una alta seguridad ya que la clave debe volver a definirse individualmente para el descifrado y solo la guarda el usuario.
Huella dactilar	La clave pública utilizada y la huella decimal se presentan en formato hexadecimal.

28.3.2.12 Seguridad > VPN > Admin. certificados > Certif. de entidad emisora de confianza > Certificados configurados

Descripción de parámetros de la pestaña:

- **Importar certif. de entidad emisora de confianza (X.509)**

Parámetros	Descripción
Nombre del certif.	Entrada del nombre que va a tener el certificado.
Archivo con certificado	Ruta y nombre de archivo del certificado. Al hacer clic en Examinar se abre un cuadro de búsqueda para buscar el lugar de almacenamiento del archivo.

28.3.2.13 Seguridad > VPN > Certificados de par

Descripción de parámetros de las pestañas:

- **Generar solicitud de certificado (CSR)**
- **Importar certificado de par (PKCS#12)**

Parámetros	Descripción
Nombre de la solicitud de certif.	Se puede generar un certificado de par firmado por entidad emisora (basado en un certificado de entidad emisora). El requisito es que se haya generado, como mínimo, un certificado de entidad emisora. El certificado creado se guarda en un archivo PKCS#12. Los archivos PKCS#12 (PKCS#12 Estándar de sintaxis de intercambio de información personal) guardan certificados con una clave privada. De esta forma, un archivo PKCS#12 contiene los datos esenciales para el cifrado y descifrado personal.
Tipo algoritmo firma	Seleccione el algoritmo de firma que desea utilizar para este certificado. Rango de valores: sha25RSA, sha512RSA
Longitud de la clave pública	Rango de valores: 2048
Solicitante	Indicación de los datos para el solicitante del certificado según las convenciones del estándar X.509 (p. ej., en el campo País (C) DE para Alemania).
País (C)	Código de país de dos cifras
Organización (O)	Nombre completo de la empresa legal
Unidad organizativa (OU)	La Unidad organizativa es la división de la compañía que solicita el certificado.
Nombre común (CN)	Nombre de dominio completo (FQDN)
Solicitante alternativo	Esta entrada adicional distingue entre el Formato del nombre DN (entradas como en Solicitante) y Otro formato (por ejemplo, entrada de una dirección IP). La máscara de entrada depende del formato elegido. Si se selecciona otro formato, se pueden configurar varias entradas SAN.
Formato del nombre DN	También se suele proporcionar como RDN del nombre común en el campo Asunto del certificado principal.
País (C)	Código de país de dos cifras
Organización (O)	Nombre completo de la empresa legal
Unidad organizativa (OU)	La Unidad organizativa es la división de la compañía que solicita el certificado.
Nombre común (CN)	Nombre de dominio completo (FQDN)

Parámetros	Descripción
Otro formato	Otros nombres, dados como un nombre general
Nombre alternativo solicitante, extensión	Rango de valores: Nombre DNS, Dirección IP, Dirección e-mail, URI, Indicador universal de recursos, Otros
Nombre alternativo solicitante	Esta entrada adicional distingue entre el Formato del nombre DN (entradas como en Solicitante) y Otro formato (por ejemplo, entrada de una dirección IP). La máscara de entrada depende del formato elegido.
Importar certificado de par [PKCS#12]	
Nombre del certif.	Entrada del nombre que va a tener el certificado.
Clave de descifrado	Contraseña para descifrar el certificado de par Rango de valores: mín. 7 y máx. 32 caracteres
Archivo con certificado	Haga clic en Examinar. Aparece un cuadro de diálogo de búsqueda.
Mostrar huella dactilar de certif.	Haga clic en este botón para verificar la integridad del certificado.
Importar certif. de archivo	Haga clic en este botón para importar un certificado.

28.3.2.14 Seguridad > VPN > Servicios > Servicios activos

Descripción de parámetros de la pestaña:

- **Mostrar servicios IPsec**

Parámetros	Descripción
Nombre servicio	Este campo incluye los nombres de los servicios configurados.
Estado en pila IP	
Puerto origen	Indicación del número de puerto de origen. Si aparece como puerto el número "0", se refiere a cualquier puerto o a un puerto desconocido.
Puerto destino	Indicación del número de puerto de destino. Si aparece como puerto el número "0", se refiere a cualquier puerto o a un puerto desconocido.
Protocolo IP	Indicación del protocolo IP utilizado para la transferencia.
Regla 'pass' correspond.	Indicación de la regla "Pass" correspondiente. Con estas reglas se asignan reglas y servicios.
Regla 'deny' correspond.	Indicación de la regla "Deny" correspondiente. Con estas reglas se asignan reglas y servicios.

28.3.2.15 Seguridad > VPN > Servicios > Servicios configurados

Descripción de parámetros de las pestañas:

- **Mostrar servicios IPsec**

- **Añadir servicios IPSec**
- **Modificar servicios IPSec**
- **Cambiar el nombre de servicios IPSec**
- **Borrar servicios IPSec**

Parámetros	Descripción
Nombre servicio	Campo de entrada para el nombre del servicio configurado. Introduzca una cadena de caracteres en este campo.
Puerto origen	Número del puerto que se quiere utilizar para la transferencia de datos en el lado de envío. Si se establece "0" como puerto, se corresponde con cualquier puerto o con un puerto desconocido.
Puerto destino	Número del puerto que se quiere utilizar para la transferencia de datos en el lado del receptor. Si se establece "0" como puerto, se corresponde con cualquier puerto o con un puerto desconocido.
Protocolo IP	Protocolo IP que se va a utilizar para la transferencia Rango de valores: ICMP, TCP, UDP
Nombre servicio	Campo de entrada para el nombre del servicio que se va a configurar.
Puerto origen	Número del puerto que se quiere utilizar para la transferencia de datos en el lado de envío. Si se establece "0" como puerto, se corresponde con cualquier puerto o con un puerto desconocido.
Puerto destino	Número del puerto que se quiere utilizar para la transferencia de datos en el lado del receptor. Si se establece "0" como puerto, se corresponde con cualquier puerto o con un puerto desconocido.
Protocolo IP	Seleccione el protocolo IP utilizado para la transferencia Rango de valores: ICMP, TCP, UDP
Nombre servicio	Campo de entrada para el nombre del servicio que se va a configurar.
	Solo se puede borrar si el servicio no tiene asignada ninguna regla.

28.3.2.16 Seguridad > VPN > Túnel > Túneles activos

Descripción de parámetros de las pestañas:

- **Mostrar datos generales de túnel**
- **Mostrar reglas de todos túneles**

Parámetros	Descripción
Nombre del túnel	Este campo incluye el nombre del túnel configurado.
Estado en pila IP	Mecanismo de estado en la pila IP. Rango de valores: activo / no activo
Tipo punto terminal túnel local	Indicación de la dirección de punto terminal en el lado de envío del túnel (se puede indicar un nombre host o un nombre DNS).

Parámetros	Descripción
Dir. punto terminal túnel local	Indicación de la dirección de punto terminal en el túnel local.
Tipo punto terminal túnel remoto	Indicación del tipo de punto terminal del túnel remoto.
Dir. punto terminal túnel remoto	Indicación del tipo de punto terminal del túnel remoto. Si se muestra la dirección 0.0.0.0, significa que se ha detectado el punto terminal del túnel. En tal caso, será siempre el colateral (p. ej., teletrabajador) el encargado de establecer el túnel.
Vigencia propuesta de las claves de sesión	Indicación de la validez aceptada para las claves de sesión (Session Keys) en uso. Terminado ese tiempo, no se intercambiarán más datos dentro de esa sesión. Para sustituir las claves de sesión invalidadas, se negocian automáticamente nuevas claves de sesión.
Vigencia propuesta de la sesión de intercamb. claves	Indicación de la validez aceptada para la sesión de intercambio de claves. Terminada la sesión de intercambio de claves, se negociarán automáticamente nuevas claves para la sesión de intercambio de claves mediante IKE (protocolo de cifrado).
Reglas correspond.: Regla envío correspond.	Configuración de la regla de envío en VPN>Reglas
Reglas correspond.: Regla recepción correspond.	Configuración de la regla de recepción en VPN>Reglas
Datos túnel	
Nombre del túnel	Este campo incluye el nombre del túnel configurado.
Estado en pila IP	Mecanismo de estado en la pila IP. Rango de valores: activo / no activo
Tipo punto terminal túnel local	Indicación de la dirección de punto terminal en el lado de envío del túnel (se puede indicar un nombre host o un nombre DNS).
Dir. punto terminal túnel local	Indicación de la dirección de punto terminal en el túnel local.
Tipo punto terminal túnel remoto	Indicación del tipo de punto terminal del túnel remoto.
Dir. punto terminal túnel remoto	Indicación del tipo de punto terminal del túnel remoto. Si se muestra la dirección 0.0.0.0, significa que se ha detectado el punto terminal del túnel. En tal caso, será siempre el colateral (p. ej., teletrabajador) el encargado de establecer el túnel.
Datos regla	
Destino	Indicador de estado del destino. Rango de valores: Enviar/Recibir

Parámetros	Descripción
Prioridad	Indicación de la prioridad para la secuencia de procesamiento. La prioridad máxima se indica con 1. Se asigna una prioridad propia a cada regla de una ruta. Una regla y la regla de la dirección contraria correspondiente siempre deben tener la misma prioridad. Las reglas de la dirección opuesta solo se pueden configurar con la opción de menú correspondiente.
Acción para la regla	Muestra cómo gestiona la regla los paquetes IP: "pass" significa que los paquetes IP se transfieren; con "deny", no se transfieren los paquetes IP.
Cifrado obligatorio	Indicación de un cifrado para esta regla. El procedimiento de cifrado se define mediante el túnel asignado.
Estado de regla	Indicador de estado en la regla. Rango de valores: Activado/Desactivado
Estado en pila IP	Mecanismo de estado en la pila IP. Rango de valores: activo / no activo
Dirección orig. Indicación de la dirección de origen y de destino en el formato adecuado para el tipo seleccionado. La indicación depende del tipo de dirección seleccionado. Si hay que usar cualquier dirección IP, aparece 0.0.0.0. Si se ha especificado 0.0.0.0 como dirección de destino para enviar paquetes en un túnel, en la interfaz con la red de destino hay que desactivar NAT. Como alternativa también se puede indicar una IP entre 0.0.0.1 y 255.255.255.254 para enviar paquetes en un túnel.	
Tipo	Indicación del tipo de dirección de origen y de destino (opciones: Host, Subred, Área direcciones IP y Nombre DNS).
Dirección (últ. del área)	Indicación de la dirección de origen y de destino en el formato adecuado para el tipo seleccionado. La máscara de entrada depende del tipo de dirección seleccionado. Si hay que usar cualquier dirección IP, aparece 0.0.0.0. Si se ha especificado 0.0.0.0 como dirección de destino para enviar paquetes en un túnel, en la interfaz con la red de destino hay que desactivar NAT. Como alternativa también se puede indicar una IP entre 0.0.0.1 y 255.255.255.254 para enviar paquetes en un túnel.
Másc. de subred/primera direcc. del área	Se establece en caso de que haga falta definir un rango de direcciones de origen/destino para la transmisión
Dir. destino	
Tipo	Indicación del tipo de dirección de origen y de destino (opciones: Host, Subred, Área direcciones IP y Nombre DNS).
Dirección (últ. del área)	Indicación de la dirección de origen y de destino en el formato adecuado para el tipo seleccionado. La máscara de entrada depende del tipo de dirección seleccionado. Si hay que usar cualquier dirección IP, aparece 0.0.0.0. Si se ha especificado 0.0.0.0 como dirección de destino para enviar paquetes en un túnel, en la interfaz con la red de destino hay que desactivar NAT. Como alternativa también se puede indicar una IP entre 0.0.0.1 y 255.255.255.254 para enviar paquetes en un túnel.
Másc. de subred/primera direcc. del área	Se establece en caso de que haga falta definir un rango de direcciones de origen/destino para la transmisión

Parámetros	Descripción
Datos servicio Indicación del servicio al que se restringe el cifrado. Si el cifrado no va a estar restringido a un solo servicio, seleccione "Cualquier servicio".	
Nombre servicio	Campo de entrada para el nombre del servicio que se va a configurar.
Puerto origen	Indicación del túnel de la dirección de recepción al que se aplica esta regla. Los paquetes recibidos por la red se toman de este túnel. Seleccione Ninguna asignación túnel, si no desea asignar ningún túnel el la dirección de recepción.
Puerto destino	Indicación del túnel de la dirección de envío al que se aplica esta regla. A este túnel se envían los paquetes IP que hay que enviar a la red. Seleccione Ninguna asignación túnel, si no desea asignar ningún túnel en la dirección de envío.
Protocolo IP	Seleccione el protocolo IP utilizado para la transferencia Rango de valores: ICMP, TCP, UDP

28.3.2.17 Seguridad > VPN > Túnel > Túneles config.

Descripción de parámetros de las pestañas:

- **Mostrar datos generales de túnel**
- **Mostrar reglas de todos túneles**
- **Añadir túnel / Editar datos de túnel**
- **Datos de intercambio de claves**

Parámetros	Descripción
	Un túnel designa un transporte de paquetes de datos cifrados hasta un punto terminal definido de forma fija. Los túneles activos son túneles configurados tras una activación de la configuración. En total, se pueden configurar hasta 256 túneles por gateway.
Nombre del túnel	Este campo incluye el nombre del túnel configurado.
Estado en pila IP	Mecanismo de estado en la pila IP. Rango de valores: activo / no activo
Tipo punto terminal túnel local	Indicación de la dirección de punto terminal en el lado de envío del túnel (se puede indicar un nombre host o un nombre DNS).
Dir. punto terminal túnel local	Indicación de la dirección de punto terminal en el túnel local.
Tipo punto terminal túnel remoto	Indicación del tipo de punto terminal del túnel remoto.
Dir. punto terminal túnel remoto	Indicación del tipo de punto terminal del túnel remoto. Si se muestra la dirección 0.0.0.0, significa que se ha detectado el punto terminal del túnel. En tal caso, será siempre el colateral (p. ej., teletrabajador) el encargado de establecer el túnel.

Parámetros	Descripción
Vigencia propuesta de las claves de sesión	Indicación de la validez aceptada para las claves de sesión (Session Keys) en uso. Terminado ese tiempo, no se intercambiarán más datos dentro de esa sesión. Para sustituir las claves de sesión invalidadas, se negocian automáticamente nuevas claves de sesión.
Vigencia propuesta de la sesión de intercamb. claves	Indicación de la validez aceptada para la sesión de intercambio de claves. Terminada la sesión de intercambio de claves, se negociarán automáticamente nuevas claves para la sesión de intercambio de claves mediante IKE (protocolo de cifrado).
Reglas correspond.: Regla envío correspond.	Configuración de la regla de envío en VPN>Reglas
Reglas correspond.: Regla recepción correspond.	Configuración de la regla de recepción en VPN>Reglas
Datos túnel	
Nombre del túnel	Este campo incluye el nombre del túnel configurado.
Estado en pila IP	Mecanismo de estado en la pila IP. Rango de valores: activo / no activo
Tipo punto terminal túnel local	Indicación de la dirección de punto terminal en el lado de envío del túnel (se puede indicar un nombre host o un nombre DNS).
Dir. punto terminal túnel local	Indicación de la dirección de punto terminal en el túnel local.
Tipo punto terminal túnel remoto	Indicación del tipo de punto terminal del túnel remoto.
Dir. punto terminal túnel remoto	Indicación del tipo de punto terminal del túnel remoto. Si se muestra la dirección 0.0.0.0, significa que se ha detectado el punto terminal del túnel. En tal caso, será siempre el colateral (p. ej., teletrabajador) el encargado de establecer el túnel.
Datos regla	
Destino	Indicador de estado del destino. Rango de valores: Enviar/Recibir
Prioridad	Indicación de la prioridad para la secuencia de procesamiento. La prioridad máxima se indica con 1. Se asigna una prioridad propia a cada regla de una ruta. Una regla y la regla de la dirección contraria correspondiente siempre deben tener la misma prioridad. Las reglas de la dirección opuesta solo se pueden configurar con la opción de menú correspondiente.
Acción para la regla	Muestra cómo gestiona la regla los paquetes IP: "pass" significa que los paquetes IP se transfieren; con "deny", no se transfieren los paquetes IP.
Cifrado obligatorio	Indicación de un cifrado para esta regla. El procedimiento de cifrado se define mediante el túnel asignado.
Estado de regla	Indicador de estado en la regla. Rango de valores: Activado/Desactivado

Parámetros	Descripción
Estado en pila IP	Mecanismo de estado en la pila IP. Rango de valores: activo / no activo
Dirección orig. Indicación de la dirección de origen y de destino en el formato adecuado para el tipo seleccionado. La indicación depende del tipo de dirección seleccionado. Si hay que usar cualquier dirección IP, aparece 0.0.0.0. Si se ha especificado 0.0.0.0 como dirección de destino para enviar paquetes en un túnel, en la interfaz con la red de destino hay que desactivar NAT. Como alternativa también se puede indicar una IP entre 0.0.0.1 y 255.255.255.254 para enviar paquetes en un túnel.	
Tipo	Indicación del tipo de dirección de origen y de destino (opciones: Host, Subred, Área direcciones IP y Nombre DNS).
Dirección (últ. del área)	Indicación de la dirección de origen y de destino en el formato adecuado para el tipo seleccionado. La máscara de entrada depende del tipo de dirección seleccionado. Si hay que usar cualquier dirección IP, aparece 0.0.0.0. Si se ha especificado 0.0.0.0 como dirección de destino para enviar paquetes en un túnel, en la interfaz con la red de destino hay que desactivar NAT. Como alternativa también se puede indicar una IP entre 0.0.0.1 y 255.255.255.254 para enviar paquetes en un túnel.
Másc. de subred/primera direcc. del área	Se establece en caso de que haga falta definir un rango de direcciones de origen/destino para la transmisión
Dir. destino	
Tipo	Indicación del tipo de dirección de origen y de destino (opciones: Host, Subred, Área direcciones IP y Nombre DNS).
Dirección (últ. del área)	Indicación de la dirección de origen y de destino en el formato adecuado para el tipo seleccionado. La máscara de entrada depende del tipo de dirección seleccionado. Si hay que usar cualquier dirección IP, aparece 0.0.0.0. Si se ha especificado 0.0.0.0 como dirección de destino para enviar paquetes en un túnel, en la interfaz con la red de destino hay que desactivar NAT. Como alternativa también se puede indicar una IP entre 0.0.0.1 y 255.255.255.254 para enviar paquetes en un túnel.
Másc. de subred/primera direcc. del área	Se establece en caso de que haga falta definir un rango de direcciones de origen/destino para la transmisión
Datos servicio Indicación del servicio al que se restringe el cifrado. Si el cifrado no va a estar restringido a un solo servicio, seleccione "Cualquier servicio".	
Nombre servicio	Campo de entrada para el nombre del servicio que se va a configurar.
Puerto origen	Indicación del túnel de la dirección de recepción al que se aplica esta regla. Los paquetes recibidos por la red se toman de este túnel. Seleccione Ninguna asignación túnel, si no desea asignar ningún túnel el la dirección de recepción.
Puerto destino	Indicación del túnel de la dirección de envío al que se aplica esta regla. A este túnel se envían los paquetes IP que hay que enviar a la red. Seleccione Ninguna asignación túnel, si no desea asignar ningún túnel en la dirección de envío.

Parámetros	Descripción
Protocolo IP	Protocolo IP que se va a utilizar para la transferencia Rango de valores: ICMP, TCP, UDP
Nombre del túnel	Este campo incluye el nombre del túnel nuevo configurado.
Habilitar servicio remoto a través de VPN: (se puede activar a través del código de servicio)	Marque este campo si desea utilizar el túnel VPN para la administración remota.
Tipo punto terminal túnel local	Seleccione el tipo de la dirección de punto terminal en el lado de envío del túnel (se puede indicar un nombre de host o DNS).
Dir. punto terminal túnel local	Registre la dirección del remitente en el formato adecuado para el tipo de punto terminal.
Tipo punto terminal túnel remoto	Tipo de dirección de punto terminal en el lado de recepción del túnel (se admite la indicación de la dirección IP).
Dir. punto terminal túnel remoto	Dirección de recepción en el formato adecuado para el tipo de punto terminal. Si se establece la dirección 0.0.0.0, el punto terminal de túnel es desconocido. En tal caso, será siempre el colateral (p. ej., teletrabajador) el encargado de establecer el túnel.
Manejo de clave de sesión	En Manejo de clave de sesión se registra el procedimiento para el intercambio de claves (automáticamente, con el protocolo IKE).
Algoritmos de cifrado propuestos	Qué algoritmos se pueden utilizar Rango de valores: AES, 3DES
Algoritmos hash propuestos	Qué algoritmos hash (algoritmos de prueba) se pueden usar. Los algoritmos seleccionados son ofrecidos por el iniciador del intercambio IKE. Rango de valores: MD5, SHA1, SHA2
Vigencia propuesta de las claves de sesión	Validez de las claves de sesión (Session Keys) que se utilizan. Terminado ese tiempo, no se intercambiarán más datos dentro de esa sesión. En lugar de claves de sesión que han dejado de ser válidas se gestionan nuevas claves de sesión automáticamente
Vigencia propuesta de la sesión de intercamb. claves	Validez para la sesión de intercambio de claves. Terminada la sesión de intercambio de claves, se negociarán automáticamente nuevas claves para la sesión de intercambio de claves mediante IKE
Volumen de datos propuesto de las claves de sesión	Volumen de datos máximo para las claves de sesión (Session Keys). Si se supera ese volumen máximo, se negociará automáticamente una nueva clave de sesión mediante IKE. Si se selecciona "ilimitado", el volumen de datos es ilimitado.
Activar 'Perfect Forward Secrecy'	Se recomienda marcar siempre esta opción ya que con ello se activa un mecanismo de seguridad mejorado para la transferencia de datos a través del túnel
Procedim. autenticación de pares VPN	Procedimiento de autenticación para las extensiones VPN. Se pueden usar firmas digitales (autenticación mediante certificados) y Pre-Shared Keys (autenticación mediante claves manuales autodefinidas)

Parámetros	Descripción
Pre-Shared Key	Este campo solo está disponible si el procedimiento de autenticación está definido en Pre-Shared Keys. Aquí hay que registrar la contraseña que deben usar las extensiones VPN en los dos puntos terminales del túnel. Debe tener al menos 12 posiciones.
Repetición de Pre-Shared Key	Este campo solo está disponible si el procedimiento de autenticación está definido en Pre-Shared Keys.
Lista de certif. de entidad emisora	Estas opciones solo están disponibles si el procedimiento de autenticación se ha definido en Firmas digitales. Las extensiones VPN pueden utilizar para la autenticación cualquier certificado emitido (firmado) por uno de los certificados de entidad emisora marcados
Grupos Diffie-Hellman propuestos	Las extensiones VPN pueden utilizar para el intercambios de claves cualquier procedimiento marcado

Nota: La adición/borrado de un túnel VPN se debe activar en "VPN > Activar tablas VPN configuradas".

28.3.2.18 Seguridad > VPN > Reglas > Reglas activas

Descripción de parámetros de la pestaña:

- **Mostrar reglas**

Parámetros	Descripción
Prioridad	Indicación de la prioridad de la secuencia de procesamiento como número. La prioridad máxima se indica con 1. Se asigna una prioridad propia a cada regla de una ruta. Una regla y la regla de la dirección contraria correspondiente siempre deben tener la misma prioridad.
Servicio	Indicación del servicio al que se restringe el cifrado. Si el cifrado no está limitado a un servicio, se muestra "Cualquier servicio".
Acción para la regla	Indicación de cómo se gestionan los paquetes IP con esta regla: "pass" significa que los paquetes IP se transfieren; con "deny", no se transfieren los paquetes IP.
Cifrado obligatorio	Indicación del cifrado. El procedimiento de cifrado se define mediante el túnel asignado.
Estado de regla	Indicador de estado en la regla. Rango de valores: Activado / Desactivado
Estado en pila IP	Mecanismo de estado en la pila IP. Rango de valores: Activado / Desactivado
Dirección orig.	
Tipo	Indicación del tipo de la dirección de origen. Rango de valores: Host, Subred, Área direcc. IP, Nombre DNS

Parámetros	Descripción
Dirección (últ. del área)	Indicación de la dirección de origen y de destino en el formato adecuado para el tipo seleccionado. La máscara de entrada depende del tipo de dirección seleccionado. Si hay que usar cualquier dirección IP, aparece 0.0.0.0. Si se ha especificado 0.0.0.0 como dirección de destino para enviar paquetes en un túnel, en la interfaz con la red de destino hay que desactivar NAT. Como alternativa también se puede indicar una IP entre 0.0.0.1 y 255.255.255.254 para enviar paquetes en un túnel.
Másc. de subred/primera direcc. del área	Se establece en caso de que haga falta definir un rango de direcciones de origen/destino para la transmisión
Dir. destino	
Tipo	Indicación del tipo de la dirección de destino. Rango de valores: Host, Subred, Área direcc. IP, Nombre DNS
Dirección (superior del área)	
Másc. de subred/primera direcc. del área	Se establece en caso de que haga falta definir un rango de direcciones de origen/destino para la transmisión
Túnel para cifrado	
Túnel lado recepción	Indicación del túnel de la dirección de recepción al que se aplica esta regla. Los paquetes recibidos por la red se toman de este túnel. Indicación: Ninguna asignación túnel (si la dirección de recepción no hay asignado ningún túnel).
Túnel lado envío	Indicación del túnel de la dirección de envío al que se aplica esta regla. Los paquetes recibidos por la red se toman de este túnel. Indicación: Ninguna asignación túnel (si en la dirección de envío no hay asignado ningún túnel).

28.3.2.19 Seguridad > VPN > Reglas > Reglas configuradas

Las reglas establecen qué ha de suceder con un paquete IP. La acción de regla Pass significa que el paquete IP continúa siendo transportado (pasado). La acción de regla Deny significa que el paquete IP no continúa siendo transportado (ignorado). Asimismo, se puede seleccionar si el paquete IP (cifrado) utilizará o no un túnel VPN. El sistema de comunicación puede administrar 640 reglas. 6 de ellas están preasignadas (reglas predeterminadas) y 634 se pueden asignar libremente.

Descripción de parámetros de las pestañas:

- **Mostrar reglas**
- **Añadir regla**
- **Editar regla**
- **Añadir regla para dirección opuesta**
- **Borrar regla**

Parámetros	Descripción
Prioridad	Indicación de la prioridad de la secuencia de procesamiento como número. La prioridad máxima se indica con 1. Se asigna una prioridad propia a cada regla de una ruta. Una regla y la regla de la dirección contraria correspondiente siempre deben tener la misma prioridad.
Servicio	Indicación del servicio al que se restringe el cifrado. Si el cifrado no está limitado a un servicio, se muestra "Cualquier servicio".
Acción para la regla	Indicación de cómo se gestionan los paquetes IP con esta regla: "pass" significa que los paquetes IP se transfieren; con "deny", no se transfieren los paquetes IP.
Cifrado obligatorio	Indicación del cifrado. El procedimiento de cifrado se define mediante el túnel asignado.
Estado de regla	Indicador de estado en la regla. Rango de valores: Activado/Desactivado
Estado en pila IP	Mecanismo de estado en la pila IP. Rango de valores: Activado / Desactivado
Dirección orig.	
Tipo	Indicación del tipo de la dirección de origen. Rango de valores: Host, Subred, Área direcc. IP, Nombre DNS
Dirección (últ. del área)	Indicación de la dirección de origen y de destino en el formato adecuado para el tipo seleccionado. La máscara de entrada depende del tipo de dirección seleccionado. Si hay que usar cualquier dirección IP, aparece 0.0.0.0. Si se ha especificado 0.0.0.0 como dirección de destino para enviar paquetes en un túnel, en la interfaz con la red de destino hay que desactivar NAT. Como alternativa también se puede indicar una IP entre 0.0.0.1 y 255.255.255.254 para enviar paquetes en un túnel.
Másc. de subred/primera direcc. del área	Se establece en caso de que haga falta definir un rango de direcciones de origen/destino para la transmisión
Dir. destino	
Tipo	Indicación del tipo de la dirección de destino. Rango de valores: Host, Subred, Área direcc. IP, Nombre DNS
Dirección (superior del área)	
Másc. de subred/primera direcc. del área	Se establece en caso de que haga falta definir un rango de direcciones de origen/destino para la transmisión
Túnel para cifrado	
Túnel lado recepción	Indicación del túnel de la dirección de recepción al que se aplica esta regla. Los paquetes recibidos por la red se toman de este túnel. Indicación: Ninguna asignación túnel (si la dirección de recepción no hay asignado ningún túnel).

Parámetros	Descripción
Túnel lado envío	Indicación del túnel de la dirección de envío al que se aplica esta regla. Los paquetes recibidos por la red se toman de este túnel. Indicación: Ninguna asignación túnel (si en la dirección de envío no hay asignado ningún túnel).

28.3.2.20 Seguridad > VPN > Public Key Infrastructure (PKI)

Con servidor PKI designa un servidor que puede emitir, distribuir y comprobar certificados digitales. Los certificados emitidos dentro de una PKI (Infraestructura de clave pública) se utilizan para asegurar la comunicación. Al utilizar certificados (firmas digitales), se intenta utilizar la URL de PKI configurada por el servidor de PKI para descargar el CRL.

Descripción de parámetros de las pestañas:

- **Mostrar servidor PKI**
- **Añadir servidor PKI**

Parámetros	Descripción
Nombre servidor PKI	Introduzca un nombre fácilmente reconocible para el servidor.
Tipo servidor PKI	Seleccione la salida del servidor (opciones: LDAP y Enrollment).
URL de servidor PKI	Introduzca la URL del servidor (p. ej., LDAP://139.21.92.144:389).

28.3.2.21 Seguridad > SSL > Generación de certif.

El acceso de administración se realiza de forma cifrada por HTTPS y usando el protocolo TLS 1.2. Los certificados permiten autenticar la conexión. De forma predeterminada se usa un certificado con firma automática. Para aumentar la seguridad se puede utilizar un certificado específico del cliente procedente de una autoridad de certificación o entidad emisora (CA). El sistema de comunicación se autentica con el cliente de administración mediante los certificados importados o generados en la Gestión basada en Web (WBM). En el navegador se puede importar uno de estos certificados como certificado confidencial para evitar la emisión de mensajes de advertencia del navegador al establecer conexión con el servidor SSL.

Descripción de parámetros de las pestañas:

- **Generar certificado de entidad emisora**
- **Generar certif. con firma automática**

Parámetros	Descripción
Nombre del certif.	Nombre del certificado que se va a generar.
N° de serie del certificado	N.° de serie del certificado. El número debe ser una cifra entera y positiva
Tipo algoritmo firma	Algoritmo de firma que se va a utilizar Rango de valores: sha256RSA, sha512RSA
Longitud de la clave pública	Rango de valores, valor estándar: 2048

Parámetros	Descripción
Inicio de la vigencia del certif. (GMT)	
Desde cuándo será válido el certificado. La hora se interpreta como GMT (Greenwich Mean Time).	
día, mes, año, hora, minuto, segundo	Unidades para la indicación de tiempo de validez del certificado
Fin de la vigencia del certif. (GMT)	
Hasta cuándo será válido el certificado. La fecha se interpreta como GMT (hora del meridiano de Greenwich)	
día, mes, año, hora, minuto, segundo	Unidades para la indicación de tiempo de validez del certificado
Solicitante	
Indicación de los datos para el solicitante del certificado según las convenciones del estándar X.509 (p. ej., en el campo País (C) DE para Alemania). Hay que rellenar los cuatro campos.	
País (C)	Código de país de dos cifras
Organización (O)	Nombre completo de la empresa legal
Unidad organizativa (OU)	La Unidad organizativa es la división de la compañía que solicita el certificado.
Nombre común (CN)	Nombre de dominio completo (FQDN)
Solicitante alternativo	
Esta entrada adicional distingue entre el Formato del nombre DN (entradas como en Solicitante) y Otro formato (por ejemplo, entrada de una dirección IP). La máscara de entrada depende del formato seleccionado. Si se selecciona otro formato, es posible configurar más de una entrada SAN.	
Formato del nombre DN	También se suele proporcionar como RDN del nombre común en el campo Asunto del certificado principal.
Otro formato	Otros nombres, dados como un nombre general
Nombre alternativo solicitante, extensión	(opcional) Rango de valores, valor estándar: Nombre DNS, Dirección IP, Dirección e-mail, URI, Indicador universal de recursos, Otros
Nombre alternativo solicitante	
Tipo de punto de distribución CRL	Rango de valores: Nombre DNS, Dirección IP, Dirección e-mail, URI, Indicador universal de recursos, Otros
Punto distribución CRL	Aquí se puede (de forma opcional, con una URL) indicar la autoridad desde la que se distribuyen las listas de bloqueo de certificados

28.3.2.22 Seguridad > SSL > Admin. certificados

Descripción de parámetros de la pestaña:

- **Mostrar certif. de archivo**

Parámetros	Descripción
Formato PKCS#12	Si el certificado está guardado en un archivo PKCS#12, hay que activar este campo.
Clave de descifrado	Si se ha activado el campo Formato PKCS#12, en este campo hay que indicar la misma contraseña que se utilizó al generar el archivo.
Archivo con certificado	Indicación de la ruta y del nombre de archivo del certificado. En su caso, haga clic en Examinar para definir la ubicación.

28.3.2.23 Seguridad > SSL > Admin. certificados > Certificados de servidor

Descripción de parámetros de las pestañas:

- **Generar solicitud de certificado (CSR)**
- **Importar certif. servidor (PKCS#12)**
- **Mostrar certificado**
- **Borrar certificado**
- **Exportar certificado (X.509)**
- **Importar certificado renovado (X.509)**
- **Activar certificado**

Parámetros	Descripción
Nombre de la solicitud de certif.	Nombre del certificado que se va a generar.
Tipo algoritmo firma	Algoritmo de firma que se va a utilizar para el certificado Rango de valores: sha256RSA, sha512RSA
Longitud de la clave pública	Rango de valores: 2048
Solicitante Indicación de los datos para el solicitante del certificado según las convenciones del estándar X.509 (p. ej., en el campo País (C) DE para Alemania). Hay que rellenar los cuatro campos.	
País (C)	Código de país de dos cifras
Organización (O)	Nombre completo de la empresa legal
Unidad organizativa (OU)	La Unidad organizativa es la división de la compañía que solicita el certificado.
Nombre común (CN)	Nombre de dominio completo (FQDN)
Solicitante alternativo Esta entrada adicional distingue entre el Formato del nombre DN (entradas como en Solicitante) y Otro formato (por ejemplo, entrada de una dirección IP). La máscara de entrada depende del formato elegido. Si se selecciona otro formato, se pueden configurar varias entradas SAN.	
Formato del nombre DN	También se suele proporcionar como RDN del nombre común en el campo Asunto del certificado principal.
Otro formato	Otros nombres, dados como un nombre general

Parámetros	Descripción
Nombre alternativo solicitante, extensión	(opcional) Rango de valores, valor estándar: Nombre DNS, Dirección IP, Dirección e-mail, URI, Indicador universal de recursos, Otros
Nombre alternativo solicitante	(opcional)
Nombre del certif.	Nombre del certificado que se va a importar.
Clave de descifrado	Contraseña que se ha utilizado al generar el archivo. Rango de valores: de 7 a 32 caracteres
Archivo con certificado	En el campo **Archivo con certificado** se puede indicar el certificado deseado o seleccionarlo con el campo Examinar. Primero hay que mostrar la **Huella dactilar** del certificado y, a continuación, se puede hacer la importación.

28.3.2.24 Seguridad > Seguridad Web

Descripción de parámetros de la pestaña:

- **Filtro de acceso Web**

Parámetros	Descripción
Clientes Web	Solo con UC Suite: activar y desactivar el acceso Web con teléfonos móviles y aplicaciones móviles (myPortal for Mobile/Tablet, myPortal to go, Application Launcher y aplicaciones de terceros mediante Web Service) Información: uso de clientes Web junto con UC Smart a través del Modo Experto > Aplicaciones > UC Smart > Ajustes básicos
Acceso a través de HTTPS	Solo se permiten conexiones cifradas.
Acceso a través de HTTP	Se permiten las conexiones sin cifrar.
Guardar datos de inicio de sesión en el terminal	Si esta opción esta activa, no hay que indicar los datos de inicio de sesión cada vez que se inicia la aplicación

28.3.2.25 Seguridad > Seguridad SQL

Descripción de parámetros de la pestaña:

- **Contraseña de acceso SQL**

Parámetros	Descripción
Generar nuevo	Se genera una contraseña SQL cifrada que el usuario no conoce.
Activar predeterminado	Contraseña SQL predeterminada activa.

28.3.3 Interfaces de red

En **Interfaces de red** se reunen distintas funciones como, por ejemplo, la configuración de las distintas interfaces LAN. Las interfaces se pueden configurar de forma totalmente independiente entre sí.

28.3.3.1 Interfaces de red > Placa base > Nombre de host

Descripción de parámetros de las pestañas:

- **Editar nombre host**

Parámetros	Descripción
Nombre de host	Nombre host del sistema de comunicación (libre). Ejemplo: `commsystem` Si el nombre y la dirección IP del sistema de comunicación están memorizados en el servidor DNS, se puede resolver el nombre. El nombre del sistema de comunicación se compone del nombre host y del nombre de dominio. Ejemplo: `commsystem.mynet.home`

28.3.3.2 Interfaces de red > Placa base > LAN 1 (WAN)

Descripción de parámetros de las pestañas:

- **Mostrar modo LAN 1**
- **Editar interfaz LAN 1**
- **Editar ACD**

Parámetros	Descripción
Selección del proveedor de servicios de Internet	Selección para determinar cómo se produce el acceso a un ISP (Proveedor de servicios de Internet) a través de la interfaz WAN.
Selección del proveedor de servicios de Internet: No configurado o deshabilitado	La interfaz WAN no se utiliza.
Selección del proveedor de servicios de Internet: Tipo de conexión LAN TCP/IP	La interfaz WAN se utiliza para acceder a un ISP, que ya está configurado en un enrutador de Internet externo. No es necesario que el sistema de comunicación y el enrutador de Internet estén en el mismo segmento LAN, pero la interfaz WAN debe estar conectada al segmento LAN del enrutador de Internet.
Selección del proveedor de servicios de Internet: T-Online, T-DSL Business, …	El sistema de comunicación funciona como un enrutador de Internet. La interfaz WAN se utiliza para acceder a un ISP preconfigurado.
Selección del proveedor de servicios de Internet: Proveedor PPPoE	El sistema de comunicación funciona como un enrutador de Internet. La interfaz WAN se utiliza para acceder a un ISP mediante PPPoE. PPPoE es el protocolo más comúnmente utilizado por los módems DSL.
Selección del proveedor de servicios de Internet: Proveedor PPTP	El sistema de comunicación funciona como un enrutador de Internet. La interfaz WAN se utiliza para acceder a un ISP mediante PPTP. Esta variante es común en Austria, por ejemplo.

Parámetros	Descripción
Acceso a Internet a través de un enrutador externo	El acceso a Internet se produce a través de un enrutador externo. Esta bandera es utilizada internamente por el asistente de **configuración de Internet** y no debe modificarse.
Configuración automática de direcciones (a través de DHCP)	Un servidor DHCP externo (posiblemente el servidor DHCP del enrutador de Internet) asigna una dirección IP al sistema de comunicación.
Aceptar la dirección IP del enrutador predeterminado	El servidor DHCP externo comunica la dirección IP del enrutador predeterminado (por ejemplo, el enrutador de Internet) al sistema de comunicación.
Aceptar la dirección IP del servidor DNS	El servidor DHCP externo comunica la dirección IP del servidor DNS al sistema de comunicación.
Aceptar la dirección IP del servidor SNTP	El servidor DHCP externo comunica la dirección IP del servidor SNTP al sistema de comunicación.
Dirección IP	Dirección IP de la interfaz LAN.
Máscara de subred:	Máscara de red del segmento LAN.
Dirección MAC	Muestra la dirección MAC de la interfaz LAN.
Modo de enlace Ethernet	Modo de interfaz WAN.
Modo de enlace Ethernet: Automático	Cambio automático entre modo dúplex completo de 100 y 1000 Mbps.
Modo de enlace Ethernet: 100HDX	100 Mbps, dúplex completo.
Modo de enlace Ethernet: 100FDX	100 Mbps, dúplex completo.
Modo de enlace Ethernet: 1000FDX	1000 Mbps, dúplex completo.
NAT	NAT (traducción de direcciones de red) está activado. Esta tarea normalmente ya la asume el router externo.
Control de ancho de banda para conexiones de voz	Este campo habilita el control del ancho de banda para conexiones de voz.
Ancho de banda para descargas	Valora el ancho de banda en Kbit/seg para la descarga desde el ISP.
Ancho de banda para cargas	Valora el ancho de banda en Kbit/seg para la carga al ISP.
Ancho de banda utilizado para voz/fax (%)	Porcentaje de ancho de banda disponible para conexiones de voz/fax. Rango de valores, valor predeterminado: 0 - 100, 80
Etiquetado IEEE802.1p/q	Si se selecciona esta casilla de verificación, se incluye un "tipo de servicio" en los paquetes Ethernet (Capa 2) para fines de priorización. La opción está desactivada de forma predeterminada.

Parámetros	Descripción
ID de VLAN IEEE802.1p/q	Introduzca el número de identificación de la VLAN si el conmutador utilizado tiene problemas con el valor predeterminado "0".
Clase QoS de capa 2	
Datos de señalización	Clase de prioridad para la configuración de la conexión. 0 = prioridad más baja / 7 = prioridad más alta. Rango de valores, valor predeterminado: 0 - 7, 3
Carga útil de fax/módem	Clase de prioridad para los datos de fax y módem de la conexión IP. 0 = prioridad más baja / 7 = prioridad más alta. Rango de valores, valor predeterminado: 0 - 7, 5
Control de red	Clase de prioridad para los datos de control de red (transferencia de traps SNMP, por ejemplo). 0 = prioridad más baja / 7 = prioridad más alta. Rango de valores, valor predeterminado: 0 - 7, 0
Carga útil de voz	Clase de prioridad para los datos de voz de la conexión IP. 0 = prioridad más baja / 7 = prioridad más alta. Rango de valores, valor predeterminado: 0 - 7, 5
Datos de acceso a Internet para…	
ID de conexión / Nombre de usuario / Número de T-Online / Número de subusuario/Sufijo / Cuenta de acceso a Internet / Inicio de sesión DSL…	Datos de acceso del Proveedor de Servicios de Internet.
Clave CHAP	Contraseña para acceder al Proveedor de Servicios de Internet.
Escriba la contraseña otra vez	Contraseña para acceder al Proveedor de Servicios de Internet.
Parámetros de IP	
Dirección IP remota de la conexión PPP	Dirección IP del servidor ISP, si el ISP utiliza una dirección IP estática.
Dirección IP local de la conexión PPP	Dirección IP que le asignó su ISP para acceder a Internet.
Negociación de direcciones IP	Selección para determinar cómo los socios de conexión deben negociar la dirección IP durante la configuración de la conexión.
Negociación de direcciones IP: dirección IP configurada	Sólo es posible la dirección IP configurada.
Negociación de direcciones IP: acepta cualquier dirección IP	Se acepta cualquier dirección propuesta por el socio.

Parámetros	Descripción
Negociación de direcciones IP: solicitar nueva dirección IP	Se solicita una nueva dirección IP en cada conexión.
Solicitud de DNS	
Acceso a Internet con solicitud DNS	El servidor DNS se determina automáticamente.
Dirección IP del servidor DNS principal	Se selecciona un servidor DNS especial.
Parámetros generales de PPP	
Enrutador predeterminado	La conexión PPP creada aquí se utiliza como destino de enrutamiento.
Compresión de encabezado IP	El encabezado TCP está comprimido. Los encabezados UDP y RTP siempre están comprimidos.
Enviar solicitud de eco LCP	Se envía una solicitud de eco LCP. Esta función se utiliza para comprobar si la conexión sigue activa.
Reconexión automática de PPP	La conexión PPP se restablece automáticamente después de una interrupción de la conexión (por ejemplo, en el caso de acceso a un ISP con una tarifa plana y una desconexión forzada después de 24 horas).
Parámetro PPTP	
Dirección IP local de la conexión de control	Dirección IP que fue asignada por su ISP para la conexión PPTP.
Dirección IP remota de la conexión de control	Dirección IP del servidor de su ISP para la conexión PPTP.
Máscara de subred remota para la conexión de control	Máscara de subred asignada por su ISP para la conexión PPTP.
Retención corta	
Retención corta	El modo de funcionamiento de "retención corta" está activado para la conexión PPP. La siguiente entrada solo es posible cuando el modo de retención breve está habilitado.
Tiempo de retención corto (seg.)	Tiempo sin transmisiones de datos después del cual se debe borrar la conexión PPP. El temporizador de retención corta solo se activa con paquetes salientes. Rango de valores, valor predeterminado: 10 - 9999, 60
Autenticación	
Autenticación PPP	La autenticación PPP está habilitada. La configuración debe realizarse de acuerdo con las especificaciones del ISP.
Nombre usuario PPP	Nombre de usuario de libre elección que se utilizará para la autenticación mediante PAP o CHAP.
Modo autenticación PAP	Activación y tipo de autenticación PAP para la conexión PPP: No utilizado, Cliente PAP, Host PAP.

Parámetros	Descripción
Clave PAP	Contraseña para la autenticación PAP.
Modo autentificación CHAP	Activación y tipo de autenticación CHAP para la conexión PPP: No utilizado, Cliente CHAP, Host CHAP, Cliente CHAP y Host.
Clave CHAP	Contraseña para la autenticación CHAP.
Compresión de datos	
Compresión de datos DEFLATE	Para la compresión de paquetes de datos PPP con el algoritmo de compresión DEFLATE.
Compresión de datos COMPRESS	Para la compresión de paquetes de datos PPP con el algoritmo de compresión COMPRESS.
Traducción de direcciones	
NAT	NAT (traducción de direcciones de red) está activado. Se admiten los siguientes protocolos: TCP, UDP y ICMP (sólo en modo pasivo).
Mapeo de direcciones	será eliminado.
Configuración del enrutador	
Circuito de tiempo completo	Dependiendo del modelo tarifario se podrá habilitar o deshabilitar el circuito full time (conexión permanente) al ISP. El circuito de tiempo completo debe deshabilitarse para un modelo de tarifa basado en tiempo y habilitarse para un modelo de tarifa plana.
Tiempo de retención corto (seg.)	Si el circuito de tiempo completo está deshabilitado (modelo de tarifa basado en tiempo), ingrese la duración de inactividad después de la cual se interrumpirá la conexión (por ejemplo, 60 segundos). Rango de valores, valor predeterminado: 10 - 9999, 60
Desconexión forzada a las (hora:min)	Si está habilitado el Circuito de Tiempo Completo (modelo de tarifa plana), ingrese la hora en la que se desactivará la conexión a Internet (por ejemplo, 04:59).
Tiempo de conexión	Muestra el tiempo de conexión transcurrido en días-horas-minutos-segundos.
Parámetros QoS de la interfaz	
Ancho de banda para descargas	Valora el ancho de banda en Kbit/seg para la descarga desde el ISP.
Ancho de banda para cargas	Valora el ancho de banda en Kbit/seg para la carga al ISP.
Control de ancho de banda para conexiones de voz	El control del ancho de banda evita que las velocidades de transmisión disponibles se sobrecarguen con conexiones de voz dentro de una conexión de múltiples enlaces. En otras palabras, cuando la compresión de encabezado está activa, se permiten un máximo de 5 conexiones de voz en un canal B. Este campo habilita el control del ancho de banda para conexiones de voz. Aquí solo se consideran las conexiones de voz con rutas configuradas en la puerta de enlace de voz.

Parámetros	Descripción
Ancho de banda utilizado para voz/fax (%)	Porcentaje de ancho de banda disponible para conexiones de voz/fax. Rango de valores, valor predeterminado: 0 - 100, 80

Descripción de parámetros de las pestañas:

- **Editar ACD**

Parámetros	Descripción
Tiempo de conexión	Muestra el tiempo de conexión transcurrido en días-horas-minutos-segundos.
Forzar reconexión en	Hora en la que se debe liberar y restablecer la conexión.
Habilitar ACD	Habilite la limpieza automática para evitar la desconexión por parte del ISP en un momento inoportuno.

28.3.3.3 Interfaces de red > Placa base > LAN 2

Descripción de parámetros de las pestañas:

- **Editar interfaz LAN 2**

Parámetros	Descripción
Acceso a Internet a través de un router externo	Se accede a Internet a través de un router externo.
Interfaz activada	La interfaz LAN está activada.
Dirección IP	Dirección IP del sistema de comunicación.
Máscara de subred:	Máscara de red del segmento LAN en el que se encuentra el sistema de comunicación.
Dirección MAC	Indicación de la dirección MAC del sistema de comunicación.
Modo Ethernet-Link	Modo de interfaz LAN.
Modo Ethernet-Link: Auto	Conmutación automática entre 100 y 1000 Mbit/s y entre semidúplex y dúplex completo. En este modo se puede activar la gestión de la alimentación. Después de migrar a V2R3 o una versión posterior, debe pulsar la opción para aplicar encima en el modo Ethernet Link deseado en la página de la interfaz de red para que el valor se configure en Auto. De lo contrario, los sistemas deben configurarse en Auto o 100 antes de la migración.
Modo Ethernet-Link: 100HDX	100 Mbit/s, semidúplex. En este modo no se puede activar la gestión de energía.
Modo Ethernet-Link: 100FDX	100 Mbit/s, dúplex completo. En este modo no se puede activar la gestión de energía.
Modo Ethernet-Link: 1000FDX	1000 Mbit/s, dúplex completo. En este modo no se puede activar la gestión de energía.

Parámetros	Descripción
IEEE802.1p/q-Tagging	Si esta casilla de verificación está activada, en los paquetes Ethernet (capa 2) se envía un "Tipo de servicio" para la definición de prioridades. Esta opción está desactivada de forma predeterminada.
IEEE802.1p/q-VLAN-ID	El número ID de la VLAN solo se tiene que indicar si el conmutador utilizado tiene problemas con el valor estándar "0".
Clase QoS capa 2	
Datos de señalización	Clase de prioridad para el establecimiento de conexión. 0 = prioridad más baja / 7 = prioridad máxima. Rango de valores, valor estándar: 0 - 7, 3
Payload de fax/módem	Clase de prioridad para los datos de fax y módem de la conexión IP. 0 = prioridad más baja / 7 = prioridad máxima. Rango de valores, valor estándar: 0 - 7, 5
Control de red	Clase de prioridad para los datos del control de red (p. ej., transferencia de traps SNMP). 0 = prioridad más baja / 7 = prioridad máxima. Rango de valores, valor estándar: 0 - 7, 0
Payload de voz	Clase de prioridad para los datos de voz. 0 = prioridad más baja / 7 = prioridad máxima. Rango de valores, valor estándar: 0 - 7, 5

28.3.3.4 Interfaces de red > Placa base > LAN 3 (Admin)

Descripción de parámetros de las pestañas:

- **Editar interfaz LAN 3**

Parámetros	Descripción
Interfaz activada	La interfaz LAN está activada.
Configuración de dirección automática (a través de DHCP)	Un servidor DHCP externo asigna una dirección IP al sistema de comunicación.
Aceptar dirección IP del router estándar	El servidor DHCP externo comunica al sistema de comunicación la dirección IP del router estándar (p. ej., router Internet).
Aceptar dirección IP del servidor DNS	El servidor DHCP externo comunica al sistema de comunicación la dirección IP del servidor DNS.
Aceptar dirección IP del servidor SNTP	El servidor DHCP externo comunica al sistema de comunicación la dirección IP del servidor SNTP.
Dirección IP	Dirección IP de la interfaz LAN.
Máscara de subred:	Máscara de red del segmento LAN.
Dirección MAC	Indicación de la dirección MAC de la interfaz LAN.

Parámetros	Descripción
Modo Ethernet-Link	Modo de interfaz LAN.
Modo Ethernet-Link: Auto	Conmutación automática entre 100 y 1000 Mbit/s y entre semidúplex y dúplex completo.
Modo Ethernet-Link: 100HDX	100 Mbit/s, semidúplex.
Modo Ethernet-Link: 100FDX	100 Mbit/s, dúplex completo.
Modo Ethernet-Link: 1000FDX	1000 Mbit/s, dúplex completo.

28.3.3.5 Interfaces de red > Placa base > Servidor FTP

Descripción de parámetros de las pestañas:

- **Editar parámetros servidor FTP**

Parámetros	Descripción
Liberar servidor FTP	Si la casilla de verificación está activada, el servidor FTP interno está liberado.
Usuario descarga 'Phone'	
Nombre	Nombre para que los teléfonos IP accedan al servidor FTP para poder descargar actualizaciones de software actuales. El nombre no se puede modificar.
Nueva contraseña	Contraseña para que los teléfonos IP accedan al servidor FTP. Si se modifica la contraseña predefinida, también hay que cambiarla en los teléfonos IP.
Confirmar contraseña	Contraseña para que los teléfonos IP accedan al servidor FTP.
Usuario descarga 'FTP_Admin'	
Nombre	Nombre para que el administrador acceda al servidor FTP. El nombre no se puede modificar.
Nueva contraseña	Contraseña para que el administrador acceda al servidor FTP.
Confirmar contraseña	Contraseña para que el administrador acceda al servidor FTP.

28.3.3.6 Interfaces de red > Placa base > Modo DHCP

Descripción de parámetros de las pestañas:

- **Editar Modo DHCP**

Parámetros	Descripción
Sin DHCP	Si el campo de opción está activo, el servidor DHCP interno está apagado.
Servidor DHCP	Si el campo de opción está activo, el servidor DHCP interno está encendido.

Parámetros	Descripción
Agente DHCP Relay	Si el campo de opción está activo, el sistema de comunicación actúa como agente DHCP Relay. El sistema de comunicación transfiere las consultas DHCP de las extensiones IP al servidor DHCP propio. No es necesario que el servidor DHCP y las extensiones IP estén en el mismo segmento de red.

28.3.3.7 Interfaces de red > Placa base > Modo DHCP > Servidor DHCP > Parámetros globales

Los datos específicos de la red se transmiten desde el servidor DHCP a las estaciones IP.

Descripción de parámetros de las pestañas:

- **Editar parámetros globales**

Parámetros	Descripción
Habilitar el servidor DHCP	Indica que el servidor DHCP interno está habilitado y que se pueden configurar sus parámetros globales. No se puede cambiar.
Solo dispositivos Mitel/ Unify	Indica que el servidor DHCP interno solo acepta solicitudes de dispositivos Mitel y Unify phone. Si el cliente recibe más de una respuesta, por ejemplo del servidor DHCP de OpenScape Business y de otro servidor de la red, preferirá la respuesta recibida de OpenScape Business, si utiliza dispositivos compatibles: • OpenScape DeskPhone CP x00 con versión de software V1R8.4.0 (HFA) / V1R11.6.0 (SIP) o superior • OpenScape DeskPhone CP x10 con versión de software V2R0.18.0 (HFA o SIP) o superior • Mitel MiVoice 69xx / 68xx (SIP)
Máscara de subred:	La máscara de subred define el tamaño de la subred. Ejemplo: `255.255.255.0`.
Dirección de transmisión	Con la dirección de difusión se pueden direccionar todas las estaciones IP de una red o subred mediante el servidor DHCP (opcional). Ejemplo: `0.0.0.0`.
Gateway predeterminado	
Gateway 1	Dirección IP bajo la cual se puede acceder a la puerta de enlace predeterminada. Si se utiliza un enrutador de Internet en la red, el enrutador de Internet es la puerta de enlace predeterminada. Ejemplo: `192.168.1.1`. Si el sistema de comunicación está conectado directamente a un módem de Internet, el sistema de comunicación es la puerta de enlace predeterminada. Ejemplo: `192.168.1.2`.
Gateway 2	Dirección IP bajo la cual se puede acceder a un segundo gateway predeterminado (enrutador) (opcional).
Gateway 3	Dirección IP bajo la cual se puede acceder a un tercer gateway predeterminado (enrutador) (opcional).

Parámetros	Descripción
Servidor DNS	
Nombre de dominio	Nombre de dominio de la red interna, máximo 80 caracteres, p. ej., `mynet.home` (opcional).
Servidor 1	Dirección IP bajo la cual se puede acceder al servidor DNS. Si el sistema de comunicación está conectado directamente a un módem de Internet, el valor predeterminado es `0.0.0.0` No debe cambiarse. El sistema de comunicación lo utiliza para conectarse automáticamente a un servidor DNS desde Internet. También se puede introducir un servidor DNS externo. Ejemplo: el servidor DNS del enrutador de Internet (`192.168.1.1)` o un servidor DNS de Internet (`google-public-dns-a.google.com`).
Servidor 2	Dirección IP bajo la cual se puede acceder a un segundo servidor DNS (opcional).
Servidor 3	Dirección IP bajo la cual se puede acceder a un tercer servidor DNS (opcional).
Tiempo de arrendamiento en horas (0 infinito)	Periodo máximo de validez en horas, 0 = duración infinita (valor predeterminado: 1 hora).
Habilitar actualización dinámica de DNS	Si esta casilla de verificación está habilitada, el servidor DNS puede actualizarse dinámicamente. Predeterminado: no habilitado. **Nota:** Si la opción Actualización de DNS dinámico está habilitada, es obligatorio configurar el **Nombre de dominio** en el campo Nombre de dominio correspondiente del Grupo de direcciones IP.
Utilizar DLI interno	Si se selecciona esta casilla de verificación, se utiliza el DLI interno. Si esta casilla de verificación no está marcada, aparecen los parámetros de un servidor DLS externo. Predeterminado: habilitado.
Servidor DLS externo	
Dirección IP	Dirección IP bajo la cual se puede acceder al servidor DLS externo.
Puerto	Puerto a través del cual se puede acceder al servidor DLS externo.

28.3.3.8 Interfaces de red > Placa base > Modo DHCP > Servidor DHCP > Grupos de direcciones IP

Descripción de parámetros de las pestañas:

- **Mostrar grupos de direcciones IP**
- **Agregar grupo de direcciones IP**
- **Editar el grupo de direcciones IP**
- **Eliminar el grupo de direcciones IP**

Parámetros	Descripción
Dirección de subred	La dirección de subred define el rango máximo de direcciones IP. Ejemplo: `192.168.1.0`.
Máscara de subred:	La máscara de subred define el tamaño de la subred. Configuración predeterminada: `255.255.255.0`.
rango de direcciones	
Rango de direcciones 1	Límites inferior y superior del rango de direcciones IP de la subred. Ejemplo: desde `192.168.1.50` a `192.168.1.254`.
Rango de direcciones 2	Límites inferior y superior de un segundo rango de direcciones IP dentro de la misma subred (opcional).
Rango de direcciones 3	Límites inferior y superior de un tercer rango de direcciones IP dentro de la misma subred (opcional).
Gateway predeterminado	
Gateway 1	Dirección IP bajo la cual se puede acceder a la puerta de enlace predeterminada. Si se utiliza un enrutador de Internet en la red, el enrutador de Internet es la puerta de enlace predeterminada. Ejemplo: `192.168.1.1`. Si el sistema de comunicación está conectado directamente a un módem de Internet, el sistema de comunicación es la puerta de enlace predeterminada. Ejemplo: `192.168.1.2`.
Gateway 2	Dirección IP bajo la cual se puede acceder a un segundo gateway predeterminado (enrutador) (opcional).
Gateway 3	Dirección IP bajo la cual se puede acceder a un tercer gateway predeterminado (enrutador) (opcional).
Dirección de transmisión	Con la dirección de difusión se pueden direccionar todas las estaciones IP de una red o subred mediante el servidor DHCP (opcional). Por defecto: `0.0.0.0`.
Nombre de dominio	Nombre de dominio de la red interna, máximo 80 caracteres, p. ej., `mynet.home` (opcional).
Servidor DNS	
Servidor 1	Dirección IP bajo la cual se puede acceder al servidor DNS. Si el sistema de comunicación está conectado directamente a un módem de Internet, el valor predeterminado es `0.0.0.0` No debe cambiarse. El sistema de comunicación lo utiliza para conectarse automáticamente a un servidor DNS desde Internet. También se puede introducir un servidor DNS externo. Ejemplo: el servidor DNS del enrutador de Internet (`192.168.1.1)` o un servidor DNS de Internet (`google-public-dns-a.google.com`).
Servidor 2	Dirección IP bajo la cual se puede acceder a un segundo servidor DNS (opcional).

Parámetros	Descripción
Servidor 3	Dirección IP bajo la cual se puede acceder a un tercer servidor DNS (opcional).
Seguridad mejorada	
Opción de relé	Un número hexadecimal configurado por el administrador para mayor seguridad. El valor de este campo está vacío por defecto y esta opción no se tendrá en cuenta si no está configurada.
Tiempo de arrendamiento en horas (0 infinito)	Periodo máximo de validez en horas, 0 = duración infinita (valor predeterminado: 1 hora).

28.3.3.9 Interfaces de red > Placa base > Modo DHCP > Servidor DHCP > Direcciones IP estáticas

Descripción de parámetros de las pestañas:

- **Mostrar dirección IP estática**
- **Agregar dirección IP estática**
- **Editar dirección IP estática**
- **Eliminar dirección IP estática**

Parámetros	Descripción
Nombre de host	Nombre o descripción de la estación IP (por ejemplo, PC o servidor) que recibirá una dirección IP fija. Ejemplo: `Servidor de impresión`.
Dirección IP	Dirección IP fija deseada. Ejemplo: `192.168.1.10`.
Identificador del cliente	Dirección MAC de la estación IP ej. Dispositivo RFP SIP-DECT de Mitel.
Máscara de subred:	Máscara de red de la subred. Ejemplo: `255.255.255.0`.
Gateway predeterminado	
Gateway 1	Dirección IP bajo la cual se puede acceder a la puerta de enlace predeterminada. Si se utiliza un enrutador de Internet en la red, el enrutador de Internet es la puerta de enlace predeterminada. Ejemplo: `192.168.1.1`. Si el sistema de comunicación está conectado directamente a un módem de Internet, el sistema de comunicación es la puerta de enlace predeterminada. Ejemplo: `192.168.1.2`.
Gateway predeterminado 1	Dirección IP bajo la cual se puede acceder a un segundo gateway predeterminado (enrutador) (opcional).
Gateway predeterminado 1	Dirección IP bajo la cual se puede acceder a un tercer gateway predeterminado (enrutador) (opcional).
Dirección de transmisión	Con la dirección de difusión se pueden direccionar todas las estaciones IP de una red o subred mediante el servidor DHCP (opcional). Ejemplo: `0.0.0.0`.

Parámetros	Descripción
Nombre de dominio	Nombre de dominio de la red interna, máximo 80 caracteres, p. ej., `mynet.home` (opcional).
Servidor DNS	
Servidor 1	Dirección IP bajo la cual se puede acceder al servidor DNS. Si el sistema de comunicación está conectado directamente a un módem de Internet, el valor predeterminado es `0.0.0.0` No debe cambiarse. El sistema de comunicación lo utiliza para conectarse automáticamente a un servidor DNS desde Internet. También se puede introducir un servidor DNS externo. Ejemplo: el servidor DNS del enrutador de Internet (`192.168.1.1)` o un servidor DNS de Internet (`google-public-dns-a.google.com`).
Servidor 2	Dirección IP bajo la cual se puede acceder a un segundo servidor DNS (opcional).
Servidor 3	Dirección IP bajo la cual se puede acceder a un tercer servidor DNS (opcional).
Seguridad mejorada	
Opción de relé	Un número hexadecimal configurado por el administrador para mayor seguridad.
Tiempo de arrendamiento en horas (0 infinito)	Periodo máximo de validez en horas, 0 = duración infinita (valor predeterminado: 1 hora).

28.3.3.10 Interfaces de red > Placa base > Modo DHCP > Servidor DHCP > Últimas concesiones activas

La dirección IP asignada por un servidor DHCP sigue siendo válida para una estación IP hasta que expire el "período de concesión", incluso si la estación IP se apaga durante ese tiempo. Aquí se muestran las últimas asignaciones activas.

Descripción de parámetros de las pestañas:

- **Mostrar arrendamiento**
- **Eliminar arrendamiento**

Parámetros	Descripción
Dirección IP	Dirección IP asignada a la estación IP por el servidor DHCP.
Dirección MAC	Dirección MAC de la estación IP a la que se le asignó una dirección IP.
ID de cliente	ID de cliente de la estación IP. Si el ID del cliente no está disponible, se muestra la dirección MAC de la estación IP.
Nombre de host	Nombre o número de llamada de la estación IP a la que se le asignó una dirección IP.

Parámetros	Descripción
Inicio del arrendamiento	Hora de inicio de la tarea. A partir de este momento, a la estación IP se le asigna una dirección IP.
Fin del arrendamiento	Hora de finalización de la tarea. Después de este período, la estación IP debe enviar una nueva solicitud de dirección IP.

28.3.3.11 Interfaces de red > Placa base > Modo DHCP > Servidor DHCP > Todos los leases

La dirección IP asignada a un servidor DHCP es válida para una extensión IP hasta que termina el "periodo de lease", aunque en ese tiempo la extensión IP haya estado apagada. Aquí se muestran todas las asignaciones.

Descripción de parámetros de las pestañas:

- **Mostrar lease**
- **Borrar lease**

Parámetros	Descripción
Dirección IP	Dirección IP de la extension IP asignada por el servidor DHCP.
Dirección MAC	Dirección MAC de la extensión IP que tiene asignada una dirección IP.
ID de cliente	ID de cliente de la extensión. Si el ID de cliente no está disponible aparece la dirección MAC de la extensión IP.
Hostname (Nombre host)	Nombre o número de teléfono de la extensión IP que tiene asignada una dirección IP.
Inicio del lease	Punto de inicio de la asignación. A partir de este momento, la extensión IP tiene asignada una dirección IP.
Fin del lease	Final de la asignación. A partir de ese momento, la extensión IP inicia una nueva solicitud de dirección IP.

28.3.3.12 Interfaces de red > Tablero de aplicaciones > Nombre de host

Descripción de parámetros de las pestañas:

- **Editar nombre host**

Parámetros	Descripción
Nombre de host	Nombre de host del tablero de aplicaciones (libre). Ejemplo: `applboard` Si el nombre y la dirección IP del tablero de aplicaciones están en un servidor DNS, se puede resolver el nombre. El nombre del tablero de aplicaciones se compone del nombre de host y del nombre de dominio. Ejemplo: `applboard.mynet.home`

28.3.3.13 Interfaces de red > Tablero de aplicaciones > LAN 1

Descripción de parámetros de las pestañas:

- **Editar interfaz LAN 1**

Parámetros	Descripción
Interfaz activada	Si esta casilla de verificación está activada, la interfaz LAN 2 del Tablero de aplicaciones está activa.
Configuración de dirección automática (a través de DHCP)	Si esta casilla de verificación está activada, el servidor DHCP asigna automáticamente la dirección IP y la máscara de red a la interfaz LAN 1. Además se puede seleccionar si el servidor DHCP va a aplicar más parámetros específicos de red.
Aceptar dirección IP del router estándar	Si esta casilla está activada, el servidor IP aplica la dirección IP del router estándar.
Aceptar dirección IP del servidor DNS	Si esta casilla está activada, el servidor DHCP aplica la dirección IP del servidor DNS.
Aceptar dirección IP del servidor SNTP	Si esta casilla está activada, el servidor DHCP aplica la dirección IP del servidor SNTP.
Dirección IP	Dirección IP con la que se puede acceder al tablero de aplicaciones.
Máscara de subred:	Máscara de red con la que se accede al tablero de aplicaciones.
Dirección MAC	Dirección MAC del tablero de aplicaciones (no se puede modificar).
Modo Ethernet-Link	Modo de la interfaz LAN 1.
Modo Ethernet-Link: Auto	Conmutación automática entre 100 y 1000 Mbit/s y entre semidúplex y dúplex completo. En este modo se puede activar la gestión de la alimentación.
Modo Ethernet-Link: 100HDX	100 Mbit/s, semidúplex. En este modo no se puede activar la gestión de energía.
Modo Ethernet-Link: 100FDX	100 Mbit/s, dúplex completo. En este modo no se puede activar la gestión de energía.
Modo Ethernet-Link: 1000FDX	1000 Mbit/s, dúplex completo. En este modo no se puede activar la gestión de energía.

28.3.3.14 Interfaces de red > Tablero de aplicaciones > LAN 2

Descripción de parámetros de las pestañas:

- **Editar interfaz LAN 2**

Parámetros	Descripción
Interfaz activada	Si esta casilla de verificación está activada, la interfaz LAN 2 del Tablero de aplicaciones está activa.
Dirección IP	Dirección IP con la que se puede acceder al tablero de aplicaciones.
Máscara de subred:	Máscara de red con la que se accede al tablero de aplicaciones.

Parámetros	Descripción
Dirección MAC	Dirección MAC del tablero de aplicaciones (no se puede modificar).
Long. máx. paquetes datos (bytes)	Longitud máxima de los paquetes aplicable al protocolo IP. Se permiten valores entre 576 y 1500.
Modo Ethernet-Link	Modo de la interfaz LAN 2.
Modo Ethernet-Link: Auto	Conmutación automática entre semidúplex y dúplex completo. En este modo se puede activar la gestión de la alimentación.
Modo Ethernet-Link: 100HDX	100 Mbit/s, semidúplex. En este modo no se puede activar la gestión de energía.
Modo Ethernet-Link: 100FDX	100 Mbit/s, dúplex completo. En este modo no se puede activar la gestión de energía.
Modo Ethernet-Link: 1000FDX	1000 Mbit/s, dúplex completo. En este modo no se puede activar la gestión de energía.
IEEE802.1p/q-Tagging	Si esta casilla de verificación está activa, se determina el formato Ethernet que envía el Tablero de aplicaciones. Esta opción está desactivada de forma predeterminada.
IEEE802.1p/q-VLAN-ID	Número ID de la VLAN que se desvía del valor estándar "0" si el conmutador utilizado tiene problemas con el valor estándar "0".
Clase QoS capa 2	
Datos de señalización	Clase de prioridad para el establecimiento de conexión. 0 = prioridad más baja / 7 = prioridad máxima.
Payload de fax/módem	Clase de prioridad para los datos de fax y módem de la conexión IP. 0 = prioridad más baja / 7 = prioridad máxima.
Control de red	Clase de prioridad para los datos del control de red (p. ej., transferencia de traps SNMP). 0 = prioridad más baja / 7 = prioridad máxima.
Payload de voz	Clase de prioridad para datos de voz de la conexión IP. 0 = prioridad más baja / 7 = prioridad máxima.

28.3.4 Encaminamiento

En **Encaminamiento** se gestionan las tablas de encaminamiento. En las redes pequeñas el administrador puede gestionar de forma manual una tabla de encaminamiento en cada router. En las grandes redes, esta tarea se automatiza con ayuda de un protocolo que distribuye las informaciones de encaminamiento en la red.

28.3.4.1 Encaminamiento > Encamin. IP > Placa base > Rutas estáticas

El sistema de comunicación solo admite rutas estáticas. Las rutas estáticas conectan entre sí dos dispositivos IP. Se crean de forma manual.

En función de la aplicación puede ser necesario configurar rutas diferentes para el sistema (placa base) y la tarjeta UC Booster Card (tablero de aplicaciones).

Descripción de parámetros de las pestañas:

- **Mostrar tabla de rutas estáticas**
- **Agregar ruta estática**
- **Editar ruta estática**
- **Borrar ruta estática**

Parámetros	Descripción
Índice ruta	El índice de ruta se asigna automáticamente y solo se muestra a título informativo. No se puede modificar.
Nombre de ruta	Nombre o descripción de la ruta estática, libre.
Red destino/host	Dirección IP de la red de destino.
Máscara de subred:	Máscara de subred de la red de destino.
Gateway de ruta	Dirección IP del siguiente router de la ruta o dirección IP de la interfaz local o remota de un socio PSTN.

28.3.4.2 Encaminamiento > Encamin. IP > Placa base > Router estándar

Según la aplicación puede ser necesario configurar un encaminamiento estándar diferente para el sistema (placa base) y la tarjeta UC Booster Card (tablero de aplicaciones).

Descripción de parámetros de las pestañas:

- **Editar router estándar**

Parámetros	Descripción
Encam. estándar vía	Activar o desactivar el encaminamiento IP mediante un router estándar.
Ninguna interfaz	Encaminamiento IP mediante un router estándar desactivado.
LAN	Encaminamiento IP mediante un router estándar activado.
Dirección IP del router estándar	Dirección IP del router estándar, si en el campo **Encam. estándar vía** se ha seleccionado la interfaz **LAN**. Ejemplo: Dirección IP del router Internet, `192.168.1.1`.

28.3.4.3 Encaminamiento > Encamin. IP > Placa base > Servidor DNS

Puede visualizar y en su caso modificar la dirección IP del servidor DNS. La configuración es necesaria para el tronqueo con direcciones IP dinámicas.

Descripción de parámetros de las pestañas:

- **Editar ajustes DNS**

Parámetros	Descripción
Dirección IP del servidor DNS	Dirección IP con la que se puede acceder al servidor DNS. Si el sistema de comunicación está conectado directamente con un módem Internet, no hay que modificar el valor estándar `0.0.0.0`. El sistema de comunicación se conecta así automáticamente con un servidor DNS desde Internet. También se puede registrar un servidor DNS externo. Ejemplo: el servidor DNS del router Internet (`192.168.1.1)` o un servidor DNS de Internet (`google-public-DNS-a.google.com`). Con un sistema OpenScape Business S, hay que reiniciar el sistema para aplicar los cambios.

28.3.4.4 Encaminamiento > Encamin. IP > Tablero de aplicaciones > Rutas estáticas

En función de la aplicación puede ser necesario configurar rutas diferentes para el sistema (placa base) y la tarjeta UC Booster Card (tablero de aplicaciones).

Descripción de parámetros de las pestañas:

- **Mostrar tabla de rutas estáticas**
- **Agregar ruta estática**
- **Editar ruta estática**
- **Borrar ruta estática**

Parámetros	Descripción
Índice ruta	El índice de ruta se asigna automáticamente y solo se muestra a título informativo. No se puede modificar.
Nombre de ruta	Nombre o descripción de la ruta estática, libre (opcional) Rango de valores: máx. 35 caracteres.
Red destino/host	Dirección IP de la red de destino.
Máscara de subred:	Máscara de subred de la red de destino.
Gateway de ruta	Dirección IP del siguiente router de la ruta o dirección IP de la interfaz local o remota de un socio PSTN.

28.3.4.5 Encaminamiento > Encamin. IP > Tablero de aplicaciones > Router estándar

Según la aplicación puede ser necesario configurar un encaminamiento estándar diferente para el sistema (placa base) y la tarjeta UC Booster Card (tablero de aplicaciones).

Descripción de parámetros de las pestañas:

- **Cambiar router estándar**

Parámetros	Descripción
Encam. estándar vía	Activar o desactivar el encaminamiento IP mediante un router estándar.
Ninguna interfaz	Encaminamiento IP mediante un router estándar desactivado.
LAN	Encaminamiento IP mediante un router estándar activado.
Dirección IP del router estándar	Dirección IP del router estándar, si en el campo "Encam. estándar vía" se ha seleccionado la interfaz LAN.

28.3.4.6 Encaminamiento > NAT

Puede mostrar, añadir, cambiar y borrar una regla NAT para la traducción de direcciones de red. Mediante el editor tablas NAT puede modificar cómodamente y al mismo tiempo todas las entradas NAT existentes y adicionales para la traducción de direcciones de red.

Descripción de parámetros de las pestañas:

- **Añadir NAT**
- **Editor tablas NAT**

Parámetros	Descripción
Regla NAT activa	
Descripción	
Dirección IP local	Dirección de destino local de la LAN.
Puerto local	Número de puerto local del protocolo configurado de la LAN.
Puerto global	Número de puerto del protocolo configurado.
Protocolo	Protocolo de transporte que se va a utilizar. El protocolo de transporte configurado es válido tanto para direcciones locales como globales.
Protocolo: **TCP**	TCP (Transmission Control Protocol) TCP es un protocolo fiable y orientado a la conexión para la transmisión de paquetes IP. Antes del comienzo de la transmisión se establece un canal virtual entre los dos puntos terminales de la conexión de red. En este canal se pueden transmitir datos en ambas direcciones. TCP se utiliza, fundamentalmente, en el área de la WorldWideWeb, del correo electrónico y en las redes Peer-to-Peer. Además, también se utiliza para la señalización de llamadas en la telefonía IP porque reconoce las pérdidas de datos en la transmisión y las resuelve automáticamente.

Parámetros	Descripción
Protocolo: **UDP**	UDP (User Datagram Protocol) UDP es un protocolo simple y sin conexión para la transmisión de paquetes IP. Antes del comienzo de la transmisión no se establece ningún canal virtual con el colateral, como sí ocurre en TCP. De esta forma, los PC pueden comenzar más rápidamente el intercambio de datos. En UDP, se incluye el número de puerto del servicio que debe recibir los datos al direccionar los paquetes de voz. Se utiliza, fundamentalmente, en el área DNS y para la transmisión de voz en la telefonía IP. Sin embargo, como en el caso de los protocolos sin conexión no se controla si el colateral ha recibido realmente los datos, pueden darse pérdidas en la transmisión de voz.

28.3.4.7 Encaminamiento > PSTN

Con estos parámetros se configura una conexión remota IP (conexión (DFÜ) a través de la red de telefonía clásica.

Descripción de parámetros de las pestañas:

- **Editar datos globales PSTN**

Parámetros	Descripción
N.º de llamada router (n.º llam. interno)	Seleccionar la marcación directa del sistema. Con este número de marcación directa se puede acceder a todas las aplicaciones que utilizan la función de router. Los colaterales de encaminamiento externos que no transmiten ningún número de teléfono deben utilizar otros números. Estos números de teléfono se configuran como MSN.
Rellamada	
Cantidad rellamadas	Intentos de rellamada que debe realizar el sistema para establecer una conexión. Rango de valores: de 0 a 255
Pausa rellamada (s)	Pausa entre rellamadas, en segundos. Rango de valores: 1-1,.000
Scripting	
Identif. 1 para scripting	Primera parte de la identificación para registrarse con los proveedores de Internet. El proveedor de Internet requiere entradas sobre el host, la identificación de usuario y una contraseña, por ejemplo: Host=ERT005, Usuario=KJUMBERT, Contraseña=123456. Las entradas son como siguen: Identif. 1 para scripting: HOST:ERT005 - Identif. 2 para scripting: USER:KJUMBERT - Clave nueva para scripting: PASSWORD: 123456.
Identif. 2 para scripting	Segunda parte de la identificación para registrarse con los proveedores de Internet.
Clave nueva para scripting	Contraseña para registrarse con los proveedores de Internet.

28.3.4.8 Encaminamiento > PSTN > Protocolo PPP

Descripción de parámetros de las pestañas:

- **Cargar vía HTTP**

Parámetros	Descripción
Cargar	El archivo de registro PPP se puede descargar mediante HTTP. Según la configuración del navegador se muestra si el archivo de registro descargado se debe guardar o abrir en el editor predeterminado.

28.3.4.9 Encaminamiento > PSTN > Colateral PSTN

Descripción de parámetros de las pestañas:

- **Añadir colateral PSTN**
- **Mostrar colateral PSTN**
- **Editar colateral PSTN**

Parámetros	Descripción
Nombre colateral	Nombre de colateral PSTN. Están disponibles los colaterales PSTN siguientes: • Colateral PSTN estándar: no se puede configurar • Colateral PSTN 1: estándar para CLA, la función se puede modificar • Colateral PSTN 2: estándar para RDSI, la función se puede modificar • Colateral PSTN 3: el nombre y la función se pueden configurar • Colateral PSTN 4: el nombre y la función se pueden configurar Rango de valores: de 1 a 14 caracteres
Tipo de conex. PSTN	Configuración de la conexión PSTN: (selección estándar: Activado).
Tipo de conex. PSTN: Sin configurar	Se pueden preconfigurar colaterales PSTN. Sin embargo, con este ajuste se impide establecer la conexión mediante este colateral PSTN.
Tipo de conex. PSTN: Activo	El colateral PSTN está activo. Con este ajuste se permite establecer una conexión mediante este colateral PSTN.
Tipo de conex. PSTN: Conm. reserva DSL	Uso del acceso DSL para la conexión PSTN (el router estándar es el acceso DSL)
Parámetros IP	
Dirección IP de colateral PSTN	Dirección IP del PC host en el colateral con el que se establece la conexión PSTN.
Dirección IP de interfaz local PSTN	Dirección IP del sistema de comunicación local que se va a utilizar para la conexión PSTN.
Negociación dirección IP	Negociación de la dirección IP entre los colaterales en el establecimiento de conexión.
Negociación dirección IP: Utilizar dirección IP config.	Solo se aceptan las direcciones IP configuradas del colateral PSTN.

Parámetros	Descripción
Negociación dirección IP: Aceptar todas dir. IP	Sin negociación de la dirección IP
Negociación dirección IP: Solicitar nueva dirección IP	La dirección IP se negocia
Parámetros PPP generales	
Router estándar	El colateral PSTN configurado aquí no solo se tiene que preconfigurar, sino que también se debe utilizar como destino de encaminamiento. Solo puede haber un router estándar. Es un acceso DSL o el colateral PSTN configurado aquí.
Acceso a Internet con consulta DNS	El acceso se debe utilizar como acceso a Internet. Solo se puede activar un acceso a Internet por sistema (un colateral PSTN o un acceso DSL).
Entrada servicio	En caso de llamada al MSN del colateral PSTN hay que desactivar la comprobación de números de teléfono. La opción Entrada servicio solo se puede activar si el colateral PSTN tiene un número MSN y se ha activado una autenticación PAP o CHAP.
MSN/Marc. dir. (n.º llam. interno)	Configuración del número MSN. Si el colateral transmite su número de teléfono, tiene que estar configurado. De lo contrario, se rechaza la llamada. Si por el contrario hay configurados números de teléfono del colateral, sí se establece la conexión, aunque el colateral no transmita ninguno.
Canales B	Número de canales B utilizados. Rango de valores: 1 o 2
Devol. llam.	Se rechaza una llamada y el colateral puede devolver la llamada inmediatamente. Esto impide el acceso de colaterales no autorizados. El puesto que realiza la llamada debe transmitir el número de teléfono en el canal D de la conexión RDSI y permitir el acceso telefónico mediante el sistema. En el colateral PSTN, este número de teléfono tiene que estar configurado con dirección saliente. Si "Devolución de llamada" está activada, solo se aceptan conexiones salientes de este colateral. Si el colateral también es un gateway y también se ha activado para esta conexión "Devolución de llamada", no se puede establecer ninguna conexión, porque ninguno de los colaterales acepta un establecimiento de conexión entrante. Si en una configuración errónea de este tipo solo se activa la "devolución de llamada sin rellamada", se puede detectar el problema y anular un establecimiento de conexión permanente. Sin embargo, si la opción Rellamada está activada, no se detecta el problema.
Colateral V.34	Aceptar un colateral V.34 (por ejemplo, un módem).
Volver a conect. automát. PPP	La conexión PPP se restablece automáticamente tras un corte de conexión (por ejemplo, con un acceso ISP con tarifa plana y una desconexión forzosa tras 24 horas).
Enviar solicitud eco LCP	Se emite una solicitud echo de LCP. Esta función permite comprobar si la conexión sigue activa.
Modo reten. breve	

Parámetros	Descripción
Modo reten. breve	El modo de servicio "Reten. breve" está activado para la conexión PPP. Las siguientes entradas solo se pueden realizar si el modo Reten. breve está activado.
Tiempo reten. breve (s)	Tiempo sin transmisiones de datos que debe transcurrir para que se desconecte la conexión PPP. El temporizador de Reten. breve solo se activa con paquetes salientes. Rango de valores: de 10 a 9999
Eval. impulso tasas reten. breve	Optimización del modo Reten. breve tomando en consideración el impulso de tasas. Para las llamadas con PPP se evalúa dicho impulso (evaluación de los mensajes Facility con elementos informativos AoC). Si el proveedor de servicios de Internet no suministra información de tarifas, utiliza 0 como valor de tiempo de espera predeterminado.
Autenticación	
Autenticación PPP	Se activa la autenticación PPP.
Nombre usuario PPP	Nombre de usuario libre que se utilizará en la autenticación con PAP o CHAP.
Modo autenticación PAP	Activación y tipo de autenticación PAP para la conexión PPP: Sin utilizar, Cliente PAP, Host PAP.
Clave PAP	Contraseña para la autenticación PAP.
Modo autentificación CHAP	Activación y tipo de la activación CHAP para la conexión PPP: Sin utilizar, Cliente CHAP, Host CHAP, Cliente y host CHAP.
Clave CHAP	Contraseña para la autenticación CHAP.
Compresión encabezam.	
Compresión encabezam. IP	La compresión del IP/TCP o del encabezamiento IP/UDP/RTP está activa. La compresión de encabezamiento mejora la transmisión de datos en escenario Voice-over-PPP. Se comprimen todos los paquetes de voz cuyos números de puerto UDP estén dentro del rango configurado.
Compresión datos	
Compresión datos DEFLATE	Compresión con el algoritmo DEFLATE
Compresión datos COMPRESS	Compresión con el algoritmo COMPRESS
Traduc. dirección	
Traducción dirección red (NAT)	NAT (Network Adress Translation) está activado. Se admiten los siguientes protocolos: TCP, UDP y ICMP (solo en modo pasivo).
Mapping direcc.	El mapping de direcciones está activo.
Parámetros QoS de la interfaz	

Parámetros	Descripción
Control ancho banda para conex. voz	El control de ancho de banda impide que las tasas de transmisión tengan overbooking con conexiones de voz dentro de una conexión multienlace. En otras palabras, si la compresión de encabezamiento está activada, se admiten como máximo 5 conexión de voz (G.729 / 60 ms o G.723 / 60 ms) a través de un canal B. Este campo activa el control de ancho banda para conexiones de voz. Solo se toman en consideración conexión de voz que tengan las rutas configuradas en el gateway de voz.
Ancho banda para conex. voz/fax (%)	Porcentaje del ancho de banda disponible para conexiones de voz/fax. Rango de valores, valor estándar: 0 - 95, 80

Descripción de parámetros de las pestañas:

- **Reponer a estado de suministro**

Parámetros	Descripción
Aplicar	Los valores del colateral PSTN seleccionado se restablecen a los valores de fábrica.

Descripción de parámetros de las pestañas:

- **Añadir n° de llamada**
- **Editar n.º de llamada**
- **Borrar n° de llamada**

Parámetros	Descripción
Número de llamada	Número de teléfono con el que se puede acceder al colateral PSTN. Este número debe ser unívoco dentro de la configuración global y puede constar de un máximo de 22 cifras decimales (del 0 al 9). Se pueden utilizar guiones. Se pueden configurar hasta cinco números de teléfono por cada colateral PSTN. Si se transfiere el número de teléfono, se comprueba y solo se aceptan las llamadas si para el número de teléfono entrante hay definido un colateral PSTN con la autorización de llamada correspondiente.
Ruta llam.	La conexión se realiza con el número de teléfono registrado arriba.
Ruta llam.: Bloqueado	El número no se puede utilizar.
Ruta llam. : entrante	El colateral puede llamar, pero no se le puede llamar.
Dirección de llamada: saliente	Se puede llamar al colateral, pero no puede llamar.
Ruta llam. : Entrante y saliente	El colateral puede llamar y se le puede llamar.
Eliminar	Se borra el número de teléfono marcado.

28.3.5 LCR

En **LCR** se reunen las funciones de LCR como Clases de servicio, Plan de marcación, Tablas de rutas y Reglas marcación.

28.3.5.1 LCR > Flags LCR

Descripción de parámetros de la pestaña:

- **Editar flags LCR**

Parámetros	Descripción
Flags LCR	
Liberar LCR	LCR se libera y se activa la búsqueda automática de ruta.
Restablecer datos LCR	
Borrar los datos LCR configurados e inicialización con datos LCR estándares	Si se activa este campo de opción, se borran las entradas LCR configuradas (planes de marcación, tablas de rutas, reglas de marcación) y se sustituyen por las entradas estándares.

Consejo: Si el LCR se configura erróneamente, puede hacer que las conexiones salientes no funcionen o lo hagan con restricciones.

Conceptos relacionados

Datos de extensión en la página 163

28.3.5.2 LCR > Clases de servicio

Descripción de parámetros de la pestaña:

- **Modificar las clases de servicio LCR**

Parámetros	Descripción
El índice	Lista de índice jerárquica
Número de teléfono	Número de teléfono de extensión
Nombre	Nombre de la extensión
Grupo de clase de servicio	Cada extensión tiene asignado un grupo de clase de servicio LCR (Class Of Service COS). De forma predeterminada, todas las extensiones están registradas con la clase de servicio (autorización) LCR máxima (nivel 15) Rango de valores: de 1 a 15

Consejo: Una extensión solo puede ocupar una ruta si su clase de servicio es igual o superior a la clase de servicio (autorización) LCR de la tabla de rutas.

28.3.5.3 LCR > Plan de marcación

Descripción de parámetros de las pestañas:

- **Editar plan de marcación**
- **Mostrar plan de marcación**

Parámetros	Descripción
Plan de marcación	Se buscan modelos en el plan de marcación que coincidan con los dígitos marcados. El resultado se utiliza como criterio para elegir la tabla de rutas. También se comprueba si la autorización del usuario afecta a la ruta. En las conexiones externas, se comprueban todos los números de teléfono, incluido el código (hasta 24 caracteres máx., incl. el separador de campos) en el plan de marcación. A continuación, el plan de marcación determina para la extensión una tabla de rutas que se asigna a la extensión para el establecimiento de la conexión. Mediante la tabla de rutas se crean hasta 16 rutas. La tabla de reglas de marcación determina cómo se convierten los dígitos seleccionados por la extensión y cómo los marca el sistema de comunicación.
Nombre	Mediante la columna Nombre se puede asignar un nombre a cada perfil (por ejemplo, Llamada local, Llamada externa o Extranjero). El que la columna aparezca o no en pantalla depende de la versión del sistema de comunicación. Para el nombre hay que seleccionar un nombre adecuado. Los nombres se pueden utilizar varias veces. Con el asistente de números de teléfono se asignan nombres automáticamente.
Cifras marcadas	Este esquema se utiliza para evaluar el número de teléfono para hacer la ramificación a la tabla de rutas correspondiente. Se pueden utilizar los separadores de campos C y -, y los marcadores de posición X, N y Z. Números fijos 0...9, separador de campos - (evaluación mediante la regla de marcación), marcador de posición X para un dígito entre 0...9, marcador de posición N para un número entre 2...9, marcador de posición Z para uno o varios dígitos hasta el final de la marcación, tono de marcación simulado C (se puede introducir 3 veces máx.)
Tabla de rutas	En la columna Tabla de rutas se indica qué tabla de rutas se debe utilizar para el perfil. La flecha enlaza con la definición de la tabla de rutas correspondiente. Rango de valores: 1 a 254, los valores 1 a 15 están preasignados
Cód. proyecto	La casilla de verificación de esta columna se puede marcar o desmarcar para determinar si es obligatorio o no introducir un código de proyecto después del código de asignación (en los EE. UU.: después del final de marcación). Si no se selecciona esta opción, el código de proyecto solo se solicita una vez finalizada la marcación del plan de marcación y si está configurado así para la ruta.
Acceso a la red urbana	Si esta opción está seleccionada, los dígitos marcados se someten al control de marcación (Clase de servicio). Esto se aplica tanto para interconexiones como para sistemas de comunicación independientes. Con esto se pueden excluir números de teléfono determinados del control de marcación. Si hay que realizar el control de marcación, se aplican las reglas conocidas para listas de números permitidos y no permitidos.
Serv. emerg	Si se marca un número que esté configurado aquí como número de llamada de emergencia (columna Serv. emerg marcada) y no hay ninguna línea libre, se interrumpe una línea que esté en uso con un número que no sea de emergencia (columna Serv. emerg sin marcar) y se utiliza automáticamente para la llamada de emergencia.

28.3.5.4 LCR > Tabla de rutas

Descripción de parámetros de las pestañas:

- **Editar tabla de rutas**

Parámetros	Descripción
Tablas de rutas	A través de las tablas de rutas, se asigna aquí una acción (marcación) a los números de teléfono definidos en el plan de marcación. Rango de valores: 254 tablas de ruta
El índice	La tabla de rutas se consulta de arriba a abajo, en orden jerárquico. También se comprueba si la ruta está libre o si la extensión tiene la autorización LCR (Clase de servicio, COS) necesaria. Si es así, la marcación se realiza según las reglas de marcación de la tabla de rutas. Rango de valores: de 1 a 16
Ruta dedicada	Se utiliza la ruta asignada de forma fija a la extensión (por ejemplo, mediante la asignación de la ruta con Multisite Management).
Ruta	La ruta que va a ocupar, véase "Líneas/Interconexión > Rutas" Valor estándar: nombres de ruta configurados en el sistema
Regla de marcación	Las reglas de marcación LCR permiten convertir los números de teléfono introducidos en cualquier secuencia de cifras para su procesamiento ulterior. La conversión de dígitos permite acceder a los distintos proveedores de red. Definición en "Regla de marcación". Rango de valores: 254 reglas de marcación
Clase mín.	La clase de servicio mínima describe la autorización LCR que debe tener como mínimo una extensión para poder usar la ruta correspondiente. Aquí se puede definir, por ejemplo, que una extensión solo pueda telefonear con un determinado operador o solo a determinadas horas y que otras extensiones tengan una opción de desvío a otras rutas. El valor para la clase de servicio máxima es 15. Rango de valores: de 1 a 15
Advertencia	Si la ruta de enlace principal de la tabla de rutas está ocupada, LCR marcará la siguiente ruta configurada en la tabla (probablemente de mayor coste). Se le puede indicar al usuario a través de una señal acústica y/u óptica. Rango de valores: Ninguno, Tono, Display, Display + Tono
Gateway dedicado	El parámetro define cómo se identifica el nodo de colateral de destino en una interred IP. Rango de valores: Ninguno, Obligatorio, Varias ubicaciones
Gateway dedicado: **no**	El nodo de colateral se identifica con el número de teléfono de destino.
Gateway dedicado: **Forzado**	Se encamina forzosamente al gateway definido en la columna **ID de nodo de GW** por su ID de nodo.

Parámetros	Descripción
Gateway dedicado: **Varias ubicaciones**	Determinación en función del llamante del nodo de colateral: se encamina al gateway asignado al llamante correspondiente por el asistente multigateway o en la máscara de entrada **Extensiones** > **Editar datos cliente workpoint** > **ID del sistema secundario**. Para llamantes sin una entrada pertinente, se encamina al gateway definido en la columna **ID de nodo de GW con su ID** de nodo (predeterminado).
ID de nodo de GW	Indicación del ID de nodo de gateway para la selección **Forzado** o **Varias ubicaciones** del parámetro **Gateway dedicado**.
Botones	
Flecha azul en la columna **Regla de marcación**	Muestra la página con los parámetros de **Regla de marcación**.

28.3.5.5 LCR > Regla de marcación

Descripción de parámetros de la pestaña:

- **Editar regla de marcación**

Parámetros	Descripción
	Las reglas de marcación LCR permiten convertir los números de teléfono introducidos en cualquier secuencia de cifras para su procesamiento ulterior. La conversión de dígitos permite acceder a los distintos proveedores de red. La regla de marcación utiliza se determina mediante la entrada de la tabla de rutas.
Nombre de regla	Nombre definible de la regla de marcación (algunas reglas de marcación están predefinidas) Rango de valores: máx. 16 caracteres
Formato de regla de marcación	Programación para los dígitos que se van a marcar. Los distintos pasos de programación se ejecutan de izquierda a derecha. Estas son las funciones a las que equivalen los caracteres del código de programación:
A	Repetir el resto de campos (envío). "A" hace que se envíen todos los campos de dígitos siguientes. El punto de referencia es el último separador de campos presente en el campo de Cifras marcadas del plan de marcación. Si se registra "A" sin una referencia explícita, se refiere a todas las cifras que sigan al código de acceso, es decir, "A" equivale aquí a "E2A"
B	Se utiliza para la interconexión de varios gateways cuando el número de teléfono llamado desde el exterior es de "tipo" (TON, Type of Number) "desconocido", a fin de poder encaminar a nodos multigateway. Para que este número de teléfono sea único se debe ampliar en formato nacional o internacional según el TON del LCR. Es necesario si los números de marcación directa no son únicos y hay que configurarlos en formato nacional o internacional.
D (n)	Marcar secuencia de cifras (entre 1 y 25 cifras). "D" puede aparecer varias veces en la cadena de caracteres y en cualquier posición de la misma.

Parámetros	Descripción
E (n)	Emisión del contenido del campo (1 a 10). "E" puede aparecer varias veces en la cadena de caracteres y en cualquier posición de la misma. "E" puede aparecer en cualquier orden en relación con (n). Un determinado campo puede ser consultado varias veces, también consecutivas. "E" puede formar parte de cualquier otro parámetro (salvo "E1" - Access Code). En la marcación por pasos (frente a la marcación en bloque) el último elemento de la regla de marcación no puede ser E(n), sino E(n)A.
M (n)	Código de autorización (de 1 a 16). Esta letra no puede aparecer en última posición.
P (n)	P (n) puede aparecer varias veces en la cadena y se puede colocar en cualquier posición. P (n) puede estar rodeado de otros parámetros cuales quiera (de 1 a 60 veces la unidad de pausa a nivel del sistema).
S	Conmutación, cambio del método de marcación de MP a MF (con CONNECT, PROGRESS o CALL PROC con PI) "S" solo puede aparecer una vez en la cadena de caracteres y no puede aparecer en última posición. Después de "S" no se puede utilizar el parámetro "C".
C	"C" solo puede aparecer una vez en la cadena de caracteres. Los siguientes caracteres se envían sin pausa de marcación y se utilizan para el acceso de proveedor en "Single Stage", "Two Stage", "DICS" y "PRI".
U	Aplicación del procedimiento de marcación dirección SUB. "U" solo puede aparecer una vez en la cadena de caracteres y no puede aparecer en última posición. Después de "U" no se pueden utilizar los parámetros "S", "P", "M" y "C".
N (n) (¡solo para EE.UU!)	Grupo de red SFG (de 1 a 5) o número de banda (1).
L (¡solo para EE. UU.!):	"L" solo puede aparecer al final de la cadena de caracteres. "L" hace que la llamada se gestione como llamada de emergencia.
Procedimiento de acceso del ofertante de red	Selección del ofertante de red correspondiente
desconocido	Ninguna indicación explícita sobre un ofertante de red.
Operador de red principal	En caso de ocupación a través del ofertante de red principal, se realiza la marcación simple a través de marcación en bloque o marcación de dígitos individuales en la red pública.
MCL Single Stage	En MCL Single Stage el ofertante de red deseado se marca con un prefijo y, a continuación, se marca el número de teléfono. En RDSI, la marcación se realiza en el canal D o como marcación normal en líneas urbanas analógicas.
MCL Two Stage	En MCL Two Stage el ofertante de red deseado se marca con un prefijo. Tras una fase de sincronización se envía un código de autorización configurable y, a continuación, el número de teléfono de destino como dígitos MF. En la sincronización por tiempo se ha de programar una pausa de 2 a 12 segundos.
Red corporativa	Hay conectada una red corporativa directamente con OpenScape Business. La función LCR determina la ruta correspondiente a partir del número de teléfono marcado por el usuario. A continuación, encamina la llamada a través del haz de líneas de la línea urbana pública o del haz de líneas de la red propia de la empresa.

Parámetros	Descripción
Servidor de control de marcación	En este tipo LCR el ofertante de red deseado se marca con un prefijo y a través de un DICS (Dial-In Control Server) y se transmite el número de teléfono y un código de autorización configurable en la subdirección. La marcación se realiza en el canal D.
Primary Rate Interface (Interfaz de línea múltiplex primaria) (solo para EE. UU.)	En la interfaz de línea múltiplex primaria, la selección del ofertante de red o del servicio de llamadas se realiza en el mensaje de SETUP a través de los elementos de información: Network Specific Facility, Operator System Access y Transit Network Selection.
Tipo	Tipo núm.; aquí, por cada regla de marcación se pueden seleccionar en la lista desplegable los siguientes tipos de números para "Número de extensión llamada": Número de teléfono del sistema, Código de red local, Prefijo del país. Por defecto está predeterminada la entrada "Desconocido". El tipo de número solo se utiliza con E.164 y en las interconexiones el parámetro se define en "Desconocido".

28.3.5.6 LCR > Multisitio

Descripción de parámetros de la pestaña:

- **Modificar área**

Parámetros	Descripción
Código local	Entrada del prefijo local para una ubicación (incluido cero inicial, por ejemplo, `069` para Fráncfort y `030` para Berlín). Se pueden registrar prefijos locales diferentes o idénticos.
Área	Entrada del nombre para una ubicación (por ejemplo, las ciudades que se corresponden con los prefijos locales `Fráncfort` y `Berlín` o, si el prefijo es el mismo, las denominaciones de departamento `Servicio` y `Ventas`).
Ruta dedicada	Selección de la ruta o del registro de ITSP para esa ubicación.
Eliminar	Borra las entradas de ubicación marcadas.
Botones	
Guardar	Guarda los cambios.

Descripción de parámetros de la pestaña:

- **Modificar extensiones/grupos**

Parámetros	Descripción
Área	Selección de la ubicación para la extensión o el grupo.
Ruta dedicada	Selección de la ruta o del registro de ITSP para la extensión o el grupo.

Parámetros	Descripción
Buscar	Búsqueda por extensiones y grupos al introducir el término de búsqueda en los campos **N° llam.**, **Marc. dir.** o **Nombre** y, a continuación, pulsar la tecla Intro. Si todos los campos de búsqueda están vacíos y se pulsa la tecla Intro, aparece una lista de todas las extensiones y de todos los grupos. La selección **Tipo** permite visualizar todos los tipos de extensiones (por ejemplo, **Clientes SIP** o **Clientes sist.**).

28.3.6 Gateway voz

En **Gateway de voz** se reunen las funciones para la telefonía IP.

28.3.6.1 Gateway voz > Parámetros SIP

Descripción de parámetros de las pestañas:

- **Editar parámetros SIP**

Parámetros	Descripción
Protocolo de transporte SIP	
SIP vía TCP	"Transmission Control Protocol" (Protocolo de control de transmisiones). TCP es un protocolo de transporte obligatorio para SIP y no se puede desactivar aquí.
SIP vía UDP	"User Datagram Protocol" (Protocolo de datagrama de usuario). UDP es el protocolo de transporte predeterminado para SIP, pero puede desactivarse si no lo usa ningún punto terminal/línea/ITSP. Es muy recomendable mantener UDP activado.
SIP a través de TLS	"Transport Layer Security" (Seguridad de capa de transporte). TLS es el protocolo de transporte seguro para SIP y no se puede desactivar aquí.
Registrador SIP	
Duración del registro (s)	Intervalo (en segundos) en el que debe repetirse el registro de un punto de terminal SIP. El valor del intervalo no debe ser demasiado alto puesto que el registro se utiliza para determinar si un punto de terminal está fuera de servicio. (El periodo de registro para líneas ITSP se configura en los perfiles ITSP). Rango de valores, valor estándar: 10 - 86400, 120
RFC 3261 - Valores de Timer	
Tiempo de expiración de transacción (ms)	Indica el tiempo de espera (en milisegundos) antes de volver a transmitir la respuesta Invite para el temporizador D según la especificación RFC 3261. Este ajuste es relevante para la transacción de cliente Invite. Rango de valores, valor estándar: 2000 - 64000, 32000
SIP Session Timer	

Parámetros	Descripción
Utilizar RFC 4028	RFC 4028 define una ampliación del protocolo SIP (Session Initiation Protocol). Esta ampliación permite actualizar periódicamente las sesiones SIP. Los agentes de usuario y los proxies pueden determinar a través de las actualizaciones si la sesión SIP sigue activa. Aquí, la opción de configuración se utiliza para controlar la actualización de la sesión en la interfaz de línea (para ITSP, véase el perfil correspondiente).
Session Expires (s)	Define la duración de un intervalo de sesión SIP. El valor predeterminado es "1800". El valor configurado se emplea para las interfaces de línea e ITSP. Rango de valores, valor estándar: 90 - 65535, 1800
Minimal SE (s)	Define la duración mínima permitida de un intervalo de sesión SIP. El valor configurado se emplea para las interfaces de línea e ITSP. Rango de valores, valor estándar: 90 - 65535, 90
Registros DNS	
Hora de bloqueo para destino no accesible (s)	Este temporizador se utiliza para controlar la lista negra de la pila SIP. Si no se puede acceder a un servidor SIP restablecido a través de DNS, se bloqueará durante el tiempo configurado aquí. El valor estándar es 60 segundos. En casos en los que se utilicen servidores redundantes (por ejemplo, el DNS da lugar a múltiples servidores) se recomienda un valor más elevado (por ejemplo, 900).
Llamadas de proveedor	
Cant. máx. llamadas a través de proveedor	Aquí se muestra el número de llamadas simultáneas a través de todos los proveedores activados. Este valor se ajusta durante la configuración según el ancho de banda y la configuración ITSP.

28.3.6.2 Gateway de voz > Ajustes de ID de ubicación ITSP

Descripción de parámetros de las pestañas:

- Añadir información de ubicación ITSP

  La información de ubicación ITSP se utiliza en el protocolo SIP para informar al destinatario de una llamada de emergencia sobre el origen geográfico de la llamada. En el protocolo SIP, se define el formato de información de ID de ubicación RFC4119 y RFC5139 (objeto Ubicación codificado en XML en el cuerpo MIME). El ID de ubicación ITSP permite definir todos los campos definidos en los RFC pertinentes, mientras que en su despliegue concreto solo es necesario configurar un subconjunto de estos datos. (por ejemplo, en Suiza el campo NAM solo se utiliza para definir una ubicación). Su ITSP le proporciona los datos necesarios para definir una ubicación.

Parámetros	Descripción
Nombre ID de ubicación	El nombre de la ID de ubicación.
País	El país se identifica con el código ISO 3166 de dos letras.

Parámetros	Descripción
A1	Subdivisiones nacionales (estado, cantón, región, provincia, prefectura)
A2	Condado, parroquia, pistola, distrito
A3	Ciudad, el municipio, shi
A4	División de la ciudad, barrio, ciudad, distrito, de la sala, Chou
A5	Barrio, de bloques
A6	Calle
PRD	Dirección calle principal
POD	Rastrero calle sufijo
STS	Calle sufijo o tipo
HNO	Número de casa, sólo parte numérica
HNS	Casa número sufijo
LMK	Hito o vanidad
LOC	Información adicional del lugar
FLR	Piso
NAM	Nombre (residencia u Oficina ocupante).
PC	Código postal
ROOM	Habitación
PLC	Tipo de lugar
PCN	Postal nombre de la comunidad
POBOX	Apartado de correos
ADDCODE	Código Adicional
SEAT	Asiento (escritorio, cubículo, estación de trabajo)
RD	Principal de carreteras nombre
RDSEC	Sección de la carretera
RDBR	Rama carretera nombre
RDSUBBR	Sub-rama carretera nombre
PRM	Nombre de la calle antes de la modificador
POM	Nombre de la calle después de los modificadores
Activar configuración avanzada	Puede configurarse cuando los campos de parámetros avanzados están activados.
BLD	Edificio (estructura)
UNIT	Unidad (apartamento, suite)

28.3.6.3 Gateway voz > Parámetros códec

Descripción de parámetros de las pestañas:

- **Editar parámetros códec**

Parámetros	Descripción
Codec	Los parámetros de los códecs G.711 A-law, G.711 µ-law, G.729A y G.729AB se pueden editar.
Códec: G.711 A-law	G.711 (A-law y µ-law): codificación de voz con 56 o 64 Kbit/s: muy buena calidad de voz. G.711 se utiliza en el área de red fija (RDSI). El procedimiento A-law es un procedimiento de digitalización utilizado principalmente en Europa para las señales de audio analógicas en el área de las telecomunicaciones.
Códec: G.711 µ-law	G.711 (A-law y µ-law): codificación de voz con 56 o 64 Kbit/s: muy buena calidad de voz. G.711 se utiliza en el área de red fija (RDSI). En Norteamérica y Japón se utiliza el procedimiento µ-law, similar al A-law pero no compatible con él. Para la comunicación (p. ej., en una llamada telefónica entre Europa y los EE. UU.), los datos digitales se tienen que convertir utilizando el conversor adecuado.
Códec: G.729A	Codificación de voz con 8 kbps.
Códec: G.729AB	Codificación de voz con 8 kbps. Las pausas de voz se llenan con ruidos de confort.
Prioridad	Los códecs de sonido reciben asignadas prioridades del 1 (alta) a 4 (baja). El sistema de comunicación intenta automáticamente utilizar un códec de sonido con una prioridad alta en cada conexión. Si se utiliza un códec de sonido de baja compresión (buena calidad de voz), se carga más la red. Si el uso de la telefonía IP es intensivo, la calidad de voz se puede ver afectada negativamente si la red ya se sobrecarga en la transferencia de datos.
Detección pausas voz (VAD)	Activar la detección de pausas de voz (VAD, Voice Activity Detection). De esta forma, se puede reducir la carga de la red durante las pausas largas.
Tamaño marco	Se puede indicar el tamaño marco (tamaño del paquete IP) de cada códec. El valor estará entre 10 y 90 milisegundos. De esta forma, establece la frecuencia de muestreo con la que la señal de voz se dividirá en paquetes IP. Un valor más elevado (p. ej., 90 ms) significa, por un lado, una mejor relación entre carga útil y carga general de los paquetes IP. Por otro lado, sin embargo, supone también un mayor retardo en la transmisión. Los valores de configuración dependen de los códecs. Para interconectar OpenScape Business con OpenScape Voice mediante SIP-Q V2: Cordless IP y OpenScape Mobile Connect solo admiten un tamaño marco de 20 ms para el códec G.711. Si en la interred hay uno de estos dos productos, hay que definir aquí el tamaño marco en 20 ms. Rango de valores, valor estándar: 10 - máx. 90, 20
Canales de DSP mejorados	
Utilice sólo G.711	Solo se utilizan los protocolos G.711 A-law y G.711 µ-law. Con G.711 se requieren menos recursos DSP y así se pueden hacer más llamadas simultáneas.
Fax T.38	

Parámetros	Descripción
Fax T.38	Determina si se va a usar el protocolo de fax T.38. Para el sistema con la Tarjeta Booster y/o el Servidor Booster: si el flag está activado, la corrección de errores se realiza en el protocolo T.38. Aparece una ventana emergente para notificar al usuario que es necesario reiniciar el sistema de forma manual o OCAB/Booster Server.
Utilizar FillBitRemoval	Determina si al utilizar el protocolo de fax T.38, los bits de llenado se borrarán en el envío y se restablecerán en la recepción. Esto permite ahorrar ancho de banda.
Tamaño máx. datagrama UDP para fax T.38 (bytes)	Tamaño máximo de un datagrama UDP T.38 en bytes. Rango de valores, valor estándar: 1 - 1472, 1472
Corrección errores utiliz. para fax T.38 (UDP)	Determina qué método hay que utilizar para la corrección de errores. Valores: t38UDPFEC, t38UDPRedundancy Para el sistema con la Tarjeta Booster y/o el Servidor Booster: cuando se selecciona esta opción, aparece una ventana emergente para notificar al usuario que es necesario reiniciar el sistema de forma manual u OCAB/Booster Server. Valor estándar: t38UDPRedundancy
Fax T.30	
Activar ECM	Para el sistema con la Tarjeta Booster y/o el Servidor Booster: Si el flag está activado, la corrección de errores se realiza en el protocolo T.30. Aparece una ventana emergente para notificar al usuario que es necesario reiniciar el sistema de forma manual o OCAB/Booster Server. Valor estándar: activado
Modo de compatibilidad VoIP	Para el sistema con la Tarjeta Booster y/o el Servidor Booster: este flag debe activarse si encuentra problemas con la transmisión de fax en redes VoIP. Aparece una ventana emergente para notificar al usuario que es necesario reiniciar el sistema de forma manual o OCAB/Booster Server. Valor estándar: desactivado
Otros	
ClearChannel	Un ClearChannel es un canal abierto en el los puntos de terminal son responsables del protocolo del canal. Este parámetro determina si se activa o no la funcionalidad de interfaz ClearChannel.
Tamaño marco	En este campo puede determinar la tasa de muestreo. Los valores posibles son 10, 20, 30, 40, 50 y 60 milisegundos (ms). Rango de valores, valor estándar: 10 - 60, 20
RFC2833 RFC2833 determina cómo se transmitirán las señales de tono.	
Transmisión de tonos fax/ módem a RFC2833	Outband de transmisión (mediante la señalización SIP), modo de servicio recomendado para transmitir tonos de forma segura
Transmisión de tonos MF a RFC2833	Outband de transmisión (mediante la señalización SIP), modo de servicio recomendado para transmitir tonos de forma segura

Parámetros	Descripción
Tipo de Payload para RFC2833	Puede ser necesario ajustar este valor, según el interlocutor Rango de valores, valor estándar: 96 - 126, 98
Transmisión redundante de tonos RFC2833 a RFC2198	Permite aumentar la seguridad de la transferencia

28.3.6.4 Gateway voz > Parám. códec destino

Para determinados interlocutores se pueden definir prioridades para el uso de los códecs de sonido.

Descripción de parámetros de las pestañas:

- **Añadir parám. códec destino**

Parámetros	Descripción
Códec: G.711 A-law	G.711 (A-law y µ-law): codificación de voz con 56 o 64 Kbit/s: muy buena calidad de voz. G.711 se utiliza en el área de red fija (RDSI). El procedimiento A-law es un procedimiento de digitalización utilizado principalmente en Europa para las señales de audio analógicas en el área de las telecomunicaciones.
Códec: G.711 µ-law	G.711 (A-law y µ-law): codificación de voz con 56 o 64 Kbit/s: muy buena calidad de voz. G.711 se utiliza en el área de red fija (RDSI). En Norteamérica y Japón se utiliza el procedimiento µ-law, similar al A-law pero no compatible con él. Para la comunicación (p. ej., en una llamada telefónica entre Europa y los EE. UU.), los datos digitales se tienen que convertir utilizando el conversor adecuado.
Códec: G.729A	Codificación de voz con 8 kbps.
Códec: G.729AB	Codificación de voz con 8 kbps. Las pausas de voz se llenan con ruidos de confort.
Prioridad	Los códecs de sonido reciben asignadas prioridades del 1 (alta) a 4 (baja). El sistema de comunicación intenta automáticamente utilizar un códec de sonido con una prioridad alta en cada conexión. Si se utiliza un códec de sonido de baja compresión (buena calidad de voz), se carga más la red. Si el uso de la telefonía IP es intensivo, la calidad de voz se puede ver afectada negativamente si la red ya se sobrecarga en la transferencia de datos.
Destino	
Tipo dir. destino	Indicación del tipo de destino al que se van a asignar las prioridades de los códecs de sonido configuradas.
Dirección IP	Dirección IP del destino para la que sea aplicarán las prioridades de los códecs de sonido configuradas (p. ej., nodos interconectados, servidor SIP)

28.3.6.5 Gateway de voz > Proveedor de servicios de telefonía por Internet

Descripción de parámetros de las pestañas:

- **Agregar proveedor de servicios de telefonía por Internet**
- **Editar proveedor de servicios de telefonía por Internet**
- **Eliminar proveedor de servicios de telefonía por Internet**

Parámetros	Descripción
Plantilla base	Selección de una plantilla vacía (predeterminada) o una configuración de muestra predefinida para un proveedor de servicios en particular. Esto se puede adaptar para cumplir requisitos individuales y guardarlo como un nuevo ITSP.
Nombre del proveedor	Nombre deseado del ITSP. El ITSP configurado aparecerá en la lista de ITSPs con este nombre.
Habilitar proveedor	El ITSP está activado.
Identificador del proveedor en el sistema	Asignación de una designación única en el sistema. Un máximo de 8 ITSPs pueden estar activos simultáneamente. Rango de valores: Proveedores 1-8
Nombre de dominio	Nombre de dominio del gateway del ITSP a menudo no es idéntico al nombre de dominio web.
Protocolo de transporte	Protocolo de transporte deseado. Se puede seleccionar UDP o TCP.
Seguridad del transporte	Los valores posibles son **tradicionales (upd o tcp)** para llamadas tradicionales utilizando udp/tcp o **seguros (tls)** para llamadas seguras utilizando TLS. Valor predeterminado: **tradicional (udp o tcp)**
Seguridad de los medios	Los valores posibles son solo **RTP** (solo se admite el perfil AVP) o **solo SDES** (sólo se admite el perfil SAVP). Valor estándar: **Solo RTP**
Registrador de proveedores	
Registrador de uso	Debe seleccionarse si el troncal funciona con registro (predeterminado = desactivado).
Dirección IP / Nombre de host	Nombre de host o dirección IP del servidor registrador externo.
Puerto	Número de puerto del servidor registrador externo, por ejemplo, 5060. Ingrese el puerto 00 si el ITSP utiliza DNSSRV.
Intervalo de reinscripción en el proveedor (seg.)	Intervalo (en segundos) en el que se repite el registro ITSP. El valor del intervalo no debe ser 0 ni demasiado alto, ya que al repetir el registro en el ITSP también se puede detectar una conexión interrumpida y se puede seleccionar una ruta alternativa (a través de ISDN o un proveedor alternativo) si es necesario. Valor estándar: 120 segundos
Proxy del proveedor	
Dirección IP / Nombre de host	Nombre de dominio o dirección IP del servidor proxy (por ejemplo, sip-voice.de). La entrada es obligatoria y normalmente es idéntica a la entrada del registrador del proveedor.

Parámetros	Descripción
Puerto	Número de puerto del servidor proxy (por ejemplo, 5060). Por regla general, es idéntico al número de puerto del proveedor. Ingrese el puerto 0 si el ITSP utiliza varios servidores y DNSSRV.
Proxy de salida del proveedor	
Utilizar proxy de salida	Habilitar solo si el ITSP utiliza un proxy de salida diferente del proxy del proveedor. Deshabilitado por defecto.
Dirección IP / Nombre de host	Nombre de dominio o dirección IP del proxy saliente.
Puerto	Número de puerto del proxy saliente. Ingrese el puerto 0 si el ITSP utiliza varios servidores y DNSSRV.
Proxy entrante del proveedor	
Utilizar proxy entrante	Solo se establece si el ITSP envía opcionalmente solicitudes desde un segundo servidor. Deshabilitado por defecto.
Dirección IP / Nombre de host	Nombre de dominio o dirección IP del segundo servidor ITSP
Puerto	Número de puerto del segundo servidor ITSP. Ingrese el puerto 0 si el ITSP utiliza DNSSRV.
Proveedor STUN	
Usar STUN	Sólo se establece si el ITSP utiliza un servidor STUN. La configuración de todo el sistema bajo la configuración STUN se aplica como modo STUN para todos los ITSPs (predeterminado = desactivado).
Dirección IP / Nombre de host	Nombre de host o dirección IP del servidor STUN.
Puerto	Número de puerto STUN del servidor STUN.
Datos del proveedor SIP extendido	
Mostrar datos extendidos del proveedor SIP	Al habilitar esta bandera, están disponibles algunos parámetros de configuración adicionales para controlar la pila SIP y adaptar el contenido de los campos de encabezado SIP.
CLIP / CLIR	El sistema proporciona varios parámetros para controlar el formato de los campos del encabezado SIP según las necesidades del troncal nativo Se puede controlar el contenido de los siguientes campos de encabezado que describen el origen de una llamada: • De: Parte de visualización <sip:UserPart@HostPart> • P-Identidad afirmada: Parte de visualización <sip:UserPart@HostPart> • P-Identidad-Preferida: Parte de visualización <sip:UserPart@HostPart>

Parámetros	Descripción
CLIP saliente en el encabezado De - parte de visualización	Configuraciones posibles: • Omitir - se omite el campo • Número de llamada: el número configurado para una estación. Puede definir qué número se utiliza en los "parámetros de ruta" • Cuenta: el nombre de usuario asignado al tronco nativo • nombre para mostrar
CLIP saliente en el encabezado De - parte del usuario:	Configuraciones posibles: • Número de llamada • Cuenta
Encabezado de salida - parte de dominio/host:	Cambie la parte de dominio/host del URI para que se complete con la dirección IP del sistema. Este parámetro afecta a la parte del host de los tres campos de encabezado Desde:, PAI y PPI Configuraciones posibles: • nombre de dominio • Dirección IP local • Dirección IP pública
Desviación: De contiene el número de la parte que llama original:	Si se establece una llamada saliente debido a un desvío de llamadas, el sistema puede proporcionar información sobre la parte que llama original. Si está habilitado, el sistema envía la parte que llama original (A-Ext) en el campo de encabezado De:, de lo contrario, envía el número de la estación de reenvío.
Desviación: PAI contiene el número de la parte que llama original	Si se establece una llamada saliente debido a un desvío de llamadas, el sistema puede proporcionar información sobre la parte que llama original. Si está habilitado, el sistema envía la parte que llama original (A-Ext) en el campo de encabezado P-Asserted-Id; de lo contrario, envía el número de la estación de reenvío. Al configurar esta bandera, el sistema envía la parte que llama original en el campo de encabezado P-Asserted_ID: y P-Preferred-ID:.
CLIP saliente en el encabezado P-Asserted-Id - parte de visualización:	Configuraciones posibles: • Omitir - se omite el campo • Número de llamada: el número configurado para una estación. Puede definir qué número se utiliza en los "parámetros de ruta" • Cuenta: el nombre de usuario asignado al tronco nativo • nombre para mostrar
CLIP saliente en el encabezado P-Asserted-Id - parte del usuario:	Configuraciones posibles: • Omitir - se omite el campo • Número de llamada • Cuenta

Parámetros	Descripción
CLIP saliente en el encabezado P-Preferred-Id - parte de visualización:	Configuraciones posibles: • Omitir - se omite el campo • Número de llamada: el número configurado para una estación. Puede definir qué número se utiliza en los "parámetros de ruta" • Cuenta: el nombre de usuario asignado al tronco nativo • nombre para mostrar
CLIP saliente en el encabezado P-Preferred-Id - parte del usuario:	Configuraciones posibles: • Omitir - se omite el campo • Número de llamada • Cuenta
CLIP saliente en el encabezado de desvío: parte de visualización:	Configuraciones posibles: • Omitir - se omite el campo • Número de llamada: el número configurado para una estación. Puede definir qué número se utiliza en los "parámetros de ruta" • Cuenta: el nombre de usuario asignado al tronco nativo • nombre para mostrar
CLIP saliente en el encabezado de desvío - parte del usuario:	Configuraciones posibles: • Omitir - se omite el campo • Número de llamada • Cuenta
CLIP saliente en el encabezado History-Info - parte del usuario:	Configuraciones posibles: • omitir • número de llamada
CLIR saliente en el encabezado De - parte de visualización:	Configuraciones posibles: • Omitir • Número de llamada • Cuenta • Anónimo **De: Anónimo <sip: ...@...>**
CLIR saliente en el encabezado De - parte del usuario:	Configuraciones posibles: • Número de llamada • Cuenta • Completamente anónimo**De: ...<sip:anonymous@anonymous.invalid>** • Usuario anónimo **De: ... <sip:anonymous@...>**
Encabezado de privacidad saliente de CLIR	Configuraciones posibles: • Omitir • Id **Privacidad: id** • Usuario **Privacidad: usuario** • Usuario, id **Privacidad: usuario;id**

Parámetros	Descripción
COLP/TIP compatible con llamadas salientes:	En ISDN se introdujo la función COLP (Presentación de identificación de línea de conexión). En SIP, esta función a veces se denomina TIP (Presentación de identificación de terminación). RFD3324 (sección 5) define un mecanismo para transportar la identidad de la parte aceptante (C) en el campo de encabezado P-Asserted-Identity de la respuesta 200 OK: Configuraciones posibles: • COLP apoyado • COLP no compatible
Formato de número de llamada	
Llamada entrante - Número de la parte llamada:	Esta bandera se refiere a la dirección de destino de una llamada. De manera predeterminada, esto se toma de la **parte de usuario** del campo de **encabezado TO**:. Configuraciones posibles: • Línea de solicitud **INVITE sip: +498970070@...** • A la parte de visualización del encabezado **Para: +498970070 <sip:+** • A la parte de usuario del encabezado **Para: <sip: +498970070@...** • Parte de visualización del encabezado P-Called-Party-Id **P-Called-Party-ID: +498970070 <sip:..** • Parte de usuario del encabezado P-Called-Party-Id **P-Called-Party-ID: <sip: +498970070@..**
Llamada entrante - Número de la persona que llama:	Esta bandera se refiere a la dirección de origen de una llamada. De manera predeterminada, el sistema elimina la parte que llama de la parte de usuario del encabezado "De". Configuraciones posibles: • automático • Desde la parte de visualización del encabezado **De: +498970070 <sip:+** • Desde la parte de usuario del encabezado **De: <sip: +498970070@...** • Parte de visualización del encabezado P-Asserted-Id **P-Asserted-ID: +498970070 <sip:..** • Parte de usuario del encabezado P-Asserted-Id **P-Asserted-ID: <sip: +498970070@..** En el modo automático, el sistema busca en primer lugar la parte del usuario de la P-Asserted-Identity, si está presente. Si no hay ninguna P-Asserted-Identity presente, se toma la parte del usuario del campo de encabezado From:.

Parámetros	Descripción
Llamada entrante - Tipo de número (llamante):	Configuraciones posibles: • automático • internacional
Llamada entrante - Tipo de número (llamado):	Configuraciones posibles: • automático • internacional • nacional
Llamada saliente - Tipo de número (llamante):	Configuraciones posibles: • automático • internacional • nacional
Llamada saliente - Tipo de número (llamado):	Configuraciones posibles: • automático • internacional • nacional
Asignación de número de proveedor:	Configuraciones posibles: • En cualquier caso • Solo llamadas entrantes (si está configurado) • apagado
CLIP sin Soporte de proyección:	Configuraciones posibles: • no compatible • CLIP en De / número de confianza en PAI • Compatible - Sin tratamiento especial • CLIP en el número Desde/DID en PAI
Número de llamada con prefijo internacional/nacional:	Configuraciones posibles: • no • sí
Número llamado en formato E164:	Configuraciones posibles: • no • sí
Optimización de rutas:	Configuraciones posibles: • no permitido • permitido • permitido (IP local en Contacto)
MEX compatible:	Configuraciones posibles: • no • sí

Parámetros	Descripción
La URI de contacto contiene:	Este parámetro se utiliza para configurar el contenido de la parte de usuario del URI de contacto **Contacto: sip:UserPart@HostPart:port** Configuraciones posibles: • Número de llamada: la parte del usuario del URI de contacto contiene el número de llamada • Registro AOR: el URI de contacto contiene la parte de cuenta=usuario del registro.
Puerto TCP utilizado en la URI de contacto:	Este parámetro se utiliza para configurar el puerto TCP utilizado en la parte de host del URI de contacto **Contacto: sip:UserPart@HostPart:port** Configuraciones posibles: • puerto ephem.src: De forma predeterminada se utiliza el puerto de origen TCP efímero • Puerto del servidor SIP: El puerto del servidor SIP se utiliza en el URI de contacto
Registro	
El registro de contacto contiene la dirección IP:	Configuraciones posibles: • dirección IP local • nombre de dominio
ContactUriWithProtocol:	activar/desactivar
Registro BNC (SIPconnect):	Configuraciones posibles: • registro normal • Registro BNC
Intervalo de reinscripción tras fallo (seg):	
Modo de reinscripción:	Configuraciones posibles: • continuo • SIPConnect
Reinscripción tras fallo de llamada:	Configuraciones posibles: • Fallo de llamada no es un fallo de registro • Fallo de llamada es un fallo de registro
Seguridad	
Modo UDP:	Configuraciones posibles: • UDP simétrico • UDP asimétrico
Selección de pares aprobada:	Configuraciones posibles: • Confianza configurada únicamente en servidores • Servidores de confianza recibidos en respuestas SIP

Parámetros	Descripción
Varios	
Carga útil directa:	Para una conexión ITSP directa, este parámetro DEBE establecerse en falso. Si se utiliza un SBC externo delante de OpenScape Business, este parámetro se establece como verdadero.
Evitar la renegociación con los medios:	Para una conexión ITSP directa, este parámetro DEBE establecerse como verdadero. Si el parámetro de manejo de medios Carga útil directa se establece como verdadero, este parámetro NO tiene efecto. (por ejemplo, en los casos en que se utiliza un SBC externo delante del sistema OpenScape business)
Atributo de cambio de dirección:	Configuraciones posibles: • mantener atributo • cambiar a sendrecv
Atributo de supresión de silencio:	Configuraciones posibles: • apoyado • no compatible
Extensión de Mediasec:	Configuraciones posibles: • apoyado • no compatible
Filtro SDP:	Configuraciones posibles: • Por defecto • Perfil de compatibilidad • Abierto
UseRouteURIAuthentication:	Verdadero establece el comportamiento para utilizar el URI de ruta en lugar del URI de solicitud en el encabezado de autorización (proxy) para INVITE o INFO (no para REGISTER). Se utilizará la URI de solicitud cuando no haya ninguna URI de ruta presente. Para los ITSP, este parámetro DEBE establecerse en verdadero.
Ignorar 100 Rel:	Ignorar un 'Compatible: Campo de encabezado '100rel' si se recibe en INVITE. Debido a que 100rel puede interferir con la interoperabilidad con suscriptores que no sean SIP, este parámetro DEBE establecerse en verdadero.
Soporte 100rel	Al configurar este marcador, el sistema agregará un encabezado 100rel compatible en la invitación saliente. Esto permitirá que el ITSP envíe respuestas provisionales confiables seguidas de mensajes de ACTUALIZACIÓN. Este parámetro se puede utilizar para la familia de placas base y servidores OpenScape Business V3 sin restricciones.

Parámetros	Descripción
UtiliceViaRPort:	Si se establece como verdadero, el parámetro rport se agrega a Via-Header. *Vía: SIP/2.0/UDP 192.168.138.1:5060;rport;* Si se establece como falso, no se agrega ningún parámetro de informe a Via-Header. *Vía: SIP/2.0/UDP 192.168.138.1:5060;*
ACTUALIZACIÓN compatible:	Si se establece como verdadero, se utiliza UPDATE según el contenido del campo de encabezado Permitir. Si no se configura ACTUALIZACIÓN en el campo de encabezado Permitir recepción, la pila SIP nunca envía una ACTUALIZACIÓN. Si se establece como falso, el método UPDATE nunca se utilizará (se utiliza un re-INVITE en lugar de esto) Para ITSP, este parámetro DEBE establecerse en verdadero (predeterminado)
Compatibilidad con encabezados P-Early-Media:	Configuraciones posibles: • no compatible • apoyado
Compatibilidad con temporizador de sesión:	Configuraciones posibles: • no activo • Política de actualización remota
Enviar temporizador de respuesta automático 183 (seg):	Con este temporizador se activa una respuesta provisional (183) después del tiempo de espera si no hay información de progreso disponible del sistema. Esto es necesario porque algunas plataformas no detienen los temporizadores de supervisión al recibir un intento de 100 (por ejemplo, Broadsoft) 0 no se envía ninguna respuesta automática; todas las respuestas son activadas por el sistema Tiempo de espera de 1 a 10 segundos, el temporizador se inicia al recibir una solicitud INVITE del ITSP. Cuando expira el temporizador, la pila SIP envía un 183 0 (predeterminado)
UDP-Keep Alive:	Configuraciones posibles: • UdpKeepAliveON • UdpKeepAliveOFF • Opciones de SendAlive
Intervalo de Keep Alive para OPCIONES (seg):	Con este parámetro se define el intervalo para el envío de OPCIONES SIP 60 (predeterminado)
Reinscripción en caso de fallo de OPCIONES:	Configuraciones posibles: • No hay registro en caso de fallo • Registrarse en caso de fallo

Parámetros	Descripción
Respuesta a OPCIONES:	Configuraciones posibles: • Respuesta completa • Sin cuerpo
Botones	
Reiniciar ITSP	Inicia un nuevo registro con el ITSP (sólo es posible con un ITSP activado).

Descripción de parámetros de las pestañas:

- **Editar la configuración de STUN**

Parámetros	Descripción
Moda STUN	Esta configuración se aplica globalmente a todos los ITSPs, siempre que STUN esté habilitado para ellos. La necesidad de STUN o no depende de la infraestructura del ITSP y del enrutador de Internet utilizado. STUN no es necesario si el ITSP resuelve la travesía NAT en su propia red. STUN garantiza que en los mensajes SIP se utilice la dirección IP de acceso público en lugar de la dirección IP interna.
Modo STUN: Siempre	STUN siempre está activo.
Modo STUN: Automático	El tipo de NAT del enrutador a Internet se comprueba automáticamente. Si se requiere STUN, se habilita. Si no se requiere o no es posible STUN, STUN se desactiva. Esta es la configuración predeterminada recomendada.
Modo STUN: Utilice IP estática	Si el ITSP requiere autenticación de IP estática, se requiere una dirección IP estática (dirección IP pública) en el módem DSL o en el enrutador de Internet. Además, se deben especificar la dirección IP estática y el puerto.
Modo STUN: Utilice IP estática, dirección IP pública	Dirección IP estática del módem DSL o del enrutador de Internet.
Modo STUN: Utilice IP estática, puerto SIP público	Puerto del módem DSL o del enrutador de Internet.
Modo STUN: Enrutador de conservación de puertos	Si ninguno de los modos STUN mencionados anteriormente funciona, se debe probar este modo. Algunos módems y enrutadores de Internet no cambian el puerto RTP para NAT y necesitan este modo para su correcto funcionamiento.
Tipo Nat detectado	Si hay un ITSP activo, aquí se mostrará el tipo de NAT.
Servidor STUN predeterminado	
Dirección IP / Nombre de host	Dirección IP o nombre de host del servidor STUN (por ejemplo, `stun.serviceprovider.com`). Este servidor STUN se utiliza para SIP@Home cuando no se utiliza ningún ITSP o si el ITSP utilizado no ofrece ningún servidor STUN.
Puerto	Puerto del servidor STUN (por ejemplo, `3478`)

Descripción de parámetros de las pestañas:

- **Detección de tipo de NAT**

Parámetros	Descripción
Activación automática	Habilita la detección automática del tipo de NAT.
Iniciar la detección del tipo de NAT	Inicia la detección del tipo de NAT manualmente.

Descripción de parámetros de las pestañas:

- **Añadir estación de telefonía por Internet**
- **Editar estación de telefonía por Internet**
- **Eliminar estación de telefonía por Internet**

Parámetros	Descripción
Estación de telefonía por Internet	Datos de acceso de la cuenta asignada por el ITSP. En función del ITSP se utilizarán aquí distintas denominaciones (por ejemplo, Usuario SIP, ID SIP, etc. Es posible que también deba ingresar el número de cliente ITSP aquí. Si se utiliza la autenticación IP estática, aquí se debe ingresar el número PABX.
Nombre de la autorización	Nombre de autorización asignado por el ITSP. Esto suele ser idéntico al abonado a la telefonía por Internet.
Contraseña	Contraseña asignada por el ITSP. En función del ITSP se utilizarán aquí distintas denominaciones (por ejemplo, Contraseña, Contraseña SIP, etc.)
Confirmar contraseña	Contraseña asignada por el ITSP. En función del ITSP se utilizarán aquí distintas denominaciones (por ejemplo, Contraseña, Contraseña SIP, etc.)

Descripción de parámetros de las pestañas:

- **Agregar entrada de MSN**
- **Editar entrada de MSN**
- **Eliminar entrada de MSN**
- **Eliminar todas las entradas de MSN**

Parámetros	Descripción
Número de teléfono de telefonía por Internet / **Número de teléfono de telefonía por Internet** / **Número de teléfono de telefonía por Internet**	Número de llamada (único) asignado por el ITSP.
DID / **Número de llamada interna**	Número de llamada interno asignado.
Entrada predeterminada	La activación como entrada predeterminada permite a los usuarios que no disponen de un número de teléfono de telefonía por Internet propio, realizar llamadas a través de este número. La opción sólo se puede seleccionar para un MSN. (sólo para soporte de llamadas de voz, no fax)
Estación de telefonía por Internet / **Estación de telefonía por Internet**	Muestra la estación de telefonía por Internet

Descripción de parámetros de las pestañas:

- **Agregar rango DID**
- **Editar rango DID**
- **Eliminar rango DID**

Parámetros	Descripción
Número de PABX	Número de cabeza asignado por el ITSP (sin el número DID)
Banda de marcación entrante directa de … hasta	Rango de números DID asignados por el ITSP
Inicio del rango de números de llamada internos	Primer número interno a partir del cual se desea una asignación automática de números de llamada.
Asignar banda de marcación entrante directa automáticamente a las estaciones	Si se selecciona, los números DID se asignan automáticamente en orden ascendente a los números de llamada internos y se generan las entradas MSN correspondientes.

28.3.6.6 Gateway voz > Redes > Nodos

Descripción de parámetros de las pestañas:

- **Agregar nodo de redes**
- **Modificar nodo de redes**
- **Borrar nodo de redes**

Parámetros	Descripción
ID de nodo	Solo para la configuración manual sin asistente, por ejemplo, con numeración abierta: entrada de un número de nodo exclusivo en la interred.
Dirección IP	Solo para configuración manual sin asistente, por ejemplo, con numeración abierta: dirección IP del nodo
Supervisión nodos	Si se selecciona Supervisión nodos se comprueba periódicamente la comunicación con el nodo. Para ello es necesario que la supervisión de nodos también esté activada en el otro nodo.
Nivel de seguridad de cifrado de nodos	Al seleccionar "seguro" se activa el cifrado para la comunicación de voz con el nodo. Además, en el sistema debe estar configurada la opción de "Cifrado de señalización y carga útil". Rango de valores: tradicional, seguro

28.3.6.7 Gateway voz > Redes > Encaminamiento

Descripción de parámetros de las pestañas:

- **Añadir n° de llamada**
- **Borrar todos los números de llamada de extensión.**

Parámetros	Descripción
ID de nodo	Selección del número de nodo

Parámetros	Descripción
Número de teléfono	Solo para configuración manual sin asistente, por ejemplo, con numeración abierta: indicación del código con el que se puede acceder al nodo.

28.3.6.8 Gateway voz > Interconexión SIP-Q

A través de la interconexión SIP-Q se definen los parámetros para dos rutas SIP-Q externas posibles. Con ellas se pueden conectar servidores SIP externos, por ejemplo, OpenScape 4000 u OpenScape Voice. Las plantillas incluyen ejemplos pertinentes.

Descripción de parámetros de las pestañas:

- **Añadir interconexión SIPQ**
- **Editar interconexión SIPQ**
- **Borrar interconexión SIPQ**

Parámetros	Descripción
Plantilla básica	Plantilla (template) que se va a usar como base.
Nombre	Nombre del servidor SIP externo (Nombre plantilla).
Habilitar línea	La conexión con el servidor SIP externo está activa. Valor estándar: desactivado
Identificador de línea en el sistema	Selección entre dos interconexiones SIP-Q externas. Si está presente, una de las dos interconexiones SIPQ siempre está ocupada con la UC Booster Card o el UC Booster Server.
Nombre de dominio remoto	Nombre host o dirección IP del servidor SIP externo. Por norma general, el valor coincide con el valor de **Dirección IP / Nombre de host**.
Servidor SIP	
Dirección IP/nombre de host	Nombre host o dirección IP del servidor SIP externo.
Puerto	Puerto SIP del servidor SIP externo. Rango de valores: 0 o 1024-65535, valor estándar: 5060
Transporte seguro	Si se establece conexión con un OpenScape 4000 o OpenScape Voice, se puede activar la señalización SIP cifrada (Signalling and Payload Encryption feature). Valor estándar: desactivado
Registrador SIP	
Utilizar registrador del proveedor	El servidor SIP externo requiere un registro. Valor estándar: desactivado
Dirección IP/nombre de host	Nombre host o dirección IP del servidor de registrador.
Puerto	Número de puerto del servidor de registrador. Rango de valores: 0 o 1024-65535, valor estándar: 5060

Parámetros	Descripción
Intervalo de nuevo registro (s)	Intervalo (en segundos), en el que se repetirá el registro. Rango de valores: de 30 a 86400, valor estándar: 300
Outbound Proxy/Inbound Proxy	
Utilizar proxy entrante/ saliente del proveedor	Activación del proxy saliente: en algunos escenarios de redundancia (p. ej., con OpenScape Branch Proxy) las señales SIP se tienen que procesar mediante un proxy saliente. Activación del proxy entrante: en algunos escenarios de redundancia (p. ej., con OpenScape Voice) las señales entrantes llegan desde un servidor SIP independiente (proxy entrante). Valores estándar: desactivado
Dirección IP/nombre de host	Nombre host o dirección IP del proxy entrante o saliente.
Puerto	Número de puerto del proxy entrante o saliente. Rango de valores: 0 o 1024-65535

Descripción de parámetros de las pestañas:

- **Añadir extensión de interconexión SIPQ**
- **Editar extensión de interconexión SIPQ**
- **Borrar extensión de interconexión SIPQ**

Parámetros	Descripción
ID de usuario	Entrada del ID del usuario para acceder al servidor SIP.
Nombre de autorización / **Ámbito**	Entrada del nombre de autorización o del ámbito para al acceso al servidor SIP.
Contraseña	Entrada de la contraseña para acceder al servidor SIP.
Confirmar contraseña	Repetición de la contraseña para acceder al servidor SIP.

28.3.6.9 Voice Gateway > Línea de servidor SIP nativo

A continuación, se definen los parámetros para las 10 posibles rutas SIP nativas externas. Cualquier servidor SIP externo se puede conectar a través de estas rutas.

Descripción de parámetros de las pestañas:

- **Añadir línea de servidor SIP nativo**
- **Editar línea de servidor SIP nativo**
- **Eliminar línea de servidor SIP nativo**

Parámetros	Descripción
Plantilla base	Plantilla que debe utilizarse como base.
Nombre del troncal	Nombre del servidor SIP externo (nombre de la plantilla).

Parámetros	Descripción
Habilitar troncal	Se activa la conexión al servidor SIP externo. Valor estándar: desactivado
Identificador de troncal en el sistema	Elección de 10 conexiones SIP nativas externas. Los elementos en gris están ocupados por ITSP ya configurados (máximo de 8 ITSP posibles; en este caso, quedan 2 conexiones SIP nativas).
Nombre de dominio remoto	Nombre de host o dirección IP del servidor SIP externo. El valor suele ser idéntico al valor en **Dirección IP / Nombre de host**. Ejemplo: El **Nombre de dominio remoto** configurado se utiliza en la parte Host de los campos de encabezado De y PAI/PPI (ver a continuación): De: sip: +49...@DomainName P-Asserted-Identity: sip: +49...@DomainName
Protocolo de transporte	Selección del protocolo UDP o TCP.
Seguridad de transporte	Seleccione entre UDP o TCP tradicional y TLS seguro.
Seguridad de medios	Seleccione entre solo RTP, solo SDES y DTLS-SRTP. DTLS-SRTP es un protocolo que combina la seguridad de la capa de transporte de datagramas (DTLS) con el protocolo de transporte seguro en tiempo real (SRTP) para proporcionar transmisión de medios encriptada y autenticada por Internet. **Nota:** En las nuevas implementaciones (V3R4 en adelante), DTLS-SRTP es el valor predeterminado. Para cambiar de solo RT o solo SDES a DTLS-SRTP, es necesario reiniciar el tronco para que surta efecto. **Nota:** Las configuraciones restrictivas del firewall pueden causar problemas de carga de voz esporádicos o permanentes. En ese caso, deshabilite la opción DTLS-SRTP.
Servidor SIP	
Dirección IP/Nombre de host	Nombre de host o dirección IP del servidor SIP externo.
Puerto	Puerto SIP del servidor SIP externo. Valor estándar: 5060, ingrese el puerto 0 si el ITSP usa DNSSRV
Registrador SIP	
Usar registrador	Debe seleccionarse si el troncal funciona con registro (predeterminado = desactivado)
Dirección IP/Nombre de host	Nombre de host o dirección IP del servidor de registro externo

Parámetros	Descripción
Puerto	Puerto del servidor de registro externo valor estándar: 5060, ingrese el puerto 0 si se usa DNSSRV
Intervalo de reinscripción	El intervalo en el que se repite una inscripción (predeterminado = 600)
Servidor STUN	
Usar STUN	Debe seleccionarse si el troncal funciona con STUN (predeterminado = desactivado)
Dirección IP/Nombre de host	Nombre de host o dirección IP del servidor STUN
Puerto	Puerto del servidor STUN
Datos SIP extendidos	
Mostrar datos SIP extendidos	Al habilitar esta bandera, hay algunos parámetros de configuración adicionales disponibles para controlar la pila SIP y adaptar el contenido de los campos de encabezado SIP
CLIP / CLIR	El sistema proporciona varios parámetros para controlar el formato de SIP Campos de encabezado según las necesidades del trunk nativo Se pueden controlar los contenidos de los siguientes campos de encabezado que describen el origen de una llamada: • From: Mostrar parte <sip:UserPart@HostPart • P-Asserted-Identity: Mostrar parte <sip:UserPart@HostPart> • P-Preferred-Identity: Mostrar parte <sip:UserPart@HostPart>
CLIP saliente en el encabezado From - parte de visualización	Posibles configuraciones: • Omit - se omite el campo • Número de llamada - el número configurado para una estación. Puede definir qué número se utiliza en los "parámetros de ruta" • Account - el nombre de usuario asignado al trunk nativo • Mostrar nombre
CLIP saliente en el encabezado From - parte de usuario:	Posibles configuraciones: • Número de llamada • Account
Encabezado From saliente - parte de dominio/host:	Cambie la parte de dominio/host de la URI para que se complete con la dirección IP del sistema. Este parámetro afecta a la parte del host de los tres campos de encabezado From:, PAI y PPI Posibles configuraciones: • nombre de dominio • Dirección IP local • Dirección IP pública
Desvío: Desde contiene el número de la parte que llama original:	Si se establece una llamada saliente debido a un reenvío de llamadas, el sistema puede proporcionar información sobre la parte que llama originalmente. Si se establece en verdadero, el sistema envía la parte que llama originalmente (A-Ext) en el campo de encabezado From:, de lo contrario, envía el número de la estación que reenvía.

Parámetros	Descripción
Desvío: PAI contiene el número de la parte que llama originalmente	Si se establece una llamada saliente debido a un reenvío de llamadas, el sistema puede proporcionar información sobre la parte que llama originalmente. Si se establece en verdadero, el sistema envía la parte que llama originalmente (A-Ext) en el campo de encabezado P-Asserted-Id, de lo contrario, envía el número de la estación que reenvía. Al establecer este indicador, el sistema envía la parte que llama originalmente en el campo de encabezado P-Asserted_ID: y P-Preferred-ID:.
CLIP saliente en el encabezado P-Asserted-Id - parte de visualización:	Posibles configuraciones: • Omit - se omite el campo • Número de llamada - el número configurado para una estación. Puede definir qué número se utiliza en los "parámetros de ruta" • Account - el nombre de usuario asignado al trunk nativo • Mostrar nombre
CLIP saliente en el encabezado P-Asserted-Id - parte del usuario:	Posibles configuraciones: • Omit - se omite el campo • Número de llamada • Account
CLIP saliente en el encabezado P-Preferred-Id - parte para mostrar:	Posibles configuraciones: • Omit - se omite el campo • Número de llamada - el número configurado para una estación. Puede definir qué número se utiliza en los "parámetros de ruta" • Account - el nombre de usuario asignado al trunk nativo • Mostrar nombre
CLIP saliente en el encabezado P-Preferred-Id - parte del usuario:	Posibles configuraciones: • Omit - se omite el campo • Número de llamada • Account
CLIP saliente en el encabezado Diversion - parte para mostrar:	Posibles configuraciones: • Omit - se omite el campo • Número de llamada - el número configurado para una estación. Puede definir qué número se utiliza en los "parámetros de ruta" • Account - el nombre de usuario asignado al trunk nativo • Mostrar nombre
CLIP saliente en el encabezado de desvío - parte del usuario:	Posibles configuraciones: • Omit - se omite el campo • Número de llamada • Account
CLIP saliente en el encabezado History-Info - parte del usuario:	Posibles configuraciones: • omitir • callnumber

Parámetros	Descripción
CLIR saliente en el encabezado From - parte para mostrar:	Posibles configuraciones: • Omitir • Número de llamada • Account • Anónimo <45>From:</45> **Anónimo <sip: ...@...>**
CLIR saliente en el encabezado From - parte del usuario:	Posibles configuraciones: • Número de llamada • Account • Completamente anónimo<47><48>De:</48></47> **...<sip:anonymous@anonymous.invalid>** • Usuario anónimo<49>De:</49> **... <sip:anonymous@...>**
Encabezado de privacidad de salida de CLIR	Posibles configuraciones: • Omitir • Id<51> Privacidad: id</51> • Usuario<52> Privacidad: usuario</52> • Usuario, id<53> Privacidad: usuario;id</53>
COLP/TIP compatible con llamadas salientes:	En ISDN se introdujo la función COLP (Presentación de identificación de línea de conexión). En SIP, esta función a veces se denomina TIP (Presentación de identificación de terminación). RFD3324 (sección 5.) define un mecanismo para transportar la identidad de la parte que acepta (C) en el campo de encabezado P-Asserted-Identity de la respuesta 200 OK: Posibles configuraciones: • COLP compatible • COLP no compatible
Formato de número de llamada	
Llamada entrante - Número de la parte llamada:	Este indicador se refiere a la dirección de destino de una llamada. De manera predeterminada, se toma de la **parte del usuario** del campo de **TO:encabezado**. Posibles configuraciones: • Línea de solicitud **INVITE sip: +498970070@...** • Parte de visualización del encabezado A **Para: +498970070 <sip:+** • Parte de usuario del encabezado A **Para: <sip: +498970070@...** • Parte de visualización del encabezado P-Called-Party-Id **P-Called-Party-ID: +498970070 <sip:..** • Parte de usuario del encabezado P-Called-Party-Id **P-Called-Party-ID: <sip: +498970070@..**

Parámetros	Descripción
Llamada entrante - Número de la parte que llama:	Este indicador hace referencia a la dirección de origen de una llamada. De manera predeterminada, el sistema elimina a la parte que llama de la parte de usuario del encabezado Desde. Posibles configuraciones: • automático • Desde la parte de visualización del encabezado **From: +498970070 <sip:+** • Desde la parte de usuario del encabezado **From: <sip: +498970070@...** • Parte de visualización del encabezado P-Asserted-Id **P-Asserted-ID: +498970070 <sip:..** • Parte de usuario del encabezado P-Asserted-Id **P-Asserted-ID: <sip: +498970070@..** En el modo automático, el sistema busca primero en la parte de usuario de P-Asserted-Identity, si está presente. Si no hay P-Asserted-Identity presente, se toma la parte de usuario del campo de encabezado From:.
El URI de contacto contiene:	Este parámetro se utiliza para configurar el contenido de la parte de usuario del URI de contacto **Contacto: sip:UserPart@HostPart:port** Posibles configuraciones: • Número de llamada: la parte de usuario del URI de contacto contiene el número de llamada • AOR de registro: el URI de contacto contiene la parte de cuenta=usuario del registro.
Puerto TCP utilizado en la URI de contacto:	Este parámetro se utiliza para configurar el puerto TCP utilizado en la parte de host de la URI de contacto **Contacto: sip:UserPart@HostPart:port** Posibles configuraciones: • ephem.src-port: Por defecto se utiliza el puerto TCP de origen efímero • Puerto del servidor SIP: El puerto del servidor SIP se utiliza en la URI de contacto

Descripción de parámetros de las pestañas:

- **Add Native SIP Server Trunk User**
- **Edit Native SIP Server Trunk User**
- **Delete Native SIP Server Trunk User**

Parámetros	Descripción
UserId	Entrada del ID de usuario para el acceso al servidor SIP.
Nombre de autorización	Entrada del nombre de autorización para el acceso al servidor SIP.
Contraseña	Entrada de la contraseña para el acceso al servidor SIP.

Parámetros	Descripción
Confirmar contraseña	Repetición de la contraseña para el acceso al servidor SIP.

28.3.7 Extensiones

En **Extensiones** se reunen las funciones para todas las extensiones. Entre estas funciones se incluyen, por ejemplo, el nombre y número de teléfono del usuario y la programación de teclas.

28.3.7.1 Extensiones > Extensiones > Extensiones UP0

Descripción de parámetros de las pestañas:

- **Modificar extensión**

Parámetros	Descripción
N° llam.	Número de teléfono interno de la extensión.
Marcación directa	Número de marcación directa de la extensión.
Nombre	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Apellido	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Mostrar	Nombre de la extensión (libre). De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización. Rango de valores: máx. 16 caracteres
Nombre	Nombre de la extensión (libre). Rango de valores: máx. 16 caracteres
Clip/Lin	Cadena numérica que ve el usuario llamado al hacerse una llamada saliente externa. Esta cadena aparece en lugar del número de teléfono real (p. ej. para el servicio de emergencia E911 EE. UU.) Rango de valores: máx. 16 cifras
Activo	Indica si la extensión está operativa.
Tipo disposit.	Indicación del terminal asignado a la extensión.
Número de teléfono de fax	Si hay configurado un buzón de voz (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que indicar aquí el número de fax con el que la extensión puede recibir mensajes de fax de forma interna.

Parámetros	Descripción
N° llam. marc. directa de fax	Si hay configurado un buzón de fax (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que introducir aquí el número de teléfono de fax con el que la extensión puede recibir mensajes de fax de forma externa.
Acceso	Indicación de la interfaz física con la que está conectado el terminal.
ID de ubicación ITSP	El ID de ubicación ITSP de una extensión.
Buscar	También puede mostrar selección extens. Introduzca término búsqueda en campos **búsqueda** y confirme la entrada con Intro. Se muestran las extensiones que se corresponden con el concepto de búsqueda. Si todos los campos de **búsqueda** están vacíos y se pulsa la tecla Intro, aparece de nuevo una lista de todas las extensiones.
Elementos por página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
Flecha azul en la columna **N° llam.**	Abre la página con las pestañas **Editar parámetros exten.**, **Editar flags exten.**, **Editar datos cliente workpoint** y **Editar grupos/RWS**.
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

Descripción de parámetros de las pestañas:

- **UP0 Master/Slave**

  Esta pestaña solo existe con OpenScape Business X8, ya que en este sistema los puertos esclavos se administran dinámicamente. En OpenScape Business X1/X3/X5 los puertos esclavos tienen una asignación fija.

Parámetros	Descripción
N° llam.	Número de teléfono interno de la extensión.
Marcación directa	Número de marcación directa de la extensión.
Nombre	Nombre de la extensión (libre). Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Acceso	Indicación de la interfaz física con la que está conectado el terminal.
Añadir zona esclava	Si esta casilla de verificación está activada, al puesto maestro seleccionado se le asigna un puerto esclavo. Después de guardar la selección con **Aplicar**, se puede configurar el número de teléfono, el número de marcación directa y el nombre del teléfono del sistema esclavo. Si a continuación se conecta el teléfono del sistema esclavo con el adaptador esclavo del teléfono del sistema maestro, se asigna al puerto esclavo seleccionado previamente. Si el teléfono del sistema esclavo se conecta sin tener un puerto esclavo predefinido, se ocupa automáticamente el siguiente puerto libre (a partir del puerto 384).

Parámetros	Descripción
Borrar zona esclava	Si esta casilla de verificación está activada, se borra la configuración previa del teléfono del sistema esclavo. Si hay un teléfono del sistema esclavo conectado con el adaptador esclavo del teléfono del sistema maestro, la casilla de verificación está en gris. La configuración previa no se puede borrar.
Buscar	También puede mostrar selección extens. Introduzca término búsqueda en campos **búsqueda** y confirme la entrada con Intro. Se muestran las extensiones que se corresponden con el concepto de búsqueda. Si todos los campos de **búsqueda** están vacíos y se pulsa la tecla Intro, aparece de nuevo una lista de todas las extensiones.
Elementos por página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

Descripción de parámetros de las pestañas:

- **Información de dispositivo**

Parámetros	Descripción
N° llam.	Número de teléfono interno de la extensión.
Nombre	Nombre de extensión.
Tipo disposit.	Indicación del terminal asignado a la extensión.
Versión de software actual	Versión de software del terminal asignado (si está disponible).
Versión de hardware	Versión de hardware del terminal asignado (si está disponible).
Elementos por página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

28.3.7.2 Estación > Estación > Clientes IP

Descripción de parámetros de las pestañas:

- **Editar suscriptor**

Parámetros	Descripción
Número que llama	Número de teléfono interno de la extensión.
DID	Número de marcación directa de la extensión.
Primer nombre	Primer nombre de libre elección para la estación. Rango de valores: máx. 32 caracteres.
Apellidos	Apellidos de la extensión (libre). Rango de valores: máx. 32 caracteres.
Mostrar	Nombre de libre elección para la estación. De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Tipo	Tipo de la extensión.
Tipo: **Sin puerto**	Esta señal de llamada aún no está asignada a ninguna estación.
Tipo: **Cliente del sistema**	Un cliente del sistema es una estación IP que puede utilizar todas las funciones del sistema de comunicación a través de CorNet-IP (anteriormente llamado cliente del sistema HFA)
Tipo: **RAS User**	Un usuario RAS (usuario del Servicio de Acceso Remoto) obtiene acceso a Internet a través de la conexión ISDN. Esto permite que el sistema de comunicación pueda ser mantenido y licenciado de forma remota.
Tipo: **SIP Client**	Un cliente SIP es una estación IP que utiliza el protocolo SIP. Solo puede acceder a funcionalidades limitadas del sistema de comunicación a través de SIP.
Tipo: **Usuario de Deskshare**	Un usuario de Deskshare es un usuario IP que puede iniciar sesión en un teléfono de otro sistema IP (inicio de sesión móvil) y luego usar este teléfono como si fuera suyo propio (incluido el número de llamada).
Clip/Lin	Cadena numérica que ve el usuario llamado al hacerse una llamada saliente externa. Esta cadena aparece en lugar del número de teléfono real (p. ej. para el servicio de emergencia E911 EE. UU.)
Activo	Indica si la estación está operativa.
Número de llamada de fax.	Si hay configurado un buzón de voz (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que indicar aquí el número de fax con el que la extensión puede recibir mensajes de fax de forma interna.
Fax DID	Si hay configurado un buzón de fax (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que introducir aquí el número de teléfono de fax con el que la extensión puede recibir mensajes de fax de forma externa.
ID de ubicación del ITSP	El ID de ubicación ITSP de una estación.

Parámetros	Descripción
Buscar	También puede visualizar suscriptores seleccionados introduciendo un término de búsqueda en los campos de **búsqueda** y pulsando la tecla Enter. Se muestran los suscriptores que coinciden con el término de búsqueda. Si deja todos los campos de **búsqueda** vacíos y pulsa la tecla Enter, se volverá a mostrar la lista de todos los suscriptores.
Elementos por página	Selección para determinar si se mostrarán 10, 25, 50 o 100 elementos por página.
Botones	
Flecha azul en la columna **Número que llama**	Abre la página con las pestañas **Editar parámetros de estación**, **Editar indicadores de estación**, **Editar datos del cliente del punto de trabajo** y **Editar grupo/CFW**.
>	Avanza una página.
<	Retrocede una página.
>|	Se desplaza al final de la lista.
|<	Se desplaza al principio de la lista.

Descripción de parámetros de las pestañas:

- **Información del dispositivo**

Tenga en cuenta que la implementación de la ordenación es estrictamente alfabética para todas las columnas. No existe una ordenación numérica específica por columna para tipos de datos específicos como la dirección IP **.** o **Versión actual del software**.

Parámetros	Descripción
Número que llama	Número de teléfono interno de la extensión.
Mostrar	Nombre de extensión.
Tipo disposit.	Muestra el tipo de dispositivo asociado a la estación.
Dirección IP	Dirección IP del dispositivo asociado; enlace directo al WBM del teléfono IP
Dirección MAC	Dirección MAC del teléfono asociado
Versión actual del software	Versión de software del dispositivo asociado (si está disponible).
Versión de hardware	Versión de hardware del dispositivo asociado (si está disponible).
Puerto PC	Si este marcador está activado, se conecta el puerto PC Ethernet de todos los teléfonos del sistema activos. Estándar: desactivado

Parámetros	Descripción
Configuración del códec	Si este marcador está activado, se aplica la siguiente priorización de códec a todos los teléfonos del sistema: G.729 - G.711 - G.722 Si este marcador está desactivado, se aplica la siguiente priorización de códec: G.722 - G.711 - G.729 **Nota:** CP100 no soporta G.722 Estándar: desactivado
Elementos por página	Selección para determinar si se mostrarán 10, 25, 50 o 100 elementos por página.
Botones	
>	Avanza una página.
<	Retrocede una página.
>|	Se desplaza al final de la lista.
|<	Se desplaza al principio de la lista.

Descripción de parámetros de las pestañas:

- **Gateway secundario**

Parámetros	Descripción
Número de llamada	Número de teléfono interno de la extensión.
Nombre	Nombre de extensión.
ID de nodo	A cada nodo de un sistema en red se le debe asignar un ID de nodo único. Esto permite identificar de forma unívoca los nodos individuales de un sistema en red.
Telefonía de respaldo	Indica si la función está activada.
Número de llamada de respaldo	El número de llamada de la estación que se utilizará en caso de fallo.
Número de llamada de respaldo sin DID	El número de llamada interno de la estación que se utilizará en caso de fallo.

Descripción de parámetros de las pestañas:

- **Alojamiento de respaldo**

Parámetros	Descripción
Número de llamada	Número de teléfono interno de la extensión.
Nombre	Nombre de extensión.
ID de nodo primario	El ID de nodo único con el que se configuró originalmente la estación.

Parámetros	Descripción
Número de llamada de respaldo	El número de llamada de la estación que se utilizará en caso de fallo.
Número de llamada de respaldo sin DID	El número de llamada interno de la estación que se utilizará en caso de un evento de fallo

28.3.7.3 Extensión > Extensión > Extensiones analógicas

Descripción de parámetros de las pestañas:

- **Modificar extensión**

Parámetros	Descripción
N° llam.	Número de teléfono interno de la extensión. **Nota:** Los números de llamada que comienzan por asterisco (*) no son válidos como destinos de fax.
Marcación directa	Número de marcación directa de la extensión.
Nombre	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Apellidos	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Mostrar	Nombre de la extensión (libre). De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Clip/Lin	Cadena numérica que ve el usuario llamado al hacerse una llamada saliente externa. Esta cadena aparece en lugar del número de teléfono real (p. ej. para el servicio de emergencia E911 EE. UU.) Rango de valores: máx. 16 cifras
Activo	Indica si la extensión está operativa.
Tipo disposit.	Indicación del terminal asignado a la extensión.
Número de teléfono de fax	Si hay configurado un buzón de voz (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que indicar aquí el número de fax con el que la extensión puede recibir mensajes de fax de forma interna.
N° llam. marc. directa de fax	Si hay configurado un buzón de fax (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que introducir aquí el número de teléfono de fax con el que la extensión puede recibir mensajes de fax de forma externa.
Acceso	Indicación de la interfaz física con la que está conectado el terminal.

Parámetros	Descripción
ID de ubicación ITSP	El ID de ubicación ITSP de una extensión.
Buscar	También puede mostrar selección extens. Introduzca término búsqueda en campos **búsqueda** y confirme la entrada con Intro. Se muestran las extensiones que se corresponden con el concepto de búsqueda. Si todos los campos de **búsqueda** están vacíos y se pulsa la tecla Intro, aparece de nuevo una lista de todas las extensiones.
Elementos por página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
Flecha azul en la columna **N° llam.**	Abre la página con las pestañas **Editar parámetros exten.**, **Editar flags exten.**, **Editar datos cliente workpoint** y **Editar grupos/RWS**.
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

28.3.7.4 Extensión > Extensión > Extensiones RDSI

Descripción de parámetros de las pestañas:

- **Modificar extensión**

Parámetros	Descripción
N° llam.	Número de teléfono interno de la extensión.
Marcación directa	Número de marcación directa de la extensión.
Nombre	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Apellidos	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Mostrar	Nombre de la extensión (libre). De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Clip/Lin	Cadena numérica que ve el usuario llamado al hacerse una llamada saliente externa. Esta cadena aparece en lugar del número de teléfono real (p. ej. para el servicio de emergencia E911 EE. UU.) Rango de valores: máx. 16 cifras
Activo	Indica si la extensión está operativa.
Tipo disposit.	Indicación del terminal asignado a la extensión.

Parámetros	Descripción
Número de teléfono de fax	Si hay configurado un buzón de voz (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que indicar aquí el número de fax con el que la extensión puede recibir mensajes de fax de forma interna.
N° llam. marc. directa de fax	Si hay configurado un buzón de fax (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que introducir aquí el número de teléfono de fax con el que la extensión puede recibir mensajes de fax de forma externa.
Acceso	Indicación de la interfaz física con la que está conectado el terminal.
ID de ubicación ITSP	El ID de ubicación ITSP de una extensión.
Buscar	También puede mostrar selección extens. Introduzca término búsqueda en campos **búsqueda** y confirme la entrada con Intro. Se muestran las extensiones que se corresponden con el concepto de búsqueda. Si todos los campos de **búsqueda** están vacíos y se pulsa la tecla Intro, aparece de nuevo una lista de todas las extensiones.
Elementos por página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
Flecha azul en la columna **N° llam.**	Abre la página con las pestañas **Editar parámetros exten.**, **Editar flags exten.**, **Editar datos cliente workpoint** y **Editar grupos/RWS**.
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

28.3.7.5 Extensión > Extensión > Extensiones DECT > SLC Número de llamada

Descripción de parámetros de las pestañas:

- **Modificar extensión**

Parámetros	Descripción
N° llam.	Número de teléfono interno de la extensión.
Marcación directa	Número de marcación directa de la extensión.
Nombre	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Apellidos	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Mostrar	Nombre de la extensión (libre). De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales

Parámetros	Descripción
Clip/Lin	Cadena numérica que ve el usuario llamado al hacerse una llamada saliente externa. Esta cadena aparece en lugar del número de teléfono real (p. ej. para el servicio de emergencia E911 EE. UU.) Rango de valores: máx. 16 cifras
Activo	Indica si la extensión está operativa.
Tipo disposit.	Indicación del terminal asignado a la extensión. Las extensiones base se muestran como extensiones S0.
Acceso	Indicación de la interfaz física con la que está conectado el terminal.
ID de ubicación ITSP	El ID de ubicación ITSP de una extensión.
Parámetros	Vista estándar de todas las extensiones, no cambiar la configuración
Buscar	También puede mostrar selección extens. Introduzca término búsqueda en campos **búsqueda** y confirme la entrada con Intro. Se muestran las extensiones que se corresponden con el concepto de búsqueda. Si todos los campos de **búsqueda** están vacíos y se pulsa la tecla Intro, aparece de nuevo una lista de todas las extensiones.
Elementos por página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
Flecha azul en la columna **N° llam.**	Abre la página con las pestañas **Editar parámetros exten.**, **Editar flags exten.**, **Editar datos cliente workpoint** y **Editar grupos/RWS**.
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

28.3.7.6 Extensiones > Extensiones > Extensiones DECT > Extensiones DECT

Descripción de parámetros de las pestañas:

- **Modificar extensión**

Parámetros	Descripción
N° llam.	Número de teléfono interno de la extensión.
Marcación directa	Número de marcación directa de la extensión.
Nombre	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Apellidos	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.

Parámetros	Descripción
Mostrar	Nombre de la extensión (libre). De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Clip/Lin	Cadena numérica que ve el usuario llamado al hacerse una llamada saliente externa. Esta cadena aparece en lugar del número de teléfono real (p. ej. para el servicio de emergencia E911 EE. UU.) Rango de valores: máx. 16 cifras
Activo	Indica si la extensión está operativa.
Tipo disposit.	Indicación del terminal asignado a la extensión. Las extensiones DECT se muestran como Comfort-PP.
Número de teléfono de fax	Si hay configurado un buzón de voz (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que indicar aquí el número de fax con el que la extensión puede recibir mensajes de fax de forma interna.
N° llam. marc. directa de fax	Si hay configurado un buzón de fax (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que introducir aquí el número de teléfono de fax con el que la extensión puede recibir mensajes de fax de forma externa.
Acceso	Indicación de la interfaz física con la que está conectado el terminal.
ID de ubicación ITSP	El ID de ubicación ITSP de una extensión.
Buscar	También puede mostrar selección extens. Introduzca término búsqueda en campos **búsqueda** y confirme la entrada con Intro. Se muestran las extensiones que se corresponden con el concepto de búsqueda. Si todos los campos de **búsqueda** están vacíos y se pulsa la tecla Intro, aparece de nuevo una lista de todas las extensiones.
Elementos por página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
Flecha azul en la columna **N° llam.**	Abre la página con las pestañas **Editar parámetros exten.**, **Editar flags exten.**, **Editar datos cliente workpoint** y **Editar grupos/RWS**.
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

28.3.7.7 Extensión > Extensión > Puertos IVM/EVM > EVM

Descripción de parámetros de las pestañas:

- **Modificar extensión**

Parámetros	Descripción
N° llam.	Número interno del puerto del buzón de voz.
Marcación directa	Número de marcación directa del puerto del buzón de voz, si lo hay.
Nombre	Nombre libre del puerto del buzón de voz. Rango de valores: máx. 32 caracteres.
Apellidos	Apellidos libres del puerto del buzón de voz. Rango de valores: máx. 32 caracteres.
Mostrar	Nombre libre del puerto del buzón de voz. De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Clip/Lin	Cadena numérica que ve el usuario llamado al hacerse una llamada saliente externa. Esta cadena aparece en lugar del número de teléfono real (p. ej. para el servicio de emergencia E911 EE. UU).
Activo	Indica si el puerto del buzón de voz está operativo.
Tipo disposit.	Para EVM se muestran extensiones S0.
Acceso	Indicación del puerto interno para el buzón de voz.
ID de ubicación ITSP	El ID de ubicación ITSP de una extensión.
Tipo de extensión	Para EVM hay que seleccionar "Phonemail", para el Company AutoAttendant hay que establecer "Estándar".
Parámetros	Vista estándar de todos los puertos del buzón de voz; no modifique los ajustes (por ejemplo, "Idioma" no es el idioma de los anuncios grabados del buzón de voz).
Buscar	Para mostrar una selección de puertos del buzón de voz, introduzca el término de búsqueda en los campos de **búsqueda** y confirme la acción con la tecla Intro. Aparecen los puertos del buzón de voz que se correspondan con el término de búsqueda. Si todos los campos de **búsqueda** están vacíos y se pulsa la tecla Intro, aparece de nuevo una lista con todos los puertos del buzón de voz.
Elementos por página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
Flecha azul en la columna **N° llam.**	Abre la página con las pestañas **Editar parámetros exten.**, **Editar flags exten.**, **Editar datos cliente workpoint** y **Editar grupos/RWS**.
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

28.3.7.8 Extensiones > Extensiones > Extensiones virtuales

Descripción de parámetros de las pestañas:

- **Modificar extensión**

Parámetros	Descripción
N° llam.	Número interno de la extensión virtual.
Marcación directa	Número de marcación directa de la extensión virtual.
Nombre	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Apellidos	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Mostrar	Nombre de la extensión (libre). De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Tipo	Extensión libre o virtual (en Mobility Entry, indicación fija)
Clip/Lin	Cadena numérica que ve el usuario llamado al hacerse una llamada saliente externa. Esta cadena aparece en lugar del número de teléfono real (p. ej. para el servicio de emergencia E911 EE. UU.)
Activo	Indica si la extensión virtual está operativa.
ID de ubicación ITSP	El ID de ubicación ITSP de una extensión.
Buscar	También puede mostrar selección extens. Introduzca término búsqueda en campos **búsqueda** y confirme la entrada con Intro. Se muestran las extensiones que se corresponden con el concepto de búsqueda. Si todos los campos de **búsqueda** están vacíos y se pulsa la tecla Intro, aparece de nuevo una lista de todas las extensiones.
Elementos por página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
Flecha azul en la columna **N° llam.**	Abre la página con las pestañas **Editar parámetros exten.**, **Editar flags exten.**, **Editar datos cliente workpoint** y **Editar grupos/RWS**.
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

28.3.7.9 Extensión > Extensión > Parámetros de extensión

Descripción de parámetros de las pestañas:

- **Editar parámetros exten.**

Parámetros	Descripción
Extensiones - ...	
Tipo	Tipo de la extensión.
Número de llamada	Número de teléfono interno de la extensión.
Primer nombre	Primer nombre de libre elección para la estación. Rango de valores: máx. 32 caracteres.
Apellidos	Apellidos de la extensión (libre). Rango de valores: máx. 32 caracteres.
Mostrar	Nombre de libre elección para la estación. De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Marcación directa	Número de marcación directa de la extensión.
Tipo disposit.	Indicación del terminal asignado a la extensión.
Clip/Lin	Cadena numérica que ve el usuario llamado al hacerse una llamada saliente externa. Esta cadena aparece en lugar del número de teléfono real (p. ej. para el servicio de emergencia E911 EE. UU.) Rango de valores: máx. 16 cifras
Acceso	Indicación de la interfaz física con la que está conectado el terminal.
Aprovisionamiento de dispositivos	Este menú solo es visible para las estaciones SIP y están disponibles los siguientes valores: • **Estándar** (valor predeterminado) • **Dispositivo DECT SIP de Mitel** (El dispositivo SIP específico se utiliza para Mitel SIP DECT). **Nota: Dispositivo DECT SIP de Mitel** Esta opción solo es compatible con hardware V3 y sistemas OSBiz S.
Configuración SIP DECT de Mitel: Este menú solo se vuelve visible cuando se selecciona **Dispositivo SIP DECT de Mitel** en **Aprovisionamiento de dispositivos**.	
PIN	El código PIN del dispositivo.
Bloqueo de teclas habilitado	Habilitar (Sí) o deshabilitar (No) el bloqueo de teclas del dispositivo.
PIN de bloqueo de teclas	El PIN para el bloqueo de las teclas.
Tiempo de bloqueo de teclas	El tiempo que tarda el bloqueo de teclas en surtir efecto.
Mostrar directorio personal	Elija si el directorio personal será visible (Sí) o no (No).
Fax	

Parámetros	Descripción
Número de llamada	Si hay configurado un buzón de voz (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que indicar aquí el número de fax con el que la extensión puede recibir mensajes de fax de forma interna.
Marcación directa	Si hay configurado un buzón de fax (p. ej. con los clientes de UC myPortal for Desktop o myPortal for Outlook), hay que introducir aquí el número de teléfono de fax con el que la extensión puede recibir mensajes de fax de forma externa.
Movilidad	
Tipo	Tipo de la extensión: • Extensión Mobility • Extensión virtual • Extensión SfB • Estación externa de confianza: tipo de estación virtual que se utilizará para crear un usuario externo de confianza
Número de llamada de estación externa móvil/Sfb/ de confianza	Solo para clientes SIP y extensiones móviles: con el servicio de número único, este número de teléfono sirve para autenticar el acceso DISA por telefonía móvil. Introduzca aquí el número de telefonía móvil de la extensión, con el código de acceso urbano (p. ej., 0017312345678). **Nota:** El campo **Número de llamada de estación externa de confianza** es obligatorio. Si procede a aplicar la configuración con el campo **Número de llamada de estación externa confiable** vacío, aparecerá una alerta informándole que "*¡El número de llamada de estación externa confiable no debe estar vacío!*". Además, después de hacer clic en **Aceptar** en la primera alerta, aparecerá una segunda que le informará que "*La entrada no se pudo manejar, verifíquela*".
Web Feature ID	Web Feature ID determina cómo iniciarán sesión las extensiones en el cliente web móvil (nombre de usuario. Se puede seleccionar entre "Ninguno" (solo Mobility Entry) o "Automático" (número de teléfono interno de la extensión); o bien, se puede seleccionar entre el número del cliente o el teléfono de la lista desplegable.
Parámetros	
Tipo de extensión	Tipo del terminal conectado (lista desplegable)
Tipo de extensión: **Estándar**	Teléfonos del sistema o teléfonos analógicos
Tipo de extensión: **Fax**	Equipo de fax, por ejemplo, no se admite la intercalación
Tipo de extensión: **Altavoz**	Para un sistema de avisos por puerto a/b

Parámetros	Descripción
Tipo de extensión: **Contestador automático**	Solo con analógicos: si en esta interfaz hay conectado un contestador automático, con este ajuste se puede aceptar una llamada del contestador desde cualquier terminal, aunque el contestador ya haya respondido a la llamada. Para ello, hay que programar en el terminal una tecla con el número de teléfono interno de la extensión analógica. Este campo se debe seleccionar, además de en el caso de contestador automático, cuando se trata de puertos virtuales en los que no se ha configurado hardware. De esta forma, se evita que el sistema de comunicación tenga que verificar si el puerto en cuestión se encuentra activo. Solo para puertos virtuales: si en el Manager E se ha configurado una extensión sin Acceso como tipo de Contestador automático, el puerto también debe configurarse como puerto virtual. Por lo demás, no aparece en la Gestión basada en Web (WBM) como extensión.
Tipo de extensión: **Ext. AB LED MW**	Para teléfonos analógicos (NoFe = teléfono normal) con LED de mensaje en espera No para EE.UU.
Tipo de extensión: **Extensión con bucle de impulso**	Si se utiliza un terminal con bucle de impulso con función abrepuertas
Tipo de extensión: **Módem**	Este ajuste no permite intercalación Se ha previsto para módems.
	Cuando se borra una extensión de fax o módem (se borran el número de llamada y el número de marcación directa), el tipo de extensión también se tiene que ajustar de nuevo al valor predeterminado.
Idioma	Idioma para el control de menús del terminal (teléfono del sistema).
Señalización de llamadas internas	Aquí se puede asignar a cada extensión una de las ocho señalizaciones de llamadas internas. De manera que se puede asignar además del tono de llamada externa un tono de llamada interna, que sonará cuando haya una llamada interna. Valor estándar: Tipo. llam. 1
Señalización de llamadas externas	Aquí se pueden seleccionar distintos tipos de llamada que señalizan una llamada externa: – Teléfonos del sistema: tipo de llamada 1 = llamada externa (por ejemplo, llamada doble), tipo de llamada 2 = llamada externa, línea urbana 2 (por ejemplo, llamada triple), tipo de llamada 3 = llamada externa, línea urbana 3 (por ejemplo, corta/larga/corta) – Terminales analógicos, Alemania: tipo de llamada 1 = llamada externa, tipo de llamada 2 = llamada recordatoria, tipo de llamada 3 = timbre de puerta – Terminales analógicos, otros países: tipo de llamada 1 = llamada externa, tipo de llamada 2 = llamada externa, tipo de llamada 3 = llamada externa Valor estándar: Tipo. llam. 1

Parámetros	Descripción
Clase de servicio (LCR)	Un usuario solo puede ocupar una ruta si su clase de servicio es igual o superior a la clase de servicio LCR de la tabla de rutas, es decir, un usuario con la clase de servicio 7 no puede ocupar una ruta con clase de servicio 8. De forma predeterminada, todas las extensiones tienen registrada la autorización LCR máxima (15). Valor estándar: 15
Modo hot-line	Selección de las opciones de hot-line
Modo hot-line: **desactivado**	Función hot-line desactivada.
Modo hot-line: **Llamada de socorro**	La llamada al hot-line se hace al cabo de un tiempo de espera predefinido (tiempo de llamada de socorro), véase Telefonía/Ajustes básicos/teléfono/Interceptación/PO/Hot-line
Modo hot-line Hot-line	La función hot-line está activada. Al descolgar el auricular se establece conexión inmediatamente con el destino de hot-line, véase Telefonía/Ajustes básicos/teléfono/Interceptación/PO/Hot-line
Hot-line	Selección de los destinos de hot-line, véase Telefonía/Ajustes básicos/teléfono/Interceptación/PO/Hot-line
Línea directa: **ninguno**	Sin destino definido
Hot-line: **Cifras 1 a 6**	Destinos de hot-line, véase Telefonía/Ajustes básicos/teléfono/Interceptación/PO/Hot-line
Seguridad de Payload (para clientes del sistema IP)	Active o desactive el cifrado de llamadas telefónicas (SPE). Para ello, todas las extensiones pertinentes deben haber activado SPE. Valor estándar: activado
Seguridad de Payload (para teléfonos TDM/analógicos)	Indica si el punto terminal concreto está protegido o no desde el punto de vista de la infraestructura, puesto que la seguridad de payload solo funciona con teléfonos IP. Si este parámetro se define en activado y el flag del sistema Soporte SPE está activado, se muestra si está cifrada o no la ruta de conexión entre esta extensión y una extensión IP. Si el parámetro está desactivado, no se muestra información. Valor estándar: Desact.
Protocolo MWI	Selección del protocolo MWI para extensiones analógicas. Solo disponible para SLMAVx (OpenScape Business X8), 4SLAV onboard y SLAVx OpenScape Business X3,X5.
Protocolo MWI: Comtel3	El protocolo Comtel 3 está seleccionado. Valor estándar.
Protocolo MWI: Alta tensión	El protocolo de Alta tensión está seleccionado. Solo disponible para SLMAVx (OpenScape Business X8).
Botones	
>	Pasa a la siguiente extensión. Si las extensiones que coinciden con el término de búsqueda introducido en los campos **Buscar** se han filtrado antes, solo es posible moverse entre esas extensiones concretas.
<	Retrocede una extensión.

Descripción de parámetros de las pestañas:

- **Editar flags exten.**

Parámetros	Descripción
Extensiones - ...	
Tipo	Tipo de la extensión.
Número de llamada	Número de teléfono interno de la extensión.
Nombre	Nombre de extensión.
Flags de extensión	
Permiso intercal. act.	Si el flag está activado, la extensión puede intercalarse en la conexión existente de una extensión interna. Las extensiones afectadas reciben una notificación de la intercalación mediante un tono de aviso y un mensaje en pantalla. Valor estándar: Desactivado
Romper No molestar	Si el flag está activado: si la extensión da con una extensión interna con el estado No molestar activo, puede interrumpir dicho estado. Transcurridos cinco segundos la extensión llamada recibe indicación de la llamada. Si el flag está desactivado, no se puede interrumpir No molestar. Si la extensión da con una extensión interna con el estado No molestar activo, recibe un tono de ocupado. Valor estándar: Desactivado
AUL externo permitido	Si el flag está activado, la extensión puede activar un desvío de llamadas a un destino externo. Las tasas resultantes de la realización de un desvío de llamadas externo se asignan a la extensión que ha activado dicho desvío. Valor estándar: Activado
Bloqueo mens. directo desact.	Si el flag está activado, la extensión puede ser contactada directamente. De esta forma se permite un establecimiento de conexión interno sin que el usuario tenga que descolgar el auricular. El altavoz de la extensión se activa automáticamente. Valor estándar: Activado
Autorización DISA	Si el flag está activado, la extensión puede activar o desactivar funciones del sistema de comunicación y establecer llamadas externas saliente mediante DISA (Direct Inward System Access), como una extensión interna. Se incluye, por ejemplo, la activación y desactivación de desvíos de llamadas del modo No molestar y del código de candado telefónico. Valor estándar: Desactivado
Activar tránsito al colgar	Si el flag está activado, la extensión puede transferir una llamada externa a otra extensión externa al colgar. Ejemplo: La extensión es el controlador de conferencia y cuelga: si otras extensiones internas permanecen en la conferencia, la extensión interna que lleva más tiempo en la conferencia se convierte automáticamente en el controlador de conferencia. Si solo permanecen en la conferencia extensiones externas, la conferencia finaliza y se interrumpen todas las conexiones. Valor estándar: Desactivado

Parámetros	Descripción
Reponer candado	Si el flag está activado, la extensión puede restablecer el candado telefónico individual de otra extensión interna al código estándar. Valor estándar: Desactivado
CLIP entrante para analóg. (solo para extensiones analógicas)	Si el flag está activado, en el display del teléfono de la extensión analógica se muestra el número de teléfono del llamante. Para ello es necesario que el teléfono analógico de la extensión admita CLIP (Calling Line Identification Presentation o Indicación del número llamante en la extensión llamada). Valor estándar: Activado
Acceso para identif. llam. malic.	Si el flag está activado, la extensión puede identificar las llamadas externas no deseadas mediante la línea urbana RDSI. Para ello es necesario que se haya solicitado al proveedor de red la habilitación de la prestación "Identif." (MCID, "Malicious Call Identification" o Identificación de llamadas maliciosas) y que se haya hecho así. Después de que el proveedor de red habilite la prestación "Identif." hay que tener en cuenta lo siguiente: con cada conexión entrante de la línea urbana RDSI, después de colgar el auricular la activación de la conexión con la extensión llamada se retarda durante un tiempo a fin de que dicha extensión pueda activar la prestación "Identif.". De esta forma se reduce la disponibilidad de las líneas urbanas RDSI. Valor estándar: Desactivado
Registro del listín telefónico	Si el marcador está activado, se muestran el nombre y el número de teléfono de la extensión en el listín del sistema (incluido ODS). Valor estándar: Activado
Editar marcación	Si el flag está activado, la extensión puede modificar (editar) los dígitos del número de teléfono introducidos mediante el teclado de marcación antes de la emisión de la marcación. Para ello es necesario un teléfono de sistema con pantalla. Valor estándar: Desactivado
Sin conexión de timbre en caso ocuapdo	Si este flag está activado: el estado de la extensión con conexión de timbre adicional determina si se realizará esta conexión. La extensión está libre: se llama inmediatamente a todas las extensiones conectadas. Se puede hacer un aviso de llamada en espera en la extensión con conexión de timbre: se llama a todas las extensiones conectadas tras 5 segundos. No se puede llamar ni hacer un aviso de llamada en espera en la extensión con conexión de timbre: no se realiza ninguna conexión de timbre adicional. Valor estándar: Desactivado
Marcación asociada / servicios	Marcación asociada: Si el flag está activado, la extensión puede marcar un número de teléfono para otra extensión interna, como si la estuviera marcando esta. Servicios asociados: si el flag está activado, la extensión puede controlar prestaciones para otra extensión interna, como si lo estuviera haciendo esta. Se incluye, por ejemplo, la activación y desactivación de desvíos de llamadas, de timbres adicionales y de candados telefónicos. Valor estándar: Desactivado

Parámetros	Descripción
Call waiting rejection on	Si el flag está activado, cuando el usuario está en conversación, no recibe ninguna notificación sobre otras llamadas entrantes mediante tonos de aviso de llamada o mensajes en pantalla. Valor estándar: Activado
Mensaje discreto	Si el flag está activado, la extensión puede unirse a la conexión existente de una extensión interna. Puede escuchar la conversación sin ser advertido y hablar con la extensión interna sin que lo escuche el otro interlocutor. Para ello es necesario que se trate de una conexión entre dos partes. En las llamadas de consulta o conferencias no se puede realizar este tipo de mensaje directo que solo puede ser escuchado por uno de los participantes. Valor estándar: Desactivado
Protección mensaje discreto	Si el flag está activado, la extensión no puede ser contactada directamente. Valor estándar: Desactivado
Activación de función basada en DTMF	Solo relevante para extensiones Mobility Entry: para poder activar prestaciones durante una llamada hay que activar este flag. (Code Receiver sigue activo; atención: recursos limitados). Valor estándar: Desactivado
Casco telefónico	Si el flag está activado, se puede equipar la extensión con un casco telefónico conectado a la toma del microteléfono. Con este flag se pueden aceptar llamadas al pulsar una tecla del casco telefónico con el teléfono del sistema, sin tener que descolgar el microteléfono. El sistema de comunicación reconoce de forma automática el empleo de un casco telefónico en la conexión para cascos de un teléfono del sistema, por lo que no es necesaria una autorización de la clase de servicio. Si está activado este flag, no se pueden liberar llamadas pulsando la tecla de altavoz; se debe programar una tecla de corte para ello. Valor estándar: Desactivado
Último buzón de destino activo	Si este flag está activado y no se puede localizar a la persona llamada, la llamada se desvía al buzón de voz del suplente y el número de llamada del llamante se visualiza en el display del terminal del suplente. Valor estándar: Desactivado

Parámetros	Descripción
Llam. esp. inmed. internas/ prio.	Si el flag (Prioridad de llamada/Aviso llamada en espera tono de libre inmediato) está activado, se señalizan en el terminal del interlocutor las llamadas de esta extensión como prioritarias. Esta prioridad se establece de inmediato con la prioridad de las llamadas externas. Por tanto, las llamadas con prioridad se anteponen a las llamadas internas existentes, pero no a las llamadas existentes externas. Debe tenerse en cuenta que las llamadas nuevas existentes (no en caso de llamadas en espera) por norma general no se posponen, independientemente del tipo de llamada. Si, en caso de una llamada interna, también se desea activar la respectiva prioridad en otro nodo, para la correspondiente línea se tiene que activar además el flag de línea "Llam. esp. inmed. internas/prio" (Área: Flags de Circuit, Prioridad de llamada/Aviso llamada en espera tono de libre inmediato). Si este flag está activado, durante una llamada en espera el llamante escucha inmediatamente un tono de libre en vez del tono de ocupado. Este no influye en la señalización acústica. Las llamadas con prioridad se siguen señalando como una llamada interna. Esta prestación es importante, p.ej., para conexiones Phonemail. Valor estándar: Desactivado
Grabación de voz	Si el flag está activado, la extensión puede activar la grabación de voz durante una llamada. Además, a través de Flags, se puede utilizar el interruptor **Tono de aviso durante grabación de voz** para indicar si durante una grabación de voz se escuchará un tono de aviso. En PhoneMail debe configurarse un equipo de grabación en vivo (Live Recording) adecuado. Valor estándar: Desactivado
Comprimir salida en display	Si el flag está activado, las salidas en display se comprimen para mejorar el rendimiento. Si se modifica la visualización en el display de un terminal UP0/ E, el sistema de comunicación actualiza únicamente los datos que difieren del display inmediatamente anterior. Esta función se debe desactivar cuando se conecta una aplicación (por ejemplo, Smartset/TAPI) vía un adaptador RS 232 (adaptador de datos o de control). En aplicaciones que reciben la información de los números de llamada de las indicaciones de la pantalla del terminal, el flag debe desactivarse (es decir, salida descomprimida con número de llamada en lugar de salida compromida con nombre). Por regla general, los nombres sólo se muestran cuando está desactivado el flag "Sólo número de llamada" de "Indicar nombre / Nº llamada". Valor estándar: Activado
Liberación puerta, MF	Si el flag está activado, la extensión puede abrir una puerta mediante señalización MF, siempre que se haya conectado un relé de apertura de puerta en el correspondiente puerto. Valor estándar: Desactivado
Acept. llamada autom., CSTA (solo para teléfonos SIP OpenStage)	Si el flag está activado, al marcar o al aceptar una llamada mediante myPortal o myAttendant, en el teléfono SIP correspondiente se activa el modo “manos libres”. Hay que seguir las indicaciones de la documentación del teléfono SIP ya que puede ser necesario tener que hacer ajustes adicionales en el teléfono SIP para utilizar correctamente la prestación. Si el flag está desactivado, hay que descolgar el auricular para establecer la llamada. Valor estándar: Activado

Parámetros	Descripción
Desactivar micrófono manos libres	Si el flag está activado no se puede utilizar el micrófono manos libres. El flag sólo es admitido por teléfonos OpenStage. Valor estándar: Desactivado
Presentación de número incondicional	Si el flag está activado, en lugar del nombre se muestra el número de llamada de la extensión llamante en el display de la extensión llamada. Valor estándar: Desactivado
Uso (solo para determinados países)	Esta lista desplegable se puede utilizar para configurar la corriente de salida de las interfaces de una placa analógica (en mA, por ejemplo, 27 mA para China).
Modo operativo	En esta lista desplegable se puede seleccionar un modo de servicio de la línea de extensión.
Salida lista de llamantes	Si este flag está activado, la lista de llamadas perdidas se activa para el usuario en su teléfono (solo para teléfonos con display). Las llamadas que no responda el usuario reciben un sello horario (fecha y hora) y se añaden a una lista ordenada cronológicamente. Solo se graban las llamadas que también un número de teléfono o un nombre. Si un usuario llama repetidas veces, sólo se actualiza la indicación horaria del registro y sube el contado de llamadas del llamante.
Señalización de ocupado central	Hay que definir este flag (véase también Prestaciones QSIG) para los usuarios que tengan un sistema de comunicación centralizado o señalización de ocupado. No es válido para los EE. UU. La implementación de señalización de ocupado está limitada a un máximo de 100 extensiones por nodo.
Display de texto de emergencia	Si este flag está activado, aparece un texto de emergencia configurable en el display del teléfono en modo de emergencia.
Supervisión de llamadas	Si el flag está activado, la extensión puede escuchar la llamada de cualquier otra extensión interna. El micrófono del usuario a la escucha se desactiva automáticamente. No se notifica al usuario supervisado mediante un tono de aviso o una indicación en pantalla. Al iniciar y finalizar la supervisión de llamadas se pueden producir interrupciones en la comunicación de hasta dos segundos. Valor estándar: Desactivado
Botones	
>	Pasa a la siguiente extensión. Si las extensiones que coinciden con el término de búsqueda introducido en los campos **Buscar** se han filtrado antes, solo es posible moverse entre esas extensiones concretas.
<	Retrocede una extensión.

Descripción de parámetros de las pestañas:

- **Editar datos cliente workpoint**

Parámetros	Descripción
Extensiones - ...	
Tipo	Tipo de la extensión.

Parámetros	Descripción
Número de llamada	Número de teléfono interno de la extensión.
Nombre	Nombre de extensión.
Parámetros	
Mensaje est.	Solo para clientes del sistema: Este flag activa el mecanismo “keep-alive” de los teléfonos del sistema. Si un teléfono del sistema, por ejemplo, falla, pasará a estar identificado como inactivo al cabo de 4 minutos. Cuando se configura un teléfono del sistema como puesto de teletrabajo y cuando se utilizan las prestaciones "Short Hold" (retención breve), este flag no debe estar activado. Cuando este flag no está activado, se reduce el tráfico de noticias entre el sistema de comunicación y los teléfonos del sistema.
Autenticación activa	Si el cliente IP se tiene que identificar en el sistema de comunicación con una contraseña, la autenticación debe estar activada y debe concederse también una contraseña. Resulta especialmente útil en aquellos clientes que no se encuentran en la LAN interna, sino que acceden telefónicamente desde el exterior. Solo para clientes SIP: tiene que introducir una contraseña. Se debe utilizar la misma contraseña en el dispositivo.
Nueva contraseña	Contraseña para la autenticación. Solo para clientes SIP: si ya se ha configuración la contraseña del dispositivo, deberá usarse la misma contraseña en Aplicar para mantener activado el registro del dispositivo.
Confirmar contraseña	Repetir contraseña para la autenticación.
SIP usuario / Nombre usuario	Solo para clientes SIP: Nombre de usuario libre para la autenticación de la extensión SIP, p. ej., "SIP-120". El valor definido aquí también se tiene que introducir en el teléfono SIP.
Ámbito	Solo para clientes SIP: Nombre libre para la zona correspondiente, p. ej. "OSBIZ-SIP". Este valor debe ser el mismo en todos los clientes SIP. El valor definido aquí también se tiene que introducir en el teléfono SIP.
Utilizar dirección IP fija	Solo para clientes SIP: Introducir una dirección IP fija garantiza que solo un cliente SIP podrá iniciar sesión con esa dirección IP en el sistema. Si está activado este flag, se comprueban la dirección IP y el número de llamada. Si el flag no está activado, solo se comprueba el número de llamada.
Dirección IP	Solo para clientes SIP: dirección IP del cliente SIP (p. ej., la dirección IP del teléfono SIP)
Tipo	Solo para clientes del sistema: un cliente IP móvil (opción Móvil) no está asignado a ningún teléfono IP de forma fija. Con el número de llamada de un cliente IP móvil, una extensión se puede dar de alta mediante el procedimiento para dar de alta (*9419) en cualquier terminal IP que lo permita (opción Móvil bloqueado no está activada).
Tipo: **Móvil**	Solo para clientes del sistema: la extensión no tiene asignado de forma fija ningún terminal IP. La prestación se admite a partir del tercer puerto de extensión.

Parámetros	Descripción
Tipo: **No móvil**	Solo para clientes del sistema: el terminal IP de la extensión tiene asignado de forma fija el número de teléfono. Al utilizar un teléfono WLx, la opción No móvil debe estar activada antes de que el teléfono WLx quede registrado en el sistema de comunicación.
Tipo: **No móvil y bloqueado**	Solo para clientes del sistema: Una extensión no puede registrar en el terminal IP con un cliente del sistema móvil.
Blocked for Deskshare User	Solo para clientes del sistema: este teléfono del sistema puede estar compartido entre varias extensiones (DeskSharing).
ID del sistema secundario	Este parámetro tiene dos funcionalidades diferentes: 1. Para todas las extensiones: define el gateway multiubicación asignado a la extensión. 2. Solo para clientes del sistema: si en los sistemas interconectados está definido el flag "Serv. emerg." (en "Extensiones/Clientes IP/Gateway secundario") aquí se puede definir el ID de nodo del sistema de respaldo para los clientes del sistema.
Registro de Internet con un SBC interno	Activa la prestación SIP@Home. De esta forma se puede registrar un teléfono SIP externo con STUN mediante Internet a OpenScape Business y utilizarlo como un teléfono interno.
Botones	
>	Pasa a la siguiente extensión. Si las extensiones que coinciden con el término de búsqueda introducido en los campos **Buscar** se han filtrado antes, solo es posible moverse entre esas extensiones concretas.
<	Retrocede una extensión.

Descripción de parámetros de las pestañas:

- **Editar grupos/RWS**

Parámetros	Descripción
Extensiones - ...	
Tipo	Tipo de la extensión.
Número de llamada	Número de teléfono interno de la extensión.
Nombre	Nombre de extensión.
Desvío de llamadas	
Dest. día	Indicación de los destinos de transferencia automática diferida para llamadas externas entrantes de día (véase el asistente Telefonía de usuario/ Transferencia automática diferida)
Dest. noche	Indicación de los destinos de transferencia automática diferida para llamadas externas entrantes de noche (véase el asistente Telefonía de usuario/ Transferencia automática diferida).
Dest. interno	Indicación de los destinos de transferencia automática diferida para llamadas internas entrantes (véase el asistente Telefonía de usuario/Transferencia automática diferida).

Parámetros	Descripción
Clase de servicio	
Día	Cada extensión puede tener asignada una clase de servicio para el día. Se puede elegir entre 15 clases de servicio distintas (véase Telefonía/Clases de servicio).
Noche	Cada extensión puede tener asignada una clase de servicio para la noche. Se puede elegir entre 15 clases de servicio distintas (véase Telefonía/Clases de servicio).
Telecaptura de llamadas	
Grupo	Todos los usuarios pueden ser asignados a un grupo de telecaptura de llamadas. Puede elegir entre 32 grupos de telecaptura de llamadas (120 con OpenScape Business S; véase también Llamadas entrantes/Telecaptura de llamadas).
Botones	
>	Pasa a la siguiente extensión. Si las extensiones que coinciden con el término de búsqueda introducido en los campos **Buscar** se han filtrado antes, solo es posible moverse entre esas extensiones concretas.
<	Retrocede una extensión.

28.3.7.10 Extensión > Extensión > UC Applications

Aquí aparecen las funciones de las soluciones de Comunicaciones Unificadas UC Smart y UC Suite. Se recomienda realizar los ajustes básicos en "Configuración > Configuración básica > Instalación básica > Cambiar números de función y de llamada preconfigurados".

En función de la solución de Comunicaciones Unificadas utilizada, se muestran diferentes funciones.

Descripción de parámetros de las pestañas:

- **Modificar extensión**

Parámetros	Descripción
N° llam.	Número de teléfono del servicio
Marcación directa	Número de marcación directa del servicio
Nombre	Nombre libre del servicio. Rango de valores: máx. 32 caracteres.
Apellidos	Apellidos libres del servicio. Rango de valores: máx. 32 caracteres.
Mostrar	Nombre libre del servicio. De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales

Parámetros	Descripción
Tipo	En función de la solución de UC: UC Smart: MeetMe / Conferencia UC Suite: AutoAttendant / Fax / Fax de Contact Center / Aparcar / MeetMe / Conferencia / Grupo de fax
Clip/Lin	Cadena numérica que ve el usuario llamado al hacerse una llamada saliente externa. Esta cadena aparece en lugar del número de teléfono real (p. ej. para el servicio de emergencia E911 EE. UU.) **Nota:** El CLIP no es compatible con fax de UC. Solo es compatible con fax analógico.
Activo	Indica si el servicio está operativo.
ID de ubicación ITSP	El ID de ubicación ITSP de una extensión.
Buscar	También puede mostrar una selección de servicios. Para ello, introduzca el término de búsqueda en los campos de **búsqueda** y confirme la entrada con la tecla Intro. Aparecen los servicios correspondientes al término de búsqueda. Si todos los campos de **búsqueda** están vacíos y se pulsa la tecla Intro, aparece de nuevo una lista de todos los servicios.
Elementos por página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
Flecha azul en la columna **N° llam.**	Abre la página con las pestañas **Editar parámetros exten.**, **Editar flags exten.**, **Editar datos cliente workpoint** y **Editar grupos/RWS**.
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

28.3.7.11 Extensiones > Extensiones > Perfiles/Plantillas

Aquí se pueden definir perfiles de usuario (parámetros de extensión, flags de extensión, grupos/RWS) para ofrecer a muchos usuarios una instalación básica de forma sencilla.

Descripción de parámetros de las pestañas:

- **Editar todos los perfiles**

Parámetros	Descripción
Perfiles	Indicación del número de perfil.
Nombre	Entrada de un nombre de perfil cualquiera.

Descripción de parámetros de las pestañas:

- **Mostrar todos los usuarios de perfil**

Parámetros	Descripción
Perfiles	Indicación del número de perfil.
Nombre	Indicación del nombre de perfil.
N.º llamada de miembro	Indicación del número de teléfono interno del miembro del perfil.
Nombre de miembro	Indicación del nombre del miembro del perfil.

Descripción de parámetros de las pestañas:

- **Añadir/Borrar miembro de perfil**

Parámetros	Descripción
Perfiles - ...	Indicación del número de perfil.
Nombre	Indicación del nombre de perfil asignado.
Miembros de perfil	
Selección	Lista de las extensiones disponibles en el sistema.
Miembros	Lista de las extensiones asignadas al perfil.
Botones	
Añadir	Aplicar la extensión marcada a la lista de miembros del perfil.
Eliminar	Borrar el miembro marcado de la lista de los miembros del perfil.

Descripción de parámetros de las pestañas:

- **Importar/Exportar perfil**

Parámetros	Descripción
Cargar perfil a través de HTTP	
Nombre archivo remoto (sist. archivos PC)	Cargar un archivo de perfil ya existente en formato XML
Exportar perfil a través de HTTP	
Nombre de archivo	Indicación del nombre de archivo con el que se emite el perfil (formato XML)
Acción	Descargar el perfil
Botones	
Reponer valores estándar	Los valores de perfil de todas las extensiones asignadas al perfil se restablecen al valor predeterminado.

Descripción de parámetros de las pestañas:

- **Importar/Exportar todos los perfiles**

Parámetros	Descripción
Cargar todos los perfiles a través de HTTP	

Parámetros	Descripción
Nombre archivo remoto (sist. archivos PC)	Cargar un archivo de perfil ya existente. En este archivo también puede haber guardados varios perfiles.
Exportar todos los perfiles a través de HTTP	
Nombre de archivo	Indicación del nombre de archivo con el que se guarda el perfil.
Acción	Descarga de los perfiles en un archivo de perfil.
Botones	
Reponer valores estándar	Los valores de perfil de todos los perfiles y de las extensiones asignadas se restablecen al valor predeterminado.

Descripción de parámetros de las pestañas:

- **Editar parámetros de extensión: véase Extensiones > Extensiones > Parámetros de extensión**
- **Editar flags de extensión: véase Extensiones > Extensiones > Parámetros de extensión**
- **Editar grupos/RWS: véase Extensiones > Extensiones > Parámetros de extensión**

28.3.7.12 Extensiones > Extensiones > Extensiones de marcación directa (DID)

Aquí se muestra una vista general de los números de marcación directa configurados con las extensiones correspondientes.

Descripción de parámetros de las pestañas:

- **Mostrar extensiones de marcación directa (DID)**

Parámetros	Descripción
N° llam.	Indicación del número de teléfono de la extensión.
Nombre	Indicación del nombre de la extensión.
Marcación directa	Indicación del número de marcación directa de la extensión.
(Pueden aparecer otros campos)	

28.3.7.13 Extensión > Extensión > Mobility Entry

Se recomienda configurar las extensiones móviles a través del asistente "Telefonía de usuario > Integración de teléfono móvil".

Descripción de parámetros de las pestañas:

- **Modificar extensión**

Parámetros	Descripción
N° llam.	Entrada del número de teléfono interno de la extensión Mobility (p. ej., 777). Este número de teléfono interno todavía no puede estar asignado.

Parámetros	Descripción
Marcación directa	Entrada del número de marcación directa interno de la extensión Mobility. Este número de marcación directo interno no puede estar asignado ya.
Nombre	Nombre libre de la extensión Mobility. Rango de valores: máx. 32 caracteres.
Apellidos	Apellidos libres de la extensión Mobility. Rango de valores: máx. 32 caracteres.
Mostrar	Nombre libre de la extensión Mobility. De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Tipo	Indicación del tipo de extensión Mobility.
Tipo disposit.	Indicación del tipo de teléfono del sistema al que pertenece el archivo de imagen.
Clip/Lin	Cadena numérica que ve el usuario llamado al hacerse una llamada saliente externa. Esta cadena aparece en lugar del número de teléfono real (p. ej. para el servicio de emergencia E911 EE. UU.). Rango de valores: máx. 16 cifras
Acceso	Indicación de la interfaz física con la que está conectado el terminal.
N.º llam. móvil	Entrada del número de teléfono del teléfono móvil. Entrada con código urbano delante, p. ej. 0016012345678.
Web Feature ID	Web Feature ID determina cómo iniciarán sesión las extensiones en el cliente web móvil (nombre de usuario. Se puede seleccionar entre "Ninguno" (Mobility Entry sin myPortal to go) o "Automático" (número de teléfono interno de la extensión o MULAP); o bien, se puede seleccionar entre el número del cliente o el teléfono de la lista desplegable.
Buscar	También puede mostrar selección extens. Introduzca término búsqueda en campos **búsqueda** y confirme la entrada con Intro. Se muestran las extensiones que se corresponden con el concepto de búsqueda. Si todos los campos de **búsqueda** están vacíos y se pulsa la tecla Intro, aparece de nuevo una lista de todas las extensiones.
Elementos por página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
Flecha azul en la columna **N° llam.**	Abre la página con las pestañas **Editar parámetros exten.**, **Editar flags exten.**, **Editar datos cliente workpoint** y **Editar grupos/RWS**.
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

Descripción de parámetros de las pestañas:

- **Gateway secundario**

  Para sistemas interconectados (Multi-Location)

Parámetros	Descripción
Número de llamada	Número interno del usuario Mobility.
Nombre	Nombre de la extensión Mobility.
ID de nodo	Registro del ID de nodo con el se puede acceder a la extensión móvil desde el exterior.

28.3.7.14 Extensión > Extensión > Usuario de SfB

Descripción de parámetros de las pestañas:

- **Editor tablas ext.**

Parámetros	Descripción
Nº llam.	Entrada del número de teléfono interno de la extensión Mobility Skype for Business Client (p. ej., 777). Este número de teléfono interno todavía no puede estar asignado.
M d	Número de marcación directa del cliente Skype for Business.
Nombre	Nombre de la extensión (libre). Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales.
Apellidos	Nombre de la extensión (libre). Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales.
Display	Nombre de la extensión (libre). De forma predeterminada, se crea con parám. Nombre y Apellidos, en función de algoritmo nombre visual. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales.
Tipo	Indicación del tipo de usuario Mobility, que en este caso siempre es Extensión SfB.
Núm. tel. SfB	El número de teléfono del cliente Skype for Business.
Buscar	También puede mostrar selección extens. Introduzca término búsqueda en campos **búsqueda** y confirme la entrada con Intro. Se muestran las extensiones que se corresponden con el concepto de búsqueda. Si todos los campos de **búsqueda** están vacíos y se pulsa la tecla Intro, aparece de nuevo una lista de todas las extensiones.
Elem. página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
Flecha azul en la columna **Nº llam**	Abre la página con las pestañas **Editar parámetros exten.**, **Editar flags exten.**, **Editar datos cliente workpoint** y **Editar grupos/RWS**.
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

28.3.7.15 Extensión > Extensión > Vista general de extensiones

Muestra una lista de todas las extensiones del sistema de comunicación, ordenadas por número de teléfono (estándar). Al hacer clic en el título de otra columna, la lista se ordena por la columna seleccionada en orden ascendente; si hace clic de nuevo, el orden será descendente.

Descripción de parámetros de las pestañas:

- **Modificar extensión**

Parámetros	Descripción
N° llam.	Número de teléfono interno de la extensión.
Marcación directa	Número de marcación directa de la extensión.
Nombre	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Apellidos	Nombre de la extensión (libre). Rango de valores: máx. 32 caracteres.
Mostrar	Nombre de la extensión (libre). De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Tipo disposit.	Indicación del tipo de la extensión.
Activo	Indica si la extensión está operativa.
Acceso	Indicación de la interfaz física con la que está conectado el terminal.
Buscar	También puede mostrar selección extens. Introduzca término búsqueda en campos **búsqueda** y confirme la entrada con Intro. Se muestran las extensiones que se corresponden con el concepto de búsqueda. Si todos los campos de **búsqueda** están vacíos y se pulsa la tecla Intro, aparece de nuevo una lista de todas las extensiones.
Elementos por página	Permite seleccionar si se mostrarán 10, 25, 50 o 100 entradas por página.
Botones	
Flecha azul en la columna **N° llam.**	Abre la página con las pestañas **Editar parámetros exten.**, **Editar flags exten.**, **Editar datos cliente workpoint** y **Editar grupos/RWS**.
>	Salta una página adelante.
<	Salta una página atrás.
>|	Salta al final de la lista.
|<	Salta al comienzo de la lista.

28.3.7.16 Extensiones > Programación de teclas

Descripción de parámetros de las pestañas:

- **Programación de teclas**

  La programación de teclas solo se admite en teléfonos UP0 y clientes HFA. La función de búsqueda (campos N.º llam., Marcación directa, Nombre, Apellido, Nombre en pantalla y Tipo de dispositivo) está disponible.

Parámetros	Descripción
Lista de selección	Selección del teléfono de las extensiones.
Conmutar nivel	Si se ha configurado una tecla con la función "Conmutar nivel", aquí se puede programar el segundo nivel
analógico	Al hacer clic en el área de teclas del teléfono, se abre la asignación de teclas actual.
Campo de teclas	Indicación de la función de las teclas (rotulación de teclas)
Botón de teclas	Selección de la función deseada

Descripción de parámetros de las pestañas:

- **Copiar distribución de teclas**

Parámetros	Descripción
Copiar la configuración de teclas de la extensión	Selección de la extensión cuya configuración de teclas se va a aplicar en las extensiones seleccionadas.
Todas las extensiones	Aplicar la configuración de teclas en todas las extensiones.
Campo de selección	Aplicar la configuración de teclas solo a las extensiones seleccionadas
Extensión	Indicación del número de teléfono interno y del nombre de la extensión.
Tipo disposit.	Indicación del tipo de teléfono de la extensión. El tipo de dispositivo no se puede cambiar para extensiones ya activas.
Copiar el tipo de dispositivo de la estación	Selección de la extensión cuyo tipo de dispositivo se va a copiar en las extensiones seleccionadas
a esta extensión o extensiones:	Selección de las estaciones en las que se copiará el tipo de dispositivo. Está disponible el filtrado por tipo de dispositivo de las estaciones.

28.3.8 Cordless

En **Cordless** se reúnen las funciones de la solución Cordless integrada para el servicio de teléfonos inalámbricos (teléfonos DECT) mediante el sistema de comunicación. Aquí se configuran las extensiones base y los teléfonos DECT (extensiones internas con prestaciones HFA).

28.3.8.1 Cordless > Para todo el sistema

Descripción de parámetros de las pestañas:

- **Editar datos de todo el sistema**

Parámetros	Descripción
Datos CMI	
EIC	Entrada de la identificación del sistema DECT hexadecimal de 8 dígitos Esta se proporciona con la adquisición del sistema DECT. Consta de los siguientes elementos: 1.er dígito: E/ARC (Access Right Code) 2.º-5.º dígito: EIC (Equipment Installer's Code) 6.º-7.º dígito: FPN (Fixed Part Number) 8.º dígito: FPS (Fixed Part Subscriber)
Banda frec.	Selección de la banda de frecuencia nacional. De forma predeterminada se muestra la banda de frecuencia asignada al código de país registrado.
Codific. voz	Indicación del códec de voz a nivel de sistema (a-law, µ-law).
Cifrado	Es el cifrado de los datos en la interfaz aérea. Se puede activar y desactivar. Valor predeterminado: activado
Vent. registro	Hora de abertura de la ventana para el registro de los teléfonos DECT. Para abrir la ventana de registro, hay que marcar el código *94 2 19970707 y la contraseña en el teléfono del sistema. A continuación, se introducen los números de teléfono de los teléfonos DECT que se quieren registrar en la ventana de registro. Estándar: 10 minutos
Tratamiento de eco Estos parámetros pueden invalidar a nivel de nodo los tratamientos de eco configurados para las extensiones móviles en **Líneas** > **Parámetros/Flags generales**. Se configuran después de configurar la línea de la llamada. En cada caso hay que comprobar si se produce una mejora mediante la desactivación general o mediante la activación específica de línea.	
Supresor de eco	En función del nivel de envío del teléfono DECT, el supresor de eco (ES, Echo Suppressor) conmuta una atenuación en dirección de recepción del teléfono DECT. Si el supresor de eco está activado, si hay ruidos de fondo altos también se puede atenuar la señal de recepción. Esto puede dificultar la comprensión de la llamada. En el modo **Inactivo**, la dirección de recepción del teléfono DECT no se atenúa cuando el nivel de envío del teléfono DECT es alto. Este ajuste puede mejorar la comprensión de los usuarios de línea urbana que utilicen el teléfono DECT con una conexión de línea urbana analógica y en un entorno ruidoso. Estándar: Automático
Compensador eco	El compensador de eco (EC, Echo Canceller) elimina muchos reflujos de señal no deseados causados por una implementación de 4/2 hilos (horquilla) en la red fija. Si el compensador de eco está activado y no hay eco, pueden darse errores, ya que el compensador intentará adaptarse a un eco que no existe. En el modo **Inactivo** se impide la conmutación del parámetro y el compensador de eco siempre está desactivado. Estándar: Automático

Parámetros	Descripción
Eco artificial	Mediante la ruta de eco artificial (AE, Artificial Echo), una señal de voz de la red fija se reenvía atenuada en 24dB a una extensión remota. Puede ser necesario hacerlo por ejemplo para dar a un compensador de eco integrado una determinada carga previa (por ejemplo, en una conexión internacional). En el modo **Inactivo** se impide la conmutación del parámetro y el eco artificial siempre está inactivo. Estándar: Automático
Control de desviación PP	En las conexiones de VoIP mediante componentes teléfonos DECT, suelen producirse ecos. Para suprimir o reducir estos ecos se puede activar la función "Control de desviación PP". Esta función se aplica a todos los componentes móviles DECT conectados con el sistema de comunicación. Para aplicar la activación o la desactivación a un componente móvil, hay que apagarlo y volverlo a encender. En el modo **Inactivo** no se aplica la supresión de eco y pueden darse ecos en las conexiones de VoIP mediante componentes móviles DECT. Valor predeterminado: Inactivo
Modo ECO	
Modo ECO	El modo ECO se puede activar a nivel de sistema para todos los teléfonos DECT. La potencia de envío de los teléfonos DECT se reduce en un valor definido (estático) o cada teléfono DECT adapta automáticamente su potencia de envío a la potencia de la señal recibida (adaptativo). Valor predeterminado: Inactivo
Modo ECO: **desact.**	El modo ECO está desactivado en todo el sistema.
Modo ECO: **activado**	El modo ECO (estática) está activado en todo el sistema. La potencia de envío de los teléfonos DECT se reduce en un valor fijo.
Modo ECO: **Autoadaptable**	El modo ECO (autoadaptable) está activado en todo el sistema. Cada teléfono DECT individual adapta automáticamente su potencia de envío a la potencia de la señal recibida. Con el handover, primero se conecta con la potencia de envío completa y, a continuación, se reduce en función de la recepción.

28.3.8.2 Cordless > SLC

Descripción de parámetros de las pestañas:

- **Editar teléfonos DECT**

Parámetros	Descripción
N° llam.	Número del teléfono DECT.
Marcación directa	Número de marcación directa del teléfono DECT.
Nombre	Nombre del teléfono DECT.

Parámetros	Descripción
Activo	Estado de registro del teléfono DECT: Verde: el teléfono DECT está activo. Rojo: interruptor de bloqueo de módulos con teléfono DECT registrado establecido. Amarillo: el teléfono DECT se ha desconectado (cerrado sesión) de nuevo automáticamente porque se ha modificado el PIN. Gris: en este puerto todavía no se ha dado de alta un teléfono DECT.
Código móvil	Código PIN para registrar el teléfono DECT. El código móvil debe ser único en todo el sistema.
Acceso	Nombre, número y slot de la línea de extensión S_0.
Slot	Indicación del slot del módulo SLC insertado.
Botones	
Eliminar	El teléfono DECT se borra del sistema. Al hacerlo se borra el número de teléfono, la marcación directa y el nombre y se libera la licencia TDM User correspondiente.

Descripción de parámetros de las pestañas:

- **Añadir teléfonos DECT**

Parámetros	Descripción
EIC	Si el sistema de comunicación no pertenece a una interred (ID de nodo = 0), la identificación del sistema se preasigna con 1. Si el sistema de comunicación pertenece a una interred (ID de nodo > 0), la identificación del sistema debe coincidir con el ID de nodo (**Cordless** > **Multi SLC** > **ID del sistema**).
Slot	Slot del módulo SLC insertado.
Nº SLC	Número ID único en el sistema del módulo SLC. Rango de valores: 1-15,17-31,33-47,...,127. No se pueden utilizar múltiplos de 16.
Número de teléfonos	Número de los teléfonos DECT ya configurados del módulo SLC.
SLC Número de llamada	Número de teléfono único a nivel de sistema de la línea de extensión S_0.
Acceso	Nombre, número y slot de la línea de extensión S_0.
Añadir teléfonos DECT	
Número de teléfonos	Si el número de los teléfonos DECT es menor que el tamaño permitido en el sistema (en función de la versión), aquí se puede añadir un número permitido de teléfonos DECT para este módulo SLC. Los teléfonos DECT añadidos se muestran en la pestaña **Editar teléfonos DECT**.

28.3.8.3 Cordless > Multi-SLC

Descripción de parámetros de las pestañas:

- **Editar Multi-SLC**

Parámetros	Descripción
Nº SLC	Número ID único en el sistema del módulo SLC. Rango de valores: 1-15,17-31,33-47,...,127. No se pueden utilizar múltiplos de 16.
ID de nodo	Visualización del ID del nodo (si está configurado). Si el sistema de comunicación pertenece a una interred, se muestran todos los módulos SLC de la interred que haya configurados.
SLC Número de llamada	Número de teléfono único a nivel de sistema de la línea de extensión S_0 del módulo SLC.

28.3.8.4 Cordless > Extensión base

Descripción de parámetros de las pestañas:

- **Editar extensiones base**

Parámetros	Descripción
Slot	Visualización del slot en el que está insertado el módulo SLC de la extensión base. Para la placa base (SLUC) se muestra el Slot 2.
Tipo	Tipo de la extensión base. Con un módulo SLC solo se muestra el tipo; con SLUC se puede seleccionar el tipo. Si el tipo se modifica de **Puerto sin terminal** a **Extensión base**, se preconfiguran automáticamente 16 teléfonos DECT y se configura una línea de interconexión SLC.
Tipo: **Extensión base**	Extensión base conectada.
Tipo: **Puerto sin terminal**	No hay conectada ninguna extensión base.
Nombre	Nombre de la extensión base.
Nivel	Nivel de la extensión base. Rango de valores: 50% y 100%; valor estándar: 100% 100%
Estado	Estado de la extensión base.
Master	Con un módulo SLC se muestran los puertos con los que están conectadas las extensiones base. Con SLUC se muestran todos los puertos en los que hay conectados terminales.

28.3.9 Llamadas entrantes

En **Llamadas entrantes** se reunen las funciones para la denominada Gestión de llamadas (CM, Call Management). Entre ellas se incluyen, por ejemplo, los ajustes de grupos y Transferencia automática diferida.

28.3.9.1 Llamadas entrantes > Grupos/Grupos de caza

Para la configuración inicial de llamadas de grupo y grupos de búsqueda, se recomienda utilizar el asistente de **llamadas de grupo/grupos de caza**.

Descripción de parámetros de las pestañas:

- **Editar números de llamada de grupo**
- **Mostrar grupos utilizados**
- **Mostrar todos los miembros del grupo**
- **Agregar grupo**
- **Eliminar grupo**
- **Editar parámetros del grupo**
- **Mostrar miembros**
- **Añadir miembro**
- **Editar orden de miembro**
- **Consultar MULAPs básicos**
- **Consultar preferencia MULAP**

Parámetros	Descripción
Índice	Número consecutivo asignado por el sistema de comunicación.
Número de teléfono.	Número de teléfono del grupo de llamadas, grupo de búsqueda, MULAP básico, MULAP ejecutivo o grupo de correo de voz
DID	Número DID del grupo de llamadas, grupo de búsqueda, MULAP básico, MULAP ejecutivo o grupo de correo de voz
Primer nombre	Nombre libremente seleccionable para el grupo de llamadas, grupo de búsqueda, MULAP básico, MULAP ejecutivo o grupo de correo de voz. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Apellidos	Apellido libremente seleccionable para el grupo de llamadas, grupo de búsqueda, MULAP básico, MULAP ejecutivo o grupo de correo de voz. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Mostrar	Nombre del grupo de llamadas, grupo de búsqueda, MULAP básico, MULAP ejecutivo o grupo de correo de voz De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización.
Tipo	Definición del tipo de grupo Valor estándar: Grupo Para más información, vea: Mesa: Opciones de escritura

Parámetros	Descripción
Tipo de llamada	Define la señalización acústica de las llamadas externas entrantes al grupo Valor estándar: 1 En los teléfonos analógicos solo se puede aplicar la configuración estándar. Los cambios no tienen ningún efecto.
Tipo de timbre: 1	Dos timbres
Tipo de timbre: 2	Tono de llamada triple
Tipo de timbre3	Tono de llamada corto/largo/corto
Directorio telefónico	Cuando se activa esta bandera (Mostrar Sí), el número de llamada del grupo aparece en el directorio interno. Valor estándar: Activado
Mulap como miembro del grupo	Cuando se activa esta bandera, el grupo MULAP se puede agregar como miembro en Grupos.
Miembro del grupo	
Grupo	Número (índice) del grupo
Miembro	Número (índice) del miembro dentro del grupo
Número de llamada	Número de teléfono del miembro del grupo
Nombre	Nombre del miembro del grupo
Parámetros	Parámetros habilitados del miembro del grupo
Parámetro: M	Máster (M): MULAP básico: El miembro domina el MULAP básico. Ejecutivo MULAP: El miembro tiene funciones ejecutivas.
Parámetro: R	Llamada acústica (R): MULAP básico y MULAP ejecutivo: Las llamadas entrantes se señalan acústicamente.
Parámetro: A	Toma automática de línea saliente (A): MULAP básico: El enlace troncal MULAP básico se selecciona automáticamente para una llamada cuando levanta el auricular. Ejecutivo MULAP: El enlace troncal Executive MULAP se selecciona automáticamente para una llamada cuando levanta el auricular.
Parámetro: K	No se permite la aceptación automática de llamadas entrantes (K): MULAP básico y MULAP ejecutivo: Para aceptar una llamada entrante hay que pulsar la tecla MULAP.
Parámetro: PAGS	Liberación automática de privacidad (P): MULAP básico y MULAP ejecutivo: Puede liberar la línea MULAP reservada para una conferencia pulsando la tecla MULAP.
Tecla MULAP configurada	Indica si se ha configurado o no una clave MULAP para el miembro del grupo.

Parámetros	Descripción
Ruta	Para un miembro externo del grupo, se muestra la ruta.
Grupo	
Verificación de coherencia	Se muestran las posibles colisiones debidas a la superposición de maestros de MULAPs básicos o a la captura automática de salida de MULAPs básicos.

Tabla 63: Opciones de escritura

Parámetros	Descripción
Se permiten todas las conversiones de tipo de grupo sin eliminar miembros del grupo, excepto los tipos de grupo MULAP. **Nota:** Si un grupo de tipo *Grupo*, *Grupo de caza lineal*, *Grupo de caza cíclica* o *Buzón de voz* tiene un grupo MULAP como miembro, luego no está permitida la conversión al tipo *RNA Group* o *Grupo de llamada en espera* . **Nota:** Si un miembro del grupo activa el desvío de llamadas (*1) a otro grupo de búsqueda , *Grupo de llamadas en espera* y el grupo de ARN La llamada no se enruta. Esto no está permitido para evitar bucles de llamadas. Para llamadas directas a la estación, el desvío es válido. Para *Cíclico* y *Grupo lineal (Grupo de caza)* Los miembros pueden usar *1 para cualquier destino, excepto el correo de voz.	
Tipo: Grupo de caza lineal	Una llamada entrante siempre se señala primero en el primer miembro de un grupo de búsqueda. La señalización adicional se realiza en función de la secuencia en la que se introducen los miembros en la tabla de grupo.
Tipo: Grupo de caza cíclica	Una llamada entrante siempre se señala primero en el miembro que sigue al suscriptor que respondió la última llamada. La señalización adicional se realiza en función de la secuencia en la que se introducen los miembros en la tabla de grupo.
Tipo: Grupo	Llamada de grupo de tipo Grupo: Las llamadas entrantes se señalizan simultáneamente en todos los miembros del grupo disponibles. Los miembros del grupo disponibles son suscriptores que no están ocupados. Si todos los miembros del grupo están ocupados, las nuevas llamadas se señalizan con el tono de llamada en espera. La señalización de llamada continúa para todos los miembros del grupo (tono de aviso para los miembros del grupo ocupados) incluso si el abonado cuelga.
Tipo: RNA	Llamada de grupo de tipo ARN: Las llamadas entrantes se señalizan simultáneamente en todos los miembros del grupo. Si un miembro del grupo está ocupado, toda la llamada del grupo se marca como ocupada (solo los miembros ocupados reciben una notificación para la llamada entrante). Quienes llaman desde este grupo reciben la señal de ocupado.

Parámetros	Descripción
Tipo: MULAP básico	Las llamadas entrantes se indican visualmente en todos los teléfonos asociados con el sistema MULAP (Multiple Line Approach) básico. El abonado también puede configurar si las llamadas entrantes deben señalizarse acústicamente o no para cada miembro individual. El estado del MULAP básico cambia a ocupado y otras personas que llaman escuchan la señal de ocupado cuando se responde una llamada. El número de teléfono MULAP básico se muestra en la pantalla de la parte llamada para las llamadas salientes a través de la troncal MULAP básica.
Tipo: MULAP ejecutivo	Puede configurar MULAPs ejecutivos si desea utilizar funciones ejecutivas y de secretaria restringidas. Si una persona llama al número de teléfono del Ejecutivo MULAP, la llamada se señaliza visualmente en todos los teléfonos pertenecientes al MULAP Ejecutivo. Las llamadas entrantes también se señalan acústicamente para los miembros con funciones de secretaría.
Tipo: Aviso llam. en espera	Llamada grupal de tipo llamada en espera: Las llamadas entrantes se señalizan simultáneamente en todos los miembros del grupo disponibles. Los miembros del grupo disponibles son suscriptores que no están ocupados. En caso de llamada, los miembros del grupo ocupados recibirán como señal el tono de llamada en espera.
Tipo: Buzón de voz	Grupo de correo de voz: Un grupo de correo de voz permite que un grupo específico de suscriptores acceda a sus mensajes de voz. Cuando se realiza una llamada al número de un grupo de correo de voz, la llamada se envía directamente al buzón de voz (es decir, el correo de voz) del grupo y no a los miembros del grupo. Una vez que se deja un mensaje de voz en el buzón de voz del grupo, este se reenvía a los buzones de voz de todos los miembros. Todos los miembros reciben el mensaje de voz simultáneamente. Cuando un miembro borra un mensaje de voz, este mensaje también se borra de los buzones de voz de todos los miembros y del buzón de voz del grupo. Los mensajes de voz personales de todos los miembros no se ven afectados por esto.

28.3.9.2 Llamadas entrantes > Miembros del grupo

Descripción de parámetros de las pestañas:

- **Editar miembro**
- **Borrar miembro**

Parámetros	Descripción
Grupo	Número (Índice) del grupo
Miembro grupo	Número (Índice) del miembro de grupo
Número de teléfono	Número de teléfono del miembro del grupo
Nombre	Nombre libre del miembro del grupo. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Apellidos	Apellidos libres seleccionables del miembro del grupo. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales

Parámetros	Descripción
Nombre	Nombre del miembro del grupo De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización.
Nombre MULAP	Nombre del grupo MULAP (Multiple Line Appearance). Es el nombre MULAP que se muestra en el teléfono cuando se llama a este grupo Team. El nombre MULAP es el mismo para todos los miembros del grupo Team del mismo tipo.
N° llam. MULAP	Número del grupo MULAP.
Master (M)	MULAP básico: al activar este flag, un miembro se convierte en Maestro del MULAP básico. Si un maestro activa un desvío de llamadas, se aplicará a todos los miembros (teléfonos) del MULAP básico. MULAP Jefe: al activar este flag, se asignan funciones Jefe a un miembro. Al descolgar el microteléfono se llama automáticamente a través de la línea MULAP Jefe. Las llamadas entrantes a través del número de teléfono MULAP Jefe solo se señalizan de forma óptica.
Llamada acústica (L)	MULAP básico y MULAP Jefe: si el flag está activado, las llamadas entrantes se indican acústicamente. Valor estándar: activado para todos los maestros de un MULAP básico. Activado para todos los miembros con función Secretaria de un MULAP Jefe.
Ocupación automática saliente (A)	MULAP básico: si el flag está activado, al descolgar el auricular se llama automáticamente mediante la línea MULAP básico. MULAP Jefe: si el flag está activado, al descolgar el auricular se llama automáticamente mediante la línea MULAP Jefe. Valor estándar: activado para todos los maestros de un MULAP básico. Activado para todos los miembros con función Secretaria de un MULAP Jefe.
Sin aceptación automática de llamadas entrantes (E)	MULAP básico y MULAP Jefe: si el flag está activado, las llamadas entrantes no se pueden aceptar descolgando el auricular. Las llamadas entrantes solo se pueden aceptar pulsando la tecla MULAP. Valor estándar: Desactivado
Liberación de conferencia automática (P)	MULAP básico y MULAP Jefe: si el flag está activado, al pulsar la tecla MULAP se libera la línea MULAP ocupada para una conferencia. Todos los demás miembros reciben una indicación de la liberación: la tecla MULAP parpadea. Pulsando la tecla MULAP puede unirse a la conferencia. Valor estándar: Desactivado
Tecla MULAP configurada	MULAP básico: si el flag está activado, en el teléfono correspondiente se configura una tecla MULAP. Pulsando la tecla, se realiza una ocupación saliente a través de la línea MULAP básico. En el display del usuario llamado aparece el número de teléfono MULAP básico. MULAP Jefe: si el flag está activado, en el teléfono correspondiente se configura una tecla MULAP. Pulsando la tecla, se realiza una ocupación saliente a través de la línea MULAP Jefe. En la pantalla del destinatario de la llamada aparece el número de teléfono MULAP Jefe. Valor estándar: Activado

Parámetros	Descripción
Ruta	En los miembros externos del grupo, se muestra la ruta.
Tipo	Definición del tipo de grupo

28.3.9.3 Llamadas entrantes > Team/Top

Para la configuración inicial de grupos Team y Top es recomendable usar los asistentes **Configuración de equipo** y **Jefe / Secretaria**.

Descripción de parámetros de las pestañas:

- **Mostrar todos grupos Team/Top**
- **Mostrar grupos Team/Top utilizados**
- **Añadir grupo Team/Top**
- **Editar grupo Team/Top**
- **Borrar grupo Team/Top**
- **Editar grupo Team/Top**
- **Mostrar todos miembros de grupo Team/Top**
- **Añadir miembro Team/Top**
- **Editar miembro Team/Top**
- **Borrar miembro Team/Top**
- **Mostrar buzones de fax**
- **Agregar buzón de fax**

Parámetros	Descripción
El índice	Número consecutivo, asignado por el sistema de comunicación.
Nombre	Nombre libre del grupo Team/Top. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Apellidos	Apellidos de selección libre para el grupo Team/Top. Rango de valores: máx. 16 caracteres, sin diéresis ni caracteres especiales
Nombre	Nombre del grupo Team/Top De forma predeterminada, se crea con los parámetros de Nombre y Apellidos, en función del algoritmo de nombre de visualización.
Tipo	Definición del tipo de grupo
Tipo: Equipo	Los grupos Team ofrecen varias funciones prácticas para equipos. Los números de extensión de todos los miembros de equipo se programan en teclas MULAP (teclas de línea). De esta forma, cada miembro del equipo puede acceder a todas las líneas (por ejemplo, para la telecaptura de llamadas) y puede telefonear al mismo tiempo a través de varias líneas.
Tipo: Top	Un grupo Top ofrece prácticas funciones de Jefe y Secretaria (función Top) para hasta tres jefes y tres secretarias.
Equipo como miembro del grupo	Este marcador solo se puede configurar cuando el grupo Team tiene miembros con el mismo tipo de extensión, lo que da como resultado un único grupo MULAP bajo este grupo Team. Cuando se activa este marcador, el grupo MULAP se puede agregar como miembro en Grupos.

Parámetros	Descripción
Asignación de teclas a Team	Definición para la configuración de teclas MULAP de miembros del grupo Team
Asignación de teclas a Team: En primera/segunda consola	Si el marcador está activado, se configuran automáticamente las teclas MULAP en el primer o segundo dispositivo auxiliar (Key module o BLF) del teléfono Team.
Asignación de teclas a Team: las primeras teclas libres	Si el marcador está activado, se configuran automáticamente las teclas MULAP en las primeras teclas libres del teléfono Team.
Asignación de teclas a Top	Definición para configuración de las teclas MULAP de miembros del grupo Top
Asignación de teclas a Top: En primera/segunda consola	Si el marcador está activado, se configuran automáticamente las teclas MULAP en el primer o segundo dispositivo auxiliar (Key module o BLF) del teléfono Top.
Asignación de teclas a Top: las primeras teclas libres	Si el marcador está activado, se configuran automáticamente las teclas MULAP en las primeras teclas libres del teléfono Top.
Miembro grupo	
Grupo	Número (Índice) del grupo
Miembros	Número (Índice) del miembro en el grupo
Tipo	Definición del tipo de miembro
N° llam.	Número de teléfono del miembro de grupo (cambia en un grupo MULAP a **Nº llam. y está disponible internamente con ese **Nº llam.)
Nombre	Nombre del miembro del grupo
N° llam. MULAP	Número del grupo MULAP.
Duwa MULAP	Número de marcación directa del grupo MULAP
Nombre MULAP	Nombre del grupo MULAP. Es el nombre MULAP que se muestra en el teléfono cuando se llama a este grupo Team. El nombre MULAP es el mismo para todos los miembros del grupo Team del mismo tipo.
Tipo de llamada	Definición de la señalización sonora de las llamadas externas que reciba el grupo Valor estándar: 1 En los teléfonos analógicos solo se puede aplicar la configuración estándar. Los cambios no tienen ningún efecto.
Tipo de llamada: 1	Tono de llamada doble
Tipo de llamada: 2	Tono de llamada triple
Tipo. llam: 3	Tono de llamada corto/largo/corto
Listín tel.	Si el flag está activado (indicación Sí), aparece el número de teléfono del grupo en el directorio interno. Valor estándar: Activado

Parámetros	Descripción
Master (M)	Grupo Team: Al activar este marcador, un miembro se convierte en Maestro del grupo Team. Si un maestro activa un desvío de llamadas, se aplicará a todos los miembros (teléfonos) del grupo Team. Grupo Top: Al activar este marcador, se asignan a un miembro funciones de Jefe. Al descolgar el microteléfono se selecciona automáticamente la línea MULAP Jefe. De forma estándar, las llamadas entrantes a través del número de teléfono MULAP Jefe en cuestión solo se señalizan de forma visual.
Llamada acústica (L)	Grupo Team y grupo Top: si el flag está activado, las llamadas entrantes se indican acústicamente. Valor estándar: Activado para todos los miembros de un grupo Team. Activado para todos los miembros con función Secretaria de un grupo Top.
Ocupación automática saliente (A)	Grupo Team y grupo Top: Cuando este flag está activado, al descolgar el microteléfono se llama automáticamente a través de la línea MULAP de este miembro. Valor estándar: Activado
Sin aceptación automática de llamadas entrantes (E)	Grupo Team y grupo Top: si el flag está activado, las llamadas entrantes no se pueden aceptar descolgando el auricular. Las llamadas entrantes solo se pueden aceptar pulsando la tecla MULAP. Valor estándar: Desactivado
Liberación de conferencia automática (P)	Grupo Team y grupo Top: si el flag está activado, al pulsar la tecla MULAP se libera la línea MULAP ocupada para una conferencia. Todos los demás miembros reciben una indicación de la liberación: la tecla MULAP parpadea. Pulsando la tecla MULAP puede unirse a la conferencia. Valor estándar: Desactivado
Tecla MULAP configurada	Grupo Team: si el flag está activado, en el teléfono correspondiente se configura una tecla MULAP. Al pulsar la tecla se realiza una ocupación saliente a través de la línea MULAP del Maestro. En la pantalla del destinatario de la llamada aparece el número de extensión MULAP del maestro. Grupo Top: si el flag está activado, en el teléfono correspondiente se configura una tecla MULAP. Pulsando la tecla, se realiza una ocupación saliente a través de la línea MULAP Jefe. En la pantalla del destinatario de la llamada aparece el número de teléfono MULAP Jefe. Valor estándar: Desactivado para todos los miembros de un grupo Team. Activado para todos los miembros de un grupo Top.
Tipo MULAP	Definición del tipo MULAP
Tipo MULAP: MULAP básico	Las llamadas entrantes se señalizan visualmente en todos los teléfonos pertenecientes al MULAP básico. Además, se puede indicar, para cada miembro, si las llamadas entrantes también deberán ser señalizadas acústicamente. Cuando se acepta la llamada, el MULAP básico pasa a estar ocupado y todas las demás llamadas reciben en tono de ocupado. En el caso de las llamadas salientes a través de la línea MULAP básico, aparece el número de teléfono MULAP básico en el display del usuario llamado.

Parámetros	Descripción
Tipo MULAP: MULAP Jefe	Se puede acceder a todos los miembros de un MULAP Jefe a través del número de teléfono MULAP Jefe y a través de sus propios números de extensión.
Número de teléfono de fax	Número de teléfono de buzón de fax de miembro del grupo
N° llam. marc. directa de fax	Número de marcación directa del buzón de fax del miembro del grupo

28.3.9.4 Llamadas entrantes > Telecaptura de llamadas

Descripción de parámetros de las pestañas:

- **Asignar nombre grupos de telecaptura**
- **Mostrar extensiones del grupo**
- **Asignar extensiones al grupo**

Parámetros	Descripción
Grupo	
Grupo	Número (Índice) del grupo de telecaptura Rango de valores: de 1 a 32 (120 para OpenScape Business S)
Nombre	Nombre del grupo de telecaptura
Extensión	
N° llam.	Número de teléfono de la extensión interna
Nombre	Nombre de la extensión interna
Asignación del grupo X	Si el flag está activado, se asigna a la extensión el grupo de telecaptura X.
Grupo	Grupo de telecaptura, al que está asignada la extensión.

28.3.9.5 Llamadas entrantes > UCD

Descripción de parámetros de la pestaña:

- **Editar parámetros UCD**

Parámetros	Descripción
Flags UCD	
Liberar aplicaciones UCD	Si el flag está activado, la prestación Distribución de llamadas (Uniform Call Distribution, UCD) se habilita a nivel de sistema. Valor estándar: Activado

Parámetros	Descripción
Agentes disponibles permanentemente	Si el flag está activado, todos los agentes UCD son agentes permanentes. De esta forma, un agente disponible de forma permanente también permanecerá disponible para llamadas, faxes y correos electrónicos aunque no acepte una llamada, un fax o un correo electrónico. Valor estándar: Desactivado
Tiempo administrativo automático	
Tiempo administrativo (ciclos)	Definición a nivel del sistema del tiempo administrativo automático para todos los agentes UCD en ciclos de llamadas, es decir, en pasos de 5 segundos. Durante el tiempo administrativo, se exceptúa temporalmente a un agente de la distribución de llamadas, dándole así un tiempo para procesar la llamada recién finalizada. Valor estándar: 0
Prioridad para llamadas internas	
Prioridad interna	Definición a nivel del sistema de la prioridad para llamadas internas mediante 10 niveles de prioridad (1 = alto, 10 = bajo). Valor estándar: 10
Prioridad para llamadas externas	
Slot / línea	Indicación del módulo, del slot y del número de la línea (del canal B). En el caso de las llamadas externas, la prioridad se asigna en función de la línea (por canal B), se trate de líneas IP o TDM.
Prioridad	Definición de la prioridad para llamadas externas que entran por la línea correspondiente (canal B). La definición se hace mediante 10 niveles de prioridad (1 = alto, 10 = bajo). Valor estándar: 1

Descripción de parámetros de las pestañas:

- **Mostrar Grupos UCD**
- **Editar Grupo UCD**

Parámetros	Descripción
Número de llamada	Número de teléfono del grupo UCD
MSN	Número de marcación directa del grupo UCD
Nombre	Nombre del grupo UCD
Cicl. llam. prim.	Definición del ciclo de llamada primario: La entrada se realiza en ciclos de llamada, esto es, en intervalos de 5 segundos. Se configura el tiempo que permanecerá una llamada en la cola de espera si no es aceptada por el agente que lleve más tiempo en estado Disponible. A continuación, la llamada se transfiere al siguiente agente disponible. Valor estándar: 3 ciclos

Parámetros	Descripción
Cicl. llam. sec.	Definición del ciclo de llamada secundario: La entrada se realiza en ciclos de llamada, esto es, en intervalos de 5 segundos. Se configura el tiempo que permanecerá una llamada en la cola de espera si no es aceptada por el siguiente agente disponible. Valor estándar: 3 ciclos
Llamadas en espera	Definición del número máximo de llamadas en espera: Si se supera el número máximo de llamadas en espera, las demás llamadas se pueden desviar a un destino de desbordamiento (un destino externo, otro grupo UCD, una extensión interna o un grupo). Valor estándar: 10 (Valor estándar: último grupo UCD: 72)
AICC	Definición de AICC (Automatic Incoming Call Connection). Este ajuste se aplica a todos los agentes del grupo UCD, estén equipados o no los teléfonos de agente con cascos telefónicos. Valor estándar: no
AICC: Sí	Los agentes de este grupo UCD pueden aceptar llamadas entrantes sin realizar más pasos de control. El agente es informado de la entrada de una llamada mediante un tono audible en el casco telefónico. La llamada se pasa a continuación de forma automática.
AICC: No	Los agentes de este grupo UCD no pueden aceptar llamadas entrantes sin dar los pasos de control anteriores (por ejemplo, descolgar el auricular).
Cambio de mensaje	Definition de cambio de mensaje posible Valor estándar: una vez
Cambio de mensaje: indiv.	Los llamantes que están en la cola reciben un anuncio grabado una vez.
Cambio de mensaje: Cíclico	El último y el penúltimo anuncio de la configuración se repiten cíclicamente.
Tiempo de desbordamiento	Definición del tiempo de desbordamiento en segundos: Si la aplicación UCD no acepta una llamada en espera en el tiempo de desbordamiento, el sistema de comunicación procesa la llamada siguiendo las indicaciones de Gestión de llamadas (Call Management). Este ajuste solo es relevante si hay conectada una aplicación UCD externa. Valor estándar: 600
Retraso de anuncio grabado	Definición del retraso de anuncio grabado en segundos: Al terminar este tiempo, un llamante que esté en la cola escucha un anuncio grabado. Valor estándar: 0

Descripción de parámetros de la pestaña:

- **Editar parámetros de grupo UCD**

Parámetros	Descripción
Índice de destinos	Por cada grupo UCD se pueden definir hasta siete destinos (índice 1 a 7) para anuncios grabados. Los llamantes que estén en la cola de espera escuchan una reproducción anuncios grabados de los destinos, uno tras otro.

Parámetros	Descripción
Anuncio grabado	Anuncio grabado para el índice de destino correspondiente.
Tiempo de espera	El anuncio grabado se puede reproducir cíclicamente (máx. 9 ciclos de 5 s cada uno = 45 s) o de forma continua. Cuando termina ese tiempo, los llamantes que estén en la cola de espera escuchan el anuncio grabado del siguiente índice (no en el modo de reproducción **continua**). Valor estándar: Continua

Descripción de parámetros de la pestaña:

- **Añadir-Borrar miembros de grupo UCD**

Parámetros	Descripción
Selección	Lista de todos los ID de agente UCD. Los ID de agente UCD no se corresponden con los números de teléfono del sistema de comunicación.
Miembros	Lista de los ID de agente UCD del grupo UCD seleccionado
Botones	
Añadir	Añade los ID de agente UCD marcados al grupo UCD.
Eliminar	Borra los ID de agente UCD marcados del grupo UCD.

Descripción de parámetros de la pestaña:

- **Asignar extensiones**

Parámetros	Descripción
ID de agente	Lista de los ID de agente UCD del grupo UCD seleccionado.
Extensiones	Lista de las extensiones que se pueden asignar a los ID de agente UCD del grupo UCD.

28.3.9.6 Llamadas entrantes > Desvío de llamadas

Descripción de parámetros de las pestañas:

- **Listas de destinos de llamada - Definición**

Parámetros	Descripción
Lista destinos llam.	Selección de la lista de destinos de llamada que se va a editar. Rango de valores: de 1 a 740
Modificar Transferencias automáticas diferidas Para buscar más rápido un destino llamada, en **1. - 4. destino** también puede introducir una o varias cifras. Entonces se pasa directamente a la entrada de lista que comience con la secuencia de cifras introducida. También se puede introducir secuencia letras.	

Parámetros	Descripción
Destino 1 - 4: **Ningún registro**	Se omite el destino de llamada.
Destino 1 - 4: **Destino externo**	Ruta y número de teléfono externo con código de línea urbana.
Destino 1 - 4: *** Ext. marcada**	Extensión llamada.
Destino 1 - 4: **** Usuario definido**	Destino del desvío de llamadas diferido por la extensión (si está configurado).
Destino 1 - 4: **#9 Búsqueda de sistema**	Siguiente extensión disponible (salvo extensión Jefe).
Destino 1 - 4: **#201 - #260**	Distr. llamadas (Grupo UCD).
Destino 1 - 4: **#801 - #817**	Disp. an.
Destino 1 - 4: 100, 101, ...	Número de teléfono de una extensión o de un grupo (p.ej. buzón de voz)
Tr. autom. difer. después de	Tiempo tras el cual las llamadas se desviarán al siguiente destino de llamada. En los grupos UCD, la transferencia sigue los mecanismos de los ciclos de llamada primarios y secundarios (véase Grupos UCD). Rango de valores: 5/10/15/...75 s; valor estándar: 15 s
Desvíos de llamadas	En caso de ocupado, la llamada se desvía inmediatamente al siguiente destino de llamada. Valor estándar: activado
Segundo timbre	
Destino de segundo timbre	Extensión interna adicional en la que también se señaliza la llamada o un contacto (relé) de un módulo de contactos/sensores para un timbre central.
Tipo de segundo timbre	La llamada se puede señalizar en la extensión inmediatamente o una vez transcurrido todo el tiempo de transferencia de llamadas. Valor estándar: Inmediatamente

Descripción de parámetros de las pestañas:

- **Listas de destinos de llamada - Asignación**

Parámetros	Descripción
N° llam.	Número de teléfono de la extensión o del grupo.
Nombre	Nombre de la extensión o del grupo.
Tipo	Tipo extensión, p. ej., U_{P0}, cliente de sistema, AB, RDSI, SIP.
Día	Número lista dest. llamada para llamadas externas entrantes durante horario trabajo (servicio diurno) Valor estándar: 14

Parámetros	Descripción
Noche	Núm. lista dest. llamada para llamadas externas entrantes con servicio nocturno activado Valor estándar: 15
Interna	Número de la lista de destinos de llamada para llamadas internas entrantes Valor estándar: 16
Buscar	Si en los campos de búsqueda **N° llam.** o **Nombre** se introduce un término de búsqueda y, a continuación, se pulsa la tecla Intro, aparecen todos los resultados que incluyen el término de búsqueda. Si por ejemplo se escribe `521` como número de teléfono, aparecerían los resultados `+495213535` y `+498967521`. O por ejemplo, si se escribe `co` como nombre, aparecerían los resultados `Collins`, `Mcoin` y `Branco`. Si no hay nada en ningún campo de búsqueda y se pulsa la tecla Intro, aparecen todas las entradas.

Descripción de parámetros de las pestañas:

- **Miembros de la lista de destinos**

Parámetros	Descripción
Mostrar a todos los miembros con la lista de destinos de llamada	Se muestran todas las extensiones o todos los grupos que utilizan la lista de destinos de llamada seleccionada.

Descripción de parámetros de las pestañas:

- **Copiar listas de destinos de llamada**

Parámetros	Descripción
Lista destinos llam.	Selección de la lista de destinos de llamada a la que se va a asignar la extensión. Rango de valores: de 1 a 740
Día	Lista dest. llamada para llamadas ext. entrantes durante el horario de trabajo (servicio diurno)
Noche	Lista dest. llamada es para llamadas ext. entrantes con servicio nocturno activ.
Interna	Lista dest. llamada es para llam. internas entr.
Listas de dest. de llamada	
Selección	Lista de todas las extensiones.
Miembros	Lista de las extensiones a las que está asignada la lista de destinos de llamada.
Botones	
Añadir	Las extensiones marcadas se añaden desde la ventana de selección a la ventana de miembros.
Eliminar	Las extensiones marcadas se borran de ventana miembros.

28.3.10 Líneas/Interconexión

En **Líneas/Interconexión** se reunen las funciones para las líneas urbanas y las rutas.

28.3.10.1 Líneas/Interconexión > Líneas

Descripción de parámetros de las pestañas:

- **Mostrar todas las líneas**
- **Cambiar ruta**

Parámetros	Descripción
Línea	Indicación de la línea urbana física conectada con el sistema de comunicación.
Box-Sl-Pt-Lín. o Box/Slot/ Puerto/Línea	Indicación del tipo de módulo, número de puerto (físico) y slot para la conexión de la línea con el sistema de comunicación.
Código	Indicación o configuración del código de ruta. Al introducir este número, el sistema de comunicación ocupa la línea asignada. Se utiliza para probar la línea de enlace o para programar teclas de línea. Si se utilizan aplicaciones CSTA, se debe establecer el valor para este parámetro.
Ruta	Indicación o selección de la ruta asignada a la línea (ninguna o Ruta 1 a Ruta 12). Si para la línea activa se configura la selección "ninguno", el sistema tendrá un comportamiento inestable. Además, el sistema podrá recibir llamadas en esa línea, pero no podrá transferirlas.
Estado	Indicación del estado de la línea. Las líneas inactivas están marcadas con estrellas.
Tipo	Indicación del tipo de línea. Las líneas inactivas tienen la indicación "No Port" (Puerto sin termina).

Descripción de parámetros de las pestañas:

- **Asignación llam. todas las líneas**

Parámetros	Descripción
Línea	Indicación de la línea urbana física conectada con el sistema de comunicación.
Box-Sl-Pt-Lín. o Box/Slot/ Puerto/Línea	Indicación del tipo de módulo, número de puerto (físico) y slot para la conexión de la línea con el sistema de comunicación.
Día N° llam.	Indicación del número de puerto asignado para el servicio de día
Día Nombre	Indicación del nombre del número de teléfono asignado para el servicio de día
Noche N° llam.	Indicación del número de teléfono asignado para el servicio de noche
Noche Nombre	Indicación del nombre del número de teléfono asignado para el servicio de noche

Descripción de parámetros de las pestañas:

- **Agregar línea**

Parámetros	Descripción
Cantidad	Número de líneas que se van a agregar.

Descripción de parámetros de las pestañas:

- **Cambiar dirección**

Parámetros	Descripción
Línea	Muestra el número de la línea.
saliente	En la línea pueden realizarse llamadas salientes. **Nota:** Se pueden hacer llamadas de emergencia incluso si el flag está desactivado.
entrante	En la línea pueden realizarse llamadas entrantes.

Descripción de parámetros de las pestañas:

- **Editar línea**
- **Borrar línea**

Parámetros	Descripción
Línea	Indicación del número de línea.
Box/Slot/Puerto/Línea	Indicación del puerto físico de la línea (Box/Slot/Puerto/Línea).
Código	Indicación o entrada del código de ruta.
Ruta	Indicación o selección de la ruta asignada a la línea (ninguna o Ruta 1 a Ruta 12).
Asignación llam. lín.	
Día N° llam.	Número de teléfono para una conexión entrante que no admita la marcación directa de día.
Noche N° llam.	Número de teléfono para una conexión entrante que no admita la conexión directa en el servicio de noche.

Descripción de parámetros de las pestañas:

- **Editar flags RDSI**

Parámetros	Descripción
Protocolo: Descripción	Las entradas de una plantilla de protocolo constan de interfaz, protocolo e información adicional: conexión básica S0 2B+D mediante interfaz S0, conexión básica BRI 2B+D mediante interfaz U2B1Q (EE. UU.), conexión múltiplex primaria S2 30B+D, conexión múltiplex primaria T1 23B+D (EE. UU.)
Lógico/físico	Numeración lógica o física de los canales
Negociación canal B esclavo: Maestro	Configuración del maestro/esclavo en la capa 3. En las conexiones, hay que configurar un lado como esclavo y el otro, como maestro.

Parámetros	Descripción
Asignación canal B arriba: Abajo	Definición de la numeración de canales B (debe ser igual en los dos sistemas)
Formato CHI S0: S2M	Formato de protocolo CHI, debe definirse como S0 (formato breve) o S2M (formato amplio)
Simétrico/asimétrico	Uso simétrico o no simétrico de elementos de protocolo L3
Automático/fijo	Tratamiento automático o asignación fija de la simetría
Longitud 1 CR: 2	Formato de protocolo, extensión de referencia de llamada (Call Reference-CR)
Señalización de alarmas	Uso de señalizaciones de alarma en el protocolo de capa 3
Temporizador de protocolo activado	Uso del temporizador de capa 3
Arranque rápido de PRI	Uso del procedimiento de arranque rápido PRI
IE_TNS	Uso del elemento de información Transit Network Selection (TNS)
IE_OSA	Uso del elemento de información Open Service Access (OSA)
CIDL	Uso de la señalización de ID de enlace y llamada (CIDL) en la interconexión
Por parte del usuario/de la red	Definición de protocolo de capa 2 (L1). En el colateral hay que realizar un ajuste duplicado
Red/extensión	Definición de protocolo de capa 2 (L1). En el colateral hay que realizar un ajuste duplicado
PP/PMP	Definición de punto a punto (PP) o punto a multipunto (PMP), solo relevante con S0
Permanentemente activo	Capa 2 activa permanentemente
Verificar TEI activo	Activar control TEI
Por parte del usuario/de la red	Definición de protocolo de capa 1 (L1). En el colateral hay que realizar un ajuste duplicado
PP/PMP	Definición de protocolo de capa 1 (L1). Se deben realizar los mismos ajustes de configuración en ambos lados
Tipo bus S: L	Bus corto/largo (alcances)
Permanentemente activo	Definición de protocolo de capa 1 (L1). Se deben realizar los mismos ajustes de configuración en ambos lados
Comprobar CRC4	Definición de protocolo de capa 1. Solo relevante con S2M, debe hacerse el mismo ajuste en ambos lados
Informando CRC4	Definición de protocolo de capa 1. Solo relevante con S2M, debe hacerse el mismo ajuste en ambos lados

Descripción de parámetros de las pestañas:

- **Cambiar canal B**

Parámetros	Descripción
Canal B	Indicación del número de canal B.
Saliente	En el canal B se pueden hacer llamadas salientes.
Entrante	En el canal B se pueden recibir llamadas entrantes.

Descripción de parámetros de las pestañas:

- **Cambiar dirección**

Parámetros	Descripción
Línea	Indicación del número de línea.
Saliente	En la línea pueden realizarse llamadas salientes.
Entrante	En la línea pueden realizarse llamadas entrantes.

28.3.10.2 Troncales/Enrutamiento > Grupo troncal

Descripción de parámetros de las pestañas:

- **Cambiar ruta**

Parámetros	Descripción
Nombre de la ruta	Nombre de la ruta. El nombre introducido reemplaza el número de ruta predeterminado en la lista de rutas.
Códigos de intervención	Aquí se introducen los códigos de asignación para cada ruta. Los códigos de enrutamiento introducidos deben estar libres de colisiones, tanto entre sí como dentro del plan de numeración de llamadas completo del sistema de comunicación. Utilice el botón Comprobar para detectar colisiones. El código de intervención es el código que hace que el sistema de conmutación proporcione una línea a la estación que marcó el código. Los códigos de intervención solo funcionan si LCR no se ha activado.
Código CO (2.º código de troncal)	Se define un segundo código de troncal (código CO) si el sistema de comunicación es un subsistema de otro sistema de comunicación o está conectado en red con varios otros sistemas de comunicación. Solo es relevante para rutas de red (tipo de ruta = PABX). En este caso, el segundo código de troncal es el código de interrupción del sistema principal. Dentro de una red, los códigos para la toma del tronco, el/los código(s) de toma de ruta y el segundo código CO deben configurarse de manera uniforme. El valor predeterminado en Alemania es 0.
Ubicación del gateway	
Código de país	Muestra el código de país de la ubicación del gateway propio. Configurar mediante Ajustes básicos/Gateway/Ubicaciones del Gateway
Código de red local	Muestra el código de área local de la ubicación del Gateway. Configurar mediante Ajustes básicos/Gateway/Ubicaciones del Gateway
Número de PABX	Muestra el número de la centralita PABX de la propia ubicación del Gateway. Configurar mediante Ajustes básicos/Gateway/Ubicaciones del Gateway

Parámetros	Descripción
Número de estación del sistema - entrante	
Código de país	Se utiliza para el análisis de dígitos en llamadas entrantes. Código de país sin ceros a la izquierda (por ejemplo, 1 en EE. UU., 49 en Alemania)
Código de red local	Se utiliza para el análisis de dígitos en llamadas entrantes. Código de área local sin ceros a la izquierda (por ejemplo, 89 para Múnich)
Número de PABX	Se utiliza para el análisis de dígitos en llamadas entrantes. Número de centralita (número de teléfono de la centralita de la empresa, por ejemplo, 777)
Número de ubicación	Se utiliza para el análisis de dígitos de números de teléfono públicos para conexiones salientes. Comprueba la información de marcación para determinar si el número de destino llamado se encuentra en el propio sistema.
Número de estación del sistema - saliente Info: Los cambios en los números de centralita PABX salientes deben coordinarse con los proveedores de red. (Clip sin censura)	
Código de país	Se utiliza para la identificación de llamadas salientes. El código de país sin ceros iniciales (por ejemplo, 1 en EE. UU., 49 en Alemania) se transmite a la red. Si no se introduce ningún "Número de centralita saliente", se utiliza automáticamente el "Número de centralita entrante".
Código de red local	Se utiliza para la identificación de llamadas salientes. El código de área local especificado aquí (sin ceros iniciales, por ejemplo, 89 para Múnich) se transmite a la red. Si no se introduce ningún "Número de centralita saliente", se utiliza automáticamente el "Número de centralita entrante".
Número de PABX	Se utiliza para la identificación de llamadas salientes. El número de PABX especificado aquí (número de teléfono de la centralita de la empresa, por ejemplo, 777) se transmite a la red. Si no se introduce ningún "Número de centralita saliente", se utiliza automáticamente el "Número de centralita entrante".
Suprimir Stn. Número de teléfono.	Al activar esta opción, se suprime el número DID en el identificador de llamadas.
Ruta de desbordamiento	
Ruta de desbordamiento	Si todas las líneas de la ruta configurada están ocupadas, se puede establecer un desbordamiento a otra ruta. La ruta de desbordamiento solo se aplica cuando LCR está deshabilitado.
Transmisión digital	
Transmisión digital	Aquí se determina el tipo de transmisión de dígitos para la ruta seleccionada y se muestra como texto estático (por ejemplo, tabla de rutas 6: envío en bloque) en Configuración | Ruta de menor coste | Plan de marcación después de seleccionar la tabla de rutas (consulte la lista desplegable Tabla de rutas).
Transmisión digital: Dígito por dígito	Los dígitos se transmiten sincronizados con la marcación.

Parámetros	Descripción
Transmisión digital: envío en bloque	Durante la transmisión de dígitos en bloque (marcación por bloques por ruta), los dígitos marcados son almacenados en búfer por el sistema de comunicación. La marcación solo se realiza cuando ha transcurrido un tiempo después de que se haya marcado el último dígito, cuando se ha introducido el código de fin de marcación # o si se encuentra una coincidencia exacta en la regla de marcación. En el caso de PRI en los EE. UU., la marcación con bloqueo a la central telefónica es obligatoria. Es necesario activar LCR para poder seleccionar la transmisión de dígitos en bloque. El tipo de transmisión de dígitos se establece automáticamente en transmisión de dígitos en bloque en la tabla de enrutamiento si al menos una ruta de la tabla de enrutamiento LCR está configurada con transmisión de dígitos en bloque.
Número de extensión móvil (MEX)	
Número MEX	Si el ITSP que se utiliza admite la función "Extensión móvil (MEX)", se debe ingresar aquí el número MEX (8 posiciones, solo dígitos) proporcionado por el ITSP. Esta función solo puede utilizarse con una conexión de telefonía por Internet DID (SIP como ISDN). Se utiliza para integrar teléfonos móviles/teléfonos inteligentes en el sistema de comunicación. Se puede contactar al usuario del teléfono móvil a través del Servicio de Número Único mediante un único número de teléfono, que también se comunica a la otra parte. Cuando un abonado realiza una llamada con su teléfono móvil, a la otra parte se le muestra el número de oficina del abonado, por lo que el número de su teléfono móvil permanece desconocido. Además, otros suscriptores internos pueden comprobar el estado de presencia de dichos suscriptores incluso si están hablando por sus teléfonos móviles.
Usuario externo de confianza	
Usuario externo de confianza	Usuario que puede ser asignado a una plataforma de colaboración externa como MS Teams para realizar llamadas telefónicas.

Descripción de parámetros de las pestañas:

- **Cambiar parámetros de enrutamiento**

Parámetros	Descripción
Banderas de enrutamiento	
Repetición de dígitos en	Cuando se utiliza una ruta de salida con la repetición de dígitos activada, el código de enrutamiento se envía antes del número de llamada. Esto solo se aplica si LCR está desactivado (consulte Configuración | Ruta de menor coste).
Análisis del segundo tono de marcado / Monitoreo de troncales	El análisis del segundo tono de marcado alerta al sistema de comunicación para detectar un tono de marcado adicional. Esta función se utiliza con aplicaciones de sistemas de comunicación en tándem. Esta evaluación depende del país, por ejemplo, en Bélgica después del año 00 y en Francia después del 16 o el 19. Esto no es relevante en Alemania. Esto solo se aplica a los proveedores de red que envían un segundo tono de marcado para llamadas internacionales.

Parámetros	Descripción
Intercepción por dirección	Esta bandera es necesaria para la conexión en red QSIG. Cuando se activa esta bandera, el sistema de comunicación verifica si la estación remota ha recibido una solicitud de desvío o si el sistema de comunicación ha implementado la conmutación hacia adelante a la posición de intercepción central. La estación remota recibe un mensaje que le indica si debe o no implementarse un desvío para esta llamada. Si se activa la interceptación para una ruta, todas las llamadas reenviadas a esta ruta serán interceptadas en esta posición de interceptación. Para implementar esta función, se deben configurar los números de día y de noche para cada ruta (consulte Asignación de timbre por línea). Además, no se debe introducir una posición de intercepción para el servicio diurno/nocturno (véase Intercepción/Asistente).
Servicio de audio de 3,1 kHz	Para todas las llamadas salientes en ISDN, el servicio Over. El audio de 3,1 kHz es la configuración predeterminada. Este es el tipo de transmisión estándar para llamadas salientes en una línea de Red Digital de Servicios Integrados (RDSI). Una conexión desde el sistema de comunicación a una central telefónica digital con un módem analógico debe identificarse como un servicio de datos. Esta bandera debe activarse para evitar problemas durante el funcionamiento del fax. En algunos casos, un operador de red puede no admitir el servicio de portador de audio de 3,1 kHz. Esto puede provocar fallos en la transmisión de fax a determinados números de teléfono externos. Una posible solución es desactivar la **marca de servicio de audio de 3,1 kHz.**
Agregar prefijo de dirección entrante	Cuando esta opción está activada en los teléfonos del sistema con llamadas entrantes, la visualización del número de llamada se complementa con el código de ruta.
Agregar prefijo de dirección saliente	Cuando se activa esta opción con llamada saliente, la pantalla del número de llamada se complementa con el código de acceso. Información: cambiar este parámetro afecta a la identificación de la persona que llama y, por lo tanto, debe coordinarse con los proveedores de red. (Clip sin censura)
Número de llamada con prefijo internacional/ nacional	Si esta marca está habilitada, el código nacional o internacional del número de teléfono (por ejemplo, 02302…., 00492302...) debe agregarse como prefijo para el ITSP. Estándar: activado
Tono de llamada a CO	Si esta marca está activada, se enviará un "tono de llamada de retorno" a la central ISDN en una llamada entrante. Este es un protocolo especial de manejo requerido para los proveedores Global One y Sovintel.
Segmentación	Esta área define el comportamiento del sistema al enviar mensajes ISDN en los que se excede la longitud máxima de datos de usuario de capa 2 (260 bytes).
Segmentación: sí	El mensaje a enviar se divide en segmentos de 260 bytes y se envía individualmente. El sistema de comunicación receptor debe admitir la segmentación y recopilar y organizar los segmentos individuales en un mensaje.
Segmentación: no	La segmentación no es necesaria, ya que la capa 2 subyacente puede transportar mensajes de cualquier longitud.

Parámetros	Descripción
Segmentación: Mensaje truncado	El mensaje que se va a enviar se trunca a menos de 260 bytes eliminando las partes menos importantes (como los nombres, por ejemplo) y luego se envía.
Desactivar UUS por ruta	La señalización de usuario a usuario (UUS) se puede desactivar con esta marca. Esto suprime la transmisión del nombre y el número de teléfono de la estación A en el elemento UUI (información de usuario a usuario, UUI) para el desvío de llamadas externas (FWD ext.). Esta marca debe desactivarse manualmente para Telefónica.
Utilice siempre DSP	Si se activa esta marca, la conexión con el proveedor de servicios de telefonía por Internet solo es posible a través de un DSP (procesador de señal digital). Si esta marca no está configurada, entonces existe una conexión de carga útil directa con el proveedor de servicios de telefonía por Internet. Esta marca debe configurarse para la ruta de la red de OpenScape Voice. Es posible que esta marca no se configure en el caso de transmisiones de fax (T.38) a través de un dispositivo externo (por ejemplo, Mediatrix 4102).
Nombre en CO	Esta marca está configurada para CO que admiten el nombre de la parte que llama.
Intervención de troncal análoga	Aquí se pueden seleccionar varios tiempos que determinan cuándo comienza la marcación al usar líneas de acceso telefónico analógicas (MSI). Si no se ha configurado ninguna pausa, el sistema de comunicación espera hasta que reconoce el tono de marcado. Nota para Brasil: Al utilizar la señalización DTMF desde terminales analógicas junto con troncales analógicas y la emisión de pulsos de dígitos después de la detección del tono de marcado, podrían surgir problemas con la restricción de peaje cuando el código de país esté configurado en Brasil. En este caso, las señales DTMF de los terminales analógicos van directamente a los troncales analógicos ("no se utiliza el procedimiento 1A"). Debido a esto, las señales DTMF que se marcan antes de recibir el tono de marcado se pierden. En consecuencia, en estos casos, debe habilitarse el enrutamiento de menor costo (LCR) para que el método de marcación y la restricción de peaje funcionen correctamente en el dispositivo.
Pausa de llamada de troncal	La pausa de llamada CO determina el período de tiempo que transcurre antes de que una llamada se reconozca como completada una vez que el usuario haya colgado. Esta opción se aplica únicamente a las líneas MSI. Para una llamada de troncal con, por ejemplo, 1 segundo de conexión y 4 segundos de desconexión, se debe configurar una pausa de llamada de troncal de 6 segundos. Sin embargo, en algunas Cos se aplica una pausa de 10 segundos en el timbre. En estos casos, se debe programar una pausa de llamada de troncal de 13 segundos. De lo contrario, no se podrá implementar ningún desvío de llamadas. En Estados Unidos, este ciclo consiste en dos segundos encendido, dos segundos apagado, para un total de seis segundos. La opción de seis segundos es la predeterminada, por lo que no necesitará realizar ningún cambio aquí. Rango de ajuste: Entre 2 y 13 segundos.
Tipo de intervención	Este campo especifica los criterios que se aplican si el sistema de comunicación necesita tomar posesión de una línea de salida.
Tipo de intervención: cíclico	El sistema de comunicación inicia su búsqueda cíclica de una línea libre con el siguiente número de línea basado en la última línea de salida ocupada en esta ruta.
Tipo de intervención: lineal	El sistema de comunicación siempre comienza su búsqueda con el número de línea más bajo asignado a esta ruta.

Parámetros	Descripción
Tipo de ruta	Existen dos opciones para el tipo de ruta. El tipo de ruta se puede configurar como CO (Central Office) o como PABX (Private Automatic Branch Exchange).
Tipo de ruta: CO	Las líneas asignadas a esta ruta están sujetas a restricciones de peaje. Cuando LCR está activo, la restricción de peaje está regulada por el plan de marcación (columna COS).
Tipo de ruta: Centralita telefónica (PABX)	La restricción de peaje solo se realiza si hay un segundo código CO asignado a esta ruta. Cuando LCR está activo, la restricción de peaje está regulada por el plan de marcación (columna COS). El tipo de ruta también influye en el texto predeterminado del nombre de la ruta (ver Rutas), así como en el procedimiento utilizado para reconocer el tono de marcado en las líneas MSI.
No. y tipo, saliente	El administrador puede configurar por separado el "Número de PABX, entrante" y el "Número de PABX, saliente", divididos en secciones para el código de país, el código de área local y el número de PABX (= número de conexión en la red local). Esto es necesario para la implementación de la función "CLIP sin selección". Si no se ha configurado ningún "Número PABX saliente", el sistema de comunicación siempre utilizará los datos de la configuración "Número PABX entrante". En caso de una llamada entrante en una línea ISDN, el sistema de comunicación trunca el número de la centralita (alineado a la izquierda) del número de teléfono recibido e interpreta la parte restante como el número de marcación directa entrante. Para la información del número de llamada a la PSTN, el sistema de comunicación inserta automáticamente el número de la centralita (o la parte definida en la configuración) como la parte inicial del número de llamada. Esto no se aplica a la información de marcación (dirección de destino). Los números de llamada de las estaciones internas que se envían a la estación remota se pueden componer de la siguiente manera:
Número y tipo, saliente: Desconocido	Solo número DID (configuración predeterminada)
Número y tipo, saliente: Número de PABX	Número de centralita (PABX) + Número DID
Número y tipo, saliente: Código de red local	Código de área local + número de centralita telefónica (PABX) + número DID
Número y tipo, saliente: Código de país	Código de país + código de área local + número de centralita telefónica (PABX) + número DID
Número y tipo, saliente: Interna	Solo para sistemas en red: no se pueden agregar prefijos numéricos para planes de numeración cerrados. Aquí se omiten los prefijos de las llamadas.
Tipo de número de llamada	La configuración en el área "Número y tipo, saliente" también afecta a las llamadas procedentes de una extensión en un sistema asociado (un nodo en red). Debido a esta configuración, el número de la persona que llama, que se recibe del nodo de red y se reenvía a la central telefónica, se extiende para la ruta de salida.
Tipo de número de llamada: Interna	En este caso, solo se transmite el número de llamada interna. Si el destino es una estación externa, o bien no se transmite ningún número o solo se transmite el de la consola del operador. El número de llamada interna puede mostrarse cuando el destino es una estación interna en otro nodo.

Parámetros	Descripción
Tipo de número de llamada: Marcación directa	En este caso, solo se transmite el número DID. El número de llamada interna no se proporciona para su visualización en destinos internos en otros nodos. La información del número de llamada es suficiente para destinos externos.
Tipo de número de llamada: Interno / DID	Esta configuración resulta útil para fines de red. Tanto el número de llamada interno como el número de llamada DID se transmiten a la estación de destino. Si se llama a una estación interna dentro de la red, se puede mostrar el número de llamada interna de la persona que llama para esa estación. Si la estación de destino interna ha activado el desvío de llamadas a un destino externo, por ejemplo, también se puede transmitir un número DID en este caso.
Reenrutamiento	
Cambiar ruta	Cuando esta marca está activada, también es posible enrutar la información del canal D a través de otras rutas. Esta opción permite el enrutamiento alternativo a través de otras rutas. Esta opción solo podrá activarse cuando el plan de números de llamada sea inequívoco. (Numeración cerrada o códigos de intervenciones únicos en una red. El sistema que realiza la solicitud también debe admitir esto. Si se implementa el redireccionamiento, también debe configurarse el redireccionamiento con cambio de ruta activo para la ruta correspondiente. Esta opción solo está disponible para redes CorNet NQ y debe activarse de la misma manera en ambos sistemas de comunicación en red.
Optimización de ruta activa	Para optimizar el uso del canal B, se puede realizar el desvío de llamadas según el protocolo de acuerdo con la especificación "Desvío de llamadas/ Redireccionamiento parcial". Si se rechaza el redireccionamiento parcial, se utiliza la conmutación hacia adelante.
Optimización de ruta activa: No	Al seleccionar esta opción, se desactiva el redireccionamiento. Para el desvío de llamadas, la conexión siempre se establece a través de dos canales B.
Redireccionamiento activo: Si se conoce la ruta	Cuando selecciona esta opción, el redireccionamiento solo está activo si se conoce la ruta y se produce un procedimiento de "estrechamiento de conexión" exitoso entre los dos sistemas de comunicación en red.
Optimización de ruta activa: Siempre	Si la configuración para la llamada entrante llega por la misma ruta que la ruta de destino del desvío de llamadas, la llamada será rechazada (se utiliza la función de desvío de llamadas) por el sistema de comunicación si esta opción está activada. En el caso de sistemas en red, esta opción Siempre debe activarse de la misma manera en ambos sistemas de comunicación en red.

Descripción de parámetros de las pestañas:

- **Cambio de parámetro especial**

Parámetros	Descripción
Plan de numeración Define el parámetro Plan de numeración en los mensajes salientes	
Número de la parte llamada	Comprobación del sistema = definida por el sistema; Plan de numeración ISDN, Plan de numeración privado, Plan de numeración desconocido = preestablecido manualmente

Parámetros	Descripción
Todos los demás	Por ejemplo, número de la persona que llama, número de desvío, etc. Verificación del sistema = definida por el sistema. Plan de numeración ISDN, Plan de numeración privado, Plan de numeración desconocido = preestablecido manualmente
Sitio	El parámetro Sitio (ubicación) determina cómo se configura el parámetro Ubicación en el elemento de información Q931 CAUSA e Indicador de progreso. Comprobación del sistema = definida por el sistema; alternativamente, se puede realizar manualmente la configuración "Red y estación privadas" o "Estación siempre".
COLP	Si se activa esta marca, el número de la parte llamada se mostrará al llamante en el caso de una conexión CO entrante externa. La persona que llama puede ver si la llamada ha sido desviada o contestada por otra persona. Esta función también debe ser activada por la oficina central. Si la bandera está activada y se reenvía o intercepta una llamada entrante externa, el número de llamada actualizado se señala al CO en el mensaje de conexión que envía el sistema de comunicación. Si la función COLP está activada en la centralita, el número de llamada actualizado también se muestra para la persona que llama. Info: Esta marca no afecta a la visualización del número de llamada para las conexiones salientes externas.
Notificación de envío	Este mensaje se utiliza para la transmisión de información sobre el estado de la conexión actual. El mensaje puede enviarse tanto desde la red como desde el lado del suscriptor para notificar a la otra parte (red o suscriptor) sobre una conexión interrumpida, por ejemplo, o que el desvío de llamadas está activo. Si la función de notificación no es compatible con el CO, el mensaje de notificación se puede suprimir restableciendo este indicador. Si se activa esta opción, se transmite un mensaje de "Notificación" si una llamada está en espera o estacionada, por ejemplo. La notificación de envío solo se evalúa en los protocolos DSS1, NI1 y MCI. En SIP-Q, CorNet-NQ y QSIG la notificación siempre se envía.
sin CLIP	Si se activa esta bandera, se suprimirá la información de la parte que llama a la red pública para las llamadas salientes en una línea BRI o PRI. Esta marca se puede activar o desactivar para cada ruta individualmente. Además, la estación tiene la opción de suprimir la información de la persona llamada en cada llamada individualmente mediante un código de acceso o el menú telefónico del sistema.
Sin confirmación de configuración.	Si se activa esta marca, se suprime el mensaje de confirmación de configuración del sistema de comunicación a la oficina central. Relevante para COs especiales. Ejemplo: COs Fetex150 de Fujitsu.
no DIV.LEG-Info	Si se activa esta marca, la señal de información LEG de desvío estándar (número de llamada de la parte que realiza el desvío) no se envía al CO. La DIV. LEG info debe suprimirse si se producen problemas en el caso de desvío de llamadas externo (CF ext.).
Con envío completo	Si se activa esta marca, el sistema mostrará la información opcional "Todos los dígitos enviados" una vez que se hayan transmitido todos los dígitos marcados.
Llamada interna como externa	Si se activa esta bandera, las llamadas internas de la red se señalizan acústicamente de la misma manera que las llamadas externas.

Parámetros	Descripción
Sin CCNR	Si se activa esta bandera, se señala una llamada ISDN entrante con CCNR (Call Completion on No Reply) para que el sistema pueda aceptar una solicitud de devolución de llamada. Esto significa que la persona que llama puede solicitar una devolución de llamada si la emisora no responde. En algunos casos, el proveedor ISDN no admite el mensaje. En este caso, el interruptor debe activarse para evitar que el sistema envíe CCNR.

28.3.10.3 Líneas/Interconexión > Prestaciones QSIG

En un conjunto de sistemas de comunicación interconectados, los datos de comunicación recopilados en los diferentes sistemas individuales (datos GEZ) se transfieren a un sistema de comunicación determinado de la red. Para ello, en cada sistema de comunicación se configura el número de llamada del sistema de destino (número de llamada del puesto de registro central) al que se envían los datos de conexión.

Descripción de parámetros de las pestañas:

- **Editar prestaciones QSIG**

Parámetros	Descripción
Datos del sistema propio	
Número de sistema	Con estos datos se identifica el sistema de comunicación propio dentro del conjunto de red. Estos datos son válidos tanto para la señalización de ocupado central como para el encaminamiento de los datos de conexión. En un entorno de red que conste de varios sistemas de comunicación cada sistema está provisto de un número de sistema unívoco. Si el sistema de comunicación está interconectado con este tipo de sistemas de comunicación, y se desean utilizar las prestaciones QSIG, deberá administrarse aquí también el número de sistema por razones de compatibilidad. Rango de valores: de 1 a 255
Número de grupo	En los sistemas de comunicación se puede reunir a las extensiones en grupos que reciben asignado un número de grupo único. El sistema de comunicación no ofrece este tipo de formación de grupos. No obstante, por razones de compatibilidad, deben administrarse aquí también los números de grupos. Rango de valores: de 1 a 40
Señalización de ocupado para todo el sistema	
N.º sistema destino	Con estos datos se define un sistema de comunicación que implementa la señalización de ocupado central. Puede tratarse tanto de un sistema principal como de un sistema secundario. Número de sistema del sistema de comunicación configurado para la señalización central de ocupado. Rango de valores: de 1 a 255

Parámetros	Descripción
N.° llam. sistema destino	Número de teléfono del sistema de comunicación configurado para la señalización central de ocupado. Aquí debe introducirse exclusivamente el número de teléfono del sistema y no el número de la extensión. En el plan de marcación LCR, en caso de que se introduzca para ese número de teléfono del sistema, no se introduce marcación posterior. Ejemplo: Si el número de teléfono del sistema de destino es 999, la entrada del plan de marcación debe ser -999 (no -999XXX ni -999Z).
Encaminamiento de datos de comunicación	
N.° llam. sistema destino	Con estos datos se define un sistema de comunicación que implementa el registro de datos de conexión central. Puede tratarse tanto de un sistema principal como de un sistema secundario. Número de teléfono del sistema de comunicación configurado para el puesto de registro central (véase también la advertencia XXXX.

28.3.10.4 Líneas/Interconexión > Asignar MSN

Descripción de parámetros de las pestañas:

- **Mostrar MSN**
- **Editar MSN**

Parámetros	Descripción
MSN	Indicación o entrada del MSN (número de teléfono de acceso individual).
Línea	Indicación de la asignación de la línea en la que está activo el MSN.

28.3.10.5 Líneas/Interconexión > Parámetros RDSI

Mediante el intervalo de referencia (ISDN Clock) se sincronizan procesos en líneas urbanas dentro de una red determinada o de la línea urbana. Habitualmente, el sistema de comunicación busca automáticamente la línea que actúa como emisora de referencia para todos los sistemas de comunicación de una red o de la línea urbana. Si la línea de referencia de intervalos tiene una falla, hay que configurar una o varias otras como emisoras de referencia.

Para seleccionar la línea, el sistema de comunicación sigue este orden de prioridades:

1) Lista nos. autorizados
2) Línea urbana S_{2M}
3) Línea urbana S_0
4) Línea directa S_{2M} (solo configuración de esclavo)
5) Línea directa S_0

Descripción de parámetros de las pestañas:

- **Reloj RDSI**

Parámetros	Descripción
El índice	Las posiciones reflejan las prioridades 1-4 (para la lista de números autorizados) o 1-16 (para la lista de números prohibidos).
Listas de nos. permitidos	Si la lista de números autorizados tiene entradas, se anula inmediatamente la selección automática de línea del sistema de comunicación. Los puertos RDSI registrados en la lista de números autorizados (máx. 4) se utilizan en primer lugar en la búsqueda de línea de referencia de intervalos.
Listas de nos. prohibidos	Los puertos RDSI registrados en la lista de números prohibidos (máx. 16) se omiten en la búsqueda de línea de referencia de intervalos.

28.3.11 Clases de servicio

En **Clases de servicio** se reúnen las funciones para las clases de servicio de las líneas de acceso urbano. Regulan el acceso de las extensiones a conexiones externas que pueden tener gastos asociados.

28.3.11.1 Clases de servicio > Extensiones

Descripción de parámetros de la pestaña:

- **Mostrar todas extensiones**

Parámetros	Descripción
Nº llam., **Número de llamada**	Número de teléfono de la extensión.
Nombre	Nombres de la extensión.
Día	Grupo de clase de servicio seleccionado para el día.
Noche	Grupo de clase de servicio seleccionado para la noche.
Grupo de clase de servicio Día	Selección del grupo de clase de servicio para Día. La selección que realice se refiere a la tabla **Clases de servicio Día**, que permite vincular los grupos de clase de servicio con las clases de servicio en sí.
Grupo de clase de servicio Noche	Selección del grupo de clase de servicio para Noche. La selección que realice se refiere a la tabla **Clases de servicio Noche**, que permite vincular los grupos de clase de servicio con las clases de servicio en sí.

Nota: Los textos de Clase de Grupos de Servicio se generan según **Configuración Básica** asistente > **Código de país del sistema**.

28.3.11.2 Clases de servicio > Día: Grupos de clase de servicio

Descripción de parámetros de las pestañas:

- **Modificar Nombres**

- **Modificar grupo de clase de servicio**
- **Día: Mostrar miembros del grupo**

Parámetros	Descripción
Grupo de clase de servicio	Nombre personalizado para los grupos de clase de servicio 1 a 15. Asignación de accesos a la red urbana por ruta (haz de líneas) para día y noche. En la configuración de las extensiones se puede limitar el acceso a números externos mediante la asignación de grupos de clase de servicio.
Clase de servicio	Asignación de las clases de servicio a los distintos grupos de clase de servicio para servicio diurno. Todas las restricciones se aplican únicamente en líneas de una ruta del tipo Línea urbana.
Grupo de clase de servicio: Interna	La extensión solo puede efectuar llamadas internas. Valor estándar: Estándar en Grupo de clase de servicio 1
Grupo de clase de servicio: Acceso indirecto	La extensión solo puede atender llamadas externas, pero no iniciarlas. Valor estándar: Estándar en Grupo de clase de servicio 2
Grupo de clase de servicio: Lista nos. autorizados	La extensión solo puede marcar los números de teléfono externos definidos en la lista de números autorizados. Si no hay registrado ningún número se aplica el acceso indirecto a la red urbana. Valor estándar: estándar en el grupo de clase de servicio 4
Grupo de clase de servicio: Lista nos. prohibidos	El usuario no puede marcar los números de teléfono externos definidos en la lista de números prohibidos. Si no hay registrado ningún número se aplica el acceso directo a la red urbana Valor estándar: Estándar en Grupo de clase de servicio 3, 5, 6
Grupo de clase de servicio: Sin restricciones	El usuario puede aceptar y establecer, sin ningún tipo de restricción, comunicaciones externas entrantes y salientes. Valor estándar: Estándar en Grupo de clase de servicio 7 a 15
Mostrar miembros del grupo	Indicación del número de teléfono y el nombre de los miembros del grupo de clase de servicio seleccionado.

28.3.11.3 Clases de servicio > Servicio nocturno: Grupos de clase de servicio

Descripción de parámetros de las pestañas:

- **Modificar Nombres**
- **Modificar grupo de clase de servicio**
- **Noche: Mostrar miembros del grupo**

Parámetros	Descripción
Grupo de clase de servicio	Nombre personalizado para los grupos de clase de servicio 1 a 15. Asignación de accesos a la red urbana por ruta (haz de líneas) para día y noche. En la configuración de las extensiones se puede limitar el acceso a números externos mediante la asignación de grupos de clase de servicio.

Parámetros	Descripción
Clase de servicio	Asignación de las clases de servicio a los distintos grupos de clase de servicio para servicio nocturno. Todas las restricciones se aplican únicamente en líneas de una ruta del tipo Línea urbana.
Grupo de clase de servicio: Interna	La extensión solo puede efectuar llamadas internas. Valor estándar: Estándar en Grupo de clase de servicio 1
Grupo de clase de servicio: Acceso indirecto	La extensión solo puede atender llamadas externas, pero no iniciarlas. Valor estándar: Estándar en Grupo de clase de servicio 2
Grupo de clase de servicio: Lista nos. autorizados	La extensión solo puede marcar los números de teléfono externos definidos en la lista de números autorizados. Si no hay registrado ningún número se aplica el acceso indirecto a la red urbana. Valor estándar: estándar en el grupo de clase de servicio 4
Grupo de clase de servicio: Lista nos. prohibidos	El usuario no puede marcar los números de teléfono externos definidos en la lista de números prohibidos. Si no hay registrado ningún número se aplica el acceso directo a la red urbana Valor estándar: Estándar en Grupo de clase de servicio 3, 5, 6
Grupo de clase de servicio: Sin restricciones	El usuario puede aceptar y establecer, sin ningún tipo de restricción, comunicaciones externas entrantes y salientes. Valor estándar: Estándar en Grupo de clase de servicio 7 a 15
Mostrar miembros del grupo	Indicación del número de teléfono y el nombre de los miembros del grupo de clase de servicio seleccionado.

28.3.11.4 Clases de servicio > Listas de nos. permitidos

Descripción de parámetros de las pestañas:

- **Mostrar destinos marc. abr.**
- **Añadir n° de llamada**

Parámetros	Descripción
Lista 1-6	Visualizar/Añadir/Modificar/Borrar un número de teléfono autorizado. La lista de números autorizados incluye los números de teléfono a los que puede llamar el usuario. Se pueden crear hasta 6 listas de números autorizados. La primera lista de números autorizados puede tener hasta 100 entradas, las otras 5 listas pueden tener cada una 10 entradas como máximo.
Número de teléfono	Los distintos números de teléfono pueden incluir hasta 26 posiciones (dígitos del 0 al 9 y los caracteres * y #). No es necesario recoger el número de teléfono completo. Para autorizar a una extensión a marcar todos los números 08000 gratuitos, por ejemplo, solo hay que introducir aquí 0800. Como las listas solo se refieren a llamadas externas salientes, no hace falta indicar el código de ocupación de línea urbana junto con los números de teléfono registrados.

28.3.11.5 Clases de servicio > Listas de nos. prohibidos

Descripción de parámetros de las pestañas:

- **Mostrar destinos marc. abr.**
- **Añadir n° de llamada**
- **Modificar filtro de evaluación**

Parámetros	Descripción
Lista 1-6	Visualizar/Añadir/Modificar/borrar un número de teléfono prohibido. La lista de números prohibidos incluye los números de teléfono a los que no pueden llamar las extensiones. Se pueden crear hasta 6 listas de números prohibidos. La primera lista de números prohibidos puede tener 50 entradas y las otras 5 listas, 10 cada una.
Número de teléfono	Los distintos números de teléfono pueden incluir hasta 26 posiciones (dígitos del 0 al 9 y los caracteres * y #). No es necesario recoger el número de teléfono completo. Por ejemplo, para impedir que la extensión marque números 0900 (no gratuitos), basta con introducir 0900. Si se introduce almohadilla (#) al comienzo di un número prohibido, se garantiza que se implementará el control de marcación en los teléfonos del sistema cuando se ocupe una línea urbana analógica con procedimiento de marcación MF y se cambie cambiar a MF durante la marcación. Como las listas solo se refieren a llamadas externas salientes, no hace falta indicar el codigo de acceso a linea urbana junto con los números de teléfono registrados.
Modificar filtro de evaluación A través del filtro de evaluación, puede definir, en una lista de números prohibidos, qué dígitos no deberían compararse con dicha lista. Antes de evaluar la marcación, el sistema de comunicación oculta el rango de números configurado.	
A partir de la cifra ... **hasta la cifra**	El filtro de evaluación está activo en este intervalo de números (1-25) dentro del número de teléfono.
Carácter	Al prohibir los caracteres * y #, los usuarios no pueden eludir el control de marcación introduciendo esos caracteres especiales.

28.3.11.6 Clases de servicio > Lista negra

Descripción de parámetros de las pestañas:

- **Mostrar lista**
- **Añadir n° de llamada**

Parámetros	Descripción
Número de llamada	Los distintos números de llamada pueden incluir hasta 25 posiciones (dígitos del 0 al 9 y el carácter +). El carácter “+” se refiere al prefijo internacional que está configurado en el sistema y debe introducirse en la primera posición. El primer carácter de cada entrada puede ser “+” o cualquier dígito. Los números de teléfono están ordenados numéricamente en la Lista negra. Las entradas de la lista negra deben ingresarse en formato internacional (por ejemplo, 004989) o en formato internacional canónico (por ejemplo, +4989).

Parámetros	Descripción
Bloquear llamadas anónimas	Al habilitar este indicador, se bloquean las llamadas sin número de originador o con número de originador existente pero con presentación restringida.
Función lista negra activada	Habilitar este marcador bloquea los números de llamada que se añadan. La función de lista negra se basa únicamente en el número de la parte que llama (originador de la llamada) proporcionado por el proveedor.

28.3.11.7 Clases de servicio > Servicio nocturno

Descripción de parámetros de la pestaña:

- **Editar servicio nocturno**

Parámetros	Descripción
Extensiones autorizadas para servicio nocturno	Si determinadas extensiones deben poder poner el sistema en servicio nocturno, hay que incluirlas en la lista de Extensiones autorizadas para servicio nocturno. Se pueden añadir 5 extensiones como máximo. Valor estándar: 100
Extensión	Lista de todas las extensiones presentes en el sistema de comunicación.
Extensiones autorizadas	Lista de las extensiones autorizadas a activar el servicio nocturno.
Agregar >>	Añade la extensión seleccionada a la lista de extensiones autorizadas.

28.3.11.8 Clases de servicio > Asignación de grupos VBZ

Descripción de parámetros de las pestañas:

- **Editar Asignación a grupo**
- **Línea a grupo**
- **Área de marcación abreviada de grupo**

Parámetros	Descripción
Asignación de grupos VBZ	Asignación de un grupo VBZ (1-64) a una extensión. Con la asignación de grupos VBZ puede asignar a las distintas extensiones del sistema de comunicación un grupo VBZ. Al codificar la matriz de conexión, puede acceder a estos grupos y definir qué extensiones pueden ponerse en contacto con cuáles otras. De forma predeterminada, todas las extensiones están asignadas al grupo VBZ 1. De esta forma, todas las extensiones tienen acceso ilimitado a las demás extensiones. Rango de valores: 1 - 64

Parámetros	Descripción
Línea a grupo	Asignación de una línea al grupo VBZ. Con la asignación de grupos VBZ puede asignar a las distintas líneas del sistema de comunicación un grupo VBZ. Al codificar la matriz de conexión puede acceder a estos grupos y definir qué extensiones pueden acceder a qué líneas. De forma predeterminada, todas las líneas urbanas están asignadas al grupo VBZ 1. De esta forma, todas las extensiones tienen acceso ilimitado a todas las líneas, entrantes y salientes. Rango de valores: 1 - 64
Área de marcación abreviada de grupo	A cada grupo VBZ se le asigna un área de marcaciones abreviadas (KWZ). Si una extensión marca un destino de marcación abreviada, se determina el grupo VBZ correspondiente y con ello se determina si la extensión está autorizada a seleccionar ese destino. Si el destino de marcación abreviada está en el área asignada al grupo VBZ correspondiente, se realiza la marcación. Si el destino de marcación abreviada no se corresponde con el área asignada, se emite un mensaje de error. Las áreas de números de destino de marcación abreviada (KWZ) se pueden solapar en los grupos VBZ. Si embargo, no se pueden registrar destinos de marcación abreviada en los grupos VBZ ni registrar varias áreas de destinos de marcación abreviada en un grupo VBZ. Se pueden utilizar, por ejemplo: VBZ 1: 0-99; VBZ 2: 50-150; VBZ 3: 200-500. No se pueden utilizar por ejemplo: VBZ 1: 0, 5, 10; VBZ 2: 50-100, 300-500. Rango de valores: 0-7999

28.3.11.9 Clases de servicio > Matriz VBZ

Descripción de parámetros de las pestañas:

- **Cómo modificar la matriz VBZ**

Parámetros	Descripción
Matriz VBZ	Si desea editar de forma selectiva una opción de conexión entre dos grupos VBZ, haga clic en el campo en el punto de intersección de los grupos en la matriz VBZ. Haga clic varias veces en el campo para liberar o bloquear las opciones de conexión en una dirección, en la otra dirección o en ambas direcciones. Para utilizar la matriz de conexión, hay que asignar cada extensión a un grupo mediante la asignación de grupos VBZ. En el ajuste estándar, todas las extensiones y líneas están asignadas al grupo 1. El grupo 1 tiene acceso no restringido, por lo que en la configuración estándar todas las extensiones pueden acceder a todas las demás extensiones y líneas.
Cuadrícula	La matriz muestra una lista de grupos en vertical desde la parte superior y otra lista de grupos en horizontal desde la parte inferior izquierda. En cada conjunción aparece una casilla. El tipo de flecha de esta casilla indica la relación de ambos grupos entre sí. Un campo vacío indica que no se puede establecer ninguna conexión. Así, una matriz de conexión que no tuviera ninguna flecha indicaría que se trata de un sistema de comunicación totalmente inhabilitado.
Bloquear todo	La matriz VBZ suprime el tráfico entre extensiones/líneas dentro de un grupo (sistema individual) y entre los grupos.

Parámetros	Descripción
Liberar todo	La matriz VBZ permite el tráfico entre extensiones/líneas dentro de un grupo (sistema individual) y entre los grupos.
Solo interno (grupo)	La matriz VBZ solo permite el tráfico entre extensiones/líneas dentro de un grupo (sistema individual).

28.3.11.10 Clases de servicio > Servicio autom. nocturno

Descripción de parámetros de las pestañas:

- **Mostrar todos los días**
- **Modificar día**

Parámetros	Descripción
Lunes, Martes, Miércoles, Jueves, Viernes, Sábado, Domingo, Día especial	Día que se ha configurado a través del plan horario. El plan horario incluye toda la semana (de lunes a domingo y días especiales. Los días especiales son festivos o días especiales como, por ejemplo, vacaciones.
Zona	El plan horario de un día puede dividirse en hasta 4 zonas (intervalos horarios). Las zonas pueden sucederse de forma continua de forma que, por ejemplo, la hora de fin del primer intervalo coincida con la hora de inicio del segundo. Un intervalo no puede tener la misma hora de inicio y de fin. La duración mínima de un intervalo son 15 minutos. Rango de valores: 1-4
Inicio	Hora de inicio de la zona. Si el primer intervalo de un día comienza a las 0:00 horas, la hora de inicio se debe indicar con el formato 00:00.
Fin	Hora de fin de la zona. Si el último intervalo de un día termina a las 24:00 h (12 pm), hay que indicar 23:59 (11:59) como la hora de fin.
Noche N° llam.	Número de teléfono nocturno para la zona. Si no se introduce ningún número para la noche, en el sistema se activa el servicio nocturno por línea. Los destinos se configuran en **Líneas/Interconexión** > **Editar línea** > **Asignación de llamadas por línea**. Las horas registradas a través del servicio nocturno automático rigen para todas las líneas.
OK	Se configura la línea.
Eliminar	Se elimina la zona definida.
Servicio copiar	Puede copiar las zonas configuradas a uno o más días seleccionando el día que desee al día especial seleccionando la bandera respectiva o todos a todos seleccionando **Comprobar todo**. Cuando presiona **Aplicar**, la configuración de zona en los días que ha seleccionado se sobrescribirá con las zonas configuradas en el día actual.

28.3.11.11 Clases de servicio > Días especiales

Descripción de parámetros de la pestaña:

- **Editar días especiales**

Parámetros	Descripción
Día	Al seleccionar una fecha en el calendario se registra aquí automáticamente.
Nombre	Nombre del día especial (p. ej. Día de la Constitución)

28.3.12 Conexiones

Las funciones para equipos auxiliares como Música en Espera (MoH), configuración de Anuncios o para conectar un portero automático como Abrepuertas en los puertos del sistema (troncales), se agrupan en **Equipos Auxiliares**.

28.3.12.1 Equipo auxiliar > Música en espera

Descripción de parámetros de las pestañas:

- **Editar música en espera**

Parámetros	Descripción
Tipo de MOH	El tipo de parámetro MOH le permite elegir entre tres opciones posibles. La música para esta función se puede suministrar interna o externamente.
Tipo de MOH: Sin música en espera	Si se selecciona esta opción, la función Música en espera se desactivará por completo. Esto no se aplica cuando una llamada externa se transfiere mediante una transferencia antes de la respuesta; la persona que llama entonces escucha el tono de llamada.
Tipo de MOH: MOH sin tono de llamada	Si se selecciona esta opción, en el caso de una transferencia sin máscara, la persona que llama escuchará música en espera mientras se realiza la transferencia, así como mientras la llamada está siendo transferida por la parte que transfiere y la conexión externa está sonando en el destino transferido.
Tipo de MOH: MOH con tono de llamada	Si se selecciona esta opción, en el caso de una transferencia sin máscara, la persona que llama escuchará música en espera mientras se realiza la transferencia. Tan pronto como la llamada es transferida por la parte que transfiere y la conexión externa está sonando en el destino transferido, la persona que llama escuchará un tono de llamada. La opción de MOH con tono de llamada siempre debe configurarse en un sistema de red para brindarle al cliente un entorno uniforme. ¦Si la persona que llama llega al sistema a través de un proveedor de servicios de telefonía por Internet (ITSP), esta opción no se aplicará y la persona que llama escuchará música en espera durante la transferencia.

Acceso y activación de tipos mediante Manager E.

El formato de entrada para Música en espera es un archivo wave con PCM y 16 bits. Las frecuencias de muestreo admitidas son 8, 22,05, 24, 32, 40, 44,1 y 48 kHz en mono o estéreo. El formato preferido es PCM, 16 bits, 8 kHz, mono. Se recomienda usar el formato de entrada preferido y limitar la duración de los archivos wave a aproximadamente 2 minutos. Es posible configurar un MOH para el día y otro para la noche. Es necesario reiniciar.

28.3.12.2 Equipo auxiliar > Correo telefónico

Descripción de parámetros de las pestañas:

- **Editar correo telefónico**

Parámetros	Descripción
Acceso a devolución de llamada al correo telefónico	Establecer el **número de llamada** y **Nombre** del dispositivo.
Dispositivo de grabación en vivo	Establecer el **número de llamada** del dispositivo.

28.3.12.3 Anuncios > de equipos auxiliares

Descripción de parámetros de las pestañas:

- **Editar anuncios**

Parámetros	Descripción
Archivo WAVE	Aquí puede seleccionar el archivo WAVE (.wav) para un anuncio específico (consulte Configuración > Anuncios > Cargar en el Gateway).

Parámetros	Descripción
Acceso	La conexión se define a través de Access. Aquí puede seleccionar el puerto (analógico SLA o EVM) al que está conectado este dispositivo. **Consejo:** A los puertos analógicos que se configuran como puertos de anuncios se les debe asignar el valor "Contestador automático" en **Modo Experto** > **Servidor de Telefonía** > **Estaciones** > **Analógicas** > **Editar** > **Tipo de Extensión**, como se describe en Parámetros de la estación. Los destinos externos se pueden utilizar para direccionar dispositivos de anuncio en otro nodo del sistema. Para ello, el dispositivo de anuncio se identifica como externo. Aquí se introduce el número de llamada de un puerto de anuncio en otro nodo del sistema. **Consejo:** Esta lista de equipos se refiere a la configuración de **Anuncio**, en **Modo experto** > **Servidor de telefonía** > **Llamadas entrantes** > **UCD** > **Editar parámetros del grupo UCD**, como se describe en Llamadas entrantes > UCD. Si selecciona **Destino externo** aparecen los dos campos siguientes: • **Ruta** (grupos troncales) • **Número de llamada** (dispositivo)

Parámetros	Descripción
Tipo	Puede seleccionar uno de los siguientes tipos de anuncios en el menú desplegable: • **Ninguno**: El equipo de anuncios no está conectado. • **Anuncio**: Permite la conexión de un solo dispositivo de anuncio externo a través de puertos SLA o tarjetas EVM. El anuncio proporcionado por el dispositivo de anuncio activado debe tener un inicio y un final fijos. Este dispositivo no debe reenviar la llamada una vez finalizado el anuncio (no se debe introducir un destino de conmutación). El puerto del dispositivo de anuncio correspondiente se ingresa en **Acceso**). Equivalente a **inicio/ parada** para dispositivos de destino externos. • **Música en espera**: Se repite continuamente un anuncio o música. También se pueden conectar llamadas en cola mientras se reproduce la música o el anuncio. La conexión es posible a través de puertos SLA o tarjetas EVM. El puerto del dispositivo de anuncio correspondiente se ingresa en **Acceso**. Equivalente a **continuo** para dispositivos de destino externos. • **Música interna**: Activa la música en espera interna del sistema en el sistema de comunicación. Para esta opción, se debe ingresar **Ninguno** en **Acceso**. Se escucha el MOH externo (configuración del administrador E) si se define como destino en el sistema de comunicación. Las entradas en **Acceso** no tienen efecto en ninguna de las variantes. • **PC multimedia**: Esta configuración está predefinida. La PC multimedia o la aplicación de control controla si la persona que llama escucha el anuncio desde el principio o está conectada a un anuncio en curso. • **Reproductor de anuncios**: El reproductor de anuncios es un programa de software interno que está disponible junto con la funcionalidad UC Booster (UC Booster Card o UC Booster Server). **Nota:** La funcionalidad del reproductor de anuncios solo está disponible en el modo UC Suite.
Modo	Puede seleccionar una de las dos opciones siguientes: • **iniciar/detener**: reproducción única • **continuo**: reproducción continua

Nota: El asistente de **Música en espera / Anuncios** también se puede utilizar para configurar **Anuncios**. Para obtener más información, consulte Cómo configurar anuncios.

28.3.12.4 Equipo auxiliar > Abridor de puerta

Descripción de parámetros de las pestañas:

- **Editar abridor de puertas**

Parámetros	Descripción
Extensión	Selección del número de teléfono / puerto de conexión del portero automático. El tipo de puerto de la estación debe ser P.O.T o Sin puerto.

Parámetros	Descripción
Destino	Selección del número de teléfono/puerto de conexión del destino del timbre del teléfono de entrada. Se puede especificar un número de estación o un número de grupo como destino de timbre en el que se señaliza un timbre especial cuando se presiona el botón del timbre. La llamada se señaliza de acuerdo con los algoritmos de reenvío de llamadas definidos en "Configuración - Llamadas entrantes".
Abridor de puertas	Activa la función de apertura de puerta. Al activar esta bandera se puede activar un abridor de puertas conectado al TFE-S para las estaciones.
DTMF	Al configurar esta bandera se permite activar el abridor de puerta de forma remota con un transmisor DTMF.
Reenviar	La configuración de esta bandera habilita el reenvío externo del destino del timbre del teléfono de entrada.

28.3.12.5 Equipo auxiliar > SmartVM

Descripción de parámetros de las pestañas:

- **Editar buzones SmartVM**

Parámetros	Descripción
Número de llamada del buzón.	Introducción de los números de teléfono de buzón. Un buzón de voz se identifica mediante el número de llamada del buzón de voz. Si se tiene que asignar un buzón de voz a una extensión, hay que asignar al buzón de voz el mismo número de llamada que la extensión.
Nombre	Visualización del nombre del buzón. El nombre se corresponde con el nombre de la extensión (si la hay). Para un grupo se indica el nombre del grupo.
Saludo	Selección del saludo. La utilidad de las entradas ofrecidas depende del menú telefónico (TUI) seleccionado. Con OSO TUI solo se admite el Saludo 1 para los buzones estándares.
Saludo: **Saludo 1-4**	La selección de los saludos 1-4 depende del tipo del buzón: Buzón de voz predeterminado: Saludo 1 o 2 (con OSO TUI solo Saludo 1) Buzón de puesto de operadora: Saludo 1, 2, 3 o 4
Saludo: **Día/Noche**	El saludo depende del servicio diurno/nocturno: Día - Saludo 1 / Noche - Saludo 2
Saludo: **Tipo de llamada**	Solo para buzón predeterminado: el saludo depende del estado de la extensión: Llamada no aceptada - Saludo 1 / Ocupado - Saludo 2
Saludo: **Ninguno**	No se reproduce ningún saludo. No obstante, el buzón sigue activo, por ejemplo para una transferencia de la llamada al puesto de interceptación.

Parámetros	Descripción
Grabación	Si este flag está activado, el buzón es un buzón predeterminado. En este caso no puede ser un buzón de puesto de operadora. Si el flag está desactivado (valor estándar), el buzón no puede reproducir un mensaje. El usuario puede activar la grabación la primera vez que consulte su buzón. De esta forma se garantiza que no se puedan grabar mensajes antes de la primera inicialización. Estándar: activado
AutoAttendant	Si este flag está activado, el buzón es un buzón de puesto de operadora (AutoAttendant). En este caso no puede ser un buzón predeterminado. Se pueden configurar como máximo 100 buzones de voz como buzones de puesto de conmutación. Al modificar un buzón de voz estándar a un buzón de voz con la función puesto de conmutación (AutoAttendant) se borran todos los mensajes del buzón de voz. Estándar: desactivado
Restablecer contraseña	Si este flag está activado, la contraseña del buzón se restablece a `123456`. El usuario debe modificar la contraseña cuando vuelva a acceder a su buzón. Estándar: desactivado

Descripción de parámetros de las pestañas:

- **Editar parámetros de SmartVM**

Parámetros	Descripción
Parám. generales	
Long. máx. núm. buz. voz	Longitud máxima del número de llamada del buzón de voz. Rango de valores: 2 - 16 posiciones; valor estándar: 3 posiciones
Longitud de mensaje máx. (min)	Duración máxima de un mensaje. Rango de valores: 1 o 2 minutos; valor estándar: 2 minutos
Limitación longitud nº llamada	En el caso de las conexiones salientes iniciadas por el SmartVM (Marcación posterior de AutoAttendant o Marcación abreviada de AutoAttendant) solo se pueden marcar números de teléfonos que no superen la longitud indicada. Si hay números de teléfono configurados más largos, no se establece la conexión. De forma predeterminada, la limitación de longitud del número de llamada se corresponde con la longitud de los números de teléfono del buzón (longitud de números de llamada internos), de forma que solo se permite la marcación interna. Rango de valores: de 2 a 30, valor estándar: 3
Dest. interc. fax general	Introducción del destino de intercalación de fax al que el SmartVM enviará los faxes entrantes de forma predeterminada. Si no se indica ningún destino de intercalación de fax, los faxes entrantes se rechazan. Rango de valores: máx. 16 cifras
Idioma estándar	Selección del idioma para la interfaz de usuario. Se aplica a todos los buzones. Si la interfaz no está disponible en el idioma deseado, el idioma se restablece a inglés del Reino Unido (enuk).

Parámetros	Descripción
Interfaz de usuario telefónico	Selección de la estructura del menú telefónico del buzón de voz (Telefone User Interface, TUI). La selección se aplica a todos los buzones.
Menú telefónico (Telephone User Interface, TUI): **SmartVM**	SmartVM TUI, EVM TUI (predeterminado).
Menú telefónico (Telephone User Interface, TUI): **OSO**	OSO TUI, similar a la UC Suite TUI.
Orden de fecha de anuncio	Solo visible con SmartVM TUI: Configuración de la secuencia de anuncios grabados para mensaje, fecha de grabación y número de teléfono del llamante (si se conoce).
Anuncio de orden de fecha: **Fecha después de mensaje**	Solo visible con SmartVM TUI: Mensaje -- Fecha de grabación -- Número de teléfono del llamante (si se conoce).
Anuncio de orden de fecha: **Fecha antes de mensaje**	Solo visible con SmartVM TUI: Fecha de grabación -- Número de teléfono del llamante (si se conoce) -- Mensaje. En los mensajes de extensiones internas: Nombre de la extensión interna (en su caso) -- Fecha de grabación -- Número de teléfono del llamante (si se conoce) -- Mensaje.
Cantidad de mensajes por buzón	Número máximo de mensajes para un buzón. Rango de valores: de 0 a 100, valor estándar: 30
Desactivación de EVM	Si este flag está activado, el SmartVM está desactivado. Estándar: desactivado
Permitir devolución de llamada desde VM solo a números conocidos	Cuando el UsuarioA externo llamada al UsuarioB, el UsuarioB tiene un desvío de llamadas a su buzón de voz, el UsuarioA externo deja un mensaje de voz, el UsuarioB llama a SmartVM, introduce su contraseña y, mientras escucha el mensaje, marca el dígito "8". Al marca este número, se produce una devolución de llamada al UsuarioB. Si este flag está activado, la devolución de llamada sucede si el número del UsuarioB pertenece a los números conocidos. Los números conocidos son el número de teléfono móvil y el número de teléfono de domicilio/externo de los detalles del perfil de Administración de usuarios (Aplicaciones-UC Smart-Administración de usuarios) Estándar: activado
Comportamiento AA VP Permite configurar si el AutoAttendant reproducirá automáticamente anuncios grabados en determinados casos.	
VP antes de transferencia	Si este flag está activado, en el caso de "VP antes de transferencia" se reproduce el siguiente anuncio grabado: "Espere, por favor, está siendo conectado..." Estándar: desactivado

Parámetros	Descripción
Resultado de transferencia VP	Si este flag está activado, en el caso de "Resultado de transferencia VP" se reproduce uno de los siguientes anuncios grabados: "El número del usuario no existe." "El usuario está ocupado." "El usuario no contesta." Estándar: activado
Interceptación VP	Si este flag está activado, en el caso de "Interceptación VP" se reproduce uno de los siguientes anuncios grabados: "Está siendo conectado con el operador. Espere, por favor." "Está siendo conectado con el buzón de voz del usuario." "Espere, por favor, está siendo conectado..." Estándar: activado
VP antes de activación	Si este flag está activado, en el caso de "VP antes de activación" se reproduce uno de los siguientes anuncios grabados: "Vuelva a llamar más tarde." "Muchas gracias. Hasta luego". "El número del buzón de voz no es válido." Estándar: activado

Descripción de parámetros de las pestañas:

- **Editar parámetros de operadora automática**

Parámetros	Descripción
Número de llamada	Número de teléfono del AutoAttendant (valor estándar: 352).
Interceptar después de anuncio	Si este flag está activado, después del anuncio grabado de saludo la llamada se intercepta al puesto de interceptación (p.ej., puesto de operadora). Durante el mensaje de saludo no es posible seleccionar un destino de marcación abreviada. Estándar: desactivado
ninguna marcación de sufijo	Si este flag está activado, el llamante solo puede ser desviado a otros destinos mediante la marcación de los destinos de marcación abreviada. El llamante no puede marcar números de varias posiciones. Estándar: desactivado

Descripción de parámetros de las pestañas:

- **Editar marcación abreviada/Dest. interceptación Día**
- **Editar marcación abreviada/Dest. interceptación Noche**
- **Editar marcación abreviada/Dest. interceptación 3**
- **Editar marcación abreviada/Dest. interceptación 4**

Parámetros	Descripción
Seleccionar	Selección de una extensión interna (1.ª mitad de la lista) o de un buzón de voz (2.ª mitad de la lista) como destino de marcación abreviada o puesto de interceptación.
Acción	Visualización de los 10 destinos de marcación abreviada posibles y del puesto de interceptación.
Número de llamada	Número de teléfono de la extensión seleccionada o del buzón de voz seleccionado.
Nombre	Nombre de la extensión seleccionada o del buzón de voz seleccionado.
Tipo	Selección del tipo del número de teléfono.
Tipo: **Número de llamada**	Aquí se llama a la extensión seleccionada con el dígito de marcación abreviada asignado.
Tipo: **Buzón**	Aquí se llama al buzón de voz seleccionado con el dígito de marcación abreviada asignado.

28.3.13 Payload

En **Payload** se reunen las funciones para la muestra y configuración de tipos de conexión y protocolos.

28.3.13.1 Payload > Dispositivos

Descripción de parámetros de las pestañas:

- **Mostrar ajustes globales dispositivo**
- **Reponer ajustes dispositivo a estado de suministro**

Parámetros	Descripción
Gateway global tipo G.711	Dispositivos es el término conjunto para extensiones, prestaciones y funciones que necesitan canales. Aparecen indicados el tipo de códec del gateway global, el número máximo de canales B disponibles y con registro de licencia y el número máximo de clientes LAN en un canal para música en espera (las llamadas que superen ese número no se transfieren).
Cant. máx. canales B de hardware	
Cant. clientes LAN en un canal MoH	

Para restablecer los ajustes del dispositivo hay que reiniciar el sistema de comunicación.

28.3.13.2 Payload > Media Stream Control (MSC)

Descripción de parámetros de las pestañas:

- **Editar parámetros jitter MSC**

Parámetros	Descripción
	El Media Stream Control (MSC) controla y administra los flujos de medios distribuidos por el sistema de comunicación. Se encarga de la transmisión de datos multimedia entre redes a través de gateways (TDM/IP).
Estadística tráfico (solo SNMP)	Se requiere para acceder a los datos de las estadísticas por llamada del sistema por SNMP.
Intervalo para generación de paquetes RTCP (s)	Intervalo de informe (en segundos) para paquetes RTCP (Real-time Transport Control Protocol) para gestionar y mantener los parámetros de calidad del servicio (QoS) en el intercambio periódico de mensajes de control entre remitente y destinatario). Rango de valores: de 5 a 10, valor estándar: 5

Descripción de parámetros de las pestañas:

- **Reponer ajustes MSC a estado de suministro**

Parámetros	Descripción
Reponer ajustes MSC a estado de suministro	Recuperación de todos los ajustes MSC originales.

28.3.13.3 Payload > Módulos hardware

Mantenimiento de los módulos DSP del sistema de comunicación

Descripción de parámetros de las pestañas:

- **Mostrar todos mód. hardware**
- **Editar ajustes DSP**
- **Editar ajustes jitter DSP**

Parámetros	Descripción
Tipo hardware	Indicación de los DSP (procesadores de señal digital) que se utilizan en el sistema de comunicación. Opciones: • **OnBoard** = DSP integrado de la placa base • **OCCB X-1** = DSP de un submódulo OCCB (OCCB1 u OCCB3)
Versión de firmware	Versión de firmware actual de los distintos DSP
Versión API	Versión actual de API (Application Programming Interface) de cada DSP
General	
Dirección IP	Dirección IP del módulo DSP (se puede modificar si la dirección IP ya está asignada). ***Aviso:*** El último octeto de la dirección IP no puede ser .1 (xxx.xxx.xxx.1)
Puerto	Número de puerto del módulo DSP
Mecanismo de estado	Permite determinar la disponibilidad de los DSP Valor estándar: Mensaje de estado

Parámetros	Descripción
Compensador eco	Si el flag está activado, se suprime el efecto eco en las transmisiones de voz. Valor estándar: Activado
Señaliz. fuera de banda MF	Si el flag está activado, las señales MF se transmiten en el canal de señalización independiente (outband). Valor estándar: Desactivado
Parámetros fax	
Cant. paquetes redundantes	Definición del número de paquetes de redundancia: cuando mayor sea este valor, más sólida será la transferencia de fax frente a eventuales pérdidas de paquetes. La desventaja de un uso de valores elevados es que se requiere mayor ancho de banda. Valor estándar: 2
Jitter máx. red (hex. ms)	Definición del jitter máximo de red en milisegundos: cuanto mayor sea este valor, mayor será el posible retardo del tiempo de ejecución de los paquetes de datos en las redes. Solo se pueden usar valores hexadecimales compuestos de los números 0 a 9 de las letras A a F. Si es posible, en este parámetro no debería hacerse ningún cambio. Valor estándar: 00C8
Expiración(es) de detección de tono de fax/módem	Definición del tiempo en milisegundos para la detección de tonos de fax durante una conexión. Garantiza una conmutación al protocolo de fax T.38. Una vez terminado el tiempo definido aquí se dejan de detectar tonos de fax. Si el valor es cero, la detección de tonos está activa durante toda la conexión. Valor estándar: 0
Jitter DSP	
Tipo búfer jitter	Definición del tipo de búfer jitter Valor estándar: Autoadaptable
Tipo búfer jitter: Estática	El retardo medio del búfer jitter siempre es el mismo.
Tipo búfer jitter: Autoadaptable	El búfer jitter ajusta el retardo medio a la recepción de datos. Se intenta mantener el retardo al mínimo posible y perder también los mínimos paquetes de datos posibles.
Retardo medio de voz (ms)	Definición del tiempo en milisegundos que se mantendrá en el búfer jitter un paquete como media en las transmisiones de voz basadas en IP. ***INFO:*** Con el ajuste **Tipo búfer jitter Autoadaptable**, el valor definido aquí solo es un valor inicial. Valor estándar: 40

Parámetros	Descripción
Retardo máx. de voz (ms)	Definición del tiempo máximo en milisegundos para el retardo de voz **Tipo búfer jitter Estática**: Hay que indicar cuántos milisegundos puede tener un retardo medido al recibir paquetes IP con transferencia de voz antes de que el búfer jitter intervenga para regular el flujo de datos. Con el búfer jitter estático, 80 es el valor recomendado para la mayoría de entornos. **Tipo búfer jitter Autoadaptable**: Hay que indicar cuántos milisegundos puede tener el retardo máximo de voz como promedio. Si el retardo medido supera este valor, se pierden paquetes. Con el búfer jitter autoadaptable, 120 es el valor recomendado para la mayoría de entornos. ***Aviso:*** El valor siempre debe ser superior al indicado en el campo de retardo medio de voz (ms). Valor estándar: 120
Retardo mín. de voz (ms)	Definición del tiempo mínimo en milisegundos para el retardo de voz **Tipo búfer jitter Autoadaptable**: Hay que indicar cuántos milisegundos puede tener como mínimo el retardo medio de voz . El retardo medio siempre debe ser igual o mayor que este valor. Valor estándar: 20
Pérdida paquetes/ preferencia retardo	Se define la relación entre pérdida de paquetes y retardo de tiempo de ejecución de los paquetes de datos **Tipo búfer jitter Autoadaptable**: Hay que indicar un valor entre 0 y 8. El valor depende de si en caso de grandes retardos de tiempo de ejecución se procede a la pérdida de paquetes o a aumentar el retardo. El valor 0 significa una pérdida de paquetes mínima, a costa de retardos en el tiempo de ejecución. El valor 8 significa un retardo mínimo en el tiempo de ejecución, a costa de posibles pérdidas de paquetes. Un valor recomendado para la mayoría de entornos es 4. Valor estándar: 4
Retardo medio de datos (ms)	Definición del retardo medio para datos, en milisegundos Hay que indicar cuántos milisegundos se retendrá como media un paquete de datos en el búfer jitter para las transmisiones de datos. Un valor recomendado para la mayoría de entornos es 60. Valor estándar: 60
Retardo máx. de datos (ms)	Definición del retardo máximo para datos, en milisegundos Hay que indicar cuántos milisegundos puede tener un retardo al recibir paquetes IP antes de que el búfer jitter intervenga para regular. Un valor recomendado para la mayoría de entornos es 200. ***INFO:*** Los valores mayores (a partir de aprox. 2000) no tienen efecto. En cuanto se ha terminado de recibir un paquete en la memoria intermedia, vuelve a abandonarla. Pueden indicarse valores por debajo de 100 ms, pero no es recomendable hacerlo en la práctica. Valor estándar: 200

28.3.14 Estadísticas

En **Estadísticas** se reunen las funciones de muestra de estadísticas.

28.3.14.1 Estadísticas > Estadísticas de gateway > Placa base > Estadísticas disposit.

Descripción de parámetros de las pestañas:

- **Mostrar estadística SCN**
- **Mostrar estadística LAN**

Parámetros	Descripción
Tipo disposit.	Muestra los componentes LAN y SCN (Switched Circuit Network) existentes.
Recursos ocupados actualmente	Muestra los recursos de un componente asignados actualmente (canales configurados y en uso).
Total	Muestra el total de recursos asignados actualmente.
Actualización autom.	La presentación se actualiza automáticamente cada 60 segundos.
Segundos hasta la próx. actualiz.	Muestra una cuenta atrás de 60 segundos.
Extensión DDS1	Tan pronto como un teléfono móvil se encuentre en el área de otro puesto de conmutación radiotelefónico (módulo Cordless anfitrión), se activará un enlace de prolongación a través de una conexión DSS1 iniciada por el módulo Cordless. Por lo tanto, Ext. DSS1 se refiere a la cantidad de teléfonos móviles o conexiones DSS1 establecidas en el conmutador.
Idioma HFA / IP-Networking	Este componente SCN muestra el número de canales DSP ocupados cuando se establecen las llamadas al gateway.
Música en espera	Cuando la función DMC-Interworking está activa en una red IP, las conexiones de gateway se configuran a través de canales DMC. Desde la perspectiva del usuario, un canal DMC es un canal de gateway que proporciona una conexión de gateway.
SIU	La unidad de señalización (SIU) reserva un canal DSP utilizado para detectar o generar tonos del sistema, como tonos DTMF
DMC	Muestra una cuenta atrás de 60 segundos.
H.323 (RTP)	Muestra los recursos usados en una llamada de voz.
Fax T.38	Muestra los recursos usados en una conexión de fax.
PPP	Muestra los recursos usados en una conexión de centralita RDSI.

28.3.14.2 Estadísticas > Estadísticas de gateway > Placa base > Estadísticas MSC

Descripción de parámetros de las pestañas:

- **Mostrar estadística global**

  Estadísticas MSC son estadísticas del flujo de medios que se implementa en procesadores digitales de señal entre IP y TDM (Media Stream

Control). La estadística global MSC ofrece una visión general de los datos estadísticos de todas las llamadas registradas. Ofrece información sobre los paquetes RTP/TCP enviados y no enviados, sobre los paquetes recibidos y no recibidos y sobre el número de bytes enviados y recibidos.

Descripción de parámetros de las pestañas:

- **Mostrar estadística llam. indiv.**

  La estadística de llamada individual MSC muestra en forma de tabla los parámetros y los datos de conexión que se utilizan para las conexiones que implican conversiones con procesadores digitales de señal. Se utiliza para que los expertos realicen análisis de datos.

28.3.14.3 Estadísticas > Estadística SNMP

Descripción de parámetros de las pestañas:

- **Mostrar tabla estadísticas**
- **Mostrar estadísticas**

Parámetros	Descripción
Estadística tablas "if"	Los datos registrados en SNMP sobre las distintas interfaces (if = interfaz) del sistema de comunicación, por ejemplo, interfaces Ethernet.
Estadística IP	Detalles y errores del encaminamiento IP
Estadística TCP	Detalles y errores del protocolo TCP
Estadística UDP	Detalles y errores del protocolo UDP

28.3.14.4 Estadísticas > Estadísticas de telefonía > Textos del sistema

Descripción de parámetros de las pestañas:

- **Mostrar textos del sistema**

Parámetros	Descripción
Idiomas disponibles	Indicación de los idiomas disponibles en el sistema de comunicación para los displays de los teléfonos

28.3.14.5 Estadísticas > Estadísticas de telefonía > Agentes UCD

Descripción de parámetros de las pestañas:

- **Mostrar agentes UCD**

Parámetros	Descripción
Cantidad de agentes UCD	
Total	Número total de los agentes UCD que han iniciado sesión en el sistema de comunicación

Parámetros	Descripción
Disponible	Número de agentes UCD disponibles
Estado de agentes UCD	
Número de teléfono	Número de teléfono del agente UCD
Nombre	Nombre del agente UCD
ID	Identificador del agente UCD
Grupo UCD	Grupo UCD al que está asignado el agente UCD.
Estado	Estado del agente UCD

28.3.14.6 Estadísticas > Estadísticas de telefonía > Estado de línea

Descripción de parámetros de las pestañas:

- **Mostrar estado de línea**

Parámetros	Descripción
Fecha	Fecha de la consulta de estado o del último cambio de estado de la línea
Hora	Hora de la consulta de estado o del último cambio de estado de la línea
Ranura/Puerto	Indicación del módulo, de la ranura y de la interfaz (puerto) o de la interfaz LAN
Ruta	Muestra el nombre de la ruta para ofrecer una mejor idea de a qué ITSP pertenece una línea.
Número de troncal	Código de línea
Comentario	Estado de la línea (aparece el último estado de la línea.) Estos son los estados de línea posibles: • **Reposo** (Línea en reposo) • **Aviso** (llamada en curso) • **Conectado con:** (conexión con el número de teléfono mostrado) • **Línea bloqueada** • **Línea ha fallado**

28.3.14.7 Estadísticas > Estadísticas de telefonía > Desvío

Descripción de parámetros de las pestañas:

- **Mostrar desvíos**

Parámetros	Descripción
Desvío de llamadas	

Parámetros	Descripción
Estado	Estado del desvío de llamadas: • **desactivado** (ningún desvío de llamadas activo) • Si el desvío de llamadas está activo, se muestra el tipo del desvío de llamadas y el destino del desvío.
Destino de desvío de	Indica si la extensión es el destino del desvío de llamadas de otra extensión. Se muestran el número de teléfono y el nombre de la extensión que hace el desvío.
Timbre adicional act.	
Exts.con señal.timbre	Número de teléfono y nombre de las extensiones con timbre
Conex. señal. timbre de	Se indica si la extensión es el destino de timbre de otra extensión. Se muestran el número de teléfono y el nombre de la extensión del timbre.

28.3.14.8 Estadísticas > Estadísticas de telefonía > Extensiones

Descripción de parámetros de las pestañas:

- **Mostrar parámetros de extensión**
- **Mostrar prestaciones activadas**

Parámetros	Descripción
Número de teléfono	Número de teléfono de extensión
Nombre	Nombre de la extensión
Marcación directa	Número de marcación directa de la extensión
Tipo disposit.	Tipo del teléfono, por ejemplo, OpenStage 60
Clip/Lin	Location Identification Number LIN Solo para EE. UU., Canadá: Con el servicio de emergencia avanzado E911, al realizar una llamada de emergencia se transfiere, además del número de teléfono, informaciones sobre la ubicación geográfica del llamante. Para ello, a cada conexión de extensión con números de marcación directa válidos se le asigna una LIN.
Acceso	Con teléfonos analógicos y $U_{P0/E}$, indicación del módulo, del slot y del número de la conexión. En los teléfonos $U_{P0/E}$ se indica además si es un maestro o un esclavo. Con teléfonos IP, indicación de la interfaz LAN, del tipo y del número
Parámetros	
Tipo de ext.	Tipo de extensión, por ejemplo, Estándar o Fax Valor estándar: Estándar
Idioma	Ajuste de idioma del teléfono

Parámetros	Descripción
Señalización de llamadas internas	Tipo de llamada para señalizar llamadas internas Valor estándar: Tipo. llam. 1
Señalización de llamadas externas	Tipo de llamada para señalizar llamadas externas Valor estándar: Tipo. llam. 1
Clase de servicio (LCR)	Clase de servicio de la extensión para Least Cost Routing Valor estándar: 15
Tipo de licencia	Tipo de licencia de la extensión
Prestaciones	
No molestar	Estado de la prestación No molestar Valor estándar: Desact.
Texto de respuesta	Estado de la prestación Texto de respuesta Valor estándar: Desact.
Candado telefónico	Estado de la prestación Candado telefónico Valor estándar: Desact.
Supresión de indicación n.º de llamada act.	Estado de la prestación Supresión de indicación n.º de llamada act Valor estándar: Desact.
Timbre adicional act.	Estado de la prestación Timbre adicional Valor estándar: Desact.
Activar reposo	Estado de la prestación Llamada silenciosa / reposo Valor estándar: Desact.
Línea colectiva/grupo	Estado de la prestación Línea colectiva/Llamada de grupo Valor estándar: Desact.
Aviso de llamada en espera silencioso	Estado de la prestación Aviso de llamada en espera silencioso Valor estándar: Desact.
Contestación directa	Estado de la prestación Contestación directa Valor estándar: Desact.
Liberar para aviso llam. en espera	Estado de la prestación Liberar para aviso llam. en espera Valor estándar: Desact.
Desvío de llamadas tras tiempo	Estado de la prestación Call diversion (desvío de llamadas) tras tiempo Valor estándar: Desact.
AUL	Estado de la prestación Desvío de llamadas (AUL) Valor estándar: Desact.

28.4 Aplicaciones

En **Aplicaciones** se reunen las funciones para configurar el Application Server para Comunicaciones Unificadas y para Web Services.

28.4.1 Selección de aplicación

En **Selección de aplicación** se agrupan funciones para seleccionar la solución utilizada de Comunicaciones Unificadas.

28.4.1.1 Selección de aplicación

Descripción de parámetros de las pestañas:

- **Selección de aplicación**

Parámetros	Descripción
Seleccionar paquetes de aplicación	Selección del paquete de aplicación con UC Smart o con UC Suite. En el paquete de aplicación con UC Suite en el OpenScape Business UC Booster Server se requiere además la dirección IP del UC Booster Server (dirección IP del servidor Linux).
Selección de aplicación	Indicación de los componentes compatibles según el paquete de aplicación seleccionado, incluyendo la dirección IP del servidor utilizado.

28.4.2 Servicio de integración de Active Directory

En **Servicio de integración de Active Directory** se agrupan las funciones adecuadas para la integración de Active Directory.

28.4.2.1 Servicio de integración de Active Directory

Descripción de parámetros de las pestañas:

- **Servicio de integración de Active Directory**

Parámetros	Descripción
Tipo de sincronización	Los valores que puede tener el tipo de sincronización son los siguientes: • **Libre** No se realiza ninguna sincronización del usuario con el servicio de Active Directory. • **marc. dir.** Sincronización automática del usuario con Active Directory. El número de marcación directa se emplea como una clave de sincronización. • **forzado** Sincronización manual del usuario con un usuario de Active Directory. Con una sincronización forzada, es posible sincronizar a un usuario de Active Directory con varios usuarios de OpenScape Business. • **mulap_member** El usuario sincronizado automáticamente es miembro de un grupo MULAP.
Buscar	Los campos vacíos en la parte superior de la pantalla se pueden usar para buscar un usuario determinado cuando el número de usuarios es demasiado grande para que quepa en una pantalla. En los campos **Nombre**, **Apellido**, **Nombre en pantalla** y **Marcación directa**, se realiza una búsqueda de tipo "empieza con". En el campo **Usuario de Active Directory** se realiza una búsqueda de tipo "contiene". La búsqueda se inicia después de pulsar el botón **Buscar**.
Editar	Puede usar este botón para configurar la sincronización del usuario especificado. Al seleccionar **Editar**, las acciones disponibles son los siguientes botones que aparecen.
Guardar datos	Puede seleccionar un usuario de AD determinado y forzar la sincronización con el usuario de OpenScape Business determinado. Puede sincronizar de esta forma distintos números de marcación directa con el mismo usuario de AD.
Restablecer	Intente sincronizar el usuario de OpenScape Business con cualquier usuario de Active Directory. Esta acción se puede usar, por ejemplo, si se detiene la sincronización del usuario.
No sincronizar	Detenga la sincronización del usuario de OpenScape Business especificado. No se eliminan los datos ya sincronizados para el usuario, pero se interrumpe la sincronización con AD.

28.4.3 UC Smart

En **UC Smart** se reunen las funciones de Comunicaciones Unificadas.

28.4.3.1 UC Smart > Ajustes básicos

Descripción de parámetros de las pestañas:

- **Ajustes básicos**

Parámetros	Descripción
Habilitar/Deshabilitar UC Smart	
Activo	UC Smart y UC Suite no pueden estar activos al mismo tiempo. (Después de la activación se muestran otros parámetros)
Activar / Desactivar CloudService	
Activo	Este flag controla el estado de la funcionalidad CloudService. Tenga en cuenta que la activación de la función CloudService provocará un reinicio de WebServices.
Configuración de acceso	
HTTP	Los clientes de UC Smart pueden acceder al sistema por HTTPS cifrado (recomendado) o HTTP sin cifrar (no recomendado). La selección se hace en la propia aplicación. Aquí se distribuye la clase de servicio para uno o para los dos protocolos.
HTTPS	
Política de contraseñas	
El usuario debe introducir una contraseña segura	Directrices de contraseña para los clientes UC Smart. La contraseña estándar se debe modificar en el primer inicio de sesión y debe corresponderse con las directrices aquí seleccionadas (véase el botón de exclamación). La contraseña se guarda en el cliente y si no es así, se solicita cada vez que se inicia el cliente.
Guardar datos de inicio de sesión en el terminal	Los datos de inicio de sesión también se guardan en el teléfono.
Contraseña inicial de UC Smart a nivel de sistema	A todos los usuarios de UC Smart configurados que todavía no se han registrado en UC Smart o que todavía no han modificado su contraseña inicial se les aplica una contraseña inicial a nivel de sistema. Por consiguiente, hay que asignar una contraseña individual a todos los usuarios afectados. ***INFORMACIÓN***: la asignación de una contraseña inicial de UC Smart a nivel de sistema supone un riesgo para la seguridad, sobre todo si no se asigna inmediatamente una contraseña individual a los distintos usuarios. Como alternativa se recomienda la asignación de contraseñas individuales personalizadas para cada usuario.
Horas de oficina	
Hora de inicio	Puede configurar las Horas de oficina seleccionando dos valores de las listas desplegables Hora de inicio y Hora de fin según corresponda. El horario de oficina por defecto es de 08:00 a 20:00 horas.
Hora de fin	
Presencia	
Ocultar estado de enfermo	Puede ocultar la opción de estado de presencia "Enfermo" a los usuarios de clientes UC.

28.4.3.2 UC Smart > Gestión de usuarios

Descripción de parámetros de las pestañas:

- **Gestión de usuarios**

Parámetros	Descripción
Usuario	Lista de todas las extensiones disponibles, la extensión seleccionada debe tener una licencia UC User
Configuración	
Usuarios	Indicación del número de teléfono interno del usuario.
Nombre	Indicación del nombre del usuario.
Contraseña	Aquí se puede definir la contraseña del usuario del cliente UC Smart.
Idioma	Idioma de UC Smart Assistant
El usuario debe asignar una contraseña nueva	(solo indicación)
Acceso a UC Smart Assistant	Clase de servicio para que el usuario acceda a UC Smart Assistant
Configurado como extensión Mobility	(solo indicación)
Licencia de buzón de voz	(solo indicación)
Servicios asociados	(solo indicación)
Detalles de perfil	
Número de teléfono móvil	Número de teléfono móvil de la extensión en formato canónico (p.ej. `+ 49 173 1234567`).
Número de teléfono privado/ externo	Número de teléfono adicional de la extensión en formato canónico (p.ej. `+ 49 89 987654321`).
Dirección e-mail	Dirección de email del usuario.
Buzón de voz a correo electrónico	Activación/Desactivación de la notificación por correo electrónico cuando se recibe un mensaje de voz nuevo.
Visibilidad de presencia	Permite configurar si las extensiones internas y externas podrán ver el estado de presencia, si solo podrán verlo las extensiones internas o si nadie podrá verlo.
Información de licencia	Indicación de las licencias disponibles en el sistema para la aplicación correspondiente

28.4.3.3 Estado > UC Smart

Descripción de parámetros de las pestañas:

- **Estado**

Parámetros	Descripción
Servidor de aplicaciones	Indicación del estado del servidor de aplicaciones integrado de UC Smart.
Conexiones activas	Indicación del número de conexiones activas por cliente de UC Smart.

28.4.4 OpenScape Business UC Suite

En **OpenScape Business UC Suite** se reunen funciones de Comunicaciones Unificadas como, por ejemplo, En conferencia, Departamentos y grupos, Configuración del directorio externo, planes horarios y vacacionales, el Contact Center y la configuración de servidor de UC Suite.

28.4.4.1 OpenScape Business UC Suite

Parámetros	Descripción
OpenScape Business UC Suite	Configuración de la UC Suite, incluyendo los clientes myPortal, myAgent, myAttendant y myReports, mensajes de voz y de fax y conferencias.

28.4.4.2 OpenScape Business, UC Suite > Directorio de usuario

Si desea cambiar el nombre y los apellidos, la acción debe efectuarla el administrador. De lo contrario, los cambios no se mantendrán después de una sincronización. Se produce una sincronización cuando el administrador reinicia el sistema o cuando se cambia la configuración.

La extensión es un miembro de un grupo MULAP no aparece en el directorio de usuario. Si la extensión es miembro de una línea colectiva, aparece en el directorio de usuario.

Parámetros	Descripción
Buscar	Busque un usuario de UC Suite.
Símbolo de presencia	El administrador puede cambiar el estado de presencia de cada usuario y establecer su fecha y hora de regreso en formato Día-Mes-Año (DD/MM/AA) y 24 horas (HH:MM) respectivamente. Si la figura es de color gris, significa que ese usuario no ha iniciado sesión en la UC Suite. **Nota:** Cada miembro de una línea colectiva se considera como usuario del directorio de sistema y aparece en color gris.
Editar	Editar la configuración del usuario de la UC Suite seleccionado. **Nota:** Debido a problemas de compatibilidad conocidos con el navegador, el diseño de la ventana **Editar usuario** puede diferir cuando se utilice Firefox. El diseño es uniforme con IE/ Chrome/Edge.

Parámetros	Descripción
Restablecer usuario	Los ajustes de un usuario se restablecen a los valores estándar. Al hacerlo también se borran sus mensajes de voz, los anuncios grabados personales del buzón de voz, las entradas de diario, las conferencias planificadas, los correos electrónicos y los mensajes de fax. **Nota:** En este caso, la contraseña predeterminada está configurada en 4 caracteres (1234).
Desbloquear usuario	Los usuarios bloqueados (por ejemplo si se ha introducido varias veces una contraseña errónea) se pueden desbloquear aquí (indicación del símbolo de candado). El sistema puede informar al administrador sobre el bloqueo a través del correo electrónico.
Detalles personales	Detalles personales del usuario
Detalles personales: Mis detalles personales	Nombre de inicio de sesión, Contraseña, Apellido, Extensión, Nombre, Número de correo de voz, Número de fax, Número de asistente, Correo electrónico, Departamento, Número de móvil, Número externo 1/2, Número de casa (en formato canónico, por ejemplo, 49 89 700798765). La contraseña es válida para los clientes de la UC Suite.
Detalles personales: Mi imagen	Se redimensiona automáticamente Formatos de archivo admitidos: BMP, JPG/JPEG/JFIFI, PNG. Tamaño máximo de archivo: 10MB
Detalles personales: Nivel de usuario	Solo lo puede configurar el administrador para centros de contacto: si el agente va a estar disponible permanentemente, seleccione la casilla de verificación **Agente disponible permanentemente.** De esta forma, el agente también permanecerá disponible para llamadas, faxes y correos electrónicos aunque no acepte una llamada, un fax o un correo electrónico. Cuando un usuario está configurado como agente, los derechos del agente se definen seleccionando la clase de servicio apropiada para ese agente (es decir, el nivel de autorización como Agente, Supervisor o Administrador), desde la lista desplegable **Nivel**. Los agentes con el nivel de clase de servicio Supervisor o Administrador tienen autorizaciones ampliadas.
Mis preferencias	Configuraciones específicas del usuario del cliente.
Mis preferencias: Apariencia	Colores de piel de la interfaz de usuario; idioma de la interfaz de usuario; uso o no del clásico traypop.
Mis preferencias: Notificaciones	Configuración para ventanas emergentes.
Mis preferencias: Presencia	Configuración para el estado de presencia.
Mis preferencias: Conectividad de Outlook	Generar citas de calendario: aplicación del estado de presencia en la integración en el calendario Outlook: control del estado de presencia mediante citas Outlook/iCal (la primera clave de la línea de asunto controla el estado de presencia)
Mis preferencias: Teclas de acceso rápido	Defina teclas de acceso rápido para funciones de llamada.

Parámetros	Descripción
Mis preferencias: Varios	Restablecer automáticamente el estado de presencia a "Oficina" después de finalizar la cita, habilitar el registro de registros de clientes, definir el método de transferencia, período de retención para las entradas del diario (el valor máximo es 30 días), programar teclas de función del teléfono, habilitar la búsqueda en vivo e incluir Contactos LDAP en la búsqueda en vivo de directorios, especificar un mensaje de respuesta.
Reglas de llamada	Reglas para llamadas entrantes
Reglas de llamada: Destinos de reenvío	Definición de destinos de reenvío para cada estado de presencia (Desvío de llamadas relativo al estado)
Reglas de llamada: Módulo de reglas	Definición de reglas de llamada complejas en función del estado de presencia (Desvío de llamadas basado en reglas)
Comunicaciones	Gestión de mensajes específicos de usuario
Comunicaciones: **Ajustes del buzón de voz**	Se pueden grabar mensajes de voz en el estado de presencia correspondiente; ajuste del idioma del buzón de voz Valor estándar: desactivado
Comunicaciones: **Notificación de buzón de voz**	Servicio de notificaciones para nuevos mensajes de voz - Dirección e-mail, véase Mis detalles personales, Requisito: servidor de correo y dirección de correo propia configurada en Centro de servicios > Transferencia de correos electrónicos. "Saliente" genera un outcall de usuario para el número indicado (formato canónico). Para el número de teléfono SMS véase Mis detalles personales. Para el Contenido de los SMS véase Plantillas.
Comunicaciones: **Notificación de fax**	Servicio de notificaciones para nuevos mensajes de faz. Requisito: servidor de correo y dirección de correo propia configurada en Centro de servicios > Transferencia de correos electrónicos. "Saliente" genera una llamada de usuario al número de teléfono especificado (en formato canónico), ya sea dentro del horario comercial únicamente o las 24 horas del día. Para el número de teléfono SMS véase Mis detalles personales. Para el Contenido de los SMS véase Plantillas.
Comunicaciones: **Notificaciones de llamadas perdidas**	Servicio de notificación de nuevas llamadas perdidas: consulte la dirección de correo electrónico Mis datos personales. Requisito: servidor de correo y dirección de correo propia configurada en Centro de servicios > Transferencia de correos electrónicos.
Perfiles	Perfil para AutoAttendant personal
Ocupado, Sin respuesta, Reunión, Enfermo, Descanso, Fuera de la oficina, Vacaciones, Almuerzo, Casa	Mediante la marcación posterior de un dígito del 0 al 9, los llamantes pueden ser transferidos a un destino de desvío o pueden dejar un mensaje. Para ello se requiere un anuncio grabado por cada estado de presencia.
Perfiles: Saltar saludo dinámico	Se omite el anuncio automático del estado de presencia y en su lugar los llamantes solo escuchan el anuncio grabado del nombre y luego el del AutoAttendant personal
Sensibilidad	Configuración para la protección de la confidencialidad

Parámetros	Descripción
Sensibilidad: Seguridad y acceso	Liberación de mensajes de voz para myAttendant; consultar la casilla del correo de voz desde el propio teléfono sin contraseña; permita que otros usuarios vean con quién está hablando y copie su diseño BLF.
Sensibilidad: Visibilidad de presencia	Definición de la visibilidad del estado de presencia propio para los usuarios internos
Sensibilidad: **Presencia de buzón de voz**	Indicación del estado de presencia para llamantes externos. Indicación de números de teléfono internos que bloquear, se pueden utilizar comodines.
myAttendant	Indicación solo en extensiones con licencia para myAttendant
myAttendant: Mensajes LAN	Módulos de texto para mensajes instantáneos de myAttendant, entrada libre, selección en el chat de la ventana del cliente
myAttendant: Números de llam. de marcación directa	Entrada de números de marcación directa; si desea utilizar myAttendant para varias empresas, se puede mostrar una ventana "Para"
myAttendant: Comunicaciones	Ingreso de un número interno para el desvío de llamadas en caso de emergencia o en caso de no aceptación (Desvío sin supervisión) por parte de myAttendant (para EE. UU.)

28.4.4.3 OpenScape Business UC Suite > Departamentos

Descripción de los parámetros de las pestañas:

- **Departamentos**

Parámetros	Descripción
Nombre departamento	Los departamentos agrupan a extensiones en el directorio interno según su pertenencia dentro de la organización. Con ello, por ejemplo, se puede realizar en myAttendant una asignación automática de los usuarios a los departamentos.
Línea colectiva **Añadir**	(Numeración interna sin más significado) Añadir un nuevo departamento.
Editar	Editar un departamento seleccionado.
Eliminar	Eliminar los departamentos seleccionados.

28.4.4.4 OpenScape Business UC Suite > Grupos

Un grupo de buzón de voz (grupo Contestador automático) permite a un determinado grupo de extensiones acceder a mensajes de voz. A través del número de teléfono del grupo de buzón de voz no se llama a los miembros del grupo, sino que se accede directamente al buzón de voz (voicemail) del grupo.

Con los grupos de fax (grupos de buzón de fax), un determinado grupo de extensiones puede acceder a mensajes de fax. El número de teléfono de un grupo de fax permite acceder directamente al buzón de fax del grupo.

Los grupos de favoritos le permiten crear grupos con contactos y asignarlos a los usuarios.

Descripción de parámetros de las pestañas:

- **Grupos de buzón de voz**
- **Grupo de fax**
- **Grupos de favoritos**

Tabla 64:

Parámetros	Descripción
Grupos de correo de voz	
Editar	Editar el grupo de buzón de voz seleccionado
Eliminar	Eliminar los grupos de buzón de voz seleccionados
Grupos de correo de voz	Nombre del grupo de buzón de voz
Piloto	Número de teléfono del grupo de buzón de voz
Tipo	Tipo del grupo de buzón de voz
Nº de usuarios	Número de miembros del grupo de buzón de voz
Nº de mensaje	Número de nuevos mensajes de voz para el grupo de buzón de voz
Usuarios	Miembros del grupo de buzón de voz
Grupo de fax	
Editar	Editar el grupo de fax seleccionado
Grupo de fax	Nombre del grupo de fax
Piloto	Número de teléfono del grupo de fax
Nº de usuarios	Número de miembros del grupo de fax
Nº de faxes	Número de nuevos mensajes de fax para el grupo de fax
Multiusuarios	Si se trata de un grupo de fax, se muestra **Sí**. En caso contrario, se muestra **No**.
Grupos de favoritos	
Añadir	Agregar un nuevo grupo de favoritos
Editar	Editar el grupo de favoritos seleccionado
Eliminar	Eliminar los grupos de favoritos seleccionados

Parámetros	Descripción
Nombre grupo	Nombre del grupo favorito
Número de contactos	Número de contactos que se han añadido al grupo
Editable	Seleccione si el usuario puede editar o no el grupo de favoritos.

28.4.4.5 OpenScape Business UC Suite > Plantillas

Descripción de los parámetros de las pestañas:

- **Proveedor de SMS**

Parámetros	Descripción
Añadir	Añadir una nueva plantilla. Introduzca el nombre de la plantilla y el nombre del autor. En el campo Destinatario, Asunto o Texto se pueden insertar marcadores de posición que se seleccionan individualmente en "Campos VSL".
Editar	Editar la plantilla seleccionada. Cambiar el nombre de la plantilla y el nombre del autor. Editar también los campos Destinatario, Asunto y Texto. En el campo Destinatario, Asunto o Texto se pueden insertar marcadores de posición que se seleccionan individualmente en "Campos VSL".
Eliminar	Eliminar la plantilla seleccionada.
Establecer como predeterminado	Establezca la plantilla seleccionada como predeterminada.

28.4.4.6 Directorio externo de > OpenScape Business UC Suite

Descripción de los parámetros de las pestañas:

- **Directorio externo**

Parámetros	Descripción
Añadir	Inserción manual de contactos individuales en el directorio externo. Los caracteres deben tener el formato UTF-8
Editar	Editar un contacto seleccionado del directorio externo
Eliminar	Eliminar los contactos seleccionados del directorio externo

Descripción de los parámetros de las pestañas:

- **Importar directorio externo**

Parámetros	Descripción
Importar desde	Elija si la importación de la información de los contactos se hará desde un archivo local o desde una carpeta pública de Windows.

Parámetros	Descripción
Carga de archivo	Haga clic en **Seleccionar archivo** para seleccionar el archivo que se cargará en el sistema.
Carpeta Público de Windows	Introduzca el **Nombre de archivo**, el **Nombre de usuario**, el **Dominio**y la **Contraseña** de la carpeta pública de Windows que se va a cargar en el sistema y haga clic en **Probar** para probarla.
Opciones	Esta área ofrece varias opciones en cuanto al formato del archivo csv que se va a importar. Además, hay una opción que borra los datos existentes antes de ejecutar la importación. Por último, otra opción declara el modo en que se tratan los duplicados durante una importación.

Descripción de los parámetros de las pestañas:

- **Exportar directorio externo**

Parámetros	Descripción
Exportar a	Elija dónde se guardará el archivo exportado, si localmente o en una carpeta pública de Windows.
Carpeta Público de Windows	Introduzca el **Nombre de archivo**, el **Nombre de usuario**, el **Dominio**y la **Contraseña** de la carpeta pública de Windows que se va a cargar en el sistema y haga clic en **Probar** para probarla.

28.4.4.7 OpenScape Business UC Suite > Configuración de proveedores externos

Descripción de parámetros de las pestañas:

- **Proveedores LDAP**

Parámetros	Descripción
Añadir/Editar/Eliminar	Permite añadir, editar o eliminar los datos de acceso del servidor LDAP.
Nombre	Nombre de este directorio offline externo.
Servidor/Dirección del servidor	Nombre DNS o dirección IP del servidor LDAP.
Puerto	Número de puerto del servidor LDAP externo.
Nombre de usuario	Nombre de usuario para acceder al servidor LDAP remoto.
Contraseña	Contraseña para acceder al servidor Exchange remoto.
Nombre distintivo de base (BaseDN) LDAP	Nombre distintivo de base LDAP, por ejemplo, dc=ejemplo-de-dominio, dc=net.
TLS	Habilitar el uso de solo conexiones seguras al servidor LDAP.

Parámetros	Descripción
Título, **Nombre**, **Apellido**, **Empresa 1**, **Empresa 2**, **Teléfono privado**, **Móvil**, **Empresa**, **Teléfono empresa**, **Dirección postal**, **Nombre del estado o provincia**, **Nombre del país**, **Código postal**, **Correo electrónico**, **Localizado**, **Número de fax** y **Ciudad**	Al configurar un directorio offline externo, en calidad de administrador puede adaptar la asignación de campos a los nombres del servidor LDAP utilizado. Los campos borrados se omiten al realizar búsquedas de nombre mediante número de teléfono. La búsqueda se realiza siempre con los últimos 4 dígitos del número de teléfono con el comodín preestablecido. Puede desactivar la búsqueda de nombre mediante número de teléfono en las llamadas entrantes. Introduzca la denominación de campo correspondiente del servidor LDAP. **Nota:** La asignación de campos LDAP depende del nombre de campo correspondiente según el uso del servidor LDAP externo.

Descripción de parámetros de las pestañas:

- **PST Exchange**

Parámetros	Descripción
Añadir/Editar/Eliminar	Permite añadir, editar o eliminar los datos de acceso del servidor Exchange. En un entorno Microsoft, el servidor ADS (Active Directory Server) o el servidor Exchange Server actúan también, al mismo tiempo, como servidor LDAP.
Nombre	Nombre del directorio offline externo.
Método de autenticación	Método de autenticación que se utilizará para acceder al servidor Exchange remoto. Puede elegir entre **Básico** y **OAuth 2.0**.
Servidor/Dirección del servidor	Nombre DNS o dirección IP del servidor Exchange Server.
Nombre de usuario	Nombre de usuario para acceder al servidor Exchange remoto.
Contraseña	Contraseña para acceder al servidor Exchange remoto. Visible solo si el método de autenticación seleccionado es **Básico**.
ID inquilino, ID de aplicación, **ID de cliente**, **Alcance**	**ID inquilino**, **ID de aplicación** y **ID de cliente** correspondientes a la aplicación que se ha registrado en Azure AD para la integración de directorios de Exchange. Puede solicitarlos a su administrador de Azure AD. **Alcance** que requiere la aplicación (opcional). Valor estándar: https://outlook.office365.com/.default Visible solo si el método de autenticación seleccionado es **OAuth 2.0**.

Descripción de parámetros de las pestañas:

- **Integración de calendarios de Exchange**

Parámetros	Descripción
Integración de calendarios de Exchange	La integración en el calendario permite generar automáticamente en Windows citas de Outlook con ausencia. Si no desea guardar las citas de Outlook en el archivo PST local del usuario, sino en el servidor de Exchange Server, introduzca aquí los datos de acceso.
Activar integración del calendario de Exchange	Activar la integración en el calendario Exchange
Método de autenticación	Método de autenticación que se utilizará para acceder al servidor Exchange remoto. Puede elegir entre **Básico** y **OAuth 2.0**.
Servidor	Encontrará información detallada sobre el uso de las distintas versiones de Microsoft Exchange Server en la wiki de expertos de Unify, en: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.
Nombre de usuario	Nombre de usuario para acceder al servidor Exchange remoto.
Contraseña	Contraseña para acceder al servidor Exchange remoto. Visible solo si el método de autenticación seleccionado es **Básico**.
ID inquilino, **ID de aplicación**, **ID de cliente**, **Alcance**	**ID de inquilino**, **ID de aplicación** y **ID de cliente** correspondientes a la aplicación que se ha registrado en Azure AD para la integración de calendario de Exchange. Puede solicitarlos a su administrador de Azure AD. **Alcance** que requiere la aplicación (opcional). Visible solo si el método de autenticación seleccionado es **OAuth 2.0**.

28.4.4.8 OpenScape Business UC Suite > Contact Center

Descripción de parámetros de las pestañas:

- **Plan horario**
- **Cola**
- **Nivel de servicio**
- **Prioridades de llamantes VIP**
- **Lista de llamadas VIP**
- **Agentes preferidos**
- **Descansos en el Contact Center**
- **Tratamiento posterior simple**
- **Tratamiento posterior múltiple**
- **Enlaces de cola**

Plan horario

Mediante un plan horario se define cómo se van a administrar las llamadas entrantes en determinados días y a horas determinadas. El plan horario y las reglas en él incluidas (CCV, Call Control Vector) de cada cola permiten definir cómo se administrarán las llamadas entrantes en determinados días y horas. Se debe asignar al menos una regla (Call Control Vector CCV) a un plan horario. Las reglas determinan qué llamadas entrantes se gestionarán en una determinada cola durante el tiempo de vigencia de un plan horario. Las reglas se aplican exclusivamente a llamadas, no a faxes ni correos electrónicos.

Para información detallada sobre la configuración de planes horarios, véase Procedimiento de configuración

Parámetros	Descripción
Plan horario	Nombre del horario
Cola	Nombre de la cola a la que está asignado el plan horario.
Línea colectiva	Identificador del grupo de búsqueda del grupo UCD, que se configuró durante la configuración básica del Contact Center.
Plan horario	
Nombre del horario	Nombre del horario
CCV estándar	Aparece la regla estándar del plan horario que, una vez asignada a una cola de espera, es válida las 24 horas al día y los 365 días del año. Si desea aplicar otras reglas en determinados momentos (Pausa, Fin de semana, Festivo, Vacaciones, etc.), puede asignarlas al plan horario correspondiente como reglas de excepción (CCV de excepción).
Colas	
Nombre de cola	Nombre de la cola a la que está asignado el plan horario.
Cola activa	Indica si la cola está activa o no.
Excepciones	
CCV	Nombre de la regla de excepción (CCV de excepción) Las reglas de excepción definen cómo se gestionarán las llamadas entrantes en determinados momentos excepcionales (pausas, fines de semana, festivos, vacaciones, etc.). Los planes horarios vacacionales tienen prioridad frente a otros planes horarios y reglas de una cola.
Descripción	Texto descriptivo de la regla de excepción
Tipo	Tipo de la regla de excepción
Fecha de inicio	Fecha para el comienzo de la regla de excepción
Fecha de fin	Fecha para el final de la regla de excepción
Hora de inicio	Hora para el comienzo de la regla de excepción
Hora de fin	Hora para el final de la regla de excepción
Sucede	La frecuencia con la que se programa la regla de excepción

Cola

Las colas de espera son la base del Contact Center. Las llamadas, faxes y correos electrónicos de la cola se pueden administrar en función del nivel de capacidad de los agentes, de la prioridad y del tiempo de espera. Las llamadas que se encuentran en estado de espera pueden escuchar la reproducción de anuncios grabados.

Para información detallada sobre la configuración de colas de espera, véase Procedimiento de configuración

Parámetros	Descripción
Cola	Nombre de cola
Cola activa	Indica si la cola está activa o no.
Línea colectiva	Identificador del grupo de búsqueda del grupo UCD, que se configuró durante la configuración básica del Contact Center.
Configuración general	
Nombre de cola	Nombre de cola
Cola activa	Definición del estado de la cola
Cola activa: Inactivo	La cola no está activa.
Cola activa: Activo	La cola está activa.
Línea colectiva	Identificador del grupo de búsqueda del grupo UCD, que se configuró durante la configuración básica del Contact Center.
Conmutación telefónica	Se muestra la entrada CSP
Plan horario	Se muestra el plan horario asignado
Recuento de alarma de cola	Número de umbral de alarma Si se supera el número de llamadas en espera aquí indicado, el símbolo de cola del agente cambia del color verde al naranja. Valor estándar: 0 llamadas
Hora de alarma de cola	Tiempo de umbral de alarma en segundos Si se supera el tiempo de espera de una llamada en la cola aquí indicado, la entrada correspondiente de la lista de llamadas del Contact Center del agente pasa a color rojo. Valor estándar: 0 segundos
Tiempo excedido de llamadas perdidas	Tiempo excedido de llamadas perdidas en segundos Una vez finalizado el tiempo aquí indicado, las llamadas no aceptadas se transfieren al siguiente agente libre. Valor estándar: 10 segundos
Valor umbral de llamada abandonada	Tiempo de umbral para llamadas abandonadas, en segundos El tiempo especificado aquí determina si una llamada abandonada se incluye o no en las estadísticas. Se registran de forma estadística todas las llamadas abandonadas una vez finalizado el tiempo indicado. Valor estándar: 0 segundos

Parámetros	Descripción
Ventana emergente activada	Si el flag está activado, al recibir una llamada, en myAgent aparece una ventana emergente para visualizar e introducir datos de cliente. Las ventanas emergentes son necesarias para aceptar y realizar devoluciones de llamada y para aceptar faxes y correos electrónicos. Valor estándar: Desactivado **Nota:** Opción de notificaciones a través de **myAgent** > **Configuración** > **Notificaciones** > **Aplicación emergente en llamadas entrantes** se anulan mediante la activación de la pantalla emergente a través de **WBM** > **Modo Experto** > **OpenScape Business UC Suite** > **Contact Center** > **Cola** > **Configuraciones generales** > **Pantalla emergente habilitada**.
Modo de Tratamiento posterior	Definición del modo de tratamiento posterior
Modo de Tratamiento posterior: Sin tratamiento posterior	Para la cola no se pueden definir motivos de tratamiento posterior.
Modo de Tratamiento posterior: Tratamiento posterior simple	Para la cola se pueden definir uno o varios motivos de tratamiento posterior.
Modo de Tratamiento posterior: Tratamiento posterior múltiple	Para la cola se pueden definir uno o varios motivos de tratamiento posterior, que se pueden reunir en grupos y grupos secundarios.
Tiempo de espera de pantalla emergente	Tiempo de espera de la pantalla emergente en segundos Si se establece en 0, myAgent solicitará implícitamente una ventana emergente de 20 s. Valor estándar: 20 segundos
Prioridades	Si un agente está asignado a varias colas, la prioridad de la cola se puede utilizar para definir si las llamadas de una cola con mayor prioridad deben reenviarse a este agente con prioridad sobre las llamadas de otras colas.
Modo de profundidad de cola	Definición del modo de profundidad de cola
Modo de profundidad de cola: Estática	En caso de que el modo de profundidad de cola se establezca en estático, puede configurarse WLS y Tamaño de profundidad de cola.
Modo de profundidad de cola: Ninguno	En caso de que la profundidad de cola se establezca en Ninguno, el parámetro WLS puede configurarse y afecta también a la configuración de UCD, pero el parámetro de profundidad de cola no puede establecerse
Pilotos de cola	

Parámetros	Descripción
Pilotos de fax entrante	Números de teléfono (pilotos) para mensajes de fax entrantes Los faxes dirigidos a esas direcciones se depositan en la cola de espera y se gestionan como llamadas entrantes.
Servicio de email entrante	Direcciones de correo electrónico para correos electrónicos entrantes Los correos electrónicos dirigidos a esas direcciones se depositan en la cola de espera y se gestionan como llamadas entrantes.
Añadir	Agregar un nuevo servicio de correo electrónico entrante
Editar	Editar un servicio de correo electrónico entrante seleccionado
Eliminar	Eliminar el servicio de correo electrónico entrante seleccionado
Método de autenticación	Método de autenticación a utilizar para acceder al servicio de correo electrónico entrante Puedes elegir entre **Básico** y **OAuth 2.0**.
Servidor	Nombre DNS o dirección IP del servicio de correo electrónico entrante
Puerto	Número de puerto del servicio de correo electrónico entrante
Nombre de usuario	Nombre de usuario para acceder al servicio de correo electrónico entrante
Contraseña	Contraseña para acceder al servicio de correo electrónico entrante Editable solo si el método de autenticación seleccionado es **Básico**.
Utiliza conexiones SSL	Habilitar o deshabilitar el uso de conexiones SSL según la configuración del Servicio de Correo Entrante
ID de inquilino, **ID de aplicación**, **Secreto del cliente**, **Alcance**	**ID de inquilino**, **ID de aplicación** y **Secreto de cliente** correspondiente a la aplicación que se ha registrado en Azure AD para colas de correo electrónico. Puede obtenerlos de su administrador de Azure AD. **Alcance** que la aplicación requiere (opcional). Valor predeterminado: https://outlook.office365.com/.default Visible sólo si el método de autenticación seleccionado es **OAuth 2.0**.
Varios	
Dirección de email de devolución	Dirección de email de devolución para correos electrónicos enviados El receptor de un correo electrónico enviado por un agente puede ver la dirección de correo electrónico indicada aquí.
Encaminamiento de llamadas inteligente	Si el flag está activado, las llamadas entrantes se transfieren automáticamente al último agente conectado con el llamante. Para ello es necesario que no haya definido un agente preferido para el llamante. Valor estándar: Desactivado

Nivel de servicio

Los niveles de servicio permiten evaluar la calidad de transferencia de una cola. Esto es posible mediante la comparación de los tiempos de espera de los llamantes en una cola de espera con valores nominales que se pueden predefinir de forma individual para cada cola.

Por cada llamada a la cola de espera en cuestión se transmite el nivel de servicio al finalizar la llamada y se aplica a la base de datos. Los agentes con el nivel de clase de servicio "Supervisor" o "Administrador" pueden evaluar el nivel de servicio mediante la aplicación myAgent.

Para información detallada sobre la definición de valores teóricos para el nivel de servicio, véase Procedimiento de configuración

Parámetros	Descripción
Cola	Nombre de cola
Cola activa	Indica si la cola está activa o no.
Línea colectiva	Identificador del grupo de búsqueda del grupo UCD, que se configuró durante la configuración básica del Contact Center.
Nivel de servicio	El eje horizontal indica el tiempo de espera en la cola en intervalos de diez segundos, y el eje vertical indica el valor nominal del nivel de servicio en valores porcentuales. Los puntos rojos indican los valores teóricos para la calidad de transferencia de la cola de espera. Comparando los valores nominales con los tiempos de espera reales de los llamantes se puede determinar el grado de calidad.

Prioridades de llamantes VIP

Mediante la prioridad de llamantes VIP se puede definir, de forma individualizada para cada cola, si los llamantes incluidos en la lista de llamadas VIP deben ser tratados con preferencia.

Los valores de prioridad de llamantes VIP se puede determinar libremente en función del tiempo de espera del llamante en una cola. De esta forma, el nivel de prioridad de los llamantes VIP se define frente al de los llamantes normales.

Si un llamante VIP activa una devolución de llamadas de agentes (grabación de un mensaje de voz con solicitud de devolución de llamada), en la cola de espera permanece la devolución de llamadas de agentes en lugar del llamante VIP. En este caso no se aplica la prioridad de llamantes VIP.

Para información detallada sobre la definición de la Prioridad de llamantes VIP, véase Procedimiento de configuración

Parámetros	Descripción
Cola	Nombre de cola
Cola activa	Indica si la cola está activa o no.
Línea colectiva	Identificador del grupo de búsqueda del grupo UCD, que se configuró durante la configuración básica del Contact Center.
Prioridad de llamantes VIP	El eje horizontal indica el tiempo de espera en la cola en intervalos de 30 segundos, y el eje vertical indica la prioridad de los llamantes normales que no están incluidos en la lista de llamadas VIP. Los puntos rojos definen la prioridad de los llamantes normales respecto a los llamantes VIP.

Lista de llamadas VIP

Los llamantes (directorio externo) ya registrados en el sistema de comunicación se pueden incluir en la lista de llamadas VIP. Además se pueden introducir

patrones de números de teléfono. Los patrones de números de teléfono se componen de una determinada secuencia de cifras y de un comodín (marcador de posición). De esta forma, por ejemplo, se puede incluir a todos los empleados de una empresa en la lista de llamadas VIP.

Para información detallada sobre la configuración de la lista de llamadas VIP, véase Procedimiento de configuración

Parámetros	Descripción
Cola	Nombre de cola
Cola activa	Indica si la cola está activa o no.
Línea colectiva	Identificador del grupo de búsqueda del grupo UCD, que se configuró durante la configuración básica del Contact Center.
Lista de llamadas VIP	Se muestran los llamantes incluidos en la lista de llamadas VIP y los modelos de números de teléfono. Puede agregar, editar o eliminar personas que llaman y patrones de números de llamadas de la Lista de llamadas VIP. Cuanto más a la derecha esté la barra deslizable junto a un llamante o un modelo de números de teléfono, mayor será su prioridad respecto a los demás llamantes o modelos incluidos en la lista de llamadas VIP.

Agentes preferidos

A cada llamante se le pueden asignar uno o varios agentes preferidos de una cola. En tal caso, el sistema de comunicación intenta transferir al llamante y sus solicitudes de devolución de llamada a un agente favorito en primer lugar. Si se han establecido varios agentes preferidos, se puede definir una prioridad (orden) con la que son transferidos los agentes preferidos.

Si no hay disponible ningún agente preferido, la llamada se transfiere a cualquier otro agente disponible.

Para información detallada sobre la definición de agentes preferidos, véase Procedimiento de configuración

Parámetros	Descripción
Cola	Nombre de cola
Cola activa	Indica si la cola está activa o no.
Línea colectiva	Identificador del grupo de búsqueda del grupo UCD, que se configuró durante la configuración básica del Contact Center.
Agentes preferidos	Muestra los agentes preferidos para cada persona que llama indicada en la lista de clientes. Puede agregar, eliminar y cambiar la prioridad de un agente. Si para un llamante hay definidos varios agentes preferidos, la posición de la lista indica la prioridad respecto a los demás agentes preferidos. Cuanto más alta sea la posición de un agente en la lista, mayor será su prioridad.

Parámetros	Descripción
Mostrar sólo clientes con asociaciones de agente	Si el flag está activado, en la lista de clientes solo aparecen llamantes para los que haya definido al menos un agente preferido. Valor estándar: Desactivado

Descansos en el Contact Center

Para permitir a todos los agentes pausas definidas, pueden definirse pausas de Contact Center de distinta duración. Las pausas de Contact Center están disponibles a nivel de sistema y, si es necesario, los agentes pueden seleccionarlas a través de myAgent.

Para información detallada sobre la definición de las pausas de Contact Center, véase Procedimiento de configuración

Parámetros	Descripción
Añadir	Agregar una nueva pausa en el Centro de contacto
Editar	Editar un descanso de Contact Center seleccionado
Eliminar	Eliminar la pausa del Contact Center seleccionada
Nombre	Nombre de la pausa de Contact Center
Duración	Duración de la pausa de Contact Center, en minutos
Activo	Indica si la pausa de Contact Center está activa o no.

Tratamiento posterior simple

En las colas con el modo de tratamiento posterior "Tratamiento posterior simple" se pueden definir uno o varios motivos de tratamiento posterior.

En función de los motivos de tratamiento posterior las llamadas entrantes se pueden asignar a distintos temas (pedido, reclamación, servicio técnico, etc.). La asignación la realiza un agente después de completar la llamada (durante el tiempo de trabajo) ingresando el motivo de finalización apropiado usando myAgent.

Para información detallada sobre la definición de los motivos de tratamiento posterior (códigos de tratamiento posterior), véase Procedimiento de configuración

Parámetros	Descripción
Añadir	Agregar un nuevo resumen simple
Editar	Editar un resumen simple seleccionado
Eliminar	Eliminar el resumen simple seleccionado
Cola	Nombre de cola para el que se ha configurado el Tratamiento posterior simple.
Descripción	Texto descriptivo del motivo del tratamiento posterior

Tratamiento posterior múltiple

En las colas con el modo de tratamiento posterior "Tratamiento posterior múltiple" se pueden definir uno o varios motivos de tratamiento posterior y reunirlos en grupos o grupos secundarios.

En función de los motivos de tratamiento posterior las llamadas entrantes se pueden asignar a distintos temas (pedido, reclamación, servicio técnico, etc.). La asignación la realiza un agente después de completar la llamada (durante el tiempo de trabajo) ingresando el motivo de finalización apropiado usando myAgent.

Para información detallada sobre la definición de los motivos de tratamiento posterior (códigos de tratamiento posterior), véase Procedimiento de configuración

Parámetros	Descripción
Cola	Nombre de cola para la que se ha configurado el tratamiento posterior múltiple. Se muestran los grupos y grupos secundarios definidos para la cola de espera.
Descripción	Texto descriptivo del motivo del tratamiento posterior

Enlaces de cola

Con los Enlaces de cola, se pueden asignar agentes a una o varias colas.

Para información detallada sobre la asignación de agentes a colas, véase Procedimiento de configuración

Parámetros	Descripción
Cola	Nombre de cola
Cola activa	Indica si la cola está activa o no.
Línea colectiva	Identificador del grupo de búsqueda del grupo UCD, que se configuró durante la configuración básica del Contact Center.
Asignación de agentes	
Extensión	Visualización del número de extensión del usuario
Nombre	Visualización del nombre del usuario.
Agente	Agente asignado a la cola.
Tipo	Tipo de agente Estas son las opciones: • Agente principal: el agente recibe llamadas, sea cual sea la carga de la cola. • Agente de desbordamiento: el agente solo recibe llamadas en caso de desbordamiento de la cola.
Nivel de habilidad	Indicación del nivel de habilidad, en porcentaje El nivel de habilidad controla la distribución de llamadas a los agentes de una cola de espera. Los agentes con un nivel de habilidad elevado tienen prioridad en la distribución de llamadas. Cuando todos los agentes tienen el mismo nivel de habilidad, el agente que lleve más tiempo libre recibirá la llamada.
Activar devolución de llamada de agente	Si el flag está activado el agente recibe solicitudes de devolución mediante mensajes de voz.

Parámetros	Descripción
Tiempo de actividad	Tiempo de trabajo automático en segundos
Desbordamiento después de segundos en la cola	Solo para el Agente de desbordamiento: tiempo de desbordamiento en segundos Una vez terminado el tiempo de desbordamiento, las llamadas se transfieren al agente de desbordamiento.
Desbordamiento después de llamadas en cola	Solo para el Agente de desbordamiento: Número de llamadas Las llamadas que estén más allá de ese máximo se transfieren al agente de desbordamiento.

28.4.4.9 OpenScape Business UC Suite > Planes horarios

Descripción de los parámetros de las pestañas:

- **Editar/Añadir**

Parámetros	Descripción
Puesto de operadora automático	Configuración de la función AutoAttendant de la UC Suite (Company AutoAttendant)
Plan horario	Nombre de plan horario
Cola	Nombre de la cola a la que está asignado el plan horario.
Línea colectiva	Identificador de línea colectiva del grupo UCD, establecido en la configuración básica del Contact Center.
Editar / Agregar / Eliminar	Editar o eliminar la regla seleccionada o agregar una nueva (desde el Editor de reglas)
Nombre de plan horario	El plan horario se puede guardar con cualquier nombre que usted elija. Se recomienda, eso sí, utilizar un nombre significativo.
CCV estándar	Se debe asignar al menos una regla (Call Control Vector CCV) al plan horario. Las reglas determinan cómo se tratarán las llamadas entrantes durante el tiempo correspondiente. Las reglas se aplican exclusivamente a llamadas, no a faxes ni correos electrónicos. Las reglas se crean con el editor de reglas gráfico (Editor CCV) mediante la vinculación de objetos CCV predefinidos. Hay disponibles varias plantillas estándar preconfiguradas que se pueden modificar para adaptarlas a las necesidades concretas del usuario.
Colas	Se recomienda activar solo una cola por cada plan horario (solo una marca de verificación).
Nombre de cola	La cola se puede guardar con cualquier nombre que usted elija. Se recomienda, eso sí, utilizar un nombre significativo.
Cola activa	La cola se puede activar o desactivar.
Plan horario	Selección del plan horario correspondiente

Parámetros	Descripción
Piloto	Número de teléfono del puerto virtual correspondiente en el sistema de comunicación.
Excepciones	Los planes horarios con una regla estándar, tras ser asignados a una cola de espera, se aplican 24 horas al día, 365 días al año. Si desea aplicar otras reglas en determinados momentos (Pausa, Fin de semana, Festivo, Vacaciones, etc.), puede asignarlas al plan horario correspondiente como reglas de excepción (CCV de excepción). De esta forma, se puede definir cómo se administrarán las llamadas entrantes, por ejemplo, durante las vacaciones. Los planes horarios vacacionales tienen prioridad frente a otros planes horarios y reglas.
CCV	Selección de la regla de excepción (CCV de excepción)
Descripción	Entrada libre de una descripción del plan horario de excepción
Tipo	Dentro del intervalo de uno o varios días de la semana / Definible dentro del intervalo de fecha y hora / Planes horarios vacacionales para un rango de fechas
Fecha de inicio	Inicio de la excepción (fecha)
Fecha de fin	Fin de la excepción (fecha)
Hora de inicio	Inicio de la excepción (hora)
Hora de fin	Fin de la excepción (hora)
(Día de la semana)	La excepción debe tener validez en uno o varios días de la semana
Sucede	Frecuencia con la que se programa la excepción

28.4.4.10 OpenScape Business UC Suite > Carga de archivo

Descripción de los parámetros de las pestañas:

- **Administrador de archivos de audio**

Parámetros	Descripción
Destino de carga	Aplicación para la que se utiliza el nuevo anuncio grabado
Destino de carga: Puesto de operadora automático	Anuncios grabados para la conmutación automática
Destino de carga: Perfiles	Anuncios grabados para todos los usuarios de la UC Suite o para una selección de usuarios
Destino de carga: Saludo de buzón de voz	Saludos del buzón de voz para todos los usuarios de la UC Suite o para una selección de usuarios La duración máxima del saludo del mensaje de voz es de 1 minuto.
Destino de carga: Saludo de grupo de buzón de voz	Saludo para un buzón de voz de grupo

Parámetros	Descripción
Sin tecla para: uploader	El anuncio grabado está disponible como archivo PCM para la carga y tiene las siguientes propiedades: 8 kHz, 16 bits, mono. El nombre de archivo de sonido puede tener, como máximo, 30 caracteres.
Grabadora	El anuncio se graba con el teléfono de una extensión
Archivo Wave	
Descarga	Anuncios grabados descargados.
Eliminar	Borrar los anuncios grabados descargados.
Cambiar nombre	Cambiar el nombre de los anuncios grabados descargados.
Grabadora	
Nombre archivo	Indicación del nombre de archivo del anuncio que se va a grabar.
Extensión	Selección del teléfono con el que se va a grabar el anuncio.
Realizar llamada	Se llama el teléfono con el que se va a grabar el anuncio.
Reproducir	Se reproduce el anuncio grabado.
Grabar	Comienza la grabación del anuncio.

Descripción de los parámetros de las pestañas:

- **Carga de portada de fax central**

Parámetros	Descripción
Carga de portada de fax central	
Archivo Ocp	Portada de fax disponible como archivo .ocp
Nombre	El nombre de la portada del fax central
Descripción	Descripción para la portada de fax
Carga	Cargar el archivo de portada del fax central
Editar	Editar el archivo de portada del fax central seleccionado
Eliminar	Eliminar el archivo de portada del fax central seleccionado
Establecer como predeterminado	Establecer el archivo de portada del fax central seleccionado como predeterminado
Nombre archivo	Indicación del nombre de archivo del anuncio que se va a cargar
Fecha de creación	Fecha de creación del archivo de portada del fax central

28.4.4.11 OpenScape Business UC Suite > En conferencia

Descripción de los parámetros de las pestañas:

- **En conferencia**

Parámetros	Descripción
Nombre	Nombre de conferencia (lo asigna el usuario)
Propietario	Nombre del usuario que ha iniciado la conferencia
Programado a continuación	Siguiente hora de inicio planeada
Activa	
Nº de miembros	Número de miembros de conferencia, incluyendo controladores
Mostrar	Extensiones de la conferencia seleccionada
Eliminar	Eliminar las conferencias seleccionadas

28.4.4.12 OpenScape Business UC Suite > Lista de ubicaciones

Descripción de parámetros de las pestañas:

- **Lista de ubicaciones**

Parámetros	Descripción
Nombre de ubicación	Ubicaciones del sistema de comunicación interconectado (véase Ajustes básicos > Propiedades gateway)
Dirección de ubicación	Dirección IP de la UC Booster Card, del UC Booster Server o del sistema de comunicación
Puerto de ubicación	Puerto de servidor
Líneas IP de ubicación	Líneas IP de ubicación, si las hay
Estado online	Estado de conexión del sistema de comunicación en la ubicación

28.4.4.13 OpenScape Business UC Suite > Servidor

Descripción de parámetros de las pestañas:

- **Configuración general**
- **Grabación de la llamada**
- **Protocolización**
- **Notificaciones**
- **Mantenimiento**
- **Buzón de voz**
- **Contact Card Mapping**

Parámetros	Descripción
Horas de oficina	

Parámetros	Descripción
Hora de inicio	Inicio del horario de oficina diurno (horario comercial) Ajuste para el estado de presencia de los clientes de CU Valor estándar: 07:00 **Nota:** El valor ingresado debe estar en formato de 24 horas (HH:MM).
Hora de fin	Fin del horario de oficina diurno (horario comercial) Ajuste para el estado de presencia de los clientes de CU Valor estándar: 19:00 **Nota:** El valor ingresado debe estar en formato de 24 horas (HH:MM).
Longitud de la contraseña	
Extensiones	Longitud de la contraseña de los clientes de CU. El valor mínimo es 6. ***NOTA:*** Al cambiar la longitud de la contraseña, se restablecen las contraseñas de todos los usuarios. Valor estándar: 6
Núm. de tel. de puesto de interceptación	
Número de destino	Núm. de tel. de puesto de interceptación ***INFO:*** Hay que registrar el número de teléfono del puesto de interceptación configurado en el sistema de comunicación.
Mensaje instantáneo	
Desactivar Mensajería instantánea	Si el flag está activado, no se pueden enviar mensajes instantáneos. Valor estándar: Desactivado
Extensiones analógicas	
Modo de usuario analógico	Definición de la visualización de las extensiones analógicas en el directorio interno Valor estándar: Mostrar todo
Modo de usuario analógico: Mostrar todo	Todas las extensiones analógicas se muestran en el directorio interno
Modo de usuario analógico: Mostrar sólo con nombre	En el directorio interno solo se muestran extensiones analógicas con un nombre.
Modo de usuario analógico: Sin muestra	En el directorio interno no se muestra ninguna extensión analógica.
Extensión	

Parámetros	Descripción
Longitud externa máx.	Número máximo de dígitos en los números de teléfono internos Para proteger contra el abuso de tasas no se pueden marcar números internos más largos. Valor estándar: 4
Longitud externa mín.	Número mínimo de dígitos en los números de teléfono externos Valor estándar: 3
Transferir	
SST de puesto de operadora automático normal	Si el flag está activado, se transfiere una llamada, tanto si el destino está libre como ocupado. Valor estándar: Activado
Diario	
Permitir borrado de entradas de diario	Este flag permite o impide que un usuario elimine una entrada de diario.
Longitud externa mín.	
Formato de fax	
Usar PDF como formato de fax	Si el flag está activado, el fax se puede guardar en formato PDF; si no lo está, se guarda en formato TIFF.
Servidor Directory	
Proveedor externo lento	Este flag mejora el tiempo de respuesta al hacer clic con el botón secundario sobre un correo electrónico. Además, si está activado, las búsquedas de contactos solo se ejecutan en el directorio principal de Exchange, no en los subdirectorios.
Longitud de la verificación	Se debe introducir un dígito del 4 al 8 para definir la longitud de los números CLI de la búsqueda en LDAP en myPortal for Desktop y myPortal for Outlook. El número máximo (8) se puede configurar para que la búsqueda sea más exacta y mejorar el rendimiento del sistema. Valor estándar: 4
Marcar por nombre - Buscar solo extensión local	Si este flag está activado, la función de marcación por nombre se limita al nodo en activo (función local). Si este flag no está seleccionado, la función antigua sigue estando disponible; así, se consideran todos los usuarios de la red pero el anuncio solo se reproduce después de seleccionar un usuario local.
La caché de búsqueda del directorio caduca en	Configure la cantidad de minutos o un rango de minutos que usa la memoria de la caché al buscar contactos. El rango de minutos que puede establecer es de 1 a 60 minutos. Cuando el valor es "0", esta función estará desactivada.
Buscar por número de teléfono	Cuando esta bandera está marcada, puede buscar en directorios por número de teléfono.
TLS	

Parámetros	Descripción
Se usa TLS para conexiones de cliente	Por condiciones de la red, puede ser necesario desactivar la conexión de servidor de cliente seguro. Cambiar esta configuración requiere reiniciar la aplicación UC. Esto solo se debe realizar en casos muy concretos.
Presencia	
Ocultar estado de enfermo	Cuando este indicador está activado, el estado de presencia “enfermo” no está disponible para su uso. Valor estándar: Desactivado
Nombre de usuario	
Deshabilitar la edición de nombres	Si el flag está activado, los usuarios no pueden cambiar su nombre y apellido configurados. Valor estándar: Desactivado
Tablero	
Deshabilitar tablero	Cuando este flag está activado, el Tablero no está disponible.
Mostrar nombres de agentes en el enlace de cola de myAgent	Cuando se configura este flag, junto con el número de extensión de un agente, también aparece un nombre que el usuario puede configurar. Un usuario mostrará "Hotdesk" cuando esté usando una extensión que no sea la suya. Valor estándar: Desactivado.
Grabación de la llamada	
Grabación de la llamada	Cuando esta bandera está activada, es posible la grabación de llamadas. Valor estándar: Activado
Reproducir indicación antes de la grabación	Si el flag está activado, antes de comenzar una grabación se reproduce un anuncio grabado. Valor estándar: Desactivado
Reproducir tono pip durante la grabación	Para OpenScape Business S, si el flag está activado, durante la grabación se reproduce un tono de aviso. Valor estándar: Activado
Disponibilidad de grabación en vivo de conferencias	Cuando esta bandera está activada, es posible la grabación de conferencias. Valor estándar: Desactivado
Protocolización de sistema	
Mensajes de protocolo Trace (detallados)	Si el flag está activado, los mensajes trace se graban diariamente en un archivo de protocolo. Valor estándar: Desactivado
Registros de cliente	
Ruta de registro de cliente	Ruta de carpeta para los archivos de registro de cliente (archivos de protocolo de la UC Suite)

Parámetros	Descripción
Habilitar carga de protocolos	Si el flag está activado, se guardan registros de cliente en el disco duro de la tarjeta UC Booster Card (OCAB), del servidor UC Booster Server o del sistema de comunicación OpenScape Business S. Valor estándar: Activado
Activar protocolización de cliente	Si el flag está activado, se graban registros de cliente. Valor estándar: Activado
Notificaciones de email	
Habilitar notificaciones de email para errores de sistema	Si el flag está activado, se envían correos electrónicos para informar al Destinatario o destinatarios indicados sobre el nivel de uso crítico del disco duro o sobre errores. Valor estándar: Activado
Activar correo electrónico de invitación de myPortal	Cuando se activa esta bandera, los usuarios de UC Suite recibirán un correo electrónico de invitación para instalar o actualizar el cliente myPortal. Este correo electrónico normalmente se envía a todos los usuarios de UC Suite con una dirección de correo electrónico válida en el Directorio de usuarios en una nueva instalación, cuando se agrega o cambia una dirección de correo electrónico para un usuario de UC Suite en el Directorio de usuarios o después de que se haya producido una actualización del software OpenScape Business y Nueva versión del cliente está disponible. Valor estándar: Activado
Destinatarios	Direcciones de correo electrónico a las que se envían las notificaciones de email.
Condiciones	
Enviar mensajes críticos	Si el flag está activado, las notificaciones importantes se envían por correo electrónico (por ejemplo, en caso de fallos del sistema) Valor estándar: Activado
Enviar notificaciones de caída del sistema	Si el flag está activado, se envía una notificación por correo electrónico si se produce una caída del sistema. Valor estándar: Activado
Al informar de errores, enviar las últimas … líneas del archivo de protocolo	Definición del número de líneas de un archivo de protocolos que se envían con un correo electrónico. Valor estándar: 100
Mantenimiento	

Parámetros	Descripción
Comenzar mantenimiento de sistema a las	Definición de la hora en la que cada día se borran los datos que han superado los tiempos de retención definidos: • Mensajes • Información de llamada en el diario de llamadas (Historial de llamadas) • Llamadas grabadas con myAgent (Contact Center) • Faxes y correos electrónicos recibidos y enviados del Contact Center • Archivos de protocolo Valor estándar: 2:00 horas
Mensaje	
Conservar mensajes de bandeja de entrada para	Tiempo de retención en días para mensajes de voz de la bandeja de entrada Valor estándar: 60
Conservar mensajes leídos/ reproducidos para	Tiempo de retención en días para mensajes de voz reproducidos/leídos Valor estándar: 30
Conservar mensajes guardados para	Tiempo de retención en días para los mensajes de voz guardados Valor estándar: 365
Conservar mensajes eliminados para	Tiempo de retención en días para mensajes de voz borrados Valor estándar: 30
Fax	
Conservar los faxes de bandeja de entrada durante	Tiempo de retención en días para mensajes de fax en la bandeja de entrada Valor estándar: 30
Conservar los faxes leídos durante	Tiempo de retención en días para los mensajes de fax leídos Valor estándar: 30
Conservar los faxes borrados durante	Tiempo de retención en días para los mensajes de fax eliminados Valor estándar: 30
Conservar los faxes enviados durante	Tiempo de retención en días para mensajes de fax enviados Valor estándar: 30
Mantenimiento de información de llamadas	
Conservar historial de llamadas para	Tiempo de retención en días para las llamadas del diario Valor estándar: 30
Cerrar conversación después	Tiempo de retención en días para las conversaciones de llamadas abiertas del diario. Las llamadas sin responder del/al mismo contacto durante este periodo se añadirán a la pestaña Llamadas abiertas, ligada a la misma conversación. Al finalizar este periodo, todas las llamadas de una conversación se marcan como finalizadas automáticamente y se borran de la pestaña Llamadas abiertas. Valor estándar: 3 Valor máximo: 30

Parámetros	Descripción
Centro de contactos	Tiempo de retención en días para las llamadas grabadas con myAgent y los faxes y correos electrónicos recibidos y enviados del Contact Center Valor estándar: 30
Mantenga CC en vivo grabando/devolución de llamada/correo electrónico/ llamadas de fax para	Período de retención en días para todos los datos de comunicación asociados con las llamadas, como mensajes de devolución de llamada, llamadas grabadas en vivo, llamadas de fax y correos electrónicos. Valor estándar: 30
Mantenimiento de archivo de protocolo	
Conservar información de protocolo para	Tiempo de retención en días para los archivos de protocolo Valor estándar: 10
Mensaje instantáneo	
Conservar mensajes instantáneos durante	Período de retención en días para mensajes instantáneos. Valor estándar: 30
Informes	
Restablecer contraseña	Restablece la contraseña del administrador de myReports a la contraseña predeterminada.
Restablecer todas las contraseñas de usuario	
Restablecer todas las contraseñas de usuario	Restablece las contraseñas de todos los usuarios, permite contraseñas de hasta 6 caracteres. **Nota:** En este caso, la contraseña predeterminada está configurada en 6 caracteres (123456).
Buzón de voz	
Idioma de buzón de voz	Configuración previa de idioma para el menú y los anuncios grabados del buzón de voz propios del sistema
Orden de reproducción de mensajes de voz	Definición del orden de reproducción de los mensajes de voz Valor estándar: El más reciente primero
Orden de reproducción de mensajes de voz: El más reciente primero	Primero se presenta el mensaje de voz más reciente.
Orden de reproducción de mensajes de voz: El más antiguo primero	Primero se presenta el mensaje de voz más antiguo.
Tiempo de grabación de mensaje de voz	Definición de la duración máxima de la grabación para mensajes de voz, en segundos Valor estándar: 900

Parámetros	Descripción
Modo buzón de voz	Definición del abanico de funciones del buzón de voz Valor estándar: Completo
Modo buzón de voz: Completo	Todo el volumen de funciones del buzón de voz
Modo buzón de voz: Menú abreviado	Después del anuncio grabado personalizado o relativo al estado se ofrece la conexión con la recepción.
Modo buzón de voz: Sin menú de buzón de voz	Después del anuncio de bienvenida, el llamante es transferido directamente a la grabación de voz.
Permitir devolución de llamada desde VM solo a números conocidos	Si el flag está activado, se impide que accedan al buzón de voz los llamantes cuyo número no esté memorizado en el cliente de CU. Valor estándar: Activado
Omita la indicación "por favor deje un mensaje después del tono"	Cuando se activa esta bandera, se omitirá el mensaje "deje un mensaje después del tono". Valor estándar: Desactivado
Contact Card Mapping	
Microsoft: Disponible (verde)	El estado de presencia de UC de esta fila se asigna al estado de Outlook disponible (verde).
Microsoft: Fuera del trabajo (amarillo)	El estado de presencia de UC de esta fila se asigna al estado de Outlook Fuera del trabajo (amarillo).
Microsoft: Ocupado (rojo)	El estado de presencia de UC de esta fila se asigna al estado de Outlook Ocupado (rojo).
Microsoft: Fuera de servicio (gris)	El estado de presencia de UC de esta fila se asigna al estado de Outlook Fuera de servicio (gris).

28.4.4.14 OpenScape Business UC Suite > Perfiles

Descripción de parámetros de las pestañas:

- **Añadir / Editar**

Parámetros	Descripción
Perfiles	Los perfiles de usuario guardan ajustes de configuración de usuarios de la UC Suite. Se pueden asignar varios usuarios (miembros) a un perfil de usuarios. Todos los miembros del perfil tienen (en principio) los mismos ajustes de configuración. Se pueden crear varios perfiles que permiten diferentes ajustes previos para distintos grupos de usuarios.
Nombre	Nombre del perfil (entrada libre)
Detalles personales	
Mis detalles personales	Datos personales seleccionados para los usuarios asignados. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.

Parámetros	Descripción
Mis preferencias	
Apariencia	Aspecto e idioma del cliente UC del usuario asignado. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Notificación	Notificaciones para los usuarios asignados. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Conectividad de Outlook	Integración en el calendario para los usuarios asignados. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Teclas de acceso rápido	Activación y configuración de combinaciones de teclas para acceder a varias funciones de uso habitual a través del teclado. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Varios	Retorno automático al estado de presencia "Oficina", método de transferencia y tiempo de retención del diario de llamadas para los usuarios asignados. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Reglas de llamada	
Destinos de reenvío	Destinos de reenvío para llamadas entrantes en función del estado de presencia para los usuarios asignados. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Comunicaciones	
Ajustes del buzón de voz	Grabación de mensaje de voz en función del estado de presencia para los usuarios asignados. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Notificación de buzón de voz	Notificación en caso de nuevos mensajes de voz para los usuarios asignados. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Notificación de fax	Notificación en caso de nuevos mensajes de fax para los usuarios asignados. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Notificaciones de llamadas perdidas	Servicio de notificación de llamadas perdidas.
Perfiles	
Perfiles	AutoAttendant personal para los usuarios asignados. Los usuarios correspondientes deben grabar un anuncio grabado para la selección. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Sensibilidad	
Seguridad y acceso	Permitir la escucha de mensajes de voz con myAttendant y consulta del buzón de voz desde un teléfono propio sin contraseña. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Visibilidad de presencia	Extensiones internas que pueden ver el estado de presencia. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.

Parámetros	Descripción
Presencia de buzón de voz	Llamantes internos o externos a los que hay que informar del estado de presencia a través de anuncios automáticos del buzón de voz. El símbolo del candado establece si el usuario puede modificar él mismo estos ajustes.
Favoritos	
Favoritos	Grupos favoritos con una lista de contactos que se pueden asignar al usuario.

Descripción de los parámetros de las pestañas:

- **Asignar usuarios**

Parámetros	Descripción
Usuarios asignados	Usuarios a los que se aplicará el perfil
Usuarios disponibles	Usuarios a los que se puede aplicar el perfil

Descripción de los parámetros de las pestañas:

- **Eliminar**

Parámetros	Descripción
Nombre	Nombre del perfil (entrada libre)
Usuarios	Usuarios a los que se aplicará el perfil

28.4.4.15 OpenScape Business UC Suite > Encabezados de fax

Descripción de los parámetros de las pestañas:

- **Editar**
- **Añadir**
- **Eliminar**

Parámetros	Descripción
Nombre de plantilla / Nombre	Nombre del encabezado (debe ser único).
Texto	Se pueden incluir marcadores de posición para fecha/hora, nombre de empresa, nombre de usuario, teléfono de empresa, número de página y número total de páginas.

28.4.5 Web Services

En **Web Services** se reunen las funciones para configurar las interfaces web, como p. ej. Web Collaboration.

28.4.5.1 Web Services > Web Collaboration

Para la integración de Web Collaboration mediante un Public Server (servidor de Web Collaboration como servicio en Internet) o mediante un Custom Server (servidor de Web Collaboration en la red de clientes o en un colateral).

Descripción de parámetros de las pestañas:

- **Servidor de Web Collaboration**

Parámetros	Descripción
Tipo de servidor	Selección del servidor de Web Collaboration.
Tipo de servidor: **Servidor público**	El servidor de Web Collaboration es un Public Server y está en Internet. Por ello se utiliza una conexión segura https. Además se requiere un número de licencia y una contraseña. De forma predeterminada se utiliza el puerto TCP 5100.
Tipo de servidor: **Servidor público (modo demo/modo de evaluación)**	La prueba de Web Collaboration puede durar 5 minutos. No hace falta introducir la dirección IP, el número de licencia ni la contraseña.
Tipo de servidor: **Servidor personalizado**	El servidor de Web Collaboration es un Custom Server y se encuentra en la red de clientes o en un colateral. Se puede utilizar una conexión segura https o un conexión http sin seguridad. Si la conexión se establece mediante https se requiere además un número de licencia y una contraseña. De forma predeterminada se utiliza el puerto TCP 5004.
Tipo de servidor: **Sin servidor de Web Collaboration**	No se utiliza ningún servidor de Web Collaboration. La opción para iniciar una sesión de Web Collaboration está desactivada en los clientes de Unified Communications.

URL/Dirección IP	Entrada de la dirección URL/IP del servidor de Web Collaboration correspondiente. Public Server mediante https y Custom Server mediante https o http.
	Ejemplo:
	`http://<Dirección IP Web Collaboration Server>:5004/OscInterface`
	`https://<Dirección IP Web Collaboration Server>:5100/XMLRPSecure`

Número de licencia	Número de licencia para la conexión protegida con el servidor de Web Collaboration.
Contraseña	Contraseña para la conexión protegida con el servidor de Web Collaboration.

28.4.6 Open Directory Service

En **Open Directory Service** se reúnen las funciones para configurar el Open Directory Service.

28.4.6.1 Open Directory Service > Ajustes básicos

Parámetros	Descripción
Activar/desactivar Open Directory Service	Valor estándar: desactivado
Credenciales de inicio de sesión del servidor LDAP	Credenciales de inicio de sesión del servidor de base de datos externo. Open Directory Service debe estar autorizado a acceder a la base de datos externa, en su caso hay que añadir un usuario propio en el servidor.

28.4.6.2 Fuentes de datos > Open Directory Service > Usuarios OpenScape Business

Descripción de parámetros de las pestañas:

- **Descripción general de las fuentes de datos configuradas**

Parámetros	Descripción
Usuarios OpenScape Business	Directorio interno de UC Suite. El directorio se asigna permanentemente al Open Directory Service y no se puede eliminar ni cambiar.
Directorio externo de UC Suite	Fuente de datos externa para sistemas UC Suite. El directorio se asigna permanentemente al Open Directory Service y no se puede eliminar ni cambiar.
Directorio global	Fuente de datos del directorio global para sistemas que no son UC Suite. El directorio se asigna permanentemente al Open Directory Service y no se puede eliminar ni cambiar.
Marcación rápida	Números centrales de marcación rápida. El directorio se asigna permanentemente al Open Directory Service y no se puede eliminar ni cambiar.
Añadir/Editar/Eliminar	Fuentes de datos externas para información de contacto de bases de datos con acceso de lectura mediante ODBC.

Descripción de parámetros de las pestañas:

- **Editar fuente de datos**

Parámetros	Descripción
Nueva fuente de datos	Los parámetros de las fuentes de datos añadidas se pueden cambiar aquí.

28.4.6.3 Open Directory Service > Fuentes de datos > LXV3

Parámetros	Descripción
Marcaciones abreviadas	Números de marcación directa centrales. El directorio está asignado de forma fija a Open Directory Service y no se puede borrar ni modificar.

28.4.6.4 Open Directory Service > Fuentes de datos > LXV3

Parámetros	Descripción
Resumen de las fuentes de datos configuradas	Una asignación de salida de datos LDAP establece qué campos del esquema de datos de Open Directory Service se emitirá a través de LDAP, por ejemplo, para clientes LDAP específicos o para distintos grupos de suscriptores que no deban ver todos los datos sino solo una selección. La asignación de salida de datos LDAP web está disponible de forma predeterminada y no se puede borrar ni modificar. En este tipo de asignación, todos los campos del esquema de datos de Open Directory Service están asignados a la salida LDAP. Puede configurar otras asignaciones de salida de datos LDAP.
Añadir	Añadir otras asignaciones de salida de datos. A través del parámetro dc del inicio de sesión LDAP, los clientes LDAP pueden acceder a una determinada asignación de salida de datos LDAP, por ejemplo, dc=web.

28.4.6.5 Open Directory Service > Mantenimiento

Descripción de parámetros de las pestañas:

- **Mantenimiento**

Parámetros	Descripción
Comprobar/Reiniciar el Open Directory Service	Indicación de estado de Open Directory Service (gris = desactivado; rojo = configuración errónea o fuente de datos no disponible; verde = activo)
Reinicio	Reinicio de Open Directory Service

28.4.7 Application Launcher

En **Application Launcher** se reúnen las funciones para configurar el Application Launcher.

28.4.7.1 Application Launcher

Parámetros	Descripción
Carga del archivo de configuración	Perfil con datos de configuración de Application Launcher para configurar rápidamente el Application Launcher en todos los PC cliente. Una vez concluida la configuración de Application Launcher en un usuario, el administrador puede ofrecer ese perfil con los datos de configuración de Application Launcher en el sistema de comunicación. A continuación, todos los usuarios pueden importar el perfil y utilizarlo para configurar Application Launcher.
Perfil	Tipo de archivo autorizado .xml

28.5 Middleware

Las funciones para configurar el middleware se agrupan en **Middleware**.

28.5.1 Reproductor de anuncios

Descripción de parámetros de las pestañas:

- **Configuración del reproductor de anuncios**
- **Estadísticas del reproductor de anuncios**

Parámetros	Descripción
Activación	
El servicio se iniciará automáticamente	Activación o desactivación del dispositivo de reproducción de anuncios.
Estadísticas del reproductor de anuncios	Aquí se muestra el estado del dispositivo de anuncio. Los datos se actualizan automáticamente cada 5 minutos. Sin embargo, la página también se puede actualizar manualmente.

28.5.2 Distribuidor de mensajes CSTA (CMD)

Descripción de parámetros de las pestañas:

- **Ajustes - CSTA Message Dispatcher (CMD)**
- **Estadísticas - CSTA Message Dispatcher (CMD)**

Parámetros	Descripción
Activación	
El servicio se inicia automáticamente	Activar o desactivar el CSTA Message Dispatcher (CMD). El CMD establece conexión entre los clientes OpenScape Business TAPI 120 y el sistema de comunicación y es necesario para la funcionalidad.
Registro automático	
Registro automático del cliente activado	Activar o desactivar el inicio de sesión automático de los clientes. El registro automático significa que se pueden incluir nuevas entradas en la lista del firewall CTI. El firewall CTI se configura automáticamente. Una vez registrados todos los clientes autorizados, se puede retirar la marca de verificación para impedir el registro de nuevas entradas en el firewall CTI. Se puede autorizar a un PC para que supervise una extensión determinada. Las licencias TAPI/CTI se deben adquirir por separado.
Firewall CTI	
Eliminar	Las entradas con una marca de verificación en la columna Eliminar se borran de la lista de clientes autorizados al hacer clic en el botón **Aplicar**. Se rechaza el inicio de sesión, siempre que el registro automático no esté activo.

Parámetros	Descripción
ID de aplicación	Nombre del PC desde el que se puede supervisar una extensión. Al utilizar el nombre de PC también se puede utilizar DHCP para los PC OpenScape Business TAPI 120.
Número de llamada	Número de teléfono interno de la extensión que se puede supervisar.
Estadísticas - CSTA Message Dispatcher (CMD)	Aquí aparece el estado del CMD. Durante el servicio se puede comprobar qué OpenScape Business TAPI 120 están conectados con el CMD encargado de asignar las posibles licencias. Los datos se actualizan automáticamente cada 5 minutos. No obstante, la página también se puede actualizar manualmente.

28.5.3 Proveedor de servicios CSTA (CSP)

Descripción de parámetros de las pestañas:

- **Configuración de proveedor de servicios CSTA (CSP)**
- **Estadísticas - CSTA Service Provider (CSP)**

Parámetros	Descripción
Activación	
El servicio se inicia automáticamente	Activar o desactivar el proveedor de servicios CSTA (CSP, CSTA Service Provider). El CSP se requiere para la UC Suite, para el servidor DSS (Gestor de presencia, solo en interconexión), el OpenScape Business TAPI 170 y para aplicaciones CSTA externas.
Acceso CSTA	
ID de usuario CSTA / **Contraseña de usuario CSTA**	OpenScape Business TAPI 170 y las aplicaciones CSTA externas solo se pueden registrar en el CSP con la cuenta de usuario que haya configurada aquí. Si no hay configurado ningún usuario CSTA, no se pueden utilizar OpenScape Business TAPI 170 ni las aplicaciones CSTA externas en el CSP.
Estadísticas - CSTA Service Provider (CSP)	Aquí aparece indicado el estado del CSP. Se ve cuántas aplicaciones hay conectadas con el CSP y cuáles son. Las aplicaciones desconocidas aparecen marcadas con el valor "Estándar". Se puede consultar el estado de conexión con los distintos nodos de la red/el nodo local. Los datos se actualizan automáticamente cada 5 minutos. No obstante, la página también se puede actualizar manualmente.

28.5.4 Servidor DSS

Descripción de parámetros de las pestañas:

- **Configuración de servidor DSS**
- **Estadísticas - Servidor DSS**

Parámetros	Descripción
Activación	
El servicio se inicia automáticamente	Activar o desactivar el servidor DSS.

Parámetros	Descripción
Estadísticas - Servidor DSS	Aquí se muestra el estado del servidor DSS. Los datos se actualizan automáticamente cada 5 minutos. No obstante, la página también se puede actualizar manualmente.

28.5.5 Media Extension Bridge (MEB)

Descripción de parámetros de las pestañas:

- **Configuración de Media Extension Bridge (MEB)**
- **Estadísticas - Media Extension Bridge (MEB)**

Parámetros	Descripción
Activación	
El servicio se inicia automáticamente	Activar o desactivar el Media Extension Bridge.
Estadísticas - Media Extension Bridge (MEB)	Aquí aparece indicado el estado del MEB. Los datos se actualizan automáticamente cada 5 minutos. No obstante, la página también se puede actualizar manualmente.

29 Anexo

Este anexo ofrece información de referencia, por ejemplo, sobre los idiomas admitidos, estándares, límites de ampliación y capacidades, prestaciones Euro-RDSI, códigos para activar y desactivar prestaciones, códigos de prestación a través de MF y protocolos IP y números de puerto utilizados.

29.1 Estándares admitidos

Aquí obtendrá información sobre los estándares compatibles.

Ethernet

- RFC 894 Ethernet II Encapsulation
- IEEE 802.1Q VLAN (LAN virtuales)
- IEEE 802.2 Logical Link Control
- IEEE 802.3u 100BASE-T
- IEEE 802.3ab Gigabit Ethernet
- IEEE 802.3X Full Duplex Operation

Encaminamiento IP

- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 2822 Internet Message Format
- RFC 826 ARP
- RFC 2131 DHCP
- RFC 1918 IP Addressing
- RFC 1332 El protocolo PPP de control de IP (Internet Protocol Control, IPCP)
- RFC 1334 Protocolos PPP de autenticación (PPP Authentication Protocols)
- RFC 1618 PPP sobre RDSI
- RFC 1661 El protocolo Point-to-Point (PPP)
- RFC 1877 Protocolo PPP de control de IP (Internet Protocol Control, IPCP)
- RFC 1990 El protocolo Multilink PPP (MP)
- RFC 1994 Protocolo PPP de Autenticación por Desafío Mutuo (Challenge Handshake Authentication Protocol)
- RFC 2516 Un método para la transmisión de PPP a través de Ethernet (PPPoE)
- RFC 3544 Compresión de Cabecera IP sobre PPP

Traducción dirección red (NAT)

- RFC 2663 NAT

IPSec

- RFC 2401 Arquitectura de seguridad para el Protocolo de Internet (IP)
- RFC 2402 Cabecera de autenticación IP (AH)
- RFC 2403 Autenticación IPSec: MD5
- RFC 2404 Autenticación IPsec - SHA-1

- RFC 2405 Cifrado IPSec: DES
- RFC 2406 ESP: Cifrado IPSec
- RFC 2407 IPSec DOI
- RFC 2408 ISAKMP
- RFC 2409 IKE
- RFC 2410 Cifrado IPSec: NULL
- RFC 2411 IP plan de trabajo de seguridad de documentos
- RFC 2412 OAKLEY

SNMP

- RFC 1213 MIB-II

QoS

- IEEE 802.1p Priority Tagging
- RFC 1349 Tipo de Servicio en la suite IP
- RFC 2475 Arquitectura de Servicios diferenciados
- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)

Servicios

- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)

Códecs

- G.711
- G.729

VoIP por SIP

- RFC 2198 RTP Payload for Redundant Audio Data
- RFC 2327 SDP Session Descripción Protocol
- RFC 2617 Autenticación HTTP: Autenticación de acceso básico y Digest
- RFC 2782 DNS RR para especificar la ubicación de servicios (DNS SRV)
- RFC 2833 RTP carga útil de dígitos DTMF, tonos de la telefonía y señales de telefonía
- RFC 3261 SIP Session Initiation Protocol
- RFC 3262 Provisional Response Acknowledgement (PRACK) Early Media
- RFC 3263 SIP: localización de los servidores
- RFC 3264 An Offer/Answer Model with the Session Description Protocol
- RFC 3310 HTTP Digest Authentication
- RFC 3311 Session Initiation Protocol (SIP) UPDATE Method
- RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3325 Extensiones privadas para el Session Initiation Protocol (SIP) para la identidad dentro de las redes de confianza
- RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3489 STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515 The Session Initiation Protocol (SIP) Refer Method
- RFC 3550 RTP: Protocolo de transporte para aplicaciones en tiempo real

- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3581 An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
- RFC 3891 The Session Initiation Protocol (SIP) Replaces Header

Otros

- RFC 959 FTP
- RFC 1305 NTPv3
- RFC 1951 DEFLATE

29.2 Prestaciones Euro-RDSI

Las prestaciones RDSI pueden utilizar en cualquier conexión Euro-RDSI, si el hardware disponible (por ejemplo, teléfono o tarjeta RDSI) está debidamente configurado. Las prestaciones están disponibles de forma permanente en la central o se activan y desactivan por código.

La disponibilidad de las prestaciones depende del proveedor de red. Algunas de las prestaciones indicadas están sujetas a costes.

Tema	Explicación
Número de llamada múltiple (MSN = Multiple Subscriber Number)	Pueden asignarse varios números de teléfono a cada acceso individual. Los usuarios pueden encargarse de asignar, en su terminal, estos números de teléfono a los distintos terminales.
Transmisión del número de teléfono (CLIP = Calling Line Identification Presentation)	Se transmite y muestra el número de teléfono propio al usuario llamado. Aparecerá, por ejemplo, en la pantalla del teléfono o se guarda, en caso de no contestar, en la lista de llamadas. No se pueden transmitir números de teléfono falsos. Sin embargo, los sistemas de telecomunicaciones no pueden comprobar la marcación directa. Se puede suprimir de forma permanente, o según el caso, la transmisión del número de teléfono propio.
Supresión de la indicación del número de llamada (CLIR = Calling Line Identification Restriction)	También se puede desactivar de forma permanente, o según el caso, la transmisión del número de teléfono. En tal caso, la muestra del número de teléfono en el usuario B solo será posible con determinadas conexiones definidas de forma específica (emergencias, policía, bomberos).
Identificación de llamadas maliciosas (MCID = Malicious Call Identification)	El usuario llamado puede identificar a llamantes anónimos a través del puesto de conmutación, también si la transmisión de números de teléfono está desactivada. Esta prestación está sometida a cargo.
Cambio en el bus (TP = Portabilidad de terminales)	Esta prestación permite conectar el terminal RDSI a otra toma RDSI durante una conexión en curso y continuar la conversación. La conversación debe ser aparcada antes del cambio de conexión.

Tema	Explicación
Subdireccionamiento (SUB = Subaddressing)	Esta función puede utilizarse de forma adicional al número de teléfono normal, sometida a cargo. El subdireccionamiento permite controlar un terminal llamable (por ejemplo, un programa en el PC) en función del llamante.
Señalización usuario a usuario (UUS = User-to-User Signalling)	Durante el establecimiento y cierre de la conexión pueden intercambiarse informaciones en el canal D. La transmisión es posible en ambas direcciones.
Grupo de usuarios cerrado (CUG = Closed User Group)	Si esta prestación está activada, no se pueden establecer llamadas fuera del grupo de usuarios (excepto los números de emergencia 110 y 112). También se pueden bloquear llamantes externos.
Desvío de llamada en caso de ocupado (CFB = Call Forwarding Busy)	Esta transferencia de llamadas desvía las llamadas en caso de ocupado a cualquier conexión telefónica disponible. La transferencia diferida de llamadas se realiza en el puesto de interceptación. De esta forma, los dos canales portadores se mantienen libres.
Desvío de llamada directo (CFU = Call Forwarding Unconditional)	Esta transferencia de llamadas desvía las llamadas de forma inmediata a cualquier conexión telefónica disponible. La transferencia diferida de llamadas se realiza en el puesto de interceptación. De esta forma, los dos canales portadores se mantienen libres.
Desvío de llamada diferido (CFNR = Call Forwarding No Reply)	Esta transferencia de llamadas desvía las llamadas pasados 20 segundos (si no se puede establecer comunicación) con cualquier conexión telefónica disponible. La transferencia diferida de llamadas se realiza en el puesto de interceptación. De esta forma, los dos canales portadores se mantienen libres.
Aviso de llamada en espera (CW = Call Waiting)	Durante una conexión en curso se señaliza a un segundo llamante. El llamante escucha, mientras tanto, el tono de libre. La conexión puesta en espera puede ser aceptada, rechazada o simplemente ignorada.
Alternar (Hold = Call Hold)	Durante una conexión en curso se puede establecer una segunda conexión por consulta. La comunicación alternativa se da cuando se alterna entre ambas conexiones. El interlocutor puesto en espera no puede escuchar la conversación activa.
Conferencia tripartita (3PTY = Three Party Service)	Se pueden conectar dos conexiones en curso. Permite una conferencia telefónica con 3 usuarios.
Devolución automática de llamada en caso de ocupado (CCBS = Completion of Calls to Busy Subscriber)	Si el usuario llamado está ocupado, puede activarse esta prestación. En cuanto la conexión del usuario vuelve a estar libre se recibe una señal. Al descolgar el auricular se establece la conexión.

Tema	Explicación
Indicación de tasas al final de la comunicación (AOCE = Advice of Charge (End))	Si lo desea, puede visualizar las tasas al final de la comunicación. No se tienen en cuenta posibles descuentos y tarifas.
Indicación de tasas durante la comunicación (AOCD = Advice of Charge (During))	Si lo desea, puede visualizar las tasas durante la comunicación. No se tienen en cuenta posibles descuentos y tarifas.

29.3 Puertos utilizados

Los componentes del sistema OpenScape Business utilizan diferentes puertos; es posible que deba abrirlos en el firewall, en caso necesario. Para los puertos de los clientes basados en web (por ejemplo, myPortal to go), en el router debe configurarse el desvío de puertos.

Una lista real y completa de todos los puertos utilizados de OpenScape Business está disponible en la «Base de datos de gestión de interfaces» (IFMD) a la que se puede acceder a través del portal de socios de Unify (https://unify.com/en/partners/partner-portal.

Nota: Los puertos identificados con "O" en la lista siguiente son opcionales, es decir, no están abiertos permanentemente en el firewall.

Descripción	TCP	UDP	Número de puerto	OpenScape Business X	Tarjeta de refuerzo UC	OpenScape Business S	UC Booster Server
Componentes del sistema							
Portal de administración (https)	X		443	X	X	X	X
Controles CAR Alive	X		12062	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
CLS	X		7780, 7790 (hasta V3R3) 7780, 7791 (a partir de V3R3.1)	O		O	
Programa de instalación de clientes de comunicaciones	X		8101	X	X	X	X
Distribuidor de mensajes CSTA (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	

Descripción	TCP	UDP	Número de puerto	OpenScape Business X	Tarjeta de refuerzo UC	OpenScape Business S	UC Booster Server
Proveedor de servicios CSTA (CSP)	X		8800		X	X	X
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000-40040	O		O	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Mensajería instantánea (http)	X		8101	X	X	X	X
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS servicio cloud	X		8602	X			
Servidor LDAP	X		389		X	X	X
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
NAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
Openfire Admin (https)	X		9091		X	X	X
Servicio de actualización automática OpenScape Business (http)	X		8101	X	X	X	X
OpenScape Business Multisite	X		8778		X	X	X
OpenScape Business myReports (http)	X		8101		X	X	X
OpenScape Business Status Server	X		8808	X		X	X
OpenScape Business User Portal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (incrustado)		X	29100-30530	X	X	X	X
RTP (servidor)		X	29100-30888	X	X	X	X
SIP (servidor)	X	X	5060	X		X	
SIP TLS SIPQ (servidor)	X		5061	X		X	

Descripción	TCP	UDP	Número de puerto	OpenScape Business X	Tarjeta de refuerzo UC	OpenScape Business S	UC Booster Server
SIP TLS Subscriber (servidor)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (capturas)		X	162	X		X	
VSL	X		8770-8780		X	X	X
Webadmin para Clientes	X		8803	X	X	X	X
Clientes basados en Web							
Clientes basados en Web (http)	X		8801	X	X	X	X
Clientes basados en Web (https)	X		8802	X	X	X	X

Nota: Por motivos de seguridad, recomendamos utilizar únicamente https para los clientes basados en web y configurar el desvío de puertos desde el TCP/443 externo al TCP/8802 interno.

Certificado CLS

A partir de V3R3.1 se proporciona un nuevo certificado CLS con un nombre común (CN) actualizado mediante un puerto introducido recientemente. Esto ofrece un algoritmo de compendio mejorado y más sólido, así como entidades legales actualizadas. Los sistemas con licencia en línea a través del modo CLS Connect necesitan los siguientes dos requisitos previos:

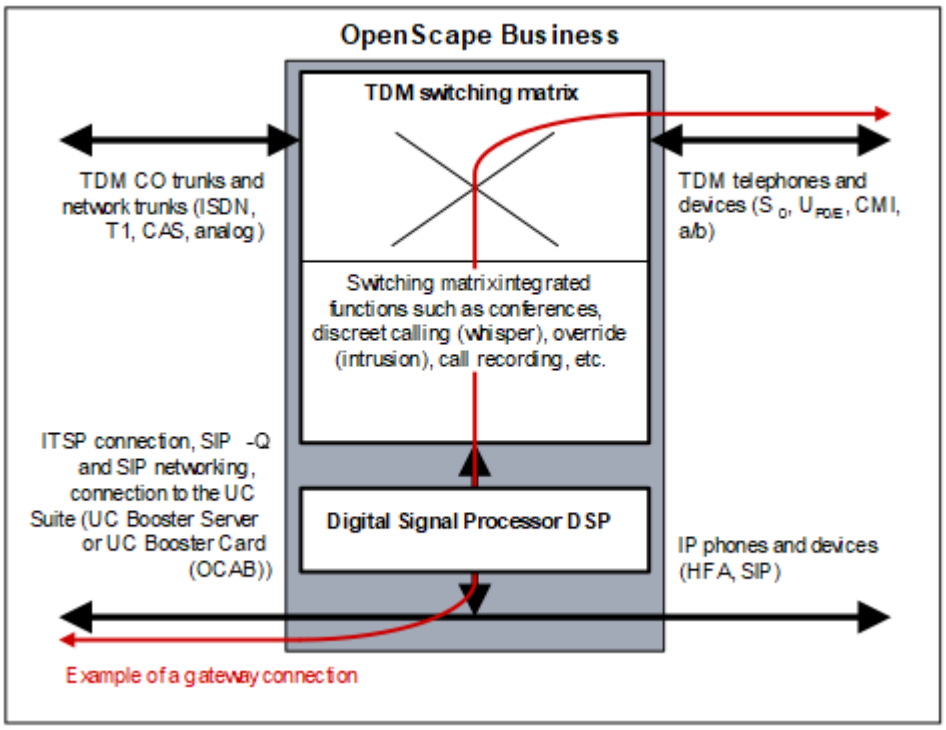
- La dirección IP 188.64.16.4 está habilitada en el cortafuegos para el tráfico saliente.
- Los puertos 7780 y 7791 están habilitados en el cortafuegos para el tráfico saliente.

Para aumentar la seguridad el puerto 7790, utilizado anteriormente, puede eliminarse de la configuración del cortafuegos tras la actualización a V3R3.1.

29.4 Planificación de proyecto de los canales DSP para los sistemas de comunicación OpenScape Business X3/X5/X8

Las conexiones entre teléfonos/líneas IP y TDM son lo que se denominan conexiones de gateway, para las que se requiere un canal DSP (Digital Signal Processor) propio. Además, se requieren canales DSP al activar la prestación Cifrado de señalización y carga útil (SPE).

No se requieren canales DSP para conexiones TDM puras ni para conexiones IP puras.



Las placas base de los sistemas de comunicación OpenScape Business X3/X5/X8 ofrece como máximo ocho canales DSP.

Si no son suficientes los canales DSP de una placa base, se pueden provisionar más canales insertando una tarjeta Voice Channel Booster Card (submódulo OCCB1 o OCCB3):

- OCCB1 ofrece hasta 40 canales DSP adicionales.
- OCCB3 ofrece hasta 120 canales DSP adicionales.

El número de canales DSP disponibles para conexiones de gateway se reduce por el uso del códec G.729 y por el uso de Cifrado de señalización y carga útil (SPE).

En última instancia, el número de conexiones de gateway simultáneas (conexiones de voz simultáneas con transición IP-TDM) determina si hay que usar un submódulo OCCB y cuál será.

En el caso de las conferencias de UC Suite y de teléfonos por IP, un sistema de comunicación OpenScape Business X3/X5/X8 puede incluir hasta ocho canales DSP. De forma predeterminada, tres canales DSP se asignan a los tres códecs predeterminados de Música en espera (MOH). Este número se puede reducir si utiliza menos códecs para la Música en espera. Además, otros dos canales DSP están reservados para la configuración del Cifrado de datos de señalización y carga útil (SPE). El resto de los canales DSP se pueden asignar a teléfonos por IP (un canal DSP por cada teléfono IP). Cuando se agoten los canales DSP disponibles, el número de canales DSP se podrá incrementar si se utilizan las tarjetas OCCB correspondientes (OCCB1 u OCCB3, como se ha indicado anteriormente).

Consejo: Para consultar datos sobre los canales DSP de la placa base disponibles cómo máximo y sobre los submódulos OCCB, véase Límites de ampliación condicionados por el sistema.

Si los canales DSP son insuficientes pueden producirse cuellos de botella DSP que se manifiestan por ejemplo mediante estados de ocupado en el establecimiento de la conexión (tono de ocupado en el establecimiento de conexión, indicación en pantalla `No disponible en este momento`).

Si se produce un cuello de botella DSP, se hace una entrada en el archivo de protocolo de sucesos (Event Log) del sistema de comunicación.

Si es frecuente que se produzcan cuellos de botella DSP, hay que tomar las siguiente medidas:

Si	**entonces**
Se utilizan los canales DSP de la placa base.	Instalar un submódulo OCCB1 o OCCB3 en la placa base.
Se utilizan los canales DSP de la placa base y del submódulo OCCB1.	Instalar un submódulo OCCB3 en la placa base.
Se utilizan los canales DSP de la placa base y del submódulo OCCB3.	Hay que comprobar si el sistema de comunicación se puede operar exclusivamente con el códec G.711. Con ello aumenta el número de canales DSP hasta el máximo. ***INFO:*** La opción **Utilizar solo G.711** pueden activarla los administradores con el perfil **Experto** en el **Modo Experto** (**Telefonía** > **Gateway voz** > **Parámetros códec**).

La siguiente tabla ofrece valores orientativos para determinar si hay que utilizar un submódulo OCCB y en su caso, cuál.

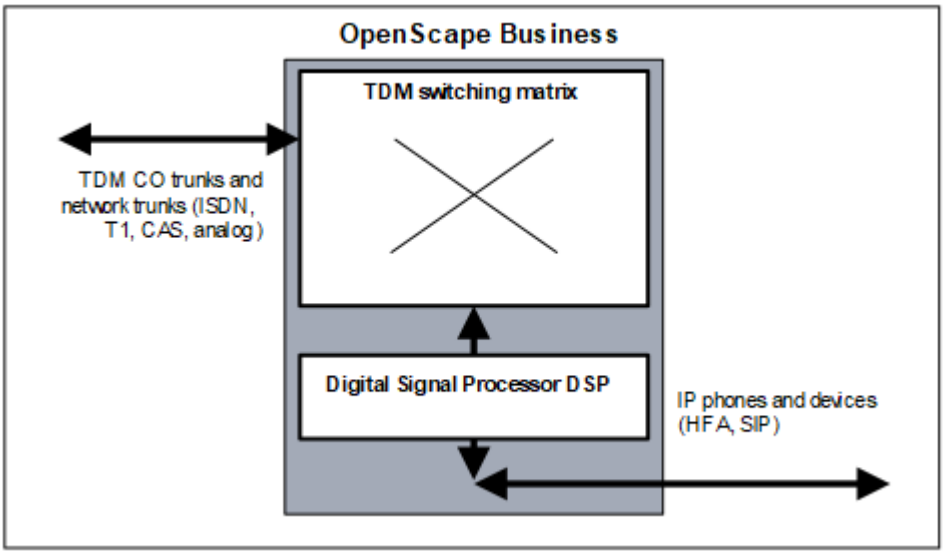
Total de canales TDM: Líneas de interconexión y línea urbana (RDSI, T1, CAS, analógico)	Total de canales IP: Conexión de ITSP, interconexión SIP-Q- y SIP, conexión con la UC Suite (UC Booster Server o UC Booster Card (OCAB))	**Total de teléfonos TDM y dispositivos TDM (S_0, $U_{P0/E}$, CMI, a/b)**	**Total de teléfonos IP y dispositivos IP (HFA, SIP)**	**¿Qué submódulo OCCB?**	**Observaciones**
Sin límite	Anuncios grabados (máx. 16) 0	Sin límite	0	Ningún submódulo OCCB	El buzón de voz Smart VM y las conferencias del sistema se editan a través de la red de conmutación.

Total de canales TDM: Líneas de interconexión y línea urbana (RDSI, T1, CAS, analógico)	Total de canales IP: Conexión de ITSP, interconexión SIP-Q- y SIP, conexión con la UC Suite (UC Booster Server o UC Booster Card (OCAB))	**Total de teléfonos TDM y dispositivos TDM (S_0, $U_{P0/E}$, CMI, a/b)**	**Total de teléfonos IP y dispositivos IP (HFA, SIP)**	**¿Qué submódulo OCCB?**	**Observaciones**
			hasta 8	Ningún submódulo OCCB	Independiente de los canales TDM. El buzón de voz Smart VM y las conferencias del sistema en combinación con teléfonos IP y dispositivos IP requieren recursos DSP.
			9 a 100	OCCB1	Independiente de los canales TDM. El buzón de voz Smart VM y las conferencias del sistema en combinación con teléfonos IP y dispositivos IP requieren recursos DSP, hasta 40 en simultáneo.
			> 100	OCCB3	Independiente de los canales TDM. El buzón de voz Smart VM y las conferencias del sistema en combinación con teléfonos IP y dispositivos IP requieren recursos DSP, hasta 120 en simultáneo.
	> 0	hasta 8		Ningún submódulo OCCB	
	> 0	9 a 100		OCCB1	máx. 40 simultáneamente
	> 0	> 100		OCCB3	Hasta 120 simultáneamente

Total de canales TDM: Líneas de interconexión y línea urbana (RDSI, T1, CAS, analógico)	Total de canales IP: Conexión de ITSP, interconexión SIP-Q- y SIP, conexión con la UC Suite (UC Booster Server o UC Booster Card (OCAB))	**Total de teléfonos TDM y dispositivos TDM (S_0, $U_{P0/E}$, CMI, a/b)**	**Total de teléfonos IP y dispositivos IP (HFA, SIP)**	**¿Qué submódulo OCCB?**	**Observaciones**
> 0	hasta 8			Ningún submódulo OCCB	En principio, la combinación es relevante con SIP-Q y la UC Suite.
> 0	hasta 9			OCCB1	En principio, la combinación es relevante con SIP-Q y la UC Suite.
> 0	> 40			OCCB3	En principio, la combinación es relevante con SIP-Q y la UC Suite.

Los ejemplos siguientes ofrecen valores orientativos para determinar si hay que utilizar un submódulo OCCB y en su caso, cuál.

Ejemplo 1: OpenScape Business con líneas urbanas TDM y teléfonos y dispositivos IP

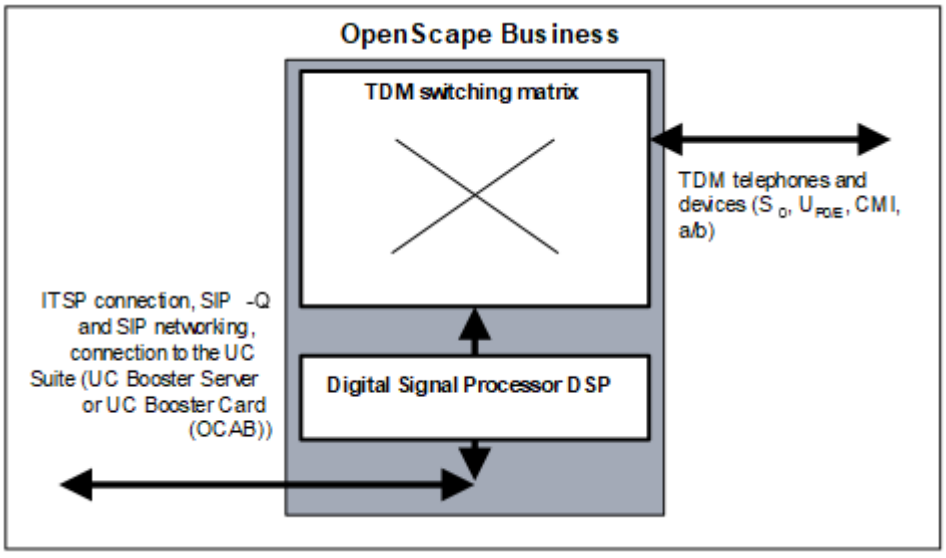


Si	entonces
OpenScape Business con: • 1 líneas urbanas TDM (RDSI) • 20 teléfonos IP (HFA, SIP)	Son suficientes los canales DSP de la placa base. No se requiere ningún submódulo OCCB.

Si	entonces
OpenScape Business con: • 1 líneas urbanas TDM (RDSI) • 100 teléfonos IP (HFA, SIP)	Se requiere el submódulo OCCB1. Como alternativa se puede usar un submódulo OCCB3.
OpenScape Business con: • 2 líneas urbanas TDM (RDSI) • 100 teléfonos IP (HFA, SIP)	Se requiere el submódulo OCCB3.
OpenScape Business con: • 4 líneas urbanas TDM (RDSI) • 500 teléfonos IP (HFA, SIP)	Se requiere el submódulo OCCB3. ***ADVERTENCIA:*** Con esta extensión de sistema solo se puede usar el códec G.711 para alcanzar el número máximo de canales DSP.

Si el sistema de comunicación también se va a equipar con teléfonos y dispositivos TDM (S_0, $U_{P0/E}$, CMI, a/b), hay que contar con canales DSP adicionales.

Ejemplo 2: OpenScape Business con conexión ITSP y teléfonos y dispositivos TDM

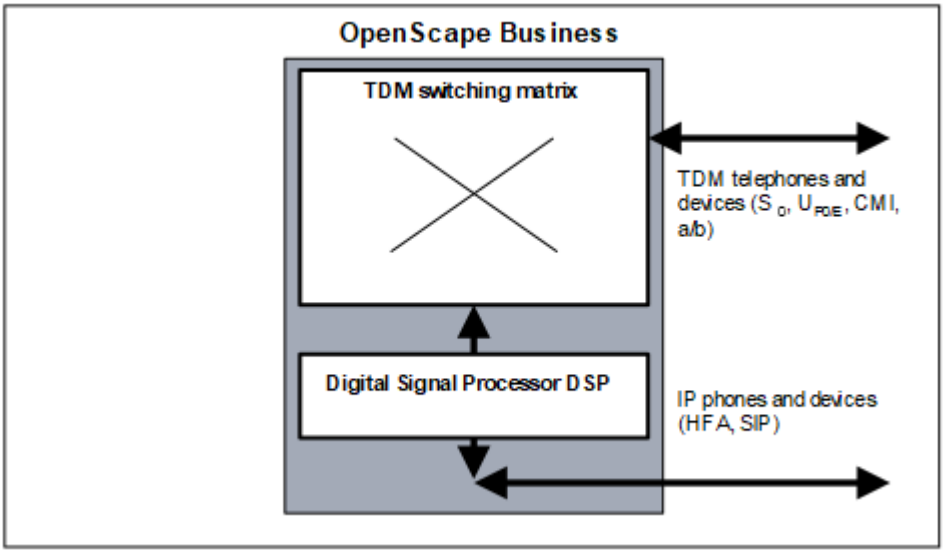


Si	entonces
OpenScape Business con: • 6 conexiones de ITSP (6 canales B) • 20 teléfonos TDM (S_0, $U_{P0/E}$, CMI, a/b)	Son suficientes los canales DSP de la placa base. No se requiere ningún submódulo OCCB.

Si	entonces
OpenScape Business con: • 30 conexiones de ITSP (30 canales B) • 100 teléfonos TDM (S0, UP0/E, CMI, a/b)	Se requiere el submódulo OCCB1. Como alternativa se puede usar un submódulo OCCB3.

Si el sistema de comunicación también se va a equipar con teléfonos y dispositivos IP (HFA, SIP), hay que contar con canales DSP adicionales.

Ejemplo 3: OpenScape Business con teléfonos y dispositivos TDM, y teléfonos y dispositivos IP



Si	entonces
OpenScape Business con: • 6 teléfonos TDM (S_0, $U_{P0/E}$, CMI, a/b) • 6 teléfonos IP (HFA, SIP)	Son suficientes los canales DSP de la placa base. No se requiere ningún submódulo OCCB.
OpenScape Business con: • 100 teléfonos TDM (S0, UP0/E, CMI, a/b) • 100 teléfonos IP (HFA, SIP)	Se requiere el submódulo OCCB3.

Si el sistema de comunicación también se va a equipar con líneas TDM o IP, hay que contar con canales DSP adicionales.

Ejemplo 4: Interconexión SIP-Q con OpenScape Business

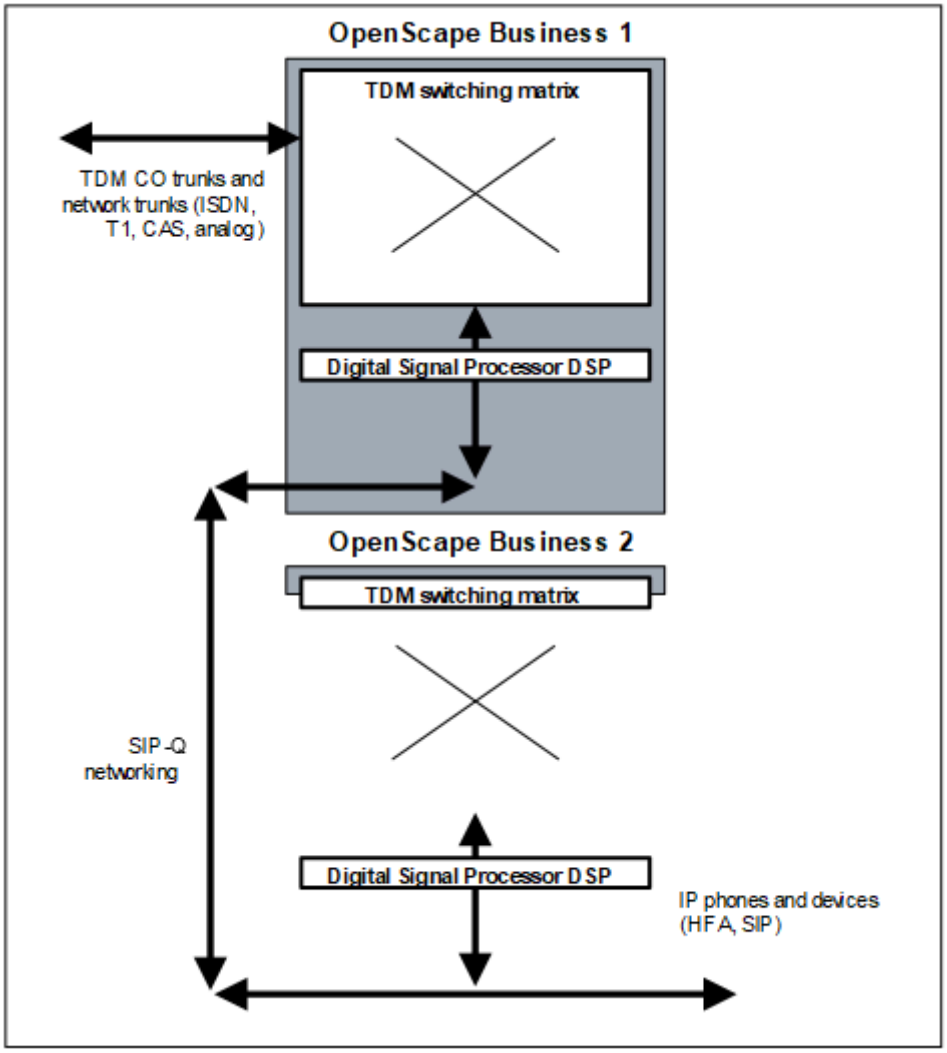
Nota: Este ejemplo expone los requisitos de un segundo sistema OpenScape Business conectado en red. No se muestran las conexiones del primer sistema para simplificar la presentación. Sin embargo, es preciso tener en cuenta los

requisitos del primer sistema, tal y como se enumeran en los ejemplos 1, 2 y 3.

El sistema de comunicación OpenScape Business 1 sirve de gateway con la línea urbana TDM.

Con el sistema de comunicación OpenScape Business 2 solo hay conectados teléfonos IP (HFA, SIP).

Al hacer la planificación de proyecto de los canales DSP para el sistema de comunicación OpenScape Business 1 hay que tener en cuenta el número de teléfonos IP del sistema de comunicación OpenScape Business 2. Solo se requieren canales DSP en el gateway TDM.



Si	entonces
OpenScape Business 1 con: • 1 líneas urbanas TDM (RDSI) OpenScape Business 2 con: • 100 teléfonos IP (HFA, SIP)	En OpenScape Business 1 se requiere el submódulo OCCB1. Como alternativa se puede usar un submódulo OCCB3. En OpenScape Business 2 no se requiere ningún submódulo OCCB.
OpenScape Business 1 con: • 2 líneas urbanas TDM (RDSI) OpenScape Business 2 con: • 100 teléfonos IP (HFA, SIP)	En OpenScape Business 1 se requiere el submódulo OCCB3. En OpenScape Business 2 no se requiere ningún submódulo OCCB.
OpenScape Business 1 con: • 4 líneas urbanas TDM (RDSI) OpenScape Business 2 con: • 500 teléfonos IP (HFA, SIP)	En OpenScape Business 1 se requiere el submódulo OCCB3. ***ADVERTENCIA:*** Con esta extensión de sistema solo se puede usar el códec G.711 para alcanzar el número máximo de canales DSP. En OpenScape Business 2 no se requiere ningún submódulo OCCB.

Si el sistema de comunicación OpenScape Business 2 también se va a equipar con líneas o teléfonos y dispositivos TDM (S_0, $U_{P0/E}$, CMI, a/b), hay que contar con canales DSP adicionales.

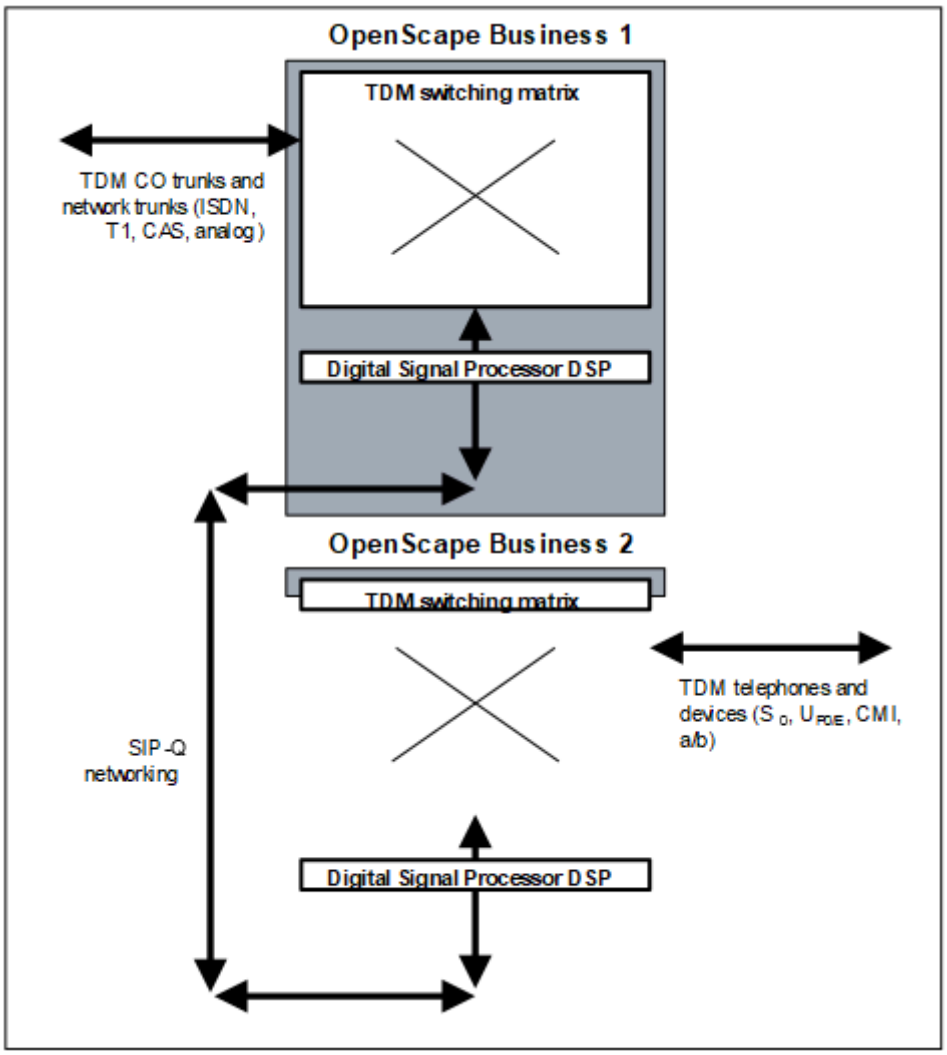
Ejemplo 5: Interconexión SIP-Q con OpenScape Business

> **Nota:** Este ejemplo expone los requisitos de un segundo sistema OpenScape Business conectado en red. No se muestran las conexiones del primer sistema para simplificar la presentación. Sin embargo, es preciso tener en cuenta los requisitos del primer sistema, tal y como se enumeran en los ejemplos 1, 2 y 3.

El sistema de comunicación OpenScape Business 1 sirve de gateway con la línea urbana TDM.

Con el sistema de comunicación OpenScape Business 2 solo hay conectados teléfonos TDM (S_0, $U_{P0/E}$, CMI, a/b).

Dado que ambos sistemas de comunicación requieren conexiones de gateway (OpenScape Business 1: líneas urbanas TDM <-> interconexión SIP-Q, OpenScape Business 2: interconexión SIP-Q <-> teléfonos TDM), ambos sistemas necesitan canales DSP.



Si	entonces
OpenScape Business 1 con: • 1 líneas urbanas TDM (RDSI) OpenScape Business 2 con: • 100 teléfonos TDM (S0, UP0/E, CMI, a/b)	En OpenScape Business 1 y en OpenScape Business 2 se requiere el submódulo OCCB1. Como alternativa se pueden usar submódulos OCCB3.
OpenScape Business 1 con: • 2 líneas urbanas TDM (RDSI) OpenScape Business 2 con: • 100 teléfonos TDM (S0, UP0/E, CMI, a/b)	Tanto en OpenScape Business 1 como en OpenScape Business 2 se requiere el submódulo OCCB3.

Si el sistema de comunicación OpenScape Business 1 también se va a equipar con teléfonos y dispositivos TDM (S_0, $U_{P0/E}$, CMI, a/b), hay que contar con canales DSP adicionales.

Ejemplo 6: OpenScape Business con teléfonos y dispositivos IP

Nota: Este ejemplo expone los requisitos de un segundo sistema OpenScape Business conectado en red. No se muestran las conexiones del primer sistema para simplificar la presentación. Sin embargo, es preciso tener en cuenta los requisitos del primer sistema, tal y como se enumeran en los ejemplos 1, 2 y 3.

Si	entonces
OpenScape Business X3/X5/X8 con: • 7 teléfonos IP (HFA, SIP)	Son suficientes los canales DSP de la placa base. No se requiere ningún submódulo OCCB.
OpenScape Business: • 30 teléfonos IP (HFA, SIP)	Se requiere el submódulo OCCB1. Como alternativa se puede usar un submódulo OCCB3.
OpenScape Business con: • 100 teléfonos IP (HFA, SIP)	Se requiere el submódulo OCCB3.

30 Glosario

El glosario explica brevemente los conceptos utilizados (por ejemplo, para protocolos y estándares).

30.1 Glosario

10BaseT, 100BaseT, 1000BaseT

Se trata de una especificación (IEEE 802.3i) para redes con transmisión de banda base de 10 MBit/s a través de un cable de par trenzado (cuatro hilos) de 100 ohmios. 100BaseT se utiliza para un ancho de banda de hasta 100MBit/s y 1000BaseT designa un ancho de banda de hasta 1000 MBit/s.

AES (Advanced Encryption Standard)

AES es un sistema de cifrado simétrico que fue dado a conocer como estándar sucesor del DES o 3DES por el National Institute of Standards and Technology. Se utiliza, por ejemplo, con VPN.

ADSL con dirección IP dinámica

ADSL son las siglas de Asymmetric Digital Subscriber Line (Línea de Abonado Digital Asimétrica) e indica una diferencia entre los anchos de banda procedentes de Internet (descarga, downstream) y dirigidos a Internet (carga, Upstream). ADSL corresponde a la conexión DSL clásica. Una dirección IP dinámica es suficiente si es el proveedor de servicios de Internet (ISP) quien ofrece los servicios Web y de correo electrónico.

ADSL con dirección IP fija

ADSL son las siglas de Asymmetric Digital Subscriber Line (Línea de Abonado Digital Asimétrica) e indica una diferencia entre los anchos de banda procedentes de Internet (descarga, downstream) y dirigidos a Internet (carga, Upstream). ADSL corresponde a la conexión DSL clásica. El ADSL con dirección IP fija es necesario si desea operar su propio servidor Web y de correo electrónico.

AF-EF (Expedited Forwarding - Assured Forwarding)

Los puntos de código AF y EF establecen las distintas priorizaciones de los paquetes IP en Calidad del Servicio (QOS).

AF: garantiza un ancho de banda mínimo para los datos.

EF: garantiza un ancho de banda constante para los datos.

ARP (Address Resolution Protocol)

ARP es un protocolo de redes que permite asignar direcciones de red a direcciones de hardware. Aunque no está limitado a los protocolos Ethernet e IP, se utiliza casi exclusivamente en relación con el direccionamiento IP en redes Ethernet.

Autenticación

La autenticación es la comprobación de la identidad de una persona o PC. La comprobación puede ejecutarse con un simple nombre de usuario, o con procedimientos mucho más complejos como huellas dactilares.

Clase de servicio (Autorización)

Autorización es la concesión de derechos (p. ej., derechos de acceso a la red de datos).

Canal B

Canal B es la vía de transmisión para la carga útil (voz y datos) de una conexión RDSI.

Panel de lámparas de ocupado (PLO)

myPortal ofrece el denominado panel de lámparas de ocupado (PLO) para indicar visualmente el estado de comunicación de usuarios definidos.

Broadcast (difusión)

Un Broadcast es un mensaje de difusión en una red informática. Un mensaje (paquete de datos) se transmite desde un punto a todas las extensiones de una red. Un mensaje de difusión se utiliza en una red de datos cuando aún no se conoce la dirección del destinatario del mensaje.

CA (Certification Authority, Autoridad de certificación o Entidad emisora)

CA es una organización que emite certificados con firmas digitales. Las firmas digitales son necesarias, por ejemplo, en las redes privadas virtuales (VPN, Virtual Private Network).

Interfaz CAPI (Common Application Programming Interface)

CAPI es una interfaz de software basada en estándares y conforme a RDSI. CAPI permite la creación de software RDSI sin conocimientos previos del hardware RDSI específico del fabricante.

Centrex

Centrex (Central Office Exchange) ofrece funciones de un sistema telefónico mediante PSTN o ITSP. También se denomina sistema telefónico virtual, Hosted PBX (Private Branch Exchange) o NetPBX.

CHAP (Challenge Handshake Authentication Protocol o Protocolo de Autenticación por Desafío Mutuo)

CHAP es un protocolo de autenticación que se aplica en el contexto del protocolo Point-to-Point.

COS (Clase de servicio)

Calidad del servicio es un procedimiento de garantiza la calidad de la transmisión de datos en redes IP.

CLIP (Calling Line Identification Presentation o Indicación del número llamante en la extensión llamada)

La Transmisión del número de llamada permite mostrar el número de teléfono del llamante al usuario llamado. De esta forma, el usuario llamado puede identificar al llamante antes de aceptar la llamada.

CLIR (Calling Line Identification Restriction o Supresión de la indicación del número llamante en la extensión llamada)

El llamante suprime la indicación de su número de teléfono en la extensión llamada. De esta forma, el usuario llamado no puede identificar al llamante antes de aceptar la llamada.

COLP (Connected Line Identification Presentation o Indicación del número de llamada en la extensión llamante)

Con Transmisión del número de llamada, el llamante puede visualizar el número de teléfono del usuario llamado en el momento en el que se establece la conexión.

COLR (Connected Line Identification Restriction o Supresión de la indicación del número de llamada en la extensión llamante)

Con Supresión de la indicación del número llamado, se suprime el número de teléfono del usuario llamado en la extensión del llamante, aunque este haya activado la prestación COLP.

Comfort User

El Comfort User es el usuario estándar del sistema de comunicación.

Comfort Plus User

Comfort Plus User es el usuario avanzado (Advanced User) del sistema de comunicación. A diferencia del Comfort User, el Comfort Plus User puede utilizar más prestaciones (como fax, Mobility, conferencias, etc.).

CorNet

CorNet es un protocolo propietario para la interconexión de sistemas de comunicación HiPath y OpenScape. Frente a QSIG, con compatibilidad general, en CorNet están integradas todas las prestaciones específicas del fabricante de los sistemas de comunicación HiPath y OpenScape.

CorNet-IP

CorNet-IP es una variante de protocolo de CorNet que permite el entrecruzamiento de sistemas o la conexión de teléfonos del sistema (por ejemplo, optiPoint) por IP.

CorNet-NQ

Un protocolo de señalización propietario basado en QSIG para la conexión de sistemas de comunicación con uno o varios sistemas de telecomunicaciones QSIG.

CSTA (Computer Supported Telecommunications Applications)

CSTA es una interfaz de protocolo para aplicaciones compatibles con el estándar ECMA (European Computer Manufacturers Association). Mediante

CSTA se controlan y supervisan las actividades de telecomunicación a través de SIP.

CSV (Character Separated Values)

Un archivo CSV es un archivo de texto para guardar o intercambiar datos de estructura sencilla. CSV equivale a "Character Separated Values" (o valores separados por caracteres), "Comma Separated Values" (o valores separados por comas) o "Colon Separated Values" (o valores separados por dos puntos), dado que los distintos valores están delimitados por un determinado especial, como coma o punto y coma. Los archivos CSV deben estar en formato ANSI/ ASCII.

CRL (Certificate Revocation Lists, listas de revocaciones de certificados)

Una lista de revocación de certificados CRL es un listado de todos los certificados revocados. Las CRL tiene que haber sido generadas por la autoridad de certificación origen de los certificados.

Retardo

En las telecomunicaciones, retardo tiene dos significados:

- El intervalo de tiempo por el que se retrasa un determinado suceso.
- El tiempo entre la aparición de un suceso y la aparición de un resultado esperado en consecuencia.

Dedicated Gateway (dedicado, con asignación fija)

Si en LCR se ha registrado un gateway dedicado para una dirección, el encaminamiento se forzará a través de ese gateway. En tal caso, dejan de ser válidas las reglas de encaminamiento divergentes.

DHCP (Dynamic Host Configuration Protocol)

DHCP es un procedimiento por el que a un PC se le asignan al arrancar determinadas configuraciones de IP (dirección IP, máscara de subred, etc.).

DS (DiffServ, Differentiated Services)

DS es un procedimiento para la administración de paquetes en redes de datos. Se establece cómo se transferirá un determinado paquete de datos y determina un determinado nivel de servicio en relación con el ancho de banda, la teoría de colas y las decisiones de descarte de paquetes.

Algoritmo Diffie-Hellman

El algoritmo Diffie-Hellman sirve para el intercambio de claves en la red privada virtual. Los datos resultantes de este algoritmo se configuran con un conjunto determinado de parámetros matemáticos. Para que el intercambio de claves funcione correctamente, ambos usuarios deben utilizar los mismos valores para estos parámetros.

DLI (Deployment License Service Integrated)

DLI permite instalar y ampliar teléfonos de sistema IP de forma automática.

DMZ (Demilitarized Zone o Zona desmilitarizada)

Con zona desmilitarizada (DMZ, o Demilitarized Zone) se hace referencia a una red informática con opciones de acceso controladas con técnicas de seguridad a los nodos de red conectados a ella (PC, routers, etc.).

DNS (Domain Name Service)

Resolución de nombre en Internet y en LAN. Los nombres de PC o páginas Web se convierten en las direcciones IP correspondientes a través de DNS.

DSL (Digital Subscriber Line)

DSL es una tecnología para proporcionar acceso a Internet de alto ancho de banda. Con la tecnología DSL se cubre el tramo entre el puesto de interceptación del proveedor y la clavija telefónica del cliente.

DSS (Direct Station Selection)

Las teclas de función de un teléfono o de un aparato auxiliar pueden configurarse como teclas de llamada directa (teclas DSS). Para hacerlo, se programan las teclas con el número de teléfono de una extensión interna o de un grupo. Pulsando una tecla DSS se inicia una llamada inmediata al destino programado.

DTMF (Dual Tone Multifrequency)

Véase MF.

EIM (Enterprise Instant Messaging)

EIM es un servicio de mensajería instantánea que se ejecuta en servidores privados de una empresa y sobre plataformas como Live Communications Server u Office Communications Server 2007 de Microsoft.

Conmutadores Enterasys

Los conmutadores Enterasys son soluciones de red seguras producidas por Enterasys Networks. Los conmutadores apilables identifican las prestaciones QoS y clasifican y dan prioridad a las aplicaciones de voz, vídeo y datos.

ESP (Encapsulating Security Payload)

ESP es un protocolo IPSec que garantiza la codificación de paquetes y la integridad y autenticidad de los mismos. La comprobación de integridad y autenticidad no se extiende al encabezado IP sino a los datos en sí (Payload o carga útil).

FoIP (Fax over IP)

FoIP es un método de transmisión de mensajes de fax a través de una red IP.

FTP

FTP (File Transfer Protocol o Protocolo de transferencia de archivos) es un protocolo de red especificado en el RFC 959 para la transmisión de archivos a través de redes TCP/IP.

Códigos de función

Los códigos de función son números de acceso telefónico o números piloto para aparcamiento, conferencias y AutoAttendant. Los códigos de función se corresponden así con extensiones virtuales. En una interred, los códigos de función deben ser únicos.

G.711

G.711 es un estándar para digitalizar señales de sonido analógicas. Se utiliza en la telefonía de red fija clásica (tecnología PCM). En Voz a través de IP (VoIP), G.711 es una posible codificación de voz.

G.729AB

G.729 designa un códec para comprimir voz en señales digitales y se aplica en la telefonía IP. G.729 consume muchos recursos de procesador. G.729AB es una versión algo más sencilla y, por tanto, no consume tantos recursos del procesador. La perdida de calidad, sin embargo, es muy pequeña.

Gateway / Módulos de gateway

Un gateway es un punto de entrada o salida a una red de comunicación que conecta dos flujos de tráfico de datos distintos.

GSM (Global System for Mobile Communications)

GSM es un estándar para las redes digitales de telefonía móvil. Su uso principal es para telefonía, pero también permite la transmisión de datos por paquetes y líneas y para los mensajes cortos (Short Messages).

Handover

Se denomina Handover a un proceso que tiene lugar en las redes de comunicación móvil y por el que el teléfono móvil cambia de una celda de radio a otra durante una llamada o conexión de datos. También se habla de Handover para el cambio entre GSM y UMTS en los teléfonos móviles de modo dual.

Valor hash

Los valores hash o de dispersión, suelen ser valores escalables de un subconjunto de cifras naturales. Los valores hash también se denominan "fingerprint" o "huella dactilar" porque son una identificación virtualmente única de una cantidad, del mismo modo que una huella dactilar es una identificación virtualmente única de una persona.

H.323

H.323 designa un grupo de estándares que definen una serie de tipos de medios para redes de paquete. Los estándares incluyen voz, datos, fax y vídeo y definen cómo se transforman las señales de analógico a digital y que señalización se utiliza.

OpenScape Business Assistant

OpenScape Business Assistant permite administrar el sistema de comunicación. Reune todos los asistentes para las tareas de administración.

Hosted Services

Hosted Services, o "Servicios alojados" son servicios TI tradicionales como correo electrónico, mensajería instantánea y Unified Communications (UC), que ofrece un proveedor de servicios de Internet a las empresas desde una ubicación remota. De esta forma, las empresas no necesitan ejecutar ni administrar dichos servicios in situ desde un servidor propio.

ICMP (Internet Control Message Protocol)

En las redes de datos, ICMP sirve para intercambiar mensajes de error y de información a través del protocolo de Internet IP.

IDS (Intrusion Detection System o Sistema de detección de intrusiones)

El IDS es un sistema de seguridad que supervisa todas las actividades de red entrantes y salientes para identificar posibles violaciones de seguridad. Entre ellas se incluyen tanto intrusiones (ataques desde fuera de la organización) como abusos (ataques desde dentro de la organización).

Estándares IEEE

Los estándares IEEE son un conjunto de especificaciones definidas por el IEEE (Institute of Electrical and Electronic Engineers) (por ejemplo, Token Ring, Ethernet) para configurar estándares de red comunes para los fabricantes.

IEEE 802.1p

IEEE 802.1p es un estándar del IEEE que regula el transporte de paquetes de datos de distintas prioridades en redes informáticas. Se asignan a los paquetes de datos clases de prioridad del 1 al 7. El estándar sólo establece que la prioridad sube de 1 a 7, pero no ofrece más información sobre cómo manejar los paquetes de datos por separado.

Protocolo IKE

El protocolo IKE tiene dos tareas distintas. En primer lugar hay que establecer una SA (Security Association o "asociación de seguridad") utilizada exclusivamente por el protocolo IKE (SA-IKE). A continuación se utiliza la SA-IKE disponible para la negociación segura de todas las demás SA necesarias para la transmisión de datos de carga útil (SA-Payload).

IM (Instant Messaging)

IM (Mensajería instantánea) es un procedimiento para el intercambio en tiempo real de mensajes de texto a través de Internet y con ayuda de PC, PDAs y teléfonos móviles. Los servicios de mensajería instantánea actuales permiten VoIP y videoconferencias, transferencia de archivos y compartición de aplicaciones de escritorio (Desktop-Application-Sharing).

IP PBX

IP PBX es un sistema de comunicación compatible con conexiones VoIP y conexiones de voz a través de líneas telefónicas convencionales.

IPSec

IPSec es una estructura de estándares abiertos para garantizar conexiones de comunicación privadas y seguras a través de redes IP aplicando distintos servicios y protocolos de seguridad.

ISP (Internet-Service-Provider)

Un ISP es una empresa que ofrece servicios de conexión a Internet a individuos, empresas u otras organizaciones. Algunos proveedores de servicios de Internet (ISP) son grandes empresas nacionales o internacionales que ofrecen acceso en distintas ubicaciones. Otros, sin embargo, tienen un ámbito reducido a nivel local o regional.

ITSP (Proveedor de servicios de telefonía por Internet)

Un ITSP es una empresa que ofrece servicios telefónicos a través de Internet a individuos, empresas u otras organizaciones.

DEC (Marcación decádica)

DEC es el procedimiento de señalización más antiguo de la conmutación telefónica automática. DEC ha sido prácticamente sustituido, hoy en día, por la marcación por multifrecuencia (MF).

Jitter

Con Jitter se hace referencia a un retardo de los paquetes de datos en las transmisiones de voz. Un retardo excesivo entre el envío de paquetes de datos y su recepción en el destino, hace la comunicación irregular y difícil de comprender.

Marcación abreviada individual (KWI)

Con la marcación abreviada individual (KWI) cada teléfono autorizado puede guardar 10 números de marcación abreviada externos individuales, además de la marcación abreviada central.

Marcación abreviada central (KWZ)

Los números de teléfono externos frecuentes se pueden depositar en la memoria de sistema del sistema de comunicación. Cada número es sustituido por un número de marcación abreviada que pueden utilizar todos los usuarios en lugar del número de teléfono completo.

Latencia

Por latencia se comprende el tiempo necesario para el transporte de un paquete de datos de una aplicación a otra, incluida la duración de la transmisión a través de la red y el tiempo de preparación y procesamiento de los datos en el equipo de envío y en el de recepción.

LCR (Least Cost Routing)

Con el LCR (Least Cost Routing o Ruta más económica) puede establecer a través de que proveedor se realizarán determinadas llamadas (por ejemplo, las llamadas urbanas, a teléfono móvil o al extranjero). A través del sistema de comunicación establece el proveedor más económico y realiza todas las llamadas correspondientes a través de la ruta definida.

LIN (Location Identification Number)

El LIN es un número inequívoco de 16 dígitos como máximo que corresponde al NANP (North American Numbering Plan) de diez dígitos.

LWCA (Leightweight CA)

LWCA es una función de certificación restringida.

Canal Media Stream

Un gateway de medios puede terminar canales B del RDSI conmutados por línea y utilizar los datos de voz transmitidos para generar canales de flujo de medios (media stream channel) para una red de paquetes basada en IP. Los canales Media Stream incluyen una combinación de medios de sonido, vídeo y T.120.

MF (Procedimiento de marcación por multifrecuencia)

El procedimiento de marcación por multifrecuencia (MF o procedimiento de marcación por tonos) es el procedimiento de marcación de la tecnología telefónica analógica y la versión más utilizada hoy en día en la tecnología de conmutación para transmitir el número de teléfono a la red telefónica.

MIM (Mensajería instantánea móvil)

MIM es un servicio de presencia y de mensajería instantánea para los teléfonos móviles.

Mobility

Mobility designa el uso de PDAs y teléfonos móviles y su integración en el sistema de comunicación de una empresa.

MOH (Música en espera)

Se puede reproducir música en espera (MOH o Music on Hold) a los llamantes si no pueden ser transferidos inmediatamente.

MSN (Multiple Subscriber Number)

Al conectar teléfonos RDSI a través de un bus S0 (acceso individual), se asigna a cada uno de los teléfonos RDSI (extensiones RDSI) un MSN o "Multiple Subscriber Number". Se puede acceder a las extensiones RDSI a través de su MSN.

MULAP (Multiple Line Appearance)

Las MULAP son grupos especiales que reunen varios teléfonos. Cada miembro del grupo puede tener asignado varios teléfonos bajo un único número de teléfono (MULAP básico). Además, en uno de esos grupos se pueden implementar prestaciones especiales necesarias para la comunicación entre jefe y secretaria o en equipos (MULAP jefe, MULAP equipo).

Multigateway

En las interconexiones multigateway, las llamadas se encaminan a través de varios diferentes.

myAttendant

myAttendant es el puesto de operadora del sistema de comunicación.

myPortal

myPortal es el portal de usuario basado en Java para el acceso de los usuarios a las funciones de Unified Communications. Además de a información sobre el estado de presencia y a las cómodas ayudas de marcado a través de favoritos y directorios, el usuario puede acceder a mensajes de voz y faxes.

myPortal for Outlook

myPortal for Outlook es el portal de usuario integrado en Microsoft Outlook para que los usuarios accedan a las funciones de Unified Communication. Es similar a myPortal. Además, myPortal for Outlook ofrece una cómoda marcación de escritorio.

NAC (Network Admission Control)

NAC (Control de admisión de red) es una tecnología que respalda la protección de virus y gusanos desde la red. Con NAC se comprueba la conformidad de los terminales respecto a una serie de directrices durante la autenticación. Si, por ejemplo, el explorador de virus no está actualizado o el sistema operativo cliente no tiene el último parche de seguridad, el terminal en cuestión será puesto en cuarentena y recibirá las últimas actualizaciones hasta que su estado se corresponda con las directrices de seguridad en vigor.

NAT (Network Address Translation)

NAT es un procedimiento para sustituir una dirección IP de un paquete de datos por otra. Se utiliza para mapear direcciones IP privadas en direcciones IP públicas. Si también se reescriben los números de puerto, se habla de enmascaramiento o PAT (Port Address Translation).

NTBA (Network Termination for ISDN Basic Access)

Una NTBA ("Network Termination for ISDN Basic Access" o "Terminación de red para Acceso básico RDSI"), también denominada NT (Terminación de red), es el dispositivo de terminación de red para la conexión básica RDSI. Es el elemento de unión entre la red digital del proveedor de red y las configuraciones RDSI del lado del usuario.

NTPM (Network Termination for Primary Rate Multiplex Access)

Una NTPM ("Network Termination for Primary Rate Multiplex Access") es el dispositivo de terminación de red para las conexiones múltiplex primarias RDSI. Es el elemento de unión entre la red digital del proveedor de red y las configuraciones RDSI del lado del usuario.

OLSR

OLSR es un protocolo Ad-hoc especial que permite optimizar la capacidad de encaminamiento inexistente en la capa 2 OSI en la capa 3 OSI.

ONS (One Number Service o Servicio de número único)

Número de teléfono asignado directamente a un usuario. Un usuario puede tener asignados varios recursos (teléfonos). Si se le llama a través del número ONS, la llamada se transfiere al teléfono que esté utilizando el usuario en ese momento (por ejemplo, el teléfono móvil).

PAP (Password Authentication Protocol)

PAP es un procedimiento de autenticación a través del protocolo PPP (Point-to-Point-Protocol). Se utiliza para realizar el acceso telefónico a un proveedor de servicios de Internet. Con el PAP, la contraseña de la autenticación se transmite como texto junto con una identificación de usuario.

PBX (Private Branch Exchange)

Un sistema telefónico (PBX) es una configuración de conmutación que une varios terminales como, por ejemplo, teléfono, fax, contestador automático, entre sí y con la red de telefonía pública.

Peer

Peer designa el punto terminal de una comunicación en una red Peer-to-Peer. Cada Peer ofrece sus servicios y utiliza los servicios de otros Peers.

Peer-to-Peer

En una red Peer-to-Peer, todos los PC tienen los mismos derechos y pueden ofrecer y recibir servicios por igual.

Autenticación de instancia Peer

La autenticación de la instancia Peer de una conexión garantiza que cumpla con las especificaciones.

PKI (Public Key Infrastructure, Infraestructura de clave pública)

Con PKI se designa en la criptología y criptografía a un sistema que permite crear, distribuir y comprobar certificados digitales. Los certificados creados dentro de una PKI se utilizan para proteger la comunicación informática.

PPP (Protocolo Point-to-Point)

PPP es un estándar IETF para transmitir paquetes IP a través de líneas seriales. PPP se utiliza, fundamentalmente, para el acceso telefónico a Internet.

PPPoE (Protocolo Point-to-Point over Ethernet)

El protocolo PPPoE (PPP over Ethernet) es el uso del protocolo de red Point-to-Point a través de una conexión Ethernet.

Pre-Shared Key

Pre-Shared Key es una clave que se establece en la configuración del túnel (en redes privadas virtuales). Para que las partes VPN en comunicación a través del túnel se puedan autenticar, ambos puntos terminales del túnel deben utilizar la misma contraseña.

PPTP (Protocolo Point-to-Point-Tunneling)

PPTP es una tecnología con la que se puede configurar una red privada virtual (VPN). Como Internet es, en esencia, una red abierta, con PPTP se garantiza la seguridad de los mensajes transferidos de un nodo VPN a otro. Con PPTP los usuarios pueden acceder telefónicamente a su red de empresa a través de Internet.

Presencia

El concepto de presencia o ausencia define la capacidad de un sistema de Comunicaciones Unificadas para poder establecer, en cualquier momento, dónde se encuentra un usuario y cuál es su estado. De esta forma, se puede proceder de forma más conveniente en la comunicación por teléfono, correo electrónico, mensajería instantánea o fax con un usuario.

Servidor proxy

El servidor proxy es el conector entre la aplicación de cliente y el servidor Web. Su tarea es filtrar las solicitudes de la aplicación cliente y descargar el servidor Web.

PSTN (Public Switched Telephone Network)

PSTN designa una red telefónica pública ligada a la línea. Las redes públicas pueden ser de propiedad privada o estatal.

QOS (Quality of Service)

En Voz por IP es importante garantizar un ancho de banda mínimo para toda la duración de la transmisión. Si varias aplicaciones con iguales derechos trabajan a través de IP, el ancho de banda disponible de un tramo de transmisión se distribuye. De esta forma, una conexión de voz puede verse afectada por pérdida de paquetes y resultar una mala calidad de voz. Hay distintos procedimientos para garantizar la máxima calidad posible en la transmisión. Se hace referencia a ellos como QoS (Quality of Service).

RAS (Remote Access Service)

Un usuario RAS (Remote Access Service) es una extensión IP (por ejemplo, un teletrabajador) que se registra en el sistema de forma remota y se comporta como una extensión IP interna. De esta forma puede utilizar todo el abanico de funciones del sistema de comunicación.

RJ45 (Registered Jack 45)

RJ45 es una conexión de ocho pines para conectar, por ejemplo, un cable 10BaseT en la tecnología de redes.

Roaming

Roaming es la capacidad de una extensión de red de telefonía móvil para realizar llamadas telefónicas en una red ajena como si fuera su propia red doméstica de forma automática o para acceder a otras prestaciones de red de telefonía móvil.

RTCP (Real-Time Control Protocol)

El protocolo de control en tiempo real (RTCP) sirve para negociar parámetros QoS (Quality of Service) mediante el intercambio periódico de mensajes de control entre remitentes y destinatarios.

RTP (Real-Time Transport Protocol)

RTP es un estándar IETF para la difusión en stream de datos multimedia en tiempo real a través de IP. RTP suele aplicarse en el protocolo UDP y utiliza puertos dinámicos UDP negociados entre el remitente y el destinatario del flujo de medios especial.

RTT (Round Trip Time)

RTT es el intervalo de tiempo que necesita un paquete de datos para ir de la fuente al destino y regresar al origen.

SA (Security Association)

SA es una asociación de seguridad entre dos unidades en comunicación de redes informáticas. Describe la forma en la que las dos partes aplican servicios de seguridad para poder comunicarse entre sí.

SDSL (Symmetric Digital Subscriber Line)

SDSL es idóneo para la telefonía por Internet, para las aplicaciones Intranet en empresas con redes locales, videoconferencias y está, por ejemplo, diseñado para teletrabajadores a los que permite enviar y recibir datos con el mismo ancho de banda. Frente al ADSL, los anchos de bandas del SDSL son igual de altos desde y hacia Internet.

Secure CLI

Secure CLI es una prestación de seguridad que ofrece interfaces de transmisión de archivos y líneas de comando seguras mediante el protocolo SFTP (Secure File Transfer Protocol).

SFTP (Secure File Transfer Protocol)

SFTP es un protocolo de seguridad para la transmisión de conjuntos de datos de conexión.

Cliente ShrewSoft VPN

El cliente ShrewSoft VPN es un cliente VPN gratuito y de fuente abierta con una interfaz gráfica. Incluye, entre otras cosas, compatibilidad ISAKMP, Xauth y RSA, protocolos de cifrado 3DES, AES, Blowfish.

Gateway único

En las interconexiones de gateway único las llamadas se encaminan a través de un solo gateway.

SIP (Session Initiation Protocol)

SIP es un protocolo de Internet estándar especificado en el RFC 3261 para el establecimiento y control de conexiones de voz y videoconferencias a través de una red IP.

SNMP (Simple Network Management Protocol)

SNMP es un procedimiento para recibir informaciones sobre el estado de los componentes de red y de los PC.

SPE (Signaling and Payload Encryption)

Cifrado de señalización y carga (SPE) ofrece seguridad a la transmisión de datos de voz. Se cifran los flujos de datos de señalización y de uso de VoIP desde al gateway y al gateway y entre teléfonos IP.

SRTP (Secure Real-Time Transport Protocol)

SRTP es un protocolo RTP codificado. Es especialmente apropiado para la transmisión de datos de comunicación a través de Internet y se utiliza en la telefonía IP.

SSH (Secure Shell)

SSH es un protocolo que ofrece compatibilidad para el registro remoto seguro, para la transferencia segura de archivos y para los desvíos TCP/IP seguros. Puede codificar, autenticar y comprimir automáticamente datos transmitidos.

SSL (Secure Socket Layer)

SSL es un protocolo para la transmisión de documentos a través de Internet. En SSL los documentos reciben una clave privada antes de ser transmitidos. Los URL que exigen una conexión SSL comienzan con https: y no con http:.

Estado

En relación con el concepto de Presencia, el estado indica si un usuario está disponible, ocupado, offline, etc. De esta forma los demás usuarios del sistema de comunicación saben si se puede acceder a dicho usuario.

STUN (Simple Traversal of UDP over NAT)

STUN es un protocolo de red para reconocer la presencia y tipo de firewalls y routers NAT y evitarlos.

Survivability

Survivability es la capacidad de una interred para mantener el servicio en caso de errores de red.

TAE (Telekommunikations-Anschluss-Einheit): estándar alemán para conectores telefónicos

TAE es un tipo de clavija de las conexiones telefónicas analógicas con interfaz a/b, y en las conexiones RDSI para conectar el NTBA al cable de conexión. Pueden conectarse teléfonos analógicos, equipos de fax y sistemas telefónicos RDSI.

TCP (Transmission Control Protocol)

El protocolo de control de la transmisión (TCP) es un protocolo que define la forma en la que se intercambian datos entre equipos. Todos los sistemas operativos de los ordenadores modernos son compatibles con TCP y lo utilizan para el intercambio de datos con otros ordenadores.

TFTP (Trivial File Transfer Protocol)

TFTP es un protocolo de transmisión de datos y admite la lectura o escritura de archivos. Muchas funciones del protocolo superior FTP no están disponibles en TFTP (por ejemplo, asignación de derechos, muestra de los archivos disponibles o identificación de usuarios).

Telnet

Un protocolo que une entre sí dos ordenadores para preparar una conexión de terminal con un equipo remoto. El usuario no accede telefónicamente al PC sino que establece conexión a través de Internet por Telnet. El usuario

inicia una sesión Telnet, establece conexión con el host Telnet e inicia sesión. A través de la conexión, el usuario puede trabajar con el PC remoto y su propio sistema aparece en el equipo remoto como si se tratase de un terminal conectado de forma local.

TOS (Tipo de servicio)

TOS es un campo en el encabezado de los paquetes de datos IP y se establece y evalúa para definir la prioridad de esos paquetes (por ejemplo, en Calidad del servicio).

UCD (Uniform Call Distribution)

UCD permite una distribución uniforme de las llamadas entrantes al sistema de comunicación entre un grupo de extensiones (grupo UCD).

UDP (User Datagram Protocol)

UDP es un protocolo de red que pertenece al nivel de transporte de la familia de protocolos de Internet. UDP transfiere datos transmitidos a través de Internet a la aplicación pertinente.

UMTS (Universal Mobile Telecommunications System)

UMTS es un estándar de telefonía móvil de tercera generación que permite unas tasas de transferencia de datos mucho más elevadas (de 384 kbps a 7,2 Mbit/s), que las propias del estándar de telefonía móvil de segunda generación o del estándar GSM.

Comunicaciones Unificadas

Comunicaciones Unificadas es la integración de distintos sistemas, medios, dispositivos y aplicaciones de comunicación dentro de un entorno (por ejemplo, telefonía IP, telefonía móvil y ligada a ubicación, correo electrónico, mensajería instantánea, aplicaciones de escritorio, buzón de voz, fax, conferencias y Unified Messaging).

Unified Messaging

Unified Messaging es la integración de distintos datos de comunicación (como correo electrónico, SMS, Fax, telefonía, etc.) en una memoria de mensajes unificada. Se puede acceder a esta memoria de mensajes a través de distintos dispositivos.

VAD (Voice Activity Detection)

VAD (Voice Activity Detection) designa una detección automática de pausas de voz en la transmisión digital de archivos de sonido.

Interfaz VCAPI

VCAPI es una interfaz CAPI virtual que simula la presencia de una tarjeta RDSI local. Si en la red interna uno de los PC tiene una tarjeta RDSI integrada, se puede ofrecer a todas las extensiones de la red dicha tarjeta RDSI a través de la interfaz VCAPI.

VDSL (Very High Speed Digital Subscriber Line)

VDSL se aplica allí donde hay que transmitir flujos de datos asimétricos o simétricos a alta velocidad y corta distancia. VDSL es una alternativa al ADSL y al SDSL, con velocidades de transmisión mucho más altas.

VoIP (Voice over IP o Voz por IP)

VoIP es la Transmisión de datos de voz a través de redes basadas en IP.

VPN (Virtual Private Network / Red privada virtual)

VPN utiliza la infraestructura pública de Internet para las redes locales y puntos de acceso de teletrabajadores. Gracias a los mecanismos de cifrado y autenticación se consigue ofrecer a los participantes externos una conexión segura a la red de datos interna.

WAN (Wide Area Network)

WAN designa redes de datos de tráfico de gran área, por ejemplo, Internet.

WBM (Web-based-management)

WBM es una interfaz de usuario que se muestra en un navegador de Internet a través de páginas HTML o Java y un protocolo Web.

Estándar X.509 (Certificado VPN)

X.509 es un estándar ITU-T para la infraestructura Public-key y, en este momento, es el estándar más importante para los certificados digitales.

XMPP (Extensible Messaging and Presence Protocol)

Estándar de Internet que se utiliza principalmente para la mensajería instantánea. XMPP admite la interacción con usuarios de otras redes como, por ejemplo, AIM, ICQ o Windows Live Messenger (WLM). XMPP y sus ampliaciones admiten, entre otras cosas, conferencias con varios usuarios (por ejemplo, Chat entre varios usuarios) y la indicación del estado online.

Segundo grado

Segundo grado significa que una extensión está llamando y, además, le espera ya una segunda llamada.

Índice

Caracteres Especiales

<$nopage>Central License Server (véase Servidor de licencias) 346
<$nopage>Distribución de llamadas uniforme (Uniform Call Distribution) (véase UCD) 758
<$nopage>medio, copia de seguridad (véase medio de copia de seguridad) 1267
<$nopage>Restore (véase Recuperar) 1272
Ámbito del buzón de voz 617
Últimos arrendamientos activos, modo experto 1629

A

acceso a Internet
configuración 378
Acceso a Internet 377
a través de un módem Internet externo 383
a través de un router de Internet externo 379
configurar a través de PPTP ISP estándar 389
configurar a través de un ISP preconfigurado 384
configurar a través del estándar ISP PPPoE 387
Acceso a la red urbana 773
agregar un número de teléfono a la lista de números autorizados 777
agregar un número de teléfono a la lista de números prohibidos 778
configurar control de marcación 777, 783
configurar el acceso a la red urbana 776, 784, 785
modificar el filtro de lista de números prohibidos 779
mostrar lista de números autorizados 779
mostrar lista de números prohibidos 778
Acceso a línea urbana
configuración del acceso a línea urbana RDSI 416
acceso remoto 1393
activar, a través de acceso a Internet con dirección IP fija 212, 214, 265, 267
Acceso remoto
activar, a través de acceso a Internet con dirección IP fija 214, 216, 267, 268, 1397
activar, a través de acceso a Internet sin dirección IP fija 1398
activar, por RDSI 1394
configurar PC 1395
configurar PC con Windows 7 1396
desactivar 1399
acceso remoto al sistema de comunicación 1393
acción automática
iniciar Notificación DLS 781, 781, 782, 1307, 1307, 1309
Acción automática 1301
detener Garbage Collection 1303
detener Notificación DLS 1305
Garbage Collection 1301
iniciar Garbage Collection 1303
iniciar Notificación DLS 1304
modificar Garbage Collection 1302
modificar Notificación DLS 1304
Notificación DLS 1303
Acción manual 1332
Acciones
Acciones automáticas, Modo Experto 1544, 1545
Acciones manuales, Modo Experto 1542
Acciones, Modo Experto 1542
Activación de licencia 318, 329
Activación de software 1273
activación, software (véase activación de software) 1273
Activar y desactivar el tono de conferencia 674, 674
actualización 1273
definida por el usuario 1283
Actualización a través de Carga de archivo, Modo Experto 1514
Actualización a través de Internet, Modo Experto 1513
Actualización de licencias 345
actualización de software (véase actualización) 1273
Actualización vía lápiz USB, Modo Experto 1515
Actualización, completa
iniciar con indicación de progreso 1278, 1287
actualización, completo
empezar en segundo plano 1281
actualización, software (véase actualización de software) 1273
actualizaciones automáticas 557
actualizaciones de software 1273
ad-hoc, conferencia 532
Admin. certificados, Modo Experto 1599, 1614
Administración de puertos, Modo Experto 1581
advertencias
atención 78
Agente de retransmisión DHCP: configurar 361
Agentes UCD, Modo Experto 1755
ajustes básicos
gestión de energía, Modo Experto 1589
Ajustes básicos 1548
Administración de puertos, Modo Experto 1581
Calidad del servicio, Modo Experto 1579
Despliegue de parámetros de teléfono, Modo Experto 1586
DynDNS, Modo Experto 1577, 1578
Fecha y hora, Modo Experto 1580, 1580, 1580
Gateway, Modo Experto 1575, 1576
Reproductor de anuncios, Modo Experto 1586
Sistema, Modo Experto 1557, 1563, 1567, 1568, 1571, 1572, 1573, 1573, 1574
Tasas de llamada, Modo Experto 1582, 1584, 1585
Ajustes básicos, Modo Experto 1548, 1794
ajustes de correo electrónico 1361
Ajustes Secure Trace, Modo Experto 1526

Ajustes SNTP, Modo Experto 1580, 1580
Almacenamiento
inmediato 1269
Almacenamiento de datos (véase Almacenamiento) 1264
Altavoz 453
Alternar 663
Anchos de banda en la LAN 1080
Anuncios grabados de buzón de voz relativos al estado 617
Anuncios grabados en UCD 769
Anuncios grabados para el buzón de voz 617
Apagado de OpenScape Business X 1291
Apagar el sistema de comunicación 1291
Aparcar 661
Aplicación de UC
reiniciar 1294, 1294
Aplicaciones, Modo experto 1796
Aplicaciones, Modo Experto 1759
Application Launcher 1215, 1795
perfil de datos de configuración 1216
Application Launcher, Modo Experto 1795
Archivo CSV 435
archivo de audio 1260
Archivo de imagen 1274
archivo de protocolo 1360
Archivo de sonido 1257
Archivo licencia 318, 329
Archivo PDF
mensaje de fax 624
notificación 629
Archivo TIFF
mensaje de fax 624
notificación 629
Archivo WAV
notificación 544, 629
Archivo Wave 1257, 1260
Asignación de grupos VBZ, Modo Experto 1739
Asignación de llamadas 676
Asignar MSN, Modo Experto 1734
asistentes 125
Asumir permiso de escritura, Modo Experto 1546
autenticación
participante de conferencia 532
AutoAttendant 616
Aviso de llamada/Tono de llamada en espera 680

B

Bloquear teléfono 791
Bloqueo de llamadas a cobro revertido por línea urbana 792
Bloqueo de mensaje directo para extensiones 653
activar 653
desactivar 653
Bloqueo de servicios (solo LX) 1018
Botones de usuario 879
diseño 879
buzón de fax 624
Buzón de voz 617, 617
anuncios grabados relativos al estado 617
captura de llamadas 617
guardar 617
Buzón de voz (UC Smart) 537
Buzón VoiceMail, véase Buzón de voz 617

C

cableado para conexiones LAN y WAN 87
Calidad del servicio, Modo Experto 1579, 1641
CallMe 570
Cambio de número de teléfono 689
canales DSP, planificar 1805
Candado telefónico individual 791
Capacidades 1466
Captura de llamadas del buzón de voz 617
Carga al Gateway, Modo experto 1508
Carga de archivo, Modo Experto 1781
Cargar al gateway, Modo Experto 1507
Carrier Select Override 795
CDP (Punto de distribución de certificado) 1057
Centro de contactos 888
anuncio de carga 939
anuncio de récord 938
añadir una pausa 957
Definición de agentes favoritos 956
descargar la regla 945, 945
regla de impresión 945, 946
Certificado de cliente DLSC, Modo Experto 1593
Certificado de entidad emisora DLSC, Modo Experto 1594
Certificado SecureTrace, Modo Experto 1526
Certificado SPE, Modo Experto 1596
Certificados act., Modo Experto 1599
Certificados configurados, Modo Experto 1600
Certificados de entidad emisora SPE, Modo Experto 1597
Certificados de par, Modo Experto 1601
Certificados de servidor, Modo Experto 1615
Certificados VPN
generar certificado de entidad emisora Lightweight 1036
generar solicitud de certificado 1038, 1039
importar 1039
importar certif. ent. emisora de confianza 1038
mostrar 1037
Cifrado de datos de señalización y carga útil (SPE) 1019
Cifrado de señalización y carga útil (SPE), Modo Experto 1596
circuito de alimentación y conexión
OpenScape Business S 86
OpenScape Business UC Booster Server 86
Clases de priorización 442
Clases de servicio
Asignación de grupos VBZ, Modo Experto 1739
Día: Grupos de clase de servicio, Modo Experto 1735
Días especiales, Modo Experto 1741
Extensiones, Modo Experto 1735

Listas de nos. permitidos, Modo Experto 1737
Listas de nos. prohibidos, Modo Experto 1738, 1738
Matriz VBZ, Modo Experto 1740
Noche: Grupos de clase de servicio, Modo Experto 1736
Servicio autom. nocturno, Modo Experto 1741
Servicio nocturno, Modo Experto 1739
Clases de servicio, Modo Experto 1646, 1735
Client Logs
descargar 1380
Cliente (UC Smart) 499
Cliente (UC Suite) 547
Cliente de sistema 444
Cliente IP 444
Cliente IP (véase Extensiones IP) 444
Cliente NCP
preparar 1043
Cliente UC Smart 499
Clientes de PC 111
Clientes de UC Suite 547
Clientes IP, modo experto 1674
Clientes IP, Modo Experto 1702
Clientes Mobility, Modo Experto 1699
Clientes NCP
activar, desactivar 1044
clientes, requisitos de hardware y software 894
Clientes, requisitos de hardware y software 551, 865, 890
CLIP
Transmisión del número de llamada del llamante 656
CLIP no screening 659
CLIR
Supresión de la indicación del número llamante en la extensión llamada 657
CMD (CSTA Message Dispatcher) 1796
Códec de sonido 438
asignar parámetros a un destino 440
configurar parámetros 439
Código de autorización de licencia (LAC) 318, 329
Códigos de servicio, Modo Experto 1574, 1574
Colateral PSTN, Modo Experto 1637
COLP - Presentación de identificación de líneas conectadas 658
COLR
Supresión de la indicación del número llamado 658
Combinación de teclas para la marcación de escritorio 597
Componente de seguimiento M5T 1337
componente trace
editar 1354
Componente trace
detener todos los componentes 1353
editar 1354
iniciar 1353
mostrar 1352
mostrar datos detallados 1352
parar 1353
Componente trace M5T
detener 1347
editar 1347
iniciar 1347
mostrar 1346
Componente trace M5T, Modo Experto 1525
componentes de seguimiento 1341
Componentes trace, Modo Experto 1531
Comportamiento en caso de emergencia 84, 84
Comprobar la conexión de red 1316
mediante ping 1316
mediante Traceroute 1316
Comunidades escritura, Modo Experto 1540
Comunidades lectura, Modo Experto 1539
Comunidades trap, Modo Experto 1540
Comunidades, Modo Experto 1539
Concepto 74
condiciones
desvío de llamadas basado en reglas 571
Condiciones de servicio (climáticas, mecánicas)
OpenScape Business S 92
OpenScape Business UC Booster Server 92
OpenScape Business X3, X5, X8 91
Conexión con CLA local;CLA
conexión local 337, 338, 348
Conexión con el CLA central;CLA
conexión central 348
conexión de banda ancha 377
conexión de sistema 1216
Conexión LDAP 1216
conexión por cable 377
Conexiones
Música en espera, modo experto 1742
Conexiones, Modo Experto 1703
conferencia 532, 609, 609
Conferencia 600
abierta 610
AdHoc 607
ampliación 600
autenticación 600
controlada por aplicación 600
controlada por teléfono 600
controlador de conferencia 600
extensiones Mobility Entry 600, 607, 608, 610
grabación 600
invitación automática por cita Outlook 600
invitación automática por correo 600
número de acceso telefónico 600
participante de conferencia 600
programada 608
sala de conferencias virtual 600
tipos de conferencias 600
tono de conferencia 600
conferencia (UC Suite) 600
Conferencia abierta 610
Conferencia Ad-hoc 607
conferencia controlada por aplicación 531
Conferencia controlada por aplicación 601
Conferencia controlada por teléfono 601
conferencia permanente 532, 609

conferencia programada 532
Conferencia programada 607, 608
conferencia, controlada por teléfono 531
configuración
  Anuncios, Modo experto 1508
Configuración
  Configuración de puerto, Modo Experto 1509
  Dirección IP del gateway, Modo Experto 1512
  Marca, Modo Experto 1512
  Música en espera (MoH), Modo Experto 1507
  SmartVM, Modo Experto 1509, 1509, 1510
configuración de equipo 720
  añadir 729
  buzón de fax 722
  tipo de llamada 722
Configuración de equipo
  agregar un buzón de fax 737
  añadir miembro 735
  borrar 731
  borrar miembro 735
  modificar 730
  modificar la ocupación de teclas telefónicas 736
  modificar las propiedades de un miembro 736
  modificar miembro 735
Configuración de formato trace, Modo Experto 1522
Configuración de hardware de OpenScape Office MX
  mostrar 493
Configuración de proveedores externos, Modo Experto 1769
Configuración de puerto, Modo Experto 1509
Configuración de sucesos, Modo Experto 1534
Configuración del acceso a línea urbana RDSI 416
Configuración Jefe/secretaria 724
  agregar miembro 737
  agregar un buzón de fax 739
  añadir 732
  borrar 734
  borrar miembro 737
  buzón de fax 727
  modificar 733
  modificar las propiedades de un miembro 738
  modificar miembro 738
  Teléfonos SIP 727
  tipo de llamada 727
Configuración, Modo Experto 1507, 1541
Configurar
  servicio de integración de Active Directory 1214
Configurar la Transferencia automática diferida 539, 670
conformidad
  normas estadounidenses y canadienses 90
  normas internacionales 91
Conformidad CE 90
Conjunto de copia de seguridad
  mostrar 1266
Conjunto de copias de seguridad 1264, 1265, 1265
  copia de seguridad inmediata 1270
  copia de seguridad programada 1272
  mostrar 1266
  Recuperar 1273
Conjunto de copias de seguridad para fines de diagnóstico 1366, 1367
Contact Center 852, 853, 853, 853, 904, 905, 905, 905
  activar cola 953
  agente 897
  agentes preferidos 898
  agregar un horario 939
  agregar una cola 946
  asignar agente a cola 961
  borrar agentes preferidos 956
  borrar un horario 944
  clase de servicio (nivel de autorización) de un agente 897
  clientes 888
  cola 902
  condiciones de servicio 963
  configurar extensiones como agentes 937
  configurar grupo UCD 937
  definir la prioridad de llamantes VIP 954
  desactivar cola 953
  devolución de llamadas de agentes 914
  editar la lista de llamantes VIP 955
  editar un horario 943
  editar una cola 950
  eliminar agente de la cola 962
  eliminar una pausa 958
  establecer valor nominal para nivel de servicio 954
  guardar regla como archivo PDF 945
  indicación de los detalles de cola de espera 914
  informes 967
  lista de llamadas VIP 915
  modificar pausa 957
  myAgent 889
  myReports 892
  nivel de clase de servicio de un agente 897
  nivel de servicio 914
  pausa 899
  plantillas de informe predefinidas 968
  prioridad de llamantes VIP 915
  procedimientos de configuración 936
  razones de resumen 913
  regla de impresión 945
  restricciones de las prestaciones del sistema 964
  resumen múltiple, agregar motivo de resumen 959
  roles de usuario de myReports 892
  solución de respaldo (solución Fallback) 916
  tablero/Wallboard 914
  tratamiento posterior 913
  tratamiento posterior múltiple, borrar motivo de tratamiento posterior 961
  tratamiento posterior múltiple, modificar el motivo de tratamiento posterior 960
  tratamiento posterior simple, agregar motivo de tratamiento posterior 958
  tratamiento posterior simple, eliminar motivo de tratamiento posterior 959

tratamiento posterior simple, modificar motivo de tratamiento posterior 958
uso de teléfonos DECT 966
Contact Center, modo experto 1771
Contact Center:configuración 919
Contact Center:configurar piloto para mensajes de fax entrantes 953
Contact Center:ejemplo de configuración de Contact Center 919
contacto 594
Contestación directa 653
Contestador automático 453
Convenciones de representación 75
Conversión de números de llamada en nombres 660
copia de seguridad
programada 1271
copia de seguridad - inmediata 1270
Copia de seguridad (véase Almacenamiento) 1264
cordless
para todo el sistema, Modo Experto 1703
Cordless
extensiones base, Modo Experto 1707
correo electrónico
invitación a conferencia 532
Correo electrónico a SMS 631
Correo electrónico, Modo Experto 1535
Cortafuegos de aplicaciones, modo experto 1591
Corte de línea para una llamada de emergencia 836
Cover Page Editor 626
CRL (Certificate Revocation List, lista de revocación de certificados) 1036
CRL (Lista de revocación de certificados) 1057
CSP (CSTA Service Provider) 1797

D

Daemon RPCAP 1358
Datos de config. 1264
datos de configuración para diagnóstico 1366
generar 1367
Datos de diagnóstico 1332
Datos de extensión
importar 437
Datos protocolo admin, Modo Experto 1541
definición de prioridades de líneas urbanas (líneas) 431
Departamentos 593
Departamentos, Modo Experto 1766
Deployment and Licensing Client (DLSC), Modo Experto 1593
descarga (véase actualización) 1273
Despliegue de parámetros de teléfono, Modo Experto 1586
Destinos de marcación abreviada, Modo Experto 1573
desvío de llamadas
basado en reglas 571
Desvío de llamadas 672
relativo al estado 571
desvío de llamadas fijo 669
desvío de llamadas no atendidas tras tiempo de espera 669
Desvío diferido 674
Desvío, Modo Experto 1756
devolución de llamada
diario 595
Devolución de llamada 679
Devolución de llamada automática 680
Devolución de llamada en caso de ocupado 680
Día
Grupos de clase de servicio, Modo Experto 1735
Diagnóstico de aplicación
Configuración del desarrollador, Modo Experto 1546, 1546
Placa base, Modo Experto 1546
Diagnóstico de aplicación, Modo Experto 1545
Diagnóstico de IP
Placa base, Modo Experto 1546, 1547, 1547
Diagnóstico de IP, Modo Experto 1546
Diagnóstico de plataforma, Modo Experto 1545
diario
tiempo de retención 595
Diario (UC Smart) 530
diario (UC Suite) 595
Días especiales, Modo Experto 1741
Dirección IP del gateway, Modo Experto 1512
Direcciones IP 1295
mostrar resumen 1297
Direcciones IP estáticas, modo experto 1628
Directorio
Mensaje instantáneo 535
Directorio de copia de seguridad 1265
Directorio de usuario, Modo Experto 1763
Directorio del sistema 523
Directorio externo 577
Directorio externo (LDAP) 581
Directorio externo, Modo Experto 1768
Directorio interno (UC Smart) 521
Directorio interno (UC Suite) 575
directorios (UC Smart) 520
Directorios (UC Suite) 572
DISA, Modo Experto 1567
Display, Modo Experto 1563
Dispositivos, Modo Experto 1750
distribución de llamadas 758
configuración 758
configuración de grupo UCD 760
configurar 760
Distribución de llamadas 759
Distribución de llamadas (UCD)
aceptar automáticamente llamadas UCD 765
AICC (Automatic Incoming Call Connection) 765
liberación de llamadas UCD a través de líneas analógicas 771
música en espera (Music On Hold MOH) 769
Distribuidor de mensajes CSTA (CMD) 1796
DNS (Domain Name Service)
definir servidor 369
DSL (Digital Subscriber Line) 377
DynDNS 368

DynDNS (Dynamic Domain Name Service) 391

E

Editar marcación 645
Editor de reglas 853, 905
Editor de tablas NAT 1014
eliminación 85
Email
    notificación 544, 629
emisión de la marcación
    seleccionar 796
Emisión de la marcación 795
en conferencia 609
En conferencia, Modo Experto 1782
encabezados de fax, Modo Experto 1792
Encaminamiento 369
    Encamin. IP, Modo Experto 1633, 1633, 1633, 1634, 1634
    NAT, Modo Experto 1635
    PSTN, Modo Experto 1636, 1637, 1637
Encaminamiento, Modo Experto 1632
Entidad emisora Lightweight 1035
Entidad emisora Lightweight, Modo Experto 1598
Entorno de ejecución de Java (JRE) 226
entorno eléctrico
    OpenScape Business S 86
    OpenScape Business UC Booster Server 86
entornos de Terminal Server/Citrix-Server 548
entradas de protocolo 1360
Envío de correo electrónico 630
Equipo auxiliar
    SmartVM, Modo Experto 1746
Escritorio compartido 985, 985
ESP-Header 1025
Esquema de direcciones IP 140, 229
estaciones 432
Estaciones
    Extensión, modo Experto 1684
Estadísticas
    Estadísticas de gateway, Modo Experto 1754, 1754
    Estadísticas de telefonía, Modo experto 1756
    Estadísticas de telefonía, Modo Experto 1755, 1755, 1756, 1757
    Estadísticas SNMP, Modo Experto 1755
Estadísticas disposit., Modo Experto 1754
Estadísticas MSC, Modo Experto 1754
Estadísticas SNMP, Modo Experto 1755
Estadísticas, Modo Experto 1754
estado de extensión 1295
Estado de extensión
    consultar 1296
Estado de ITSP 1295
    consultar 1297
Estado de la VPN 1295
Estado de línea, Modo Experto 1756
estado de módulos, Modo Experto 1520
estado de presencia 548
Estado de puerto, módulos, modo Experto 1520
estado del establecimiento de conexión 1295
Estado del establecimiento de conexión
    consultar 1296
estado del sistema de comunicación 1295
estándares 1799
Event (Suceso)
    borrar protocolo 1362
    descargar protocolo 1362
    modificar la configuración de reacción de un suceso 1363
    modificar la configuración de reacción de varios sucesos 1364
    modificar la protocolización por LAN 1362
    mostrar tabla reacción 1363
evento 1359, 1360, 1360, 1361, 1361
EVM, Modo Experto 1682
excepción
    desvío de llamadas basado en reglas 571
Extensión 1672
    Extensiones, Modo Experto 1674, 1678, 1679, 1680, 1681, 1682, 1684, 1697, 1699, 1699
    Programación de teclas, Modo Experto 1702
extensiones
    Extensión, modo Experto 1696
Extensiones
    analógicas 453
    configuración mediante asistentes 458
    IP 444
    RDSI 450
    Vista general, Modo Experto 1702
Extensiones analógicas, Modo Experto 1678
Extensiones base, modo Experto 1518, 1518
Extensiones base, Modo Experto 1680, 1707
Extensiones de marcación directa (DID), Modo Experto 1699
Extensiones DECT, Modo Experto 1681
Extensiones IP 444
extensiones Mobility Entry 609, 609
    en conferencia 532
Extensiones Mobility Entry
    conferencia 600, 607, 608, 610
Extensiones RDSI 450
Extensiones RDSI, Modo Experto 1679
Extensiones UP0, Modo Experto 1672
Extensiones virtuales, Modo Experto 1684
Extensiones, Modo Experto 1672, 1672, 1735, 1757

F

FastViewer 533, 611, 611
Fax 617
    T.38 634
Fax Grupo 3 453
Fax Grupo 4 450
Fax Printer 549, 626
Fax T.38 634
Fecha y hora, Modo Experto 1580

firewall 1010, 1216
Firma digital 1034
Flag de extensión
bloqueo de aviso de llamada en espera act. 719
bloqueo mens. directo desact 653
Flag del sistema
número de llamada en grupos de telecaptura / timbre adicional / desvío de llamada en caso de no contesta / caso de libre 716
señal de advertencia para grupos de telecaptura 716
soporte SPE 1021
telecaptura de llamadas después de llamada recordatoria 717, 1084
Flags del sistema, Modo Experto 1548
Flags LCR, Modo Experto 1641
Flex Call 688
Formato de números de teléfono 530
Formato de números de teléfono canónico 530
Formato de números de teléfono de marcación 530
Fuera de servicio, Modo Experto 1521
Función Jefe (véase Configuración Jefe/secretaria) 724
Función Secretaria (véase Configuración Jefe/secretaria) 724
Función Team (véase Configuración de equipo) 720
Funciones
myPortal 548
myPortal for Outlook 549
myPortal Smart 501

G

Garbage Collection, Modo Experto 1544
Gateway de voz
Proveedor de servicios de telefonía por Internet, modo experto 1652
Gateway voz
Interconexión SIP, modo Experto 1665
Parám. códec destino, Modo Experto 1652
Parámetros códec, Modo Experto 1650
Parámetros SIP, Modo Experto 1647
Redes, Modo Experto 1664, 1664
Gateway voz, Modo Experto 1647
Gateway, Modo Experto 1576
Generación de certif., Modo Experto 1613
Gestión basada en Web 115
gestión de conferencias 531
Gestión de conferencias 601
gestión de energía, Modo Experto 1589
Gestión de inventario 1294
grabación de llamadas (grabación de voz) 667
Grabar 598
Grupo Contestador automático (véase Grupo de buzón de voz) 751
grupo de búsqueda 703
mensaje de voz 704
Teléfonos SIP 706
tipo de llamada 706
grupo de buzón de fax
Añadir miembro 756
Borrar miembro 756
configurar 755, 756
Grupo de buzón de fax 752
modificar 756
mostrar 756
grupo de buzón de voz
añadir 752
Grupo de buzón de voz 751
agregar miembro 754
borrar 753
borrar miembro 754
modificar 753
modificar miembro 754
mostrar 753
Grupo de fax (véase Grupo de buzón de fax) 752
grupo de telecaptura 697
indicación de números de teléfono del llamante 698
indicación del nombre del llamante 698
telecaptura de llamadas fuera de un grupo de telecaptura 698
telecaptura de llamadas recordatorias 698
teléfonos SIP 698
tono de advertencia 698
Grupo de telecaptura
activar el tono de advertencia 716
activar la indicación de números de teléfono del llamante 715
activar la indicación del nombre del llamante 715
activar la telecaptura de llamadas recordatorias 716, 1083
añadir miembro 708
borrar miembro 708
configurar 707
desactivar el tono de advertencia 716
desactivar la indicación de números de teléfono del llamante 715
desactivar la indicación del nombre del llamante 715
desactivar la telecaptura de llamadas recordatorias 716, 1084
grupo team 720
añadir 729
buzón de fax 722
tipo de llamada 722
Grupo Team
agregar miembro 735
agregar un buzón de faz 737
borrar 731
borrar miembro 735
modificar 730
modificar la ocupación de teclas telefónicas 736
modificar las propiedades de un miembro 736
modificar miembro 735
grupo top 724
añadir 732
buzón de fax 727
Teléfonos SIP 727

tipo de llamada 727
Grupo Top
agregar miembro 737
agregar un buzón de fax 739
borrar 734
borrar miembro 737
modificar 733
modificar las propiedades de un miembro 738
modificar miembro 738
grupos 697
Grupos de direcciones IP, modo experto 1626
Grupos VBZ 788, 789
asignación de números de marcación abreviada 789
asignar extensiones 790
asignar línea 790
Grupos, Modo Experto 1766
Grupos/Grupos de caza, Modo experto 1708
Guardar 1264

H

hotline 834

I

ICMP (Internet Control Message Protocol) 1316
Idioma de sistema para el buzón de voz 617
Idiomas 112
Imagen software
Software del sistema, Modo Experto 1513, 1514, 1515
Imagen software, Modo Experto 1513, 1518
imágenes de teléfono
Cargar, Modo Experto 1515
Distribuir, Modo Experto 1516
Imágenes de teléfono
Distribuir por dispositivo, Modo Experto 1516
Inalámbrico (Cordless) Multi-SLC, Modo Experto 1707
Inalámbrico (Cordless) SLC, Modo Experto 1705
Indicaciones de aviso 76
advertencia 77
aviso 79
peligro 76
Indicaciones de seguridad 75
Indicaciones de seguridad para Australia 80
Indicaciones de seguridad para Brasil 80
Indicaciones de seguridad para Canadá 83
Indicaciones de seguridad para EE. UU. 80
inicio de sesión de usuario móvil 985
inicio de sesión móvil 985
instalación 136, 225, 280
Instant Message) 535
Instrucciones de uso 74
Intercalar 682
Intercambio de hardware 345
Interceptación/PO/Hot-line, Modo Experto 1568
Interconexión
eliminar nodos de la interred 1170
heterogénea, híbrida 1072
homogénea, nativa 1072
Interconexión SIP, modo Experto 1665
Interfaces de red 1625
Placa base, modo experto 1617, 1626, 1628, 1629
Placa base, Modo Experto 1617, 1622, 1623, 1624, 1624, 1630
Tablero de aplicaciones, Modo Experto 1630, 1631, 1631
Interfaces de red, Modo Experto 1617
Interfaces de salida trace, Modo Experto 1523
Interfaz de línea múltiplex primaria 804
Interfaz de Web Services 1200
interferencias de radiofrecuencia 89
interferencias electromagnéticas 89
Inventario de OpenScape Business S
consultar 1301
Inventario de OpenScape Office LX/HX
consulta 350, 350
Inventario de OpenScape Office MX
consulta 350
inventario, OpenScape Business S 1299
inventario, OpenScape Business X 1298
inventario, OpenScape Business X3/X5/X8
consultar 1299
invitación
conferencia 532
ITSP (Internet Telephony Service Provider) 183, 249, 394, 396
ITSP (Proveedor de servicios de telefonía por Internet) 394

J

Java 1216
Java Runtime Environment (JRE) 138
Jefe/secretaria (véase Configuración Jefe/secretaria) 724

L

LAN 1 (WAN), modo experto 1617
LAN 1, Modo Experto 1631
LAN 2, Modo Experto 1622, 1631
LAN 3 (Administrador), Modo Experto 1623
LCR
Clases de servicio, Modo Experto 1641
Flags LCR, Modo Experto 1641
Multisitio, Modo Experto 1646
Plan, Modo Experto 1641
Regla de marcación, Modo Experto 1644
Tabla de rutas, Modo Experto 1643
LCR (Least Cost Routing) 793
asignar/modificar clase de servicio 801
clase de servicio 801
editar plan de marcación 798
editar reglas de marcación 803
editar tabla de rutas 800
funcionalidad 793, 793

plan de marcación 797
reglas de marcación 801
tabla de rutas 799
LDAP, Modo Experto 1571
licencia 304
activar mediante el código de autorización de licencia 320, 1441
mostrar información 339, 340, 340, 341
Licencia
activar a través del archivo de licencia 320
actualizar 346
mostrar información 341, 350
Límites de ampliación 1466
línea colectiva
añadir 712
Línea colectiva
añadir miembro 714
borrar 714
borrar miembro 714
modificar 713
Línea de servidor SIP nativo, modo experto 1666
Línea privada 655
línea urbana RDSI
ocupación selectiva 805
líneas 415
modificar protocolo 420
Líneas
asignar MSN 419
configurar el tipo de ocupación 425, 429, 430
modificar código 418, 418, 419
modificar protocolo 419, 420
modificar ruta 424
tipo de ocupación 421
Líneas, Modo Experto 1722
Líneas/Interconexión
Asignar MSN, Modo Experto 1734
Líneas, Modo Experto 1722
Parámetros RDSI, Modo Experto 1734
Prestaciones QSIG, Modo Experto 1733
Líneas/Interconexión, Modo Experto 1722
lista de favoritos 594
Lista de favoritos
Mensaje instantáneo 535
Lista de favoritos (UC Smart) 522
Lista de ubicaciones, Modo Experto 1783
Listas de nos. permitidos, Modo Experto 1737
Listas de nos. prohibidos, Modo Experto 1738, 1738
Listín del sistema (UC Suite) 584
llamada
perdida 595
programada 595
llamada de grupo 699
correo de voz 700
de grupo tipo, agregar 708
de tipo Caso de libre, agregar 717
de tipo llam. en espera, agregar 717
DND para miembro del grupo 700
Teléfonos SIP 702
tipo de llamada 702
Llamada de grupo
activar el bloqueo de avisos de llamada en espera para miembro de grupo 719
borrar tipo Aviso llam. en espera 718
borrar tipo Caso de libre 718
borrar tipo Grupo 710
desactivar el bloqueo de avisos de llamada en espera para miembro de grupo 719
modificar tipo Aviso llam. en espera 718
modificar tipo Caso de libre 718
modificar tipo Grupo 709
mostrar tipo Aviso llam. en espera 718
mostrar tipo Caso de libre 718
tipo Aviso llam. en espera, añadir miembro 718
tipo Aviso llam. en espera, borrar miembro 718
tipo Caso de libre, añadir miembro 718
tipo Caso de libre, borrar miembro 719
tipo Grupo, añadir miembro 711
tipo Grupo, borrar miembro 711
llamada de socorro 834
Llamada recordatoria 664
Llamadas de emergencia
Requisitos 833
Llamadas entrantes
Grupos/Grupos de caza, Modo experto 1708
Miembros del grupo, Modo Experto 1711
Team/Top, Modo Experto 1713
Telecaptura de llamadas, Modo Experto 1716
Tr. autom diferidas, Modo Exp 1719
UCD, Modo Experto 1716
Llamadas entrantes, Modo Experto 1708
logotipo de teléfono
Cargar, Modo Experto 1517
loopback digital 1336
Loopback digital, Modo Experto 1524
LXV3, Modo Experto 1795

M

Mail Exchanger 391, 391
definir 394
Manager E 133
Mantenimiento DLI, Modo Experto 1544
Mantenimiento, modo experto 1507
Mantenimiento, Modo Experto 1795
Mapping (Presencia UC Suite) 567
Marca, Modo Experto 1512
Marcación abreviada central (KWZ) 647
Marcación abreviada individual (KWI) 651
Marcación clipboard 597
Marcación de dígitos 644
Marcación de escritorio 549, 597
Marcación en bloque 644
Marcación por teclado numérico 644
Marcación posterior 647
Marcaciones abreviadas, Modo Experto 1794

Matriz VBZ, Modo Experto 1740
MCL Single Stage 804
MCL Two Stage 804
MEB (Media Extension Bridge) 1798
Media Extension Bridge (MEB) 1798
Media Stream Control (MSC), Modo Experto 1750
Mediatrix 4102S 111
medio de copia de seguridad 1267
  añadir 1267
  Borrar 1269
  editar 1269
Medio de copia de seguridad 1264
mejora 1273
Mensaje a grupo 757, 757
  transferir llamada 758
Mensaje directo 652
Mensaje discreto) 666
mensaje instantáneo 614
Mensaje instantáneo 535, 535, 535, 614, 614
mensajería instantánea 614, 880
mensajes
  administrar 879
Mensajes de fax 617, 880
Mensajes de texto 685
Mensajes de voz (UC Smart) 537
Mensajes del buzón de voz 617, 880
Mensajes directos para grupos 757
mensajes instantáneos 880
Mensajes por ausencia 684
Menús flexibles, Modo Experto 1573
Miembros del grupo, Modo Experto 1711
mobility
  configuración de teléfonos móviles para GSM 981
Mobility
  borrar extensión 985
Mobility Entry 974
  códigos de prestación 974
Módem 453
Módem Internet 383
Módem RDSI 450
Modificar matriz VBZ 791
Modo DHCP, Modo Experto 1624
Modo Experto, Modo Experto 1506
Módulos hardware, Modo Experto 1751
MoH 1257, 1260
Mostrar lista de números autorizados 779
Mostrar lista de números prohibidos 778
Movilidad IP 985
MULAP básico 739
  agregar miembro 746
  añadir 745, 750
  borrar 746
  borrar miembro 747
  modificar 746
  modificar miembro 747
  mostrar 746
  tipo de llamada 741
MULAP Jefe 742
  agregar miembro 749
  añadir 747
  borrar 748
  borrar miembro 749
  modificar 748
  modificar miembro 749
  mostrar 748
  Teléfonos SIP 744
  tipo de llamada 744
Multi-SLC, Modo Experto 1707
música en espera 1260
Música en espera 1257, 1257
Música en espera (Music On Hold, MOH) en distribución de llamadas (UCD 769
Música en espera, modo experto 1742
Música interna en espera 1260
myAgent
  Requisitos previos 890
myPortal
  estado de presencia 548
  Funciones 548
myPortal for Outlook
  Funciones 549
myPortal Smart
  Funciones 501
myPortal to go
  Requisitos previos 972
myReports
  restablecer la contraseña de administrador 894
  roles de usuario 892

N

NAT (Network Address Translation) 1013
NAT, Modo Experto 1635
No molestar 678
Noche
  Grupos de clase de servicio, Modo Experto 1736
Nodos, Modo Experto 1664
Nombre de host, Modo Experto 1617, 1630
Nombre DNS 391
normativa de protección antiincendios 87
Notificación
  mensaje de fax 629
  mensaje de voz 544, 629
Notificación DLS, Modo Experto 1545
Notificación por SMS 631
Notificar accidente 85
Numeración
  abierta 1082
  cubierta, cerrada 1081
Numeración E.164 1082
número de acceso telefónico
  conferencia 532
Números de teléfono públicos en la red 1083

O

Objetos CCV 853, 905
Observaciones sobre el uso simultáneo de myAgent y clientes de UC Suite 896
Ofertante de red 804
Ofertante de red principal 804
Open Directory Service 1216
  Ajustes básicos, Modo Experto 1794
  Fuentes de datos, modo experto 1794
  Fuentes de datos, Modo Experto 1794, 1795
  Mantenimiento, Modo Experto 1795
Open Directory Service, Modo Experto 1793, 1795
OpenScape Business Assistant 115, 117
OpenScape Business X3R
  puesta a tierra de protección 1436, 1437, 1439
OpenScape Business X5R
  puesta a tierra de protección 1436, 1437, 1439
OpenScape Office, modo experto 1794
OpenScape Personal Edition 111
OpenStage 111
OpenStage Attendant 862
optimación de rutas 1083
optiPoint 111

P

Padding 1025
Para todo el sistema, Modo Experto 1703
Parám. códec destino, Modo Experto 1652
Parámetro global, modo experto 1625
Parámetros códec, Modo Experto 1650
Parámetros de extensión, Modo Experto 1684
Parámetros de red (LAN, WAN) 1079
Parámetros de tiempo
  supervisar una llamada UCD en una línea analógica 771
  supervisar una transferencia antes de contestar a un grupo UCD 771
Parámetros de tiempo, Modo Experto 1557
Parámetros RDSI, Modo Experto 1734
Parámetros SIP, Modo Experto 1647
path replacement 1083
Pausa interdigital 651
Payload
  Dispositivos, Modo Experto 1750
  Media Stream Control (MSC), Modo Experto 1750
  Módulos hardware, Modo Experto 1751
Payload, Modo Experto 1750
Perfil
  agregar miembros 485
  borrar miembros 486
  exportar perfil individual 486
  exportar todos los perfiles 488, 1006
  importar perfil individual 486
  importar todos los perfiles 488, 1006
  mostrar miembros 485
  mostrar perfiles 485
Perfil de datos de configuración de Application Launcher 1216
Perfil de usuarios de la UC Suite 563
perfil trace 1339
Perfil trace
  agregar 1352
  detener todos los perfiles 1351
  iniciar 1344
  mostrar 1343
  mostrar datos detallados 1351
  parar 1344
Perfil:exportar todos los perfiles 488, 1006
Perfil:importar todos los perfiles 488, 1006
perfiles
  crear un nuevo perfil 484
  edición 487
  suscriptores 483
perfiles de usuario (extensiones) 483
Perfiles trace, Modo Experto 1530
Perfiles, modo Experto 1790
Perfiles/Plantillas, Modo Experto 1697
permanente 609
Pin móvil 688
PIN para activar un Shutdown 1291
Ping, Modo Experto 1547
Placa base, modo experto 1625
Placa base, Modo Experto 1546
Plan de interconexión 1072
Plan de marcación, Modo Experto 1641
Plan de numeración 139, 229, 432, 797
  borrar 435
  importar 437, 437
  modificar 436
Plan horario 852, 904
planes de horarios vacacionales 853, 905
Planes horarios, Modo Experto 1780
Plantillas SMS 631
Plantillas, Modo Experto 1768
Portero eléctrico/Abrepuertas 1177
Pre-Shared Keys 1034
Presencia
  desvío de llamadas 571
Presencia (UC Smart) 519, 519, 519
Presencia (UC Suite) 567, 567, 567
Presentación de identificación de líneas conectadas - COLP 658
Prestaciones
  voz, a nivel de red 1078
Prestaciones Euro-RDSI 1801
Prestaciones QSIG, Modo Experto 1733
Proceso de registro de licencia 327
programación de teclas 455, 455
Programación de teclas, Modo Experto 1702
Protección de datos 89, 967
Protocolo admin. 1066
  cargar 1066
  Configuración, Modo Experto 1541

Datos protocolo admin, Modo Experto 1541
modificar idioma 1021, 1021, 1022, 1022, 1067
Protocolo admin., Modo Experto 1541
Protocolo ARP, Modo Experto 1546
Protocolo CSTA 1185
protocolo de diagnóstico 1361
Protocolo de diagnóstico 1332
abrir 1365
borrar 1365, 1366
descargar 1365
Protocolo de diagnóstico (Datos de diagnóstico)
descargar 1334
Protocolo PPP, Modo Experto 1637
Protocolo sucesos, Modo Experto 1535
protocolo trace de cliente 1337
Protocolo trace de cliente
abrir 1346
borrar 1346
descargar 1346
modificar 1345
mostrar 1345
Protocolo trace de cliente, Modo Experto 1524
Protocolo trace, Modo Experto 1524
Protocolos de diagnóstico
descargar 1334
Protocolos de diagnóstico, Modo Experto 1536, 1542
Proveedor de servicios CSTA (CSP) 1797
Proveedor de servicios de telefonía por Internet, modo experto 1652
PSTN, Modo Experto 1636
Public Key Infrastructure (PKI), Modo Experto 1613
puerto 1216
Puertos 1011
administración de puertos 1012
configurar Liberación de puerto 1012, 1167
Puesto de trabajo alternativo 570
Puntos cód. AF/EF 442

Q

Quality of Service (QoS) 442
configuración 444

R

Reasignación 689
Recarga (Reload) de la UC Booster Card 1293
Recarga (Reload) de OpenScape Business 1289
Rechazar llamadas 678
reciclaje 85
recordatorio programado; cita 692
Recuperar 1264, 1272
Red
licencia 1079
Red corporativa 804
Registro Mail-Exchange 391
Registro MX 391
Registros de cliente 1376
regla 571
Regla de marcación, Modo Experto 1644
Regla NAT
borrar 1015
configurar 1013
configurar con el editor de tablas NAT 1014
Reglas activas, Modo Experto 1610
Reglas configuradas, Modo Experto 1611
Reglas de marcación 801
Reglas NAT 1013
Reglas VPN
agregar para dirección opuesta 1055
añadir regla configurada 1053
borrar 1055
editar 1054
mostrar regla activa especial 1053
mostrar todas las reglas activas 1052
mostrar todas las reglas configuradas 1053
Reiniciar / Volver a cargar
Reiniciar / Volver a cargar, Modo Experto 1537
Reiniciar / Volver a cargar, Modo Experto 1537, 1537
Reinicio de OpenScape Business 1288
Rellamada 646
Reposición de una llamada 678
reproductor de anuncios 1796
Reproductor de anuncios, Modo Experto 1586
Requisitos de protección contra descargas 88
Requisitos LAN 1080
requisitos para Application Launcher 1216
Requisitos para myAgent 890
Requisitos para myPortal to go 972
requisitos para myReports 894
Reserva de línea 654
Restart de OpenScape Business 1288
resumen de mensajes 879
Retener 661
router estándar
configurar 370
Router estándar 369
Router estándar, Modo Experto 1633, 1634
Router Internet 379
RPCAP Daemon
activar 1359
desactivar 1359
rpcap Daemon, Modo Experto 1532
Ruta, Modo experto 1725
Ruta, Modo Experto 1664
rutas 415
Rutas 420
asignar código 424
asignar nombre 424
configurar tipo de número saliente 426
configurar tipo de números de llamada 426
introducir número de teléfono del sistema 426
introducir ruta de desbordamiento 425
introducir un segundo código de línea urbana 427

prefijo ruta entrantes 422, 427
rutas estáticas
añadir 370, 374, 374, 375
Rutas estáticas 370
borrar 371
Rutas estáticas, Modo Experto 1633, 1634

S

SA Payload 1034
SA-IKE 1033
sala de conferencias virtual 532
Salida de consola trace, Modo Experto 1546
Salida de texto multilingüe 1256
Secure Trace
cambiar la contraseña 1348
consultar estado 1348
editar frase de contraseña 1348
importar archivo X.509 1349
importar certificado a partir de archivo X.509 1349
iniciar 1347
parar 1347, 1348
Secure Trace, Modo Experto 1525
Security Associations SA 1033
Security Checklist 1010
seguimiento 1335
registro 1336
Seguimiento de pila H.323 1338
seguimiento del componente de licencia 1339
Seguimiento seguro 1337
Seguridad
Cifrado de señalización y carga útil (SPE), Modo Experto 1596, 1596, 1597
Cortafuegos de aplicaciones, modo experto 1591
Deployment and Licensing Client (DLSC), Modo Experto 1593, 1593, 1594
Seguridad SQL, Modo Experto 1616
Seguridad Web, Modo Experto 1616
SSL, Modo Experto 1613, 1614, 1615
VPN, Modo Experto 1597, 1598, 1599, 1599, 1600, 1601, 1602, 1602, 1603, 1606, 1610, 1611, 1613
Seguridad de datos 89
Seguridad SQL, Modo Experto 1616
Seguridad Web, Modo Experto 1616
Seguridad, Modo Experto 1591
Selección de aplicación 1759
Sello CE 89
señalización de alarmas, Modo Experto 1537
Señalizaciones de llamada 655
Servicio autom. nocturno, Modo Experto 1741
Servicio CallMe 570
Servicio de Active Directory 1213
Servicio de datos Kernel Crash
detener 1356
inicio 1355
Servicio de emergencia E911 837
Servicio de integración de Active Directory, modo Experto 1759
Servicio de notificación 544, 629
Servicio DynDNS 391
configurar 392, 411, 412, 413, 414, 1009
Servicio DynDNS, Modo Experto 1577
Servicio nocturno, Modo Experto 1739
Servicios activos, Modo Experto 1602
Servicios configurados VPN
borrar 1048
cambiar nombre 1047
editar 1047
Servicios configurados, Modo Experto 1602
servicios remotos 1387
Servidor de control de marcación 804
Servidor de licencia (CLS)
modificar dirección IP 326, 337, 347
servidor de licencias (CLS) 323, 346
Editar la dirección IP 213, 266, 334, 342, 343, 343, 344
Servidor DNS 369
Servidor DNS, Modo Experto 1633
Servidor DSS 1797
Servidor FTP, Modo Experto 1624
Servidor PKI
añadir 1056
mostrar 1056
Servidor, Modo Experto 1783
Shutdown
PIN de activación 1291
Signaling and Payload Encryption
activar soporte SPE 1021
desactivar soporte SPE 1021
sistema de despertador automático 692
Sistema, Modo Experto 1548
Site Of Operations, Modo Experto 1759
SLC, Modo Experto 1705
SmartVM, Modo Experto 1509, 1509, 1510, 1746
SMS
notificación 629
SNMP
Comunidades, Modo Experto 1539, 1539, 1540, 1540
Traps, Modo Experto 1540
SNMP (Simple Network Management Protocol) 1317
añadir comunidad 1329
Base de datos de información de gestión MIB 1317
borrar comunidad 1330
comunidades 1318
editar comunidad 1330
mostrar comunidades 1329
mostrar detalles de una trap 1331
mostrar traps 1331
traps 1318
SNMP, Modo Experto 1539
Solución Cordless
configuración de sistema 989
SSDP (Smart Services Delivery Platform) 1387
configurar el plugin de servicio para una red de clientes con Proxy 1390

configurar PIN para activar/desactivar el plugin de servicio 1393
desactivar plugin de servicio 1392
restablecer el plugin de servicio 1392
SSL (Secure Socket Layer) 1056
activar certificado 1064
borrar certificado 1063
exportar certificado 1063
generación de una solicitud de certificado 1061
generar certif. con firma automática 1059
generar certificado de entidad emisora 1059
importar certificado renovado 1063
importar un certificado de servidor 1061, 1062, 1065
mostrar certificados 1016, 1017, 1017, 1062
STUN (Simple Traversal of UDP over NAT) 413
suceso
modificar la configuración de correo electrónico 1363
sucesos
señalización de alarmas, Modo Experto 1537
Sucesos
Configuración de sucesos, Modo Experto 1534
Correo electrónico, Modo Experto 1535
Protocolo sucesos, Modo Experto 1535
Protocolos de diagnóstico, Modo Experto 1536
Tabla reacción, Modo Experto 1536
Sucesos, Modo Experto 1534
supervisión de llamadas, Modo Experto 1528
supervivencia 1167
Supresión de la indicación del número llamado
COLR 658
Supresión de la indicación del número llamante
CLIR 657

T

Tabla de rutas 799
Tabla de rutas, Modo Experto 1643
tabla reacción 1361
Tabla reacción, Modo Experto 1536
Tarjeta RDSI 450
Tarjeta UC Booster
reiniciar 1292, 1292
Tasas de llamada - Códigos de proyecto, Modo Experto 1585
Tasas de llamada - Factores, Modo Experto 1584
Tasas de llamada - Formato de salida, Modo Experto 1582
TCP Dump 1357
borrar 1358
detener 1358
iniciar 1357
TCP Dump, Modo Experto 1531
Team (véase Configuración de equipo) 720
Team/Top, Modo Experto 1713
Tecla de llamada directa 652
Tecla DSS 652
teclas de función 455
programa 456, 518
Teclas de función
programación 496, 497, 499, 518, 544
Telecaptura de llamadas, Modo Experto 1716
Telefon-Logo
Verteilen, Experten-Modus 1517
Telefonía Dual-Mode 979
Telefonía Internet 394
Telefonía, Modo Experto 1548
Teléfono analógico 453
Teléfono RDSI 450
Teléfonos 110
Teléfonos DECT 111
Teléfonos Gigaset 111
Teléfonos inalámbricos 111
Teléfonos SIP 111
Teléfonos WLAN 111
teletrabajo 1001
Teletrabajo 570
Textos del sistema, Modo Experto 1755
Textos, Modo Experto 1572
Tiempo actualiz. nombres DNS, Modo Experto 1578
Timbre adicional 676
Tipos de temas 74
Todos los leases, Modo Experto 1630
Tono de llamada/Aviso de llamada en espera 680
Tr. autom diferidas, Modo Exp 1719
trace
borrar registro 1342
Trace (Seguimiento)
borrar protocolo 1342
descargar protocolo 1341
modificar configuración de formato 1344
modificar interfaces de salida 1345
mostrar configuración de formato 1344
mostrar interfaces de salida 1345
Trace (Seguimiento):configuración de formato 1335
Trace (Seguimiento):interfaces de salida 1336
Trace de componentes de licencia
modificar 1351
Trace de componentes de licencia, Modo Experto 1530
Trace del servidor de medios
detener 1356
inicio 1356
Trace pila H.323
abrir protocolo 1350
borrar protocolo 1350
descargar protocolo 1350
editar módulos 1349
modificar configuración 1349
mostrar configuración 1349
Trace pila H.323, Modo Experto 1527
Traceroute, Modo Experto 1547
traces
supervisión de llamadas, Modo Experto 1528
Traces
Componente de licencia, Modo Experto 1530
Componente trace M5T, Modo Experto 1525
Componentes trace, Modo Experto 1531

Configuración de formato trace, Modo Experto 1522
Interfaces de salida trace, Modo Experto 1523
Loopback digital, Modo Experto 1524
Perfiles trace, Modo Experto 1530
Protocolo trace de cliente, Modo Experto 1524
Protocolo trace, Modo Experto 1524
rpcap Daemon, Modo Experto 1532
Secure Trace, Modo Experto 1525, 1526, 1526
TCP Dump, Modo Experto 1531
Trace pila H.323, Modo Experto 1527
Traces del servidor de medios, modo experto 1534
Traces del servidor de medios, modo experto 1534
Traces, Modo Experto 1522
Transferencia a grupo desde mensaje 758
transferencia automática de llamadas en caso de ocupado 669
transferencia automática diferida de llamadas - sin respuesta 675
transferencia de software 1273
transferencia, software (véase transferencia de software) 1273
transferir llamadas 663
Transmisión de información de número de teléfono específico del cliente 659
Transmisión del número de teléfono del llamante
CLIP 656
Traps, Modo Experto 1540
Troncales/Enrutamiento
Ruta, Modo experto 1725
Túnel activo VPN
mostrar 1048
Túnel configurado VPN
mostrar reglas 1050
Túnel IPSec 1033
Túneles act., Modo Experto 1603
Túneles config., Modo Experto 1606
Túneles configurados VPN
añadir 1050
mostrar 1049

U

Ubicación única 1073
UC Applications, modo Experto 1696
UC Smart
Ajustes básicos 1760
Estado 1762
Gestión de usuarios 1761
UC Smart
consultar estado 1386
Estado 1386
UC Smart, Modo Experto 1760
UC Suite 1763
Carga de archivo, Modo Experto 1781
Configuración de proveedores externos, Modo Experto 1769
configurar el periodo de retención de los datos del Contact Center 1386
configurar el tiempo de mantenimiento 1384
configurar notificaciones por correo electrónico para errores del sistema 1383
configurar periodo de retención de archivos de registro 1385
Contact Center, modo experto 1771
Departamentos, Modo Experto 1766
desactivar la grabación de los registros del sistema 1377
descargar Client Logs 1380
Directorio de usuario, Modo Experto 1763
Directorio externo, Modo Experto 1768
En conferencia, Modo Experto 1782
Encabezados de fax, Modo Experto 1792
Grupos, Modo Experto 1766
Lista de ubicaciones, Modo Experto 1783
notificación de email 1381
Perfiles, modo Experto 1790
permitir la grabación de los registros del sistema 1377
Planes horarios, Modo Experto 1780
Plantillas, Modo Experto 1768
Protocolización de sistema 1376
realizar el mantenimiento del sistema inmediatamente 1385
Registros de cliente 1376
Servidor, Modo Experto 1783
UC Suite:activar el registro de los Client-Logs a nivel de sistema 1377
UC Suite:activar la memorización de los registros de cliente en el disco duro 1379
UC Suite:configurar la ruta de almacenamiento para los archivos de registro de cliente 1379
UC Suite:desactivar el registro de los Client-Logs a nivel de sistema 1377
UC Suite:desactivar la memorización de los registros de cliente en el disco duro 1379
UC Suite
activar el registro de los Client-Logs a nivel de extensión 1378
desactivar el registro de los Client-Logs a nivel de extensión 1378
mantenimiento 1375, 1383
notificación 1381
supervisión 1375
UC Suite, Modo Experto 1763
UCD
aceptar automáticamente llamadas UCD, activar 765
aceptar automáticamente llamadas UCD, desactivar 765
agente UCD 761
agregar agente UCD 762
anuncios grabados 769
borrar agente UCD 762
cola 766
desbordamiento 767
estado de extensión 761
grupo UCD 759

liberación de llamadas UCD a través de líneas analógicas, modificar tiempo de liberación 771
modificar anuncios grabados 770
modificar cola 766
modificar desbordamiento 768
modificar el tiempo administrativo 763
modificar música en espera (Music On Hold MOH) 770
modificar prioridad de llamadas externas 765
modificar prioridad de llamadas internas 765
prioridad de llamadas externas 764
prioridad de llamadas internas 764
servicio nocturno 768
tiempo administrativo (tratamiento posterior 763
transferencia a grupo UCD, modificar tiempo de llamada recordatoria 771
transferir a grupo UCD 770
UCD, Modo Experto 1716
Uso adecuado de los sistemas de comunicación y servidores 85
usuaios de UC Smart
editar datos 518
Usuario online 1399, 1548
iniciar 1315, 1400
Usuario online, Modo Experto 1548
Usuario RAS 444
Usuarios de UC Smart
editar datos 518, 544
usuarios de UC Suite
cambiar longitud de la contraseña 563
Modificar contraseña 562
modificar el estado de presencia 562
Usuarios de UC Suite 558
configurar como agentes 561
editar datos 561
restablecer 561

V

Valores máximos
Prestaciones 1475
Varias ubicaciones 1073
visor de sucesos 1336
Visor de sucesos
abrir protocolo 1346
borrar protocolo 1346
descargar protocolo 1346
modificar protocolo 1345
mostrar protocolo 1345
Voice Gateway
Interconexión SIP, modo experto 1666
VPN
anchos de banda 1024
autenticación 1034
certificados 1035
clientes 1040
mecanismos de seguridad 1033
VPN - Servicios activos
mostrar servicio especial 1046
mostrar servicios 1046
VPN - Servicios configurados
mostrar servicios 1046
VPN - Túneles act.
mostrar reglas 1049
VPN (Virtual Private Network / Red privada virtual) 1023
end-to-site 1023
site-to-site 1023
VPN, Modo Experto 1597

W

WAN 391
WBM 115
página de inicio 115
web collaboration 533
Web Collaboration 611, 611, 611
Web Collaboration, Modo Experto 1793
Web Services 1216
Web Collaboration, Modo Experto 1793
Web Services, Modo Experto 1792

© 2025 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.