



A MITEL
PRODUCT
GUIDE

Mitel OpenScape Business

OpenScape Business
X3/X5/X8

OpenScape Business V4

Guía de instalación
07/2026

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 2026, Mitel Networks Corporation

All rights reserved

Contenido

1 Historial de cambios.....	9
1.1 Historial de mejoras/correcciones.....	9
2 Introducción y notas importantes.....	10
2.1 Acerca de esta documentación.....	10
2.1.1 Documentación y destinatarios.....	10
2.1.2 Tipos de temas.....	12
2.1.3 Convenciones de representación.....	12
2.2 Indicaciones de seguridad y de aviso.....	13
2.2.1 Indicaciones de aviso: Peligro.....	14
2.2.2 Indicaciones de aviso: Advertencia.....	14
2.2.3 Advertencias: Atención.....	15
2.2.4 Indicaciones de aviso: Aviso.....	16
2.2.5 Indicaciones de seguridad nacionales.....	17
2.2.5.1 Indicaciones de seguridad para Australia.....	17
2.2.5.2 Indicaciones de seguridad para Brasil.....	18
2.2.5.3 Indicaciones de seguridad para EE. UU.....	18
2.2.5.4 Indicaciones de seguridad para Canadá.....	20
2.3 Avisos importantes.....	21
2.3.1 Comportamiento en caso de emergencia.....	21
2.3.2 Uso adecuado.....	22
2.3.3 Eliminación y reciclaje adecuados.....	23
2.3.4 Normas y pautas relativas a la instalación.....	23
2.3.4.1 Conexión de OpenScape Business X al circuito de alimentación eléctrica.....	23
2.3.4.2 Conexión de OpenScape Business S y OpenScape Business UC Booster Server con el circuito de alimentación eléctrica.....	24
2.3.4.3 Cableado blindado para conexiones LAN y WAN de OpenScape Business X.....	24
2.3.4.4 Normativa de protección antiincendios.....	25
2.3.4.5 Requisitos de protección contra descargas.....	25
2.3.4.6 Identificaciones para OpenScape Business X.....	26
2.3.5 Indicaciones sobre interferencias electromagnéticas y radio interferencias de OpenScape Business X.....	26
2.3.6 Privacidad y seguridad de los datos.....	27
2.3.7 Normas técnicas y conformidad de OpenScape Business X.....	28
2.3.7.1 Conformidad CE.....	28
2.3.7.2 Conformidad con normas estadounidenses y canadienses.....	28
2.3.7.3 Conformidad con las normas internacionales.....	28
2.3.8 Condiciones de servicio.....	29
2.3.8.1 Condiciones de servicio de OpenScape Business X.....	29
2.3.8.2 Condiciones de servicio de OpenScape Business S y OpenScape Business UC Booster Server.....	30
3 Preparar la instalación de OpenScape Business X3/X5/X8.....	31
3.1 Requisitos para la instalación.....	31
3.2 Actividades previas.....	36
3.2.1 Cómo desempaquetar los componentes.....	36
3.2.2 Cómo retirar la tapa de la carcasa en X3W/X5W.....	37
4 Preparación para la instalación inicial del OpenScape Business UC Booster Server.....	39
5 Instalación de hardware por OpenScape Business X3W/X5W.....	40
5.1 Tipo de montaje.....	40

5.1.1	Cómo fijar el sistema de comunicación a una pared.....	40
5.2	Puesta a tierra de protección.....	41
5.2.1	Cómo establecer una puesta a tierra de protección para el MDFU del distribuidor principal.....	42
5.2.2	Cómo comprobar la puesta a tierra de protección.....	48
5.3	Cable de conexión para la conexión directa de teléfonos, líneas urbanas, etc.....	48
5.4	Indicaciones para la configuración.....	49
5.4.1	Slots de módulos en OpenScape Business X3W.....	50
5.4.2	Slots para módulos en OpenScape Business X5W.....	50
5.4.3	Instalación de módulos.....	52
5.4.3.1	Cómo insertar un módulo.....	52
5.4.3.2	Cómo retirar un módulo.....	52
5.5	Puerto LAN y WAN.....	52
5.5.1	Realizar la conexión LAN o WAN.....	53
5.6	Conexión urbana.....	54
5.6.1	No para EE. UU. ni Canadá: Cómo implementar una conexión de centralita RDSI o un acceso individual RDSI mediante una interfaz S_0	54
5.6.2	No para EE. UU. ni Canadá: Cómo realizar una conexión múltiplex primaria mediante una interfaz S_{2M} (solo para OpenScape Business X5W).....	55
5.6.3	Solo para EE. UU. y Canadá: Cómo realizar una conexión múltiplex primaria RDSI mediante una interfaz T1 (solo para OpenScape Business X5W).....	56
5.6.4	Solo para algunos países: Cómo hacer una conexión de línea urbana mediante una interfaz E1-CAS (solo para OpenScape Business X5W).....	56
5.6.5	Cómo realizar una conexión urbana analógica.....	57
5.7	Conexión de teléfonos y dispositivos.....	58
5.7.1	No para EE. UU., Canadá: cómo conectar directamente teléfonos RDSI.....	58
5.7.2	No para EE. UU., Canadá: Cómo conectar teléfonos RDSI por bus S_0	60
5.7.3	Cómo conectar teléfonos $U_{P0/E}$	63
5.7.4	Cómo conectar dispositivos y teléfonos analógicos.....	64
5.8	Emisiones de interferencias.....	65
5.8.1	Cómo colocar una ferrita en la línea de conexión de red.....	67
5.8.2	Cómo colocar ferritas en las líneas de conexión de periféricos.....	67
5.9	Tareas finales.....	69
5.9.1	Cómo insertar la tarjeta M.2 SSD o la tarjeta SDHC (sistema con OCCM).....	69
5.9.2	Cómo efectuar la prueba visual.....	70
5.9.3	Cómo colocar la tapa de la carcasa.....	71
5.9.4	Cómo conectar el sistema a la red eléctrica.....	72
6	Instalación de hardware por OpenScape Business X3R/X5R.....	73
6.1	Tipos de montaje.....	73
6.1.1	Cómo montar OpenScape Business X3R en un armario de 19 pulgadas.....	73
6.1.2	Cómo montar OpenScape Business X5R en un armario de 19".....	74
6.1.3	Cómo fijar el sistema de comunicación a una pared.....	76
6.2	Puesta a tierra de protección.....	77
6.2.1	Puesta a tierra de protección con montaje en armario de 19".....	77
6.2.1.1	Cómo instalar una puesta a tierra de protección para el sistema de comunicación.....	77
6.2.1.2	Cómo comprobar la puesta a tierra de protección.....	80
6.2.2	Toma de tierra en el montaje y con montaje autónomo.....	81
6.2.2.1	Cómo instalar una puesta a tierra de protección para el sistema de comunicación.....	81
6.2.2.2	Cómo comprobar la puesta a tierra de protección.....	88
6.3	Indicaciones para la configuración.....	88
6.3.1	Slots de módulos en OpenScape Business X3R.....	88
6.3.2	Slots de módulos en OpenScape Business X5R.....	89
6.3.3	Instalación de módulos.....	89
6.3.3.1	Cómo insertar un módulo.....	89
6.3.3.2	Cómo retirar un módulo.....	90
6.3.3.3	Cómo montar una placa de protección.....	90

6.4 Conexión urbana.....	90
6.4.1 No para EE. UU. ni Canadá: Cómo implementar una conexión de centralita RDSI o un acceso individual RDSI mediante una interfaz S_0	91
6.4.2 No para EE. UU. ni Canadá: Cómo realizar una conexión múltiplex primaria RDSI mediante la interfaz S_{2M} (solo para OpenScape Business X5R).....	91
6.4.3 Solo para EE. UU. y Canadá: Cómo hacer una conexión múltiplex primaria RDSI mediante la interfaz T1 (solo para OpenScape Business X5R).....	92
6.4.4 Solo para algunos países: Cómo implementar una conexión de línea urbana mediante la interfaz E1-CAS (solo para OpenScape Business X5R).....	93
6.4.5 Cómo realizar una conexión urbana analógica.....	93
6.5 Conexión de teléfonos y dispositivos.....	94
6.5.1 No para EE. UU., Canadá: cómo conectar directamente teléfonos RDSI.....	95
6.5.2 No para EE. UU., Canadá: Cómo conectar teléfonos RDSI por bus S_0	96
6.5.3 Cómo conectar teléfonos $U_{P0/E}$	98
6.5.4 Cómo conectar dispositivos y teléfonos analógicos.....	99
6.6 Tareas finales.....	100
6.6.1 Cómo insertar la tarjeta M.2 SSD o la tarjeta SDHC (sistema con OCCM).....	100
6.6.2 Cómo efectuar la prueba visual.....	100
6.6.3 Cómo conectar el sistema a la red eléctrica.....	102
7 Instalación de hardware por OpenScape Business X8.....	103
7.1 Tipos de montaje.....	103
7.1.1 Montaje autónomo.....	103
7.1.1.1 Cómo montar un sistema de box único.....	103
7.1.1.2 Sistema de box doble: Cómo montar superpuestos los armarios del sistema.....	104
7.1.1.3 Sistema de doble box: Cómo montar armarios del sistema superpuestos.....	106
7.1.2 Montaje en armario de 19 pulgadas.....	108
7.1.2.1 Cómo montar un armario de sistema en un rack de 19 pulgadas.....	108
7.2 Paneles de interconexión (opcional).....	110
7.2.1 Cómo montar un panel de interconexión en un armario de 19 pulgadas.....	114
7.3 Puesta a tierra de protección.....	114
7.3.1 Puesta a tierra de protección con montaje autónomo.....	115
7.3.1.1 Cómo establecer una puesta a tierra de protección para el MDFU del distribuidor principal.....	115
7.3.1.2 Cómo comprobar la puesta a tierra de protección.....	119
7.3.2 Puesta a tierra de protección con montaje en armario de 19".....	119
7.3.2.1 Cómo instalar una puesta a tierra de protección para el sistema de comunicación y el panel de interconexión.....	119
7.3.2.2 Cómo comprobar la puesta a tierra de protección.....	122
7.4 Notas de configuración.....	123
7.4.1 Slots de módulos del armario básico.....	123
7.4.2 Slots de módulos en el armario de ampliación.....	124
7.4.3 Slots de módulos especiales.....	125
7.4.4 Inicialización de los módulos.....	125
7.4.5 Distribución de las líneas múltiplex PCM en el armario básico.....	126
7.4.6 Distribución de las líneas múltiplex en el armario de ampliación.....	128
7.4.7 Canales múltiplex de tiempo de los módulos periféricos.....	128
7.4.8 Instalación de módulos.....	129
7.4.8.1 Cómo insertar un módulo.....	130
7.4.8.2 Cómo extraer un módulo.....	131
7.4.8.3 Cómo instalar cubiertas de blindaje.....	131
7.5 Backplanes de los armarios del sistema.....	132
7.5.1 Backplane del armario básico.....	132
7.5.2 Backplane del armario de ampliación.....	134
7.5.3 Paneles de conexión y de blindaje para backplanes.....	135
7.5.3.1 Cómo montar paneles de conexión o de blindaje.....	137
7.5.4 Conexión en backplanes.....	137

7.5.4.1	Cómo conectar el conductor de conexión entre el armario básico y el armario de ampliación (opcional).....	137
7.5.4.2	Cómo instalar un conductor de conexión al distribuidor principal externo (opcional).....	138
7.5.4.3	Cómo conectar los cables de conexión con el panel de interconexión (opcional).....	139
7.5.4.4	Cómo conectar el cable de conexión con el panel de interconexión S ₀ (opcional).....	139
7.6	Conexión de línea urbana.....	142
7.6.1	Cómo configurar una conexión de centralita RDSI o una conexión de acceso individual RDSI mediante un puerto S ₀ (no válido para EE. UU. y Canadá).....	142
7.6.2	Cómo configurar la interfaz de línea múltiplex primaria de RDSI mediante un puerto S _{2M} (no válido para EE. UU. y Canadá).....	143
7.6.3	Cómo configurar la interfaz de línea múltiplex primaria de RDSI mediante una interfaz T1 (solo para EE. UU. y Canadá).....	144
7.6.4	Solo para algunos países: Cómo hacer una conexión de línea urbana mediante una interfaz E1-CAS.....	145
7.6.5	Cómo configurar una conexión con línea analógica.....	145
7.7	Conexión de teléfonos y dispositivos.....	146
7.7.1	Cómo conectar teléfonos RDSI directamente (no válido para EE. UU. y Canadá).....	147
7.7.2	Cómo conectar teléfonos RDSI mediante el bus S ₀ (no válido para EE. UU. y Canadá).....	148
7.7.3	Cómo conectar teléfonos U _{P0/E}	151
7.7.4	Cómo conectar teléfonos y dispositivos analógicos.....	152
7.8	Tareas finales.....	153
7.8.1	Cómo insertar la tarjeta M.2 SSD o la tarjeta SDHC (sistema con OCCM).....	154
7.8.2	Cómo realizar una inspección visual.....	154
7.8.3	Solo con montaje autónomo: Cómo montar las cubiertas de plástico de un armario del sistema.....	156
7.8.4	Cómo conectar el sistema a la red eléctrica.....	156
8	Instalación del servidor Linux.....	157
8.1	Requisitos previos.....	157
8.2	Instalación en un entorno virtual.....	160
8.2.1	Política de Calidad de Servicio y Residencia Compartida de VM.....	162
8.2.2	Sincronización de hora del sistema operativo invitado Linux.....	163
8.2.2.1	Cómo onfigurar la sincronización horaria para el sistema operativo invitado Linux en VMWare... 164	164
8.3	Aspectos de seguridad de Linux y unión RAID.....	165
8.4	Arranque inicial sin RAID por software.....	166
8.4.1	Cómo instalar y configurar SLES 15 SP6/SP7 sin RAID por software.....	167
8.4.2	Cómo actualizar de SLES 12 SP5 a SLES 15 SP6/SP7.....	170
8.4.3	Cómo actualizar de SLES 15 SP6 a SLES 15 SP7.....	171
8.5	Arranque inicial con un RAID por software.....	172
8.5.1	Cómo desactivar el RAID de la BIOS.....	173
8.5.2	Cómo instalar y configurar SLES 15 SP6/SP7 con un RAID por software.....	174
8.6	Configuración de una base temporal uniforme.....	178
8.6.1	Cómo configurar el servidor SNTP.....	179
8.7	Actualizaciones.....	179
8.7.1	Cómo activar las actualizaciones automáticas en línea.....	180
8.7.2	Cómo activar manualmente las actualizaciones online.....	181
8.7.3	Cómo configurar SLES 15 SP6/SP7 Yast2-Yast Online Update.....	181
8.8	Copia de seguridad y recuperación de software de servidor.....	182
9	Puesta en servicio inicial por OpenScape Business X.....	183
9.1	Requisitos para la instalación inicial.....	183
9.2	Componentes.....	184
9.3	Plan de numeración.....	186
9.4	Esquema de direcciones IP.....	187
9.5	Puesta en servicio inicial.....	188
9.5.1	Cómo iniciar el sistema de comunicación.....	189
9.5.2	Cómo conectar el PC de administración con el sistema de comunicación.....	189

9.5.3	Cómo iniciar WBM.....	190
9.6	Integración en la LAN de clientes.....	192
9.6.1	Cómo iniciar el asistente de instalación inicial.....	192
9.6.2	Configuración de sistema.....	193
9.6.2.1	Cómo definir el logotipo de pantalla y la designación de producto.....	193
9.6.2.2	Cómo definir las direcciones IP (opcional).....	194
9.6.2.3	Cómo especificar el nombre de dispositivo.....	195
9.6.3	Configuración de DHCP	195
9.6.3.1	Cómo desactivar el servidor DHCP interno.....	196
9.6.3.2	Cómo activar y configurar el servidor DHCP interno.....	197
9.6.4	Configuración de país y hora.....	198
9.6.4.1	Cómo seleccionar el código de país y el idioma para los registros de sucesos.....	199
9.6.4.2	Cómo introducir la identificación del sistema DECT.....	199
9.6.4.3	Configuración manual de fecha y hora.....	200
9.6.4.4	Obtención de la fecha y hora de un servidor SNTP.....	201
9.6.5	Solución UC.....	201
9.6.5.1	Cómo establecer la solución UC.....	202
9.6.6	Conexión del sistema de comunicación en la LAN de clientes.....	203
9.6.6.1	Cómo conectar el sistema de comunicación en la LAN de clientes.....	203
9.7	Configuración básica.....	203
9.7.1	Cómo iniciar el Asistente Configuración básica.....	203
9.7.2	Números de teléfono del sistema e interconexión.....	204
9.7.2.1	Cómo introducir el número de teléfono del sistema para una conexión de centralita.....	205
9.7.2.2	Cómo introducir los números de teléfono del sistema para un acceso individual.....	205
9.7.2.3	Cómo activar o desactivar la interconexión.....	206
9.7.3	Datos de extensión.....	207
9.7.3.1	Cómo mostrar los datos de extensión.....	208
9.7.3.2	Cómo borrar todos los números de llamada.....	209
9.7.3.3	Adaptar los números de teléfono preconfigurados al plan de numeración individual.....	209
9.7.3.4	Cómo importar los datos de extensión mediante un archivo XML.....	210
9.7.3.5	Cómo mostrar datos de Mass.....	210
9.7.4	Configuración RDSI	211
9.7.4.1	Cómo configurar la conexión de extensiones RDSI.....	212
9.7.4.2	Cómo configurar la conexión de centralita RDSI.....	213
9.7.4.3	Cómo configurar el acceso individual RDSI.....	213
9.7.4.4	Cómo desactivar la configuración RDSI.....	214
9.7.5	Acceso a Internet	214
9.7.5.1	Cómo configurar el acceso a Internet a través de un router de Internet externo mediante la conexión LAN.....	216
9.7.5.2	Cómo configurar el acceso a Internet a través de un router de Internet externo mediante la conexión WAN.....	216
9.7.5.3	Cómo configurar el acceso a Internet a través de un ISP preconfigurado.....	217
9.7.5.4	Cómo configurar el acceso a Internet a través del PPPoE ISP estándar.....	219
9.7.5.5	Cómo configurar el acceso a Internet a través de un PPTP ISP estándar.....	221
9.7.5.6	Cómo desactivar el acceso a Internet.....	224
9.7.6	Telefonía Internet	224
9.7.6.1	Cómo configurar un ITSP predefinido.....	225
9.7.6.2	Cómo desactivar telefonía Internet.....	230
9.7.7	Extensiones.....	230
9.7.7.1	Cómo configurar extensiones RDSI	231
9.7.7.2	Cómo configurar extensiones analógicas	233
9.7.7.3	Cómo configurar extensiones UP0	236
9.7.7.4	Cómo configurar extensiones DECT.....	239
9.7.7.5	Cómo configurar extensiones IP y SIP.....	242
9.7.8	Configuración de UC Suite.....	245
9.7.8.1	Cómo configurar UC Suite.....	245

9.7.9 Configuración de los buzones de voz de UC Smart.....	246
9.7.9.1 Cómo configurar los buzones de voz de UC Smart.....	246
9.7.10 Ajustes del servidor de conferencias.....	247
9.7.10.1 Cómo modificar los ajustes del servidor de conferencias.....	247
9.7.11 Envío de correo electrónico (opcional).....	247
9.7.11.1 Cómo configurar el envío de correo electrónico.....	248
9.8 Tareas finales.....	251
9.8.1 Cómo activar y asignar las licencias.....	252
9.8.2 Cómo proporcionar el cliente UC Smart para la instalación.....	254
9.8.3 Cómo preparar los clientes de UC Suite para la instalación.....	254
9.8.4 Cómo realizar la copia de seguridad.....	256
9.9 Puesta en servicio de los teléfonos IP.....	256
9.9.1 Cómo configurar teléfono IP.....	258
9.9.2 Cómo configurar un teléfono SIP.....	259
10 Configuración inicial de OpenScape Business UC Booster.....	262
10.1 Requisitos para la puesta en servicio inicial.....	264
10.2 Copia de seguridad de los datos de configuración del sistema de comunicación.....	267
10.2.1 Cómo realizar la copia de seguridad.....	267
10.3 Puesta en servicio de la UC Booster Card.....	268
10.3.1 Montaje de la UC Booster Card.....	268
10.3.2 Configuración de la UC Booster Card.....	269
10.3.3 Actualización de software para la UC Booster Card.....	269
10.3.3.1 Cómo ejecutar una actualización de software.....	269
10.4 Puesta en servicio del UC Booster Server.....	270
10.4.1 Instalación del software de comunicación.....	270
10.4.1.1 Cómo instalar el software de comunicación en un servidor Linux o en un entorno virtual.....	271
10.4.2 Configuración del UC Booster Server.....	273
10.4.2.1 Comunicar la dirección IP del sistema de comunicación.....	274
10.4.3 Actualización de software para el UC Booster Server.....	276
10.5 Configuración básica.....	276
10.6 Tareas finales.....	277
10.7 Desinstalación del software de comunicación.....	277
10.7.1 Cómo desinstalar el software de comunicación.....	277
10.8 Actualización de UC Booster Card a UC Booster Server.....	278
10.9 Puertos utilizados.....	279
11 Componentes retirados de producción.....	282
11.1 Distribuidor principal MDFU (opcional).....	282
11.1.1 Cómo fijar a una pared el distribuidor principal MDFU.....	283
11.2 Cable de conexión con el distribuidor principal externo (opcional).....	283
11.2.1 Cómo conectar un conductor de conexión al distribuidor principal externo (opcional).....	285
Índice.....	289

1 Historial de cambios

Los cambios que se mencionan en la siguiente lista son acumulativos.

Cambios en V3R2 FR1

Capítulos afectados	Descripción de los cambios
Cómo configurar el envío de correo electrónico en la página 248	Compatibilidad con la autenticación OAuth 2.0

1.1 Historial de mejoras/correcciones

Los cambios que se mencionan en este capítulo son acumulativos.

Cambios en V3R1

ID del caso de servicio	Fecha del cambio	Descripción del cambio	Capítulos afectados
PRB000052823	21 de abril de 2021	Tabla actualizada con los requisitos mínimos para instalar el sistema de comunicación en una VM.	Instalación en un entorno virtual en la página 160

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.

2.1 Acerca de esta documentación

Este documento ofrece información sobre la instalación de hardware y la configuración inicial de los modelos de hardware OpenScape Business X3/X5/X8.

Dicha información debe considerarse solo como información adicional y no como un sustituto de cursos de formación.

Este documento está dirigido a administradores y técnicos de servicio.

Para obtener información sobre el contenido de este documento, consulte *OpenScape Business, Documentación de servicio* y *OpenScape Business, Documentación del administrador*.

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, Instrucciones 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, 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.

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 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...

2.1.3 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

Tipo de información	Visualización	Ejemplo
Énfasis especial	negritas	El nombre no se puede borrar .
Referencia cruzada	cursiva	Encontrará más información en la sección <i>Red</i> .
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 sígala 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)

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.
 - Cerciérese 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, recójalo.
 - 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 ambiente. 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 una 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 documentados 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.

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.

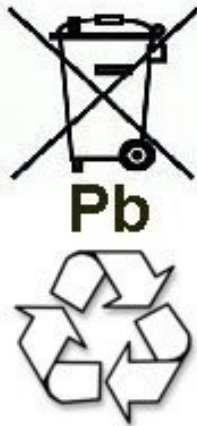
Nota: Limpie la carcasa del sistema de comunicación y del servidor solamente con un paño suave y ligeramente humedecido. No utilice detergentes agresivos ni esponjas agresivas.

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 la norma IEC 364-3.

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.

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

*) 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).

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.

En Alemania, el procesamiento y la utilización de estos datos están sujetos a lo establecido por diversas regulaciones, incluida la Ley General de Protección de datos (GDPR) y la Ley Federal de Privacidad de Datos (Bundesdatenschutzgesetz, 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.

Los 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
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

	Referencias normativas
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 H₂O/m³
- 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 Preparar la instalación de OpenScape Business X3/X5/X8

Antes de que se puedan configurar y ponerse en marcha sistemas de comunicación X3/X5/X8 por primera vez, debe encontrarse un lugar de montaje adecuado que cumpla con las condiciones servicio (consultar [Condiciones de servicio de OpenScape Business X](#)), y se deben realizar algunas actividades de preparación.

3.1 Requisitos para la instalación

Para la instalación de los sistemas de comunicación OpenScape Business X3/X5/X8 se requieren diferentes herramientas. Para seleccionar el lugar de montaje hay que tener en cuenta determinados requisitos. Para utilizar los sistemas de comunicación en los EE. UU. y Canadá hay requisitos especiales para la conexión de tensión de red.

OpenScape Business X3W y OpenScape Business X5W solo se pueden montar en una pared.

OpenScape Business X3R y OpenScape Business X5R son sistemas de comunicación con caja de rack de 19" que se pueden montar en un armario de 19", exentos (operación de escritorio) o en pared.

OpenScape Business X8 es un sistema de comunicación modular que se puede utilizar como sistema de box único (armario básico) o como sistema de box doble (armario básico + armario de ampliación). OpenScape Business X8 se puede montar de forma autónoma o en un armario de 19 pulgadas.

Atención: La instalación de los sistemas de comunicación solo debe llevarlo a cabo personal especializado y autorizado.

Herramientas y medios auxiliares

Se necesitan las siguientes herramientas y medios auxiliares:

- Alicates de corte universal, tenaza de teléfono, pelacables, tenaza de boca plana
- Juego de destornilladores planos
- Juego de destornilladores de estrella Pozidriv
- Juego de destornilladores TORX
- Metro
- Llave allen o llave de estrella de 8 mm, llave allen de 13 mm (solo para X8)
- Llave modular (solo para X8)
- Taladro, martillo, nivel (solo para montaje mural)
- Herramienta de perforación para regletas de división y de clasificación en distribuidores principales
- Multímetro digital para comprobar las conexiones a tierra y las tensiones parciales

Requisitos generales para la elección del lugar de montaje

Al elegir el lugar de montaje hay que seguir siempre estas indicaciones:

- El sistema de comunicación (y el armario de 19 pulgadas) no se puede exponer a la acción directa de fuentes de calor (p. ej., rayos de sol, radiadores, etc).
- El sistema de comunicación (y el armario de 19 pulgadas) no se puede exponer a ambientes con mucho polvo.
- Evitar todo contacto del sistema de comunicación (y del armario de 19 pulgadas) con agentes químicos.
- Hay que evitar siempre que durante el funcionamiento se produzca condensación por humedad ambiental sobre o en el sistema de comunicación.

El sistema de comunicación debe estar totalmente seco para poder ponerlo en servicio.

- Hay que evitar el uso de moquetas estándares ya que producen cargas electrostáticas.
- Hay que atender las condiciones climáticas y mecánicas del servicio del sistema de comunicación (consulte [Condiciones de servicio OpenScape Business X](#)).
- Se tiene que poder acceder fácilmente al conector del cable de conexión de red para poder interrumpir en cualquier momento la conexión del sistema de comunicación a la tensión de red.
- Hay que comprobar que haya espacio suficiente para un distribuidor principal y otros dispositivos adicionales.
- Solo para EE. UU. y Canadá: la distancia entre dispositivos de Unify GmbH & Co. KG y otros electrodomésticos debe ser de al menos 101,6 cm (40"). Según el National Electrical Code (NEC), en la parte delantera de los electrodomésticos debe guardarse una distancia mínima de 91,4 cm (36") y una distancia de 101,6 cm (40") con otras instalaciones eléctricas.

Requisitos especiales con X3R/X5R para la selección del lugar de montaje

Al elegir el lugar de montaje hay que seguir siempre estas indicaciones:

- Hay que mantener una separación mínima de 10 cm a la carcasa para garantizar una ventilación suficiente del sistema de comunicación.

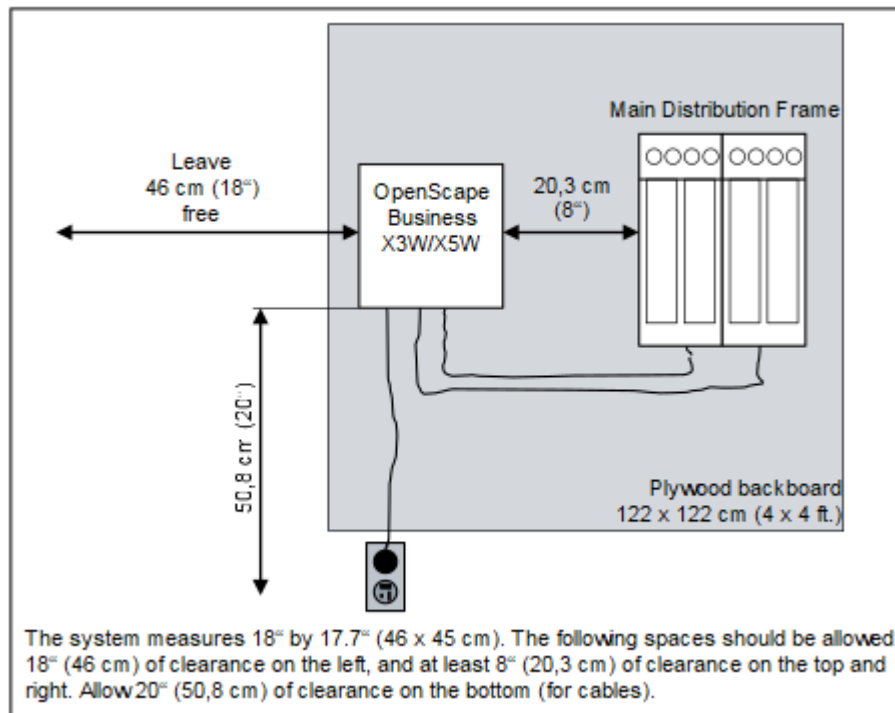
Requisitos especiales con X3W/X5W para la selección del lugar de montaje

Al elegir el lugar de montaje para el montaje mural hay que seguir siempre estas indicaciones:

- Hay que mantener libres las distancias mínimas con la carcasa indicadas a continuación para garantizar una ventilación suficiente de los sistemas de comunicación:
 - Lado izquierdo: 30 cm (para el servicio de los módulos)
 - Lado derecho, arriba y abajo: 10 cm
- Solo para EE. UU. y Canadá: la sala donde se monta el sistema de comunicación debe tener suficiente lugar para las tareas de instalación y de

mantenimiento (por ejemplo para retirar y colocar la tapa de la carcasa). La imagen siguiente muestra los requisitos de espacio.

Es recomendable utilizar una plancha de madera contrachapada con un grosor mínimo de 127 mm (0,5") y unas medidas mínimas de 122 x 122 cm (4x4 pies).



Requisitos especiales con X8 para la selección del lugar de montaje con montaje independiente

Al elegir el lugar de montaje con montaje autónomo, hay que tener siempre en cuenta lo siguiente:

- Hay que mantener una distancia mínima de 50 mm entre el borde inferior de un armario del sistema y el suelo y entre armarios del sistema montados uno sobre el otro para garantizar una ventilación suficiente de los armarios del sistema.
- En caso de montar los armarios del sistema superpuestos, el armario básico debe montarse siempre abajo.
- Delante y después de los armarios del sistema hay que mantener una distancia mínima de 10 cm para permitir el servicio de los módulos y el cableado.

Requisitos especiales con X8 para la selección del lugar de montaje con montaje en armario de 19 pulgadas

Al seleccionar el lugar de montaje para montaje en armario de 19" hay que tener siempre en cuenta lo siguiente:

- Los armarios de 19" para el montaje del sistema de comunicación OpenScape Business X8 deben tener las siguientes propiedades:
 - Los componentes instalados en el armario de 19 pulgadas deben estar accesibles por delante y por detrás.
 - Los componentes se deben montar en la parte delantera o trasera del armario de 19" (al menos cuatro largueros verticales).
 - Se recomienda un ancho de armario de 70 a 80 mm y una profundidad de como mínimo 60 mm. Una profundidad mayor del armario (80 - 90 mm) facilita el montaje y hace más cómodo el servicio de cable y la instalación de más componentes en el lado posterior del armario.
 - Las escuadras de soporte necesarias para el montaje de los armarios del sistema deben admitir una carga mínima de 40 kg. Las escuadras de montaje debe proporcionarlas el proveedor del armario de 19".
 - Los armarios del sistema deben sujetarse con las escuadras de sujeción suministradas en los largueros del armario.
- Mediante la placa gris de plástico colocada en la parte superior de los armarios del sistema debe quedar libre una unidad de altura (una unidad de altura corresponde aprox. a 1,7" = 43 mm) sobre el armario del sistema. La placa de plástico no puede ser retirada en ningún caso.
- A fin de garantizar la correcta evacuación del calor, solo está permitido montar el armario básico en la posición más baja de un armario de 19 pulgadas. Si se trata de un armario de 19 pulgadas con componentes activos ya montados (que expulsan calor) deberá vaciarse o mantenerse libre el área inferior para el montaje del armario básico. Si los componentes son inactivos (p. ej. un panel de interconexión), también está permitido montar el armario básico encima.

- Para garantizar una ventilación suficiente de los armarios del sistema en un armario de 19", hay que mantener libres las siguientes distancias mínimas:
 - Tres unidades de altura entre dos armarios del sistema superpuestos.
 - Una unidad de altura por encima de un armario del sistema, si se monta, p. ej., un panel de interconexión.

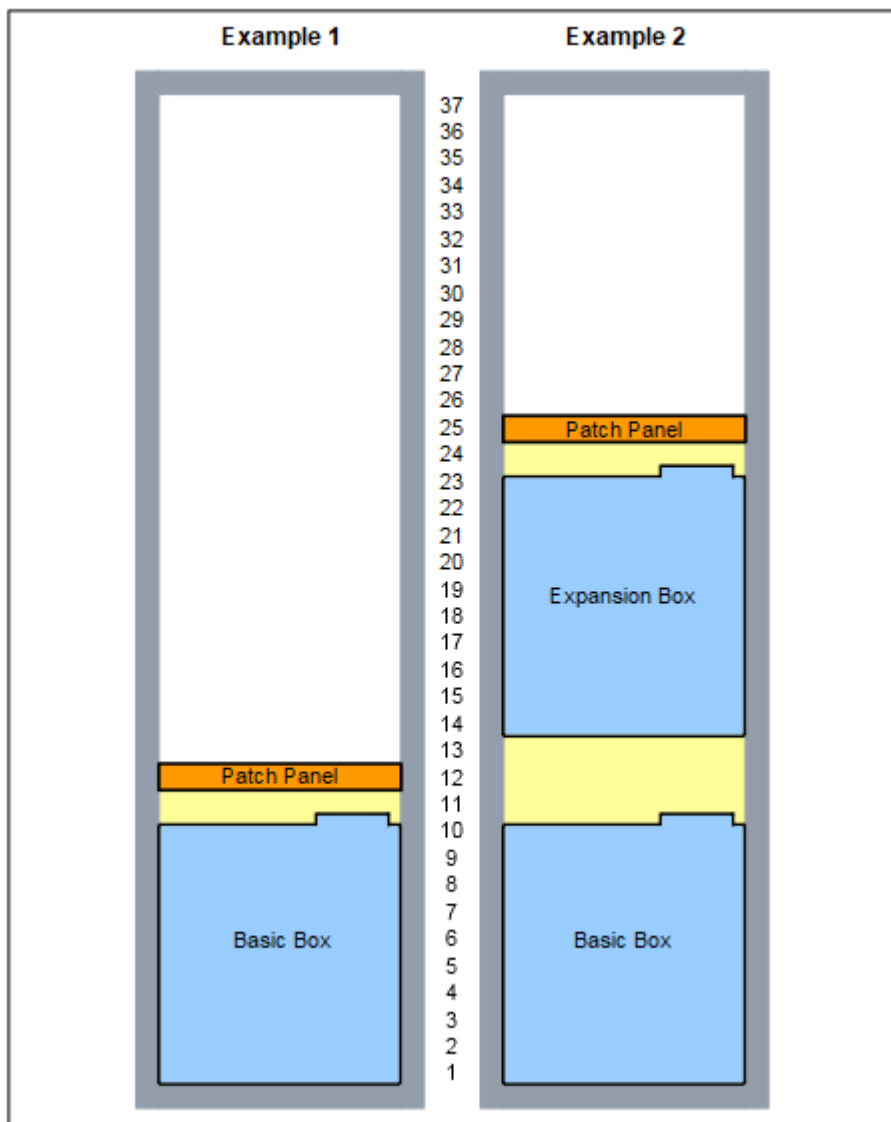


Figura 1: OpenScape Business X8 – Ejemplos para un armario de 19" con una altura de 1,92 m (37 unidades de altura)

Solo para EE. UU. y Canadá: Requisitos para la conexión de tensión de red

La conexión de tensión de red de los sistemas de comunicación debe cumplir los requisitos especificados a continuación:

Preparar la instalación de OpenScape Business X3/X5/X8

Actividades previas

- Potencias eléctricas conectadas:

Tensión nominal	Margen de tensión nominal		Margen de frecuencia nominal		Configuraciones de cajas de conexión
	desde	a	desde	a	
120 V CA/60 Hz	110 V c.a.	130 V c.a.	47 Hz	63 Hz	NEMA 5-15, 2 polos, 3 hilos, puesta a tierra

- Solo para X8: entre la caja de conexión y el sistema de comunicación debe enchufarse una protección contra sobretensión relacionada en UL o certificada en CSA. Por cada protección contra sobretensión se pueden conectar como máximo dos armarios del sistema.

Nota: El sistema de comunicación OpenScape Business X8 no se puede enchufar directamente a una toma.

- Solo para X3/X5: entre la caja de conexión y el sistema de comunicación debe enchufarse una protección contra sobretensión.
- Solo para X8: la fuente de tensión no puede distar del sistema de comunicación más de 2,4 m (8 pies) y debe suministrar una tensión de 120 V c.a. (monofásica, protegida) con 50-60 Hz y 20 A.
- Solo para X3/X5: la fuente de tensión no puede distar del sistema de comunicación más de 2 m (6 pies) y debe suministrar una tensión de 120 V c.a. (monofásica, protegida) con 50-60 Hz.
- Para cada sistema de comunicación se debería utilizar un circuito de corriente propio con un conductor de protección aislado.
- En el interruptor principal del suministro de tensión de red hay que colocar un aviso para evitar el apagado accidental del suministro de corriente de un sistema de comunicación.

3.2 Actividades previas

Antes de realizar el montaje hay que desempaquetar y comprobar los componentes suministrados.

En la placa principal hay un acumulador para la memoria temporal de fecha y hora. Es posible que las placas base de versiones anteriores se suministren con una lámina protectora de la batería. Antes de poner en servicio el sistema de comunicación hay que retirar la lámina protectora.

A partir de las siguientes versiones no se utiliza la lámina protectora de la batería:

- S30810-Q2959-X-6 (OCCM)
- S30810-Q2959-Z-5 (OCCMR)
- S30810-Q2962-X-7 (OCCL)

3.2.1 Cómo desempaquetar los componentes

Desempaquete el sistema de comunicación y los componentes suministrados siguiendo este procedimiento:

Paso a paso

- 1) Abra el embalaje sin dañar el contenido.
 - 2) Compruebe si los componentes suministrados corresponden a los datos indicados en la nota de entrega.
 - 3) Si se ha producido algún tipo de desperfecto durante el transporte, póngase en contacto con la dirección indicada en la nota de entrega.
 - 4) Elimine el material de embalaje siguiendo las normas específicas de cada país
-



Atención:

Descarga eléctrica al tocar los cables con tensión

Utilice solo sistemas de comunicación, equipos y medios operativos que se encuentren en perfecto estado. Está prohibido poner en servicio dispositivos con daños externos.

3.2.2 Cómo retirar la tapa de la carcasa en X3W/X5W

Paso a paso

- 1) Suelte los dos cierres atornillables de la tapa de la carcasa con un destornillador plano.
 - 2) Retire la tapa de la carcasa
-



PRECAUCIÓN: Heridas por cortes provocados con los cantos afilados de la chapa de protección

Preparar la instalación de OpenScape Business X3/X5/X8

Coja la tapa de carcasa siempre desde fuera. De lo contrario, existe peligro de sufrir cortes por la chapa protectora del interior de la carcasa, que podría tener cantos cortantes.



4 Preparación para la instalación inicial del OpenScape Business UC Booster Server

Para poder instalar y poner en servicio por primera vez del servidor OpenScape UC Business Booster, hay que hacer algunos preparativos.

El servidor UC Booster Server solamente es compatible en combinación con las siguientes placas base:

- OCCM
- OCCMR
- OCCL

El siguiente sistema no requiere un servidor UC Booster Server:

- OCCMA
- OCCMB
- OCCMRA
- OCCMRB
- OCCLA

Para OpenScape UC Business Booster Server, el software de comunicación de OpenScape Business se instala en un servidor Linux.

Puede consultar los requisitos previos del servidor Linux y la instalación del sistema operativo Linux en [Instalación del servidor Linux](#) en la página 157.

Puede consultar los requisitos previos de OpenScape Business UC Booster Server y la instalación del software de comunicación OpenScape Business en [Configuración inicial de OpenScape Business UC Booster](#) en la página 262.

5 Instalación de hardware por OpenScape Business X3W/X5W

Se describe el montaje estándar más realizado para los sistemas de comunicación OpenScape Business X3W y OpenScape Business X5W.

OpenScape Business X3W y OpenScape Business X5W solo se pueden montar en una pared.



Atención:

Descarga eléctrica al tocar los cables con tensión

- Solo se puede trabajar con la carcasa abierta si el sistema está sin tensión.
- Antes de iniciar cualquier trabajo, compruebe si todos los circuitos de corriente están sin tensión. Jamás dé por sentado que al desconectar un fusible o un interruptor principal se han interrumpido efectivamente todos los circuitos de corriente.

5.1 Tipo de montaje

Los sistemas de comunicación OpenScape Business X3W y OpenScape Business X5W solo se pueden utilizar con montaje mural.

5.1.1 Cómo fijar el sistema de comunicación a una pared

Requisitos previos

Se han tenido en cuenta los requisitos para elegir el lugar de montaje (consulte [Requisitos para la instalación](#) en la página 31).

Hay una pared con capacidad de carga y con espacio suficiente para el montaje del sistema de comunicación y demás componentes (p.ej., un distribuidor principal).

Paso a paso

- 1) Fije las plantillas para taladro suministradas en el lugar de montaje deseado.
- 2) Haga tres agujeros.
- 3) Inserte los tacos en los agujeros del taladro y fije los tornillos dejándolos sobresalir unos 5 mm.

- 4) Cuelgue el sistema de comunicación en los orificios de fijación y alinéelo.

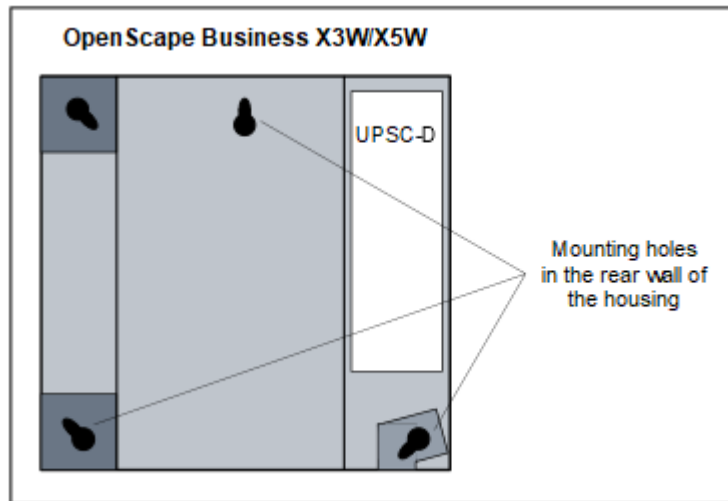


Figura 2: OpenScape Business X3W/X5W – Orificios de fijación en la pared trasera de la carcasa

- 5) Apriete los tres tornillos.

5.2 Puesta a tierra de protección

La puesta a tierra de protección brinda una conexión segura al potencial de tierra para protegerlo frente a altas tensiones de contacto en caso de un funcionamiento incorrecto.



Atención:

Descarga eléctrica al tocar los cables con tensión

- Utilice conductores de protección de tierra independientes para brindar una puesta a tierra de protección para los sistemas de comunicación OpenScape Business X3W y OpenScape Business X5W y, posiblemente, para cualquier distribuidor que se utilice. Conecte su sistema de comunicación y su distribuidor principal al conductor de protección de tierra antes de poner en servicio el sistema y conectar los teléfonos y líneas.
- Asegúrese de que los conductores de protección de tierra colocados estén protegidos y sin tensión.



Atención:

Montaje de terminal de puesta a tierra de protección

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: Montaje del terminal de puesta a tierra de protección](#).

A continuación, el conductor de protección a tierra tiene que conectarse como se describe en [Cómo proporcionar una puesta a tierra de protección para el distribuidor principal MDFU](#).

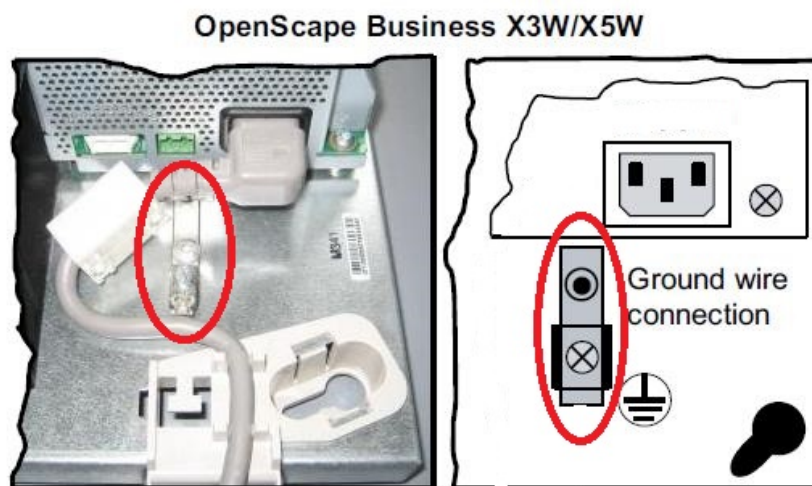


Figura 3: Montaje del terminal de puesta a tierra de protección

5.2.1 Cómo establecer una puesta a tierra de protección para el MDFU del distribuidor principal

Requisitos previos

Hay disponible una conexión de puesta a tierra de baja impedancia.



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.



Atención:

Descarga eléctrica al tocar los cables con tensión

- Utilice conductores de protección de tierra independientes para brindar una puesta a tierra de protección para los sistemas de comunicación OpenScape Business X3W y OpenScape Business X5W y, posiblemente, para cualquier distribuidor que se utilice. Conecte su sistema de comunicación y su distribuidor principal al conductor de protección de tierra antes de poner en servicio el sistema y conectar los teléfonos y líneas.
- Asegúrese de que los conductores de protección de tierra colocados estén protegidos y sin tensión.

La puesta a tierra del sistema de comunicación y del distribuidor principal externo debe ejecutarse desde el punto de toma de tierra, en configuración de estrella.

Es obligatorio cumplir las normas de implementación especificadas en las normativas IEC 60364, IEC 60950-1 e IEC 62368-1 durante la instalación.

Nota: Los requisitos enumerados también son aplicables si utiliza un modelo de distribuidor principal de otro proveedor, en lugar del MDFU.

Siga este procedimiento para garantizar una correcta puesta a tierra de protección:

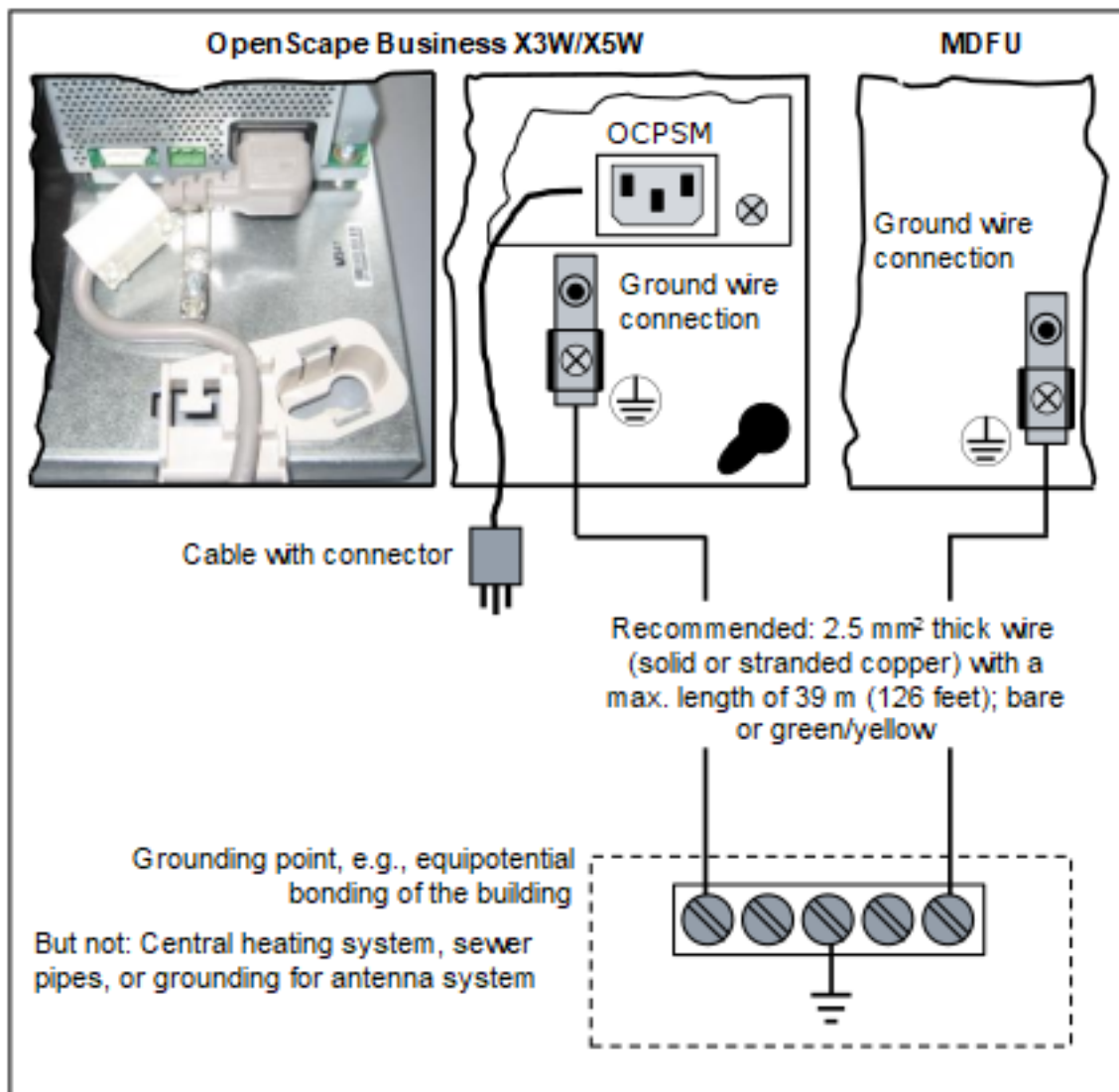
Paso a paso

- 1) Fije un conductor de puesta a tierra independiente al terminal de puesta a tierra del sistema de comunicación.
- 2) Utilice una brida para fijar el conductor de puesta a tierra al sistema de comunicación y librarlo de cualquier tensión.
- 3) Si hay presente un MDFU: Fije un conductor de puesta a tierra independiente al terminal de puesta a tierra del distribuidor principal MDFU.
- 4) Si hay presente un MDFU: Utilice una brida para fijar el conductor de puesta a tierra a la carcasa del distribuidor principal MDFU y librarlo de cualquier tensión.

5) Elija una de estas opciones:

- **No válido para EE. UU. y Canadá - Varilla de compensación de potencial**

Conecte los conductores de puesta a tierra independientes con la toma de tierra (por ejemplo, la varilla de compensación de potencial del edificio), tal y como muestra el diagrama conceptual.

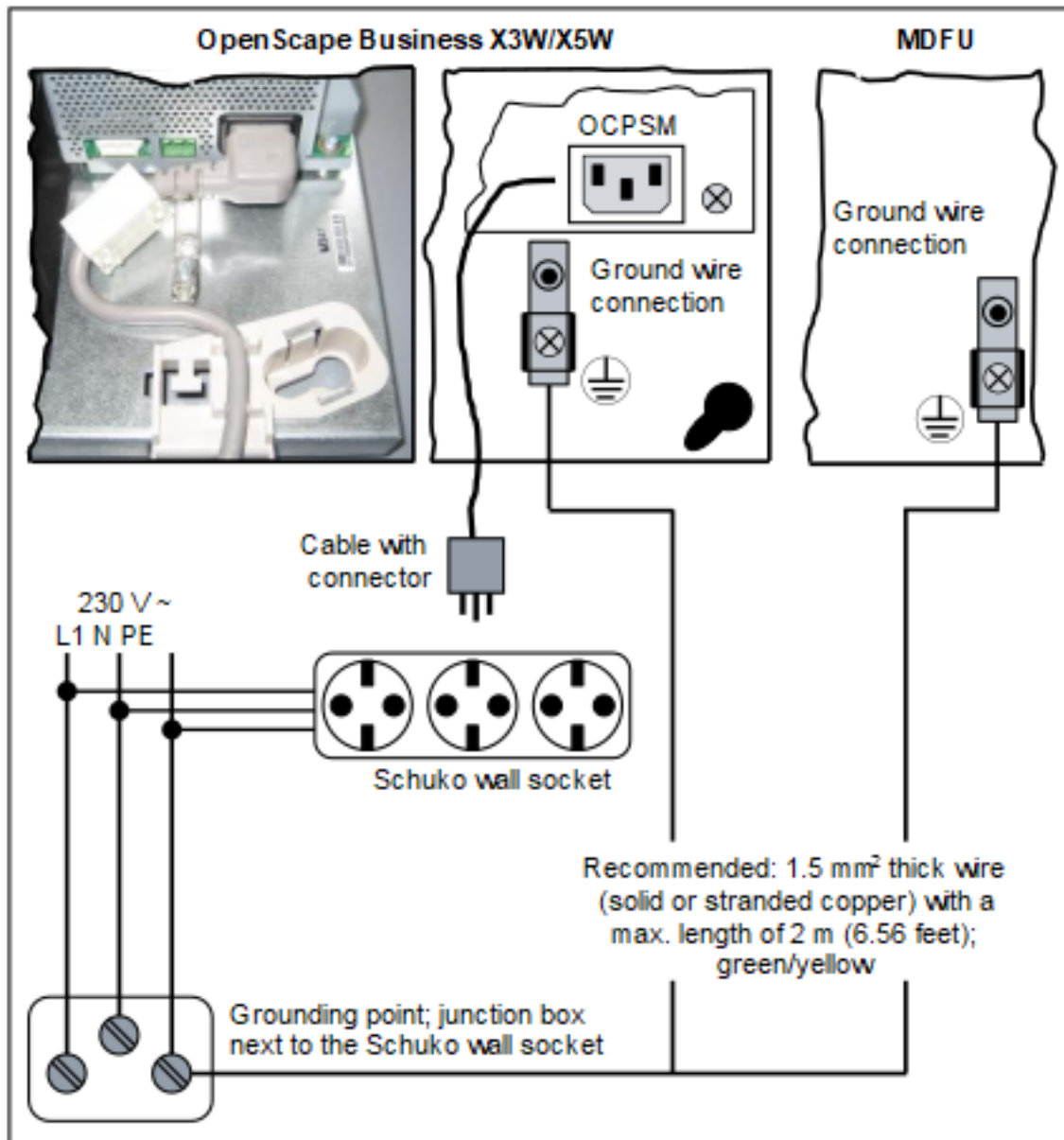


Asegúrese de que todos los conductores de protección de tierra colocados estén protegidos y sin tensión. La sección transversal mínima de los conductores es de 12 AWG/2,5 mm². Si no es posible proteger un conductor de puesta a tierra, se necesita una sección transversal mínima del conductor de 10 AWG/4 mm² para bloquear los efectos de factores externos.

- **No válido para EE. UU. y Canadá - Salida a la red de baja tensión**

Conecte una caja de empalmes a la red de baja tensión cerca de la toma Schuko de la pared a la cual esté enchufada el sistema de comunicación. Utilice un conductor de puesta a tierra independiente para establecer una

conexión fija a la caja de empalmes, como se muestra en el diagrama conceptual.

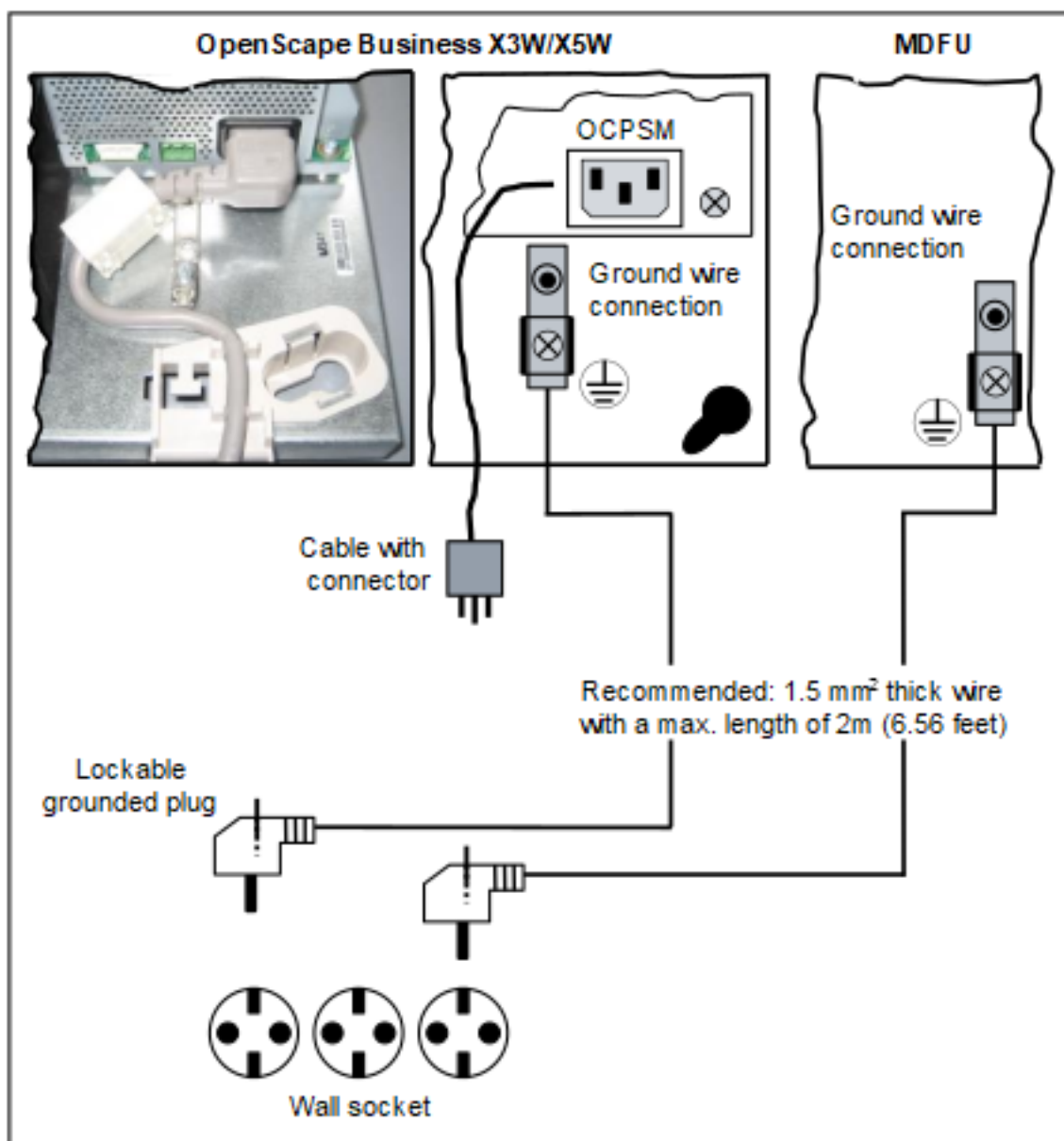


Asegúrese de que todos los conductores de protección de tierra colocados estén protegidos y sin tensión. La sección transversal mínima de los conductores es de 16 AWG/1,5 mm².

- **No válido para EE. UU. y Canadá - Enchufe bloqueable con puesta a tierra para conexión a la red de baja tensión**

Inserte el enchufe bloqueable con puesta a tierra (un modelo de Schuko especial equipado con un conductor de toma de tierra de protección fijo) en una toma de pared de la red de baja tensión y bloquee el enchufe. Utilice el conductor de puesta a tierra conectado al enchufe para establecer una conexión fija al sistema de comunicación, como

se muestra en el diagrama conceptual. Utilice un segundo enchufe bloqueable con puesta a tierra si hay instalado un MDFU.

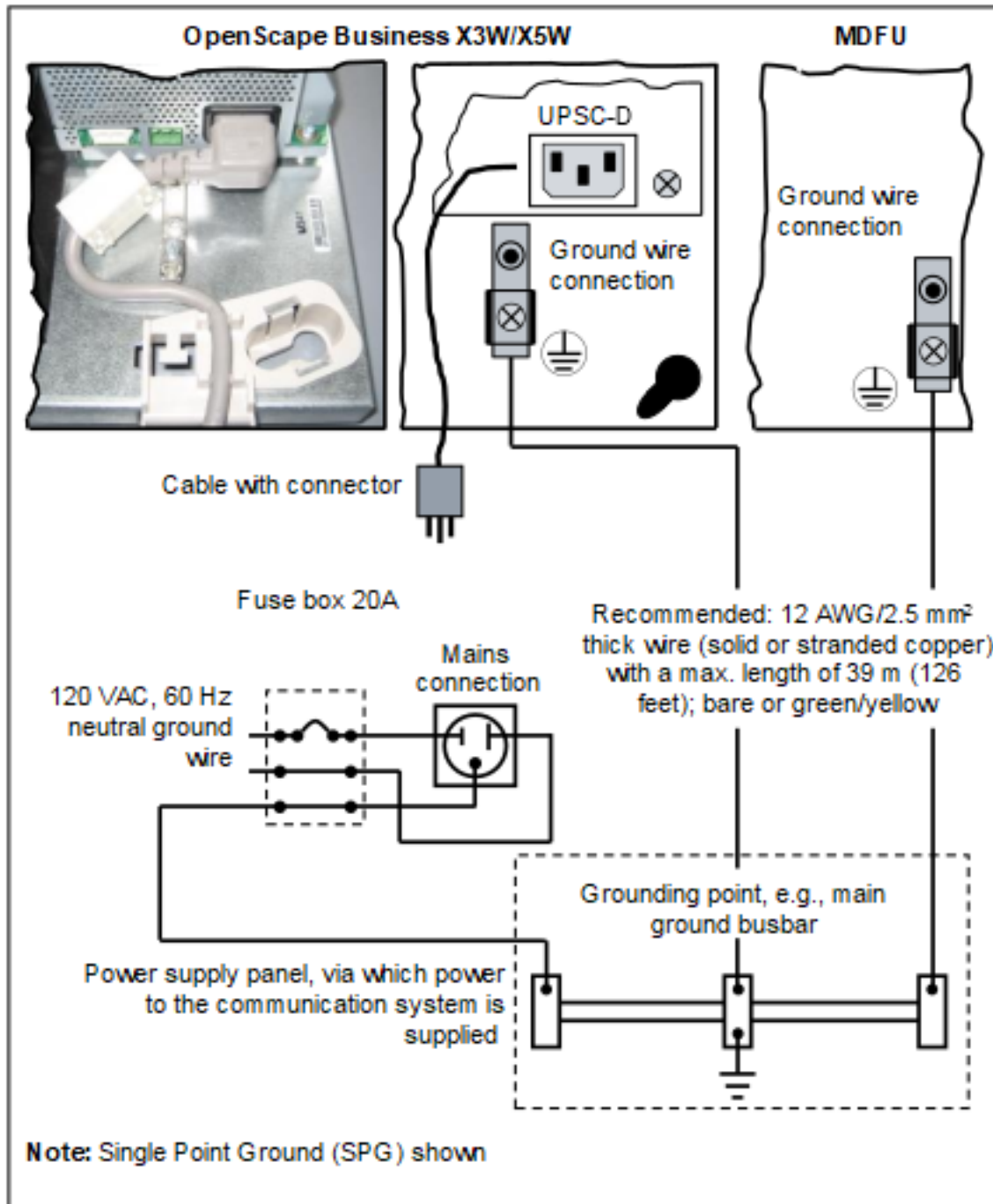


Asegúrese de que todos los conductores de protección de tierra colocados estén protegidos y sin tensión. La sección transversal mínima

del conductor es de 16 AWG/1,5 mm² hasta 2 metros y de al menos 12 AWG/2,5 mm² para 2 o más metros.

- **Solo para EE. UU. y Canadá: Barra principal de toma de tierra**

Conecte los conductores de puesta a tierra independientes con la toma de tierra (por ejemplo, la pica principal de toma de tierra o un electrodo de toma de tierra), tal y como muestra el diagrama conceptual.



Asegúrese de que todos los conductores de protección de tierra colocados estén protegidos y sin tensión. La sección transversal mínima de los conductores es de 12 AWG/2,5 mm². Si no es posible proteger un conductor de puesta a tierra, se necesita una sección transversal mínima

Instalación de hardware por OpenScape Business X3W/X5W

Cable de conexión para la conexión directa de teléfonos, líneas urbanas, etc.

del conductor de 10 AWG/4 mm² para bloquear los efectos de factores externos.

5.2.2 Cómo comprobar la puesta a tierra de protección

Requisitos previos

El sistema de comunicación **aún** no está conectado con la red de baja tensión a través del cable de conexión de red.

La puesta a tierra de protección por separado para el sistema de comunicación y para el distribuidor principal utilizado (en su caso) está conectada.

Antes de la puesta en servicio, realice este test para garantizar una correcta puesta a tierra de protección del sistema de comunicación y del distribuidor principal, en su caso.

Paso a paso

- 1) Compruebe la resistencia óhmica de la conexión del conductor independiente de protección con el sistema de comunicación:

La medición se realiza entre el contacto de puesta a tierra de una caja de conexión de la red doméstica (en el lugar de conexión del sistema de comunicación) y la carcasa del sistema de comunicación.

- 2) Si se utiliza un distribuidor principal, compruebe la resistencia óhmica de la conexión del conductor independiente de protección con el distribuidor principal.

La medición se realiza entre el contacto de puesta a tierra de una caja de conexión de la red doméstica (en el lugar de conexión del sistema de comunicación) y la carcasa del distribuidor principal.

El resultado (valor nominal) de la medición debe ser claramente inferior a 10 ohmios.

Si se obtuviera otro resultado, póngase en contacto con un técnico eléctrico cualificado. Deberá comprobar la compensación de potencial de la instalación principal y garantizar el bajo ohmiaje del enlace de cable de protección.

5.3 Cable de conexión para la conexión directa de teléfonos, líneas urbanas, etc.

Con el modelo para montaje mural de OpenScape Business, los teléfonos, líneas urbanas, etc. se conectan directamente con el módulo.

CABLU C39195-A7001-B126

CABLU con

- ocho bornes atornillables Wieland para la conexión directa en los conectores de tarjeta de los módulos de los modelos de OpenScape Business para montaje mural

- 8 x cuatro tomas RJ45 para la conexión de teléfonos U_{P0/E} y de teléfonos y dispositivos analógicos

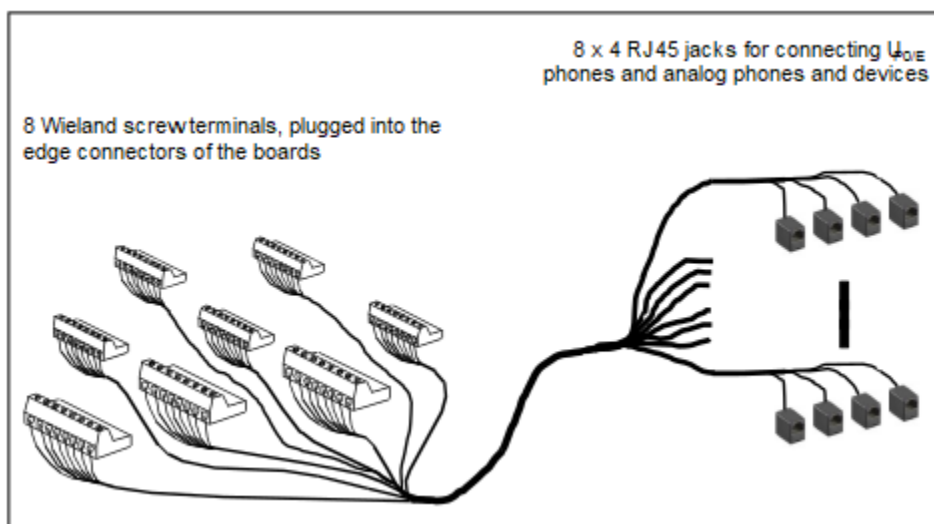


Figura 4: CABLU C39195-A7001-B126

Borne atornillable Wieland

Si se utilizan bornes atornillables Wieland sueltos, las líneas de conexión de los teléfonos, de las líneas analógicas, etc. también se deben conectar por separado.

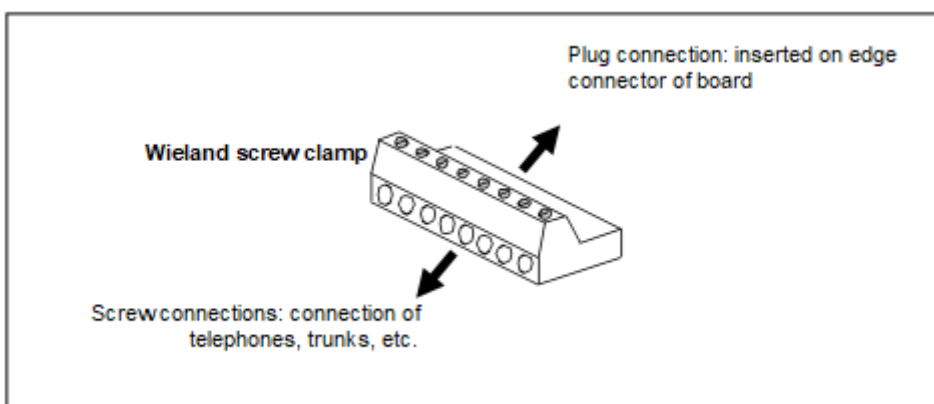


Figura 5: Borne atornillable Wieland

5.4 Indicaciones para la configuración

Las indicaciones de configuración incluyen información sobre los slots para módulos de los sistemas de comunicación OpenScape Business X3W y OpenScape Business X5W.

5.4.1 Slots de módulos en OpenScape Business X3W

OpenScape Business X3W incluye un soporte para módulos que cuenta con tres niveles de slots para el equipamiento con módulos y componentes opcionales.

- Nivel de slots 1: slots para dos módulos periféricos
- Nivel de slots 2: slot para la placa base OCCM
- Nivel de slots 3: slots para cinco opciones

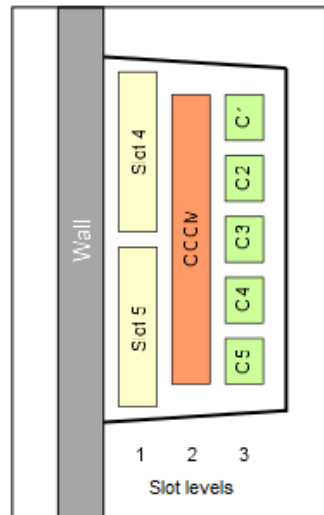


Figura 6: OpenScape Business X3W – Slots de módulos

5.4.2 Slots para módulos en OpenScape Business X5W

OpenScape Business X5W incluye un soporte para módulos con seis niveles de slots.

Los niveles de slots vienen equipados de la siguiente manera:

- Niveles de slots 1 a 3: slots para dos módulos periféricos cada uno
- Nivel de slots 4: slot para la placa base OCCM, OCCMA y OCCMB
- Nivel de slots 6: slot para cinco opciones

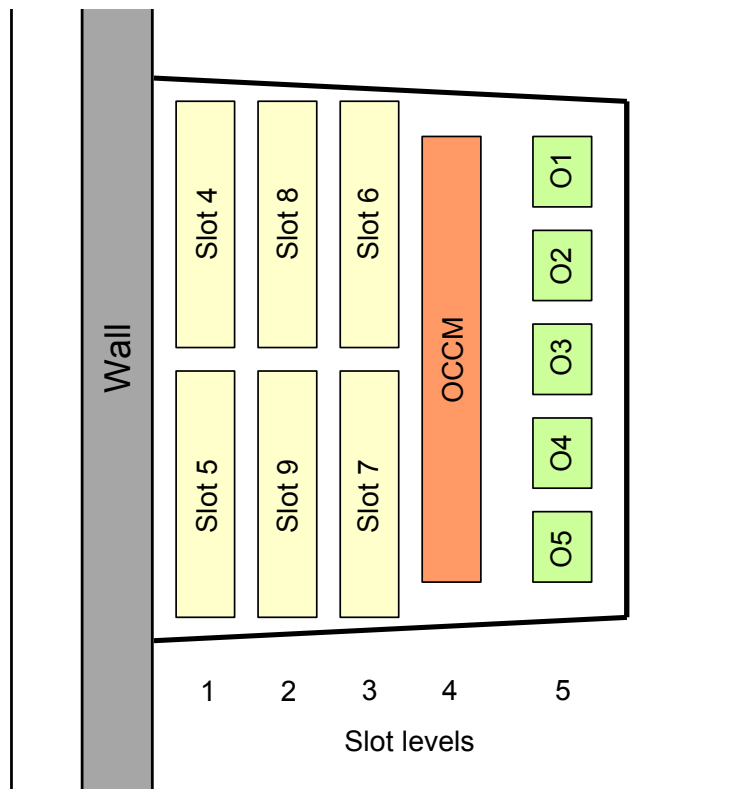


Figura 7: OpenScape Business X5W - Slots para módulos

En los sistemas nuevos únicamente se puede utilizar el kit de ventiladores nuevo (L30251-U600-A985). No se pueden conectar los kits de ventiladores existentes (L30251-U600-A918).

Nota: En caso de que se sustituya una fuente de alimentación UPSC-D/DR por un OCPSM, no es necesario actualizar los sistemas OpenScape Business a nuevos backplanes. El kit de actualización de la PSU adecuado contiene todos los adaptadores y cables necesarios.

Al migrar de HiPath 33xx / 35xx a OpenScape Business, no es necesario sustituir el backplane existente si se utiliza una fuente de alimentación OCPSM en lugar de la PSU y se emplea el kit de actualización de la PSU adecuado.

Los slots del nuevo backplane se reconocen a partir de OpenScape Business V2. Es necesario actualizar los sistemas de la versión de software V1 a la versión V2 antes de sustituir el backplane antiguo por uno nuevo.

Importante: (*) Con los nuevos backplanes, los sistemas murales OpenScape Business X5W ya no proporcionan el nivel de slots 5 (slot 10). Las tarjetas con regletas de enchufes SIPAC (SLMO24, SLC16N) no se pueden usar junto con el nuevo backplane.

5.4.3 Instalación de módulos

5.4.3.1 Cómo insertar un módulo

Requisitos previos

La tapa de la carcasa está desmontada.

Hay disponible un slot para módulos libre.

Nota: Al trabajar con módulos hay que llevar siempre puesto un brazalete de puesta a tierra.

Hay que respetar y seguir las medidas de protección contra descargas electrostáticas (consulte [Indicaciones de aviso: Aviso](#) en la página 16)

Paso a paso

- 1) Retire la cubierta de estabilizador.
- 2) Introduzca el módulo con ayuda de los rieles guía hasta el tope en el slot de módulo deseado.
- 3) Monte la tapa del estabilizador.

5.4.3.2 Cómo retirar un módulo

Requisitos previos

La tapa de la carcasa está desmontada.

Nota: Al trabajar con módulos hay que llevar siempre puesto un brazalete de puesta a tierra.

Hay que respetar y seguir las medidas de protección contra descargas electrostáticas (consulte [Indicaciones de aviso: Aviso](#) en la página 16)

Paso a paso

- 1) Retire la cubierta de estabilizador.
- 2) Extraiga el módulo del soporte para módulos.
- 3) Monte la tapa del estabilizador.

5.5 Puerto LAN y WAN

Los sistemas de comunicación OpenScape Business X3W y OpenScape Business X5W ofrecen diferentes opciones para las conexiones LAN y WAN.

Nota: Para garantizar un blindaje electromagnético suficiente según EN 55032, el blindaje de cada cable LAN y WAN se debe

conectar con conducción a la carcasa metálica del sistema de comunicación.

5.5.1 Realizar la conexión LAN o WAN

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra su sistema de comunicación y todos los distribuidores principales que pudiera haber en uso con conductores de protección a tierra independientes.



PRECAUCIÓN:

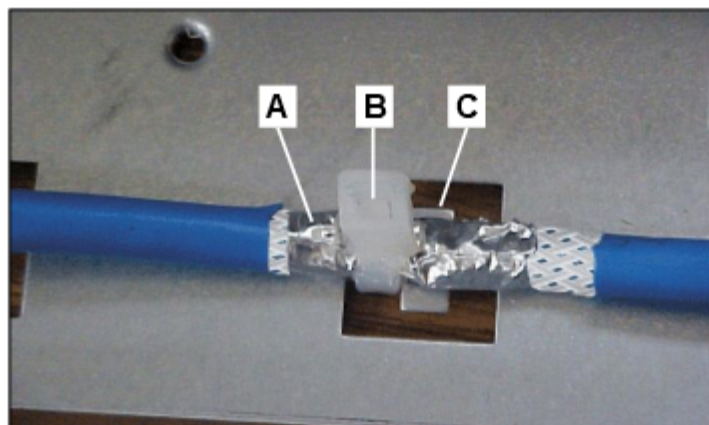
Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor. Se recomiendan cables Cat.5 blindados (cables de varios hilos de hasta 100 MHz para la sección horizontal y vertical conforme a la especificación EN 50288). Tienen especificado un diámetro de entre 0,4 y 0,8 mm.

Hay disponible al menos una interfaz LAN o WAN libre (placa base OCCM o Tablero de aplicaciones OCAB).

Paso a paso

- 1) Pele el blindaje del cable LAN/WAN unos 3 cm. El blindaje pelado debe estar en el alcance de una lengüeta en T de la carcasa.
- 2) Enrolle el blindaje pelado del cable LAN/WAN con cinta adhesiva conductora (al menos 1,5 vueltas).
- 3) Fije el blindaje enrollado con cinta adhesiva [A] del cable LAN/WAN con una brida [B] a una lengüeta en T [C] de la carcasa, de forma que se garantice una conexión conductora permanente entre el blindaje y la carcasa.



- 4) Conecte la conexión LAN o WAN deseada con el dispositivo que desea conectar (interruptor LAN, teléfono IP, módem DSL, etc.).

5.6 Conexión urbana

Los sistemas de comunicación OpenScape Business X3W y OpenScape Business X5W ofrecen distintas opciones para la conexión de línea urbana y, con ello, para el acceso a la red de comunicación pública.

De entre las siguientes opciones, seleccione la conexión o conexiones de línea urbana requeridas para su sistema de comunicación:

- Conexión de centralita RDSI y acceso individual RDSI a través de una interfaz S_0 (no para EE. UU., Canadá)
- Solo para OpenScape Business X5W: conexión múltiplex primaria RDSI mediante interfaz S_{2M} (no para EE. UU. ni Canadá)
- Solo para OpenScape Business X5W: conexión múltiplex primaria RDSI mediante interfaz T1 (solo para EE. UU. y Canadá)
- Solo para OpenScape Business X5W: conexión urbana con protocolo CAS mediante interfaz CAS (solo para algunos países)
- Conexión urbana analógica

5.6.1 No para EE. UU. ni Canadá: Cómo implementar una conexión de centralita RDSI o un acceso individual RDSI mediante una interfaz S_0

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra su sistema de comunicación y todos los distribuidores principales que pudiera haber en uso con conductores de protección a tierra independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

Hay al menos una interfaz S_0 libre (placa base OCCM o módulo periférico STLSX2, STLSX4, STLS2, STLS4).

La interfaz S_0 utilizada se debe configurar como conexión de centralita RDSI o acceso individual RDSI al hacer la puesta en servicio.

Hay disponible una conexión de centralita RDSI o un acceso individual RDSI.

Paso a paso

Conecte la conexión S_0 deseada con el NTBA de la conexión de centralita RDSI o del acceso individual RDSI.

Elija una de estas opciones:

- Si la conexión se va a establecer a través del distribuidor principal externo MDFU, conecte el cable de conexión con el NTBA en la regleta divisora/de clasificación deseada del MDFU.
- Si desea realizar la conexión directamente con el sistema de comunicación (es decir, mediante un CABLU con bornes atornillables Wieland), inserte el cable de conexión con el NTBA en la toma RJ45 deseada del CABLU.

5.6.2 No para EE. UU. ni Canadá: Cómo realizar una conexión múltiplex primaria mediante una interfaz S_{2M} (solo para OpenScape Business X5W)

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra su sistema de comunicación y todos los distribuidores principales que pudiera haber en uso con conductores de protección a tierra independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

OpenScape Business X5W equipa un módulo TS2N.

Hay disponible una conexión múltiplex primaria RDSI.

Paso a paso

Conecte la interfaz S_{2M} con el NTPM de la conexión múltiplex primaria RDSI.

Elija una de estas opciones:

- Si utiliza una línea simétrica (120 ohmios), la conexión se realiza mediante el conector de tarjeta X2 del módulo TS2N. Inserte un borne atornillable Wieland en el conector de tarjeta y conecte el cable de conexión con el NTPM.
- Si utiliza una línea Western (cable de interconexión), la conexión se realiza mediante una toma RJ45 X5 del módulo TS2N. Inserte el cable de conexión con el NTPM en la toma RJ45.

5.6.3 Solo para EE. UU. y Canadá: Cómo realizar una conexión múltiplex primaria RDSI mediante una interfaz T1 (solo para OpenScape Business X5W)

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra su sistema de comunicación y todos los distribuidores principales que pudiera haber en uso con conductores de protección a tierra independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

OpenScape Business X5W equipa un módulo TST1.

Hay disponible una CSU (Channel Service Unit) aprobada según FCC Parte 68 y que cumple con la directriz ANSI T1.403. La interfaz T1 no se puede conectar directamente a la PSTN (Public Switched Telephone Network). Es necesario activar una CSU entre el sistema de comunicación y la conexión urbana digital. Mediante la CSU, OpenScape Business X5W recibe estas características: aislamiento y protección de sobretensión del sistema de comunicación, opciones de diagnóstico en caso de error (como Signal Loop Back, Inserción de señales de prueba y patrones de prueba) y ajuste de la señal de salida de acuerdo a la longitud de línea especificada por el proveedor de red. Una CSU no es un componente de suministro del sistema de comunicación OpenScape Business X5W.

Hay disponible una conexión múltiplex primaria RDSI.

Paso a paso

Conecte la interfaz T1 con la CSU (Channel Service Unit).

La conexión se realiza a través del conector de tarjeta X2 del módulo TST1. Inserte un borne atornillable Wieland en el conector de tarjeta y conecte el cable de conexión con el CSU.

5.6.4 Solo para algunos países: Cómo hacer una conexión de línea urbana mediante una interfaz E1-CAS (solo para OpenScape Business X5W)

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra su sistema de comunicación y todos los distribuidores principales que pudiera haber en uso con conductores de protección a tierra independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

OpenScape Business X5W equipa un módulo TCAS-2.

Hay disponible una conexión de línea urbana con el protocolo CAS.

Paso a paso

Conecte la interfaz CAS deseada del módulo TCAS-2 con el NT de la conexión de línea urbana.

5.6.5 Cómo realizar una conexión urbana analógica

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra su sistema de comunicación y todos los distribuidores principales que pudiera haber en uso con conductores de protección a tierra independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos TLANI2, TLANI4 y TLANI8 con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

El sistema de comunicación equipa al menos un módulo TLANI2, TLANI4 o TLANI8.

Solo para EE. UU., Canadá: hay disponible al menos un elemento de seguridad conforme a UL 497A o CSA C22.2 núm. 226. Las indicaciones de instalación exigen que la conexión de las líneas urbanas analógicas se realicen a través de elementos de seguridad conformes al UL 497A o CSA C22.2 N° 226.

Hay disponible una conexión urbana analógica con sistema de señalización de teléfonos principales (Ground Start/Arranque tierra o Loop Start/Arranque bucle).

Paso a paso

Conecte la conexión a/b deseada del módulo deseado con la toma de conexión TAE de la conexión urbana analógica.

Elija una de estas opciones:

- Si la conexión se va a establecer a través del distribuidor principal externo MDFU, conecte el cable de conexión con la caja de conexión TAE en la regleta divisora/de clasificación deseada del MDFU.
- Si desea realizar la conexión directamente con el sistema de comunicación (es decir, mediante un CABLU con bornes atornillables Wieland), inserte el cable de conexión con la caja de conexión TAE en la toma RJ45 deseada del CABLU.

5.7 Conexión de teléfonos y dispositivos

Los modelos de pared de OpenScape Business ofrecen varias opciones para conectar teléfonos y dispositivos.

Puede seleccionar las conexiones que requiera para su sistema de comunicación de entre las siguientes opciones:

- Conexión directa de teléfonos RDSI (excepto EE. UU. y Canadá)
- Conexión de teléfonos RDSI mediante el bus S_0 (excepto EE. UU. y Canadá)
- Conexión de teléfonos $U_{P0/E}$
- Conexión de teléfonos y dispositivos analógicos

Nota: Solo se puede conectar un dispositivo analógico a una interfaz a/b.

5.7.1 No para EE. UU., Canadá: cómo conectar directamente teléfonos RDSI

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra su sistema de comunicación y todos los distribuidores principales que pudiera haber en uso con conductores de protección a tierra independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Solo para las interfaces que se utilizan para conexiones de extensión: con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos OCCM, STLSX2, STLSX4, STLS2 y STLS4 con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

Hay al menos una interfaz S_0 libre (placa base OCCM o módulo periférico STLSX2, STLSX4, STLS2, STLS4).

Las interfaces S_0 utilizadas tienen que configurarse en la puesta en servicio como una conexión S_0 interna.

Los teléfonos RDSI a conectar deben disponer de alimentación propia, por ejemplo, con un alimentador enchufable. La alimentación no se puede realizar a través de las interfaces S_0 de los módulos OCCM, STLSX2, STLSX4, STLS2 y STLS4.

Paso a paso

1) Conecte la conexión S_0 deseada con el teléfono RDSI.

Elija una de estas opciones:

- Si la conexión se va a establecer a través del distribuidor principal externo MDFU, conecte el cable de conexión con el teléfono RDSI en la regleta divisora/de clasificación del MDFU.
- Si desea realizar la conexión directamente con el sistema de comunicación (es decir, mediante un CABLU con bornes atornillables

Wieland)), inserte el cable de conexión con el teléfono RDSI en la toma RJ45 deseada del CABLU.

Consejo:

Siga las indicaciones de las instrucciones de instalación del teléfono que desea conectar.

-
- 2) Si lo desea, conecte más teléfonos RDSI con el sistema de comunicación siguiendo el mismo procedimiento.

5.7.2 No para EE. UU., Canadá: Cómo conectar teléfonos RDSI por bus S₀

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra su sistema de comunicación y todos los distribuidores principales que pudiera haber en uso con conductores de protección a tierra independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Solo para las interfaces que se utilizan para conexiones de extensión: con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos OCCM, STLSX2, STLSX4, STLS2 y STLS4 con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

Hay al menos una interfaz S₀ libre (placa base OCCM o módulo periférico STLSX2, STLSX4, STLS2, STLS4).

Las interfaces S₀ utilizadas tienen que configurarse en la puesta en servicio como una conexión S₀ interna.

Los teléfonos RDSI a conectar deben disponer de alimentación propia, por ejemplo, con un alimentador enchufable. La alimentación no se puede realizar a través de las interfaces S_0 de los módulos OCCM, STLSX2, STLSX4, STLS2 y STLS4.

Todos los teléfonos RDSI (extensiones RDSI) deben tener asignado un MSN (Multiple Subscriber Number) único. Esta asignación se realiza en el menú de configuración de la extensión RDSI.

Paso a paso

- 1) Conecte la conexión S_0 deseada con la toma de paso Mini-Western del bus S_0 .

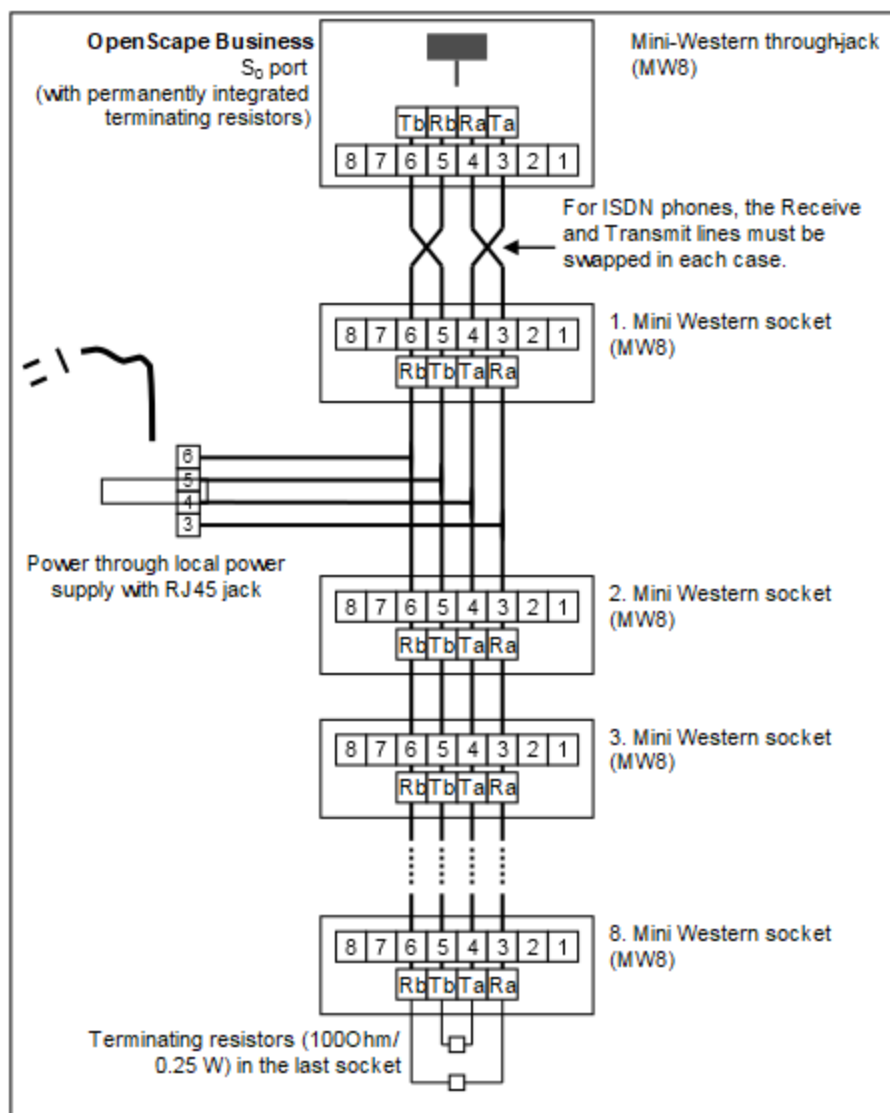
Elija una de estas opciones:

- Si la conexión se va a establecer a través del distribuidor principal externo MDFU, conecte el cable de conexión con la caja de paso Mini-Western del bus S_0 en la regleta divisora/de clasificación deseada del MDFU.
- Si desea realizar la conexión directamente con el sistema de comunicación (es decir, mediante un CABLU con bornes atornillables Wieland), inserte el cable de conexión con la caja de paso Mini-Western del bus S_0 en la toma RJ45 del CABLU.

Consejo:

Siga las indicaciones de las instrucciones de instalación del teléfono que desea conectar.

- 2) Para realizar el resto del cableado, siga las indicaciones de la imagen siguiente.



- 3) Instale resistencias de terminación (100 Ohmios/0,25 W) en la última caja de conexión del bus S₀.
- 4) Asegúrese de que solo hay resistencias de terminación en los dos extremos del bus S₀. Las demás cajas de conexión del bus S₀ no necesitan resistencias de terminación.

Consejo:

Como las resistencias de terminación ya están integradas en OpenScape Business X3W y OpenScape Business X5W, el

sistema de comunicación constituye uno de los extremos de un bus S_0 .

Consejo:

Siga las indicaciones de las instrucciones de instalación del teléfono que desea conectar.

5.7.3 Cómo conectar teléfonos $U_{P0/E}$

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra su sistema de comunicación y todos los distribuidores principales que pudiera haber en uso con conductores de protección a tierra independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos OCCM, SLU8, SLMO8 y SLMO24 con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

Hay al menos una interfaz $U_{P0/E}$ libre (placa base OCCM o módulo periférico SLU8, SLMO8 (solo OpenScape Business X5W) o SLMO24 (solo OpenScape Business X5W)).

Paso a paso

1) Conecte la conexión U_{P0/E} deseada con el teléfono U_{P0/E}.

Elija una de estas opciones:

- Si la conexión se va a establecer a través del distribuidor principal externo MDFU, conecte el cable de conexión con el teléfono U_{P0/E} en la regleta divisora/de clasificación del MDFU.

Consejo: Solo para OpenScape Business X5W: si se utilizan interfaces U_{P0/E} de los módulos periféricos SLMO8 y SLMO24, la conexión solo se puede realizar a través de un distribuidor principal externo.

- Si desea realizar la conexión directamente con el sistema de comunicación (es decir, mediante un CABLU con bornes atornillables Wieland), inserte el cable de conexión con el teléfono U_{P0/E} en la toma RJ45 deseada del CABLU..

Consejo:

Siga las indicaciones de las instrucciones de instalación del teléfono que desea conectar.

2) Si lo desea, conecte más teléfonos U_{P0/E} con el sistema de comunicación siguiendo el mismo procedimiento.

5.7.4 Cómo conectar dispositivos y teléfonos analógicos

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra su sistema de comunicación y todos los distribuidores principales que pudiera haber en uso con conductores de protección a tierra independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos OCCM, SLAD4, SLAD8, SLAD16, 4SLA, 8SLA, 16SLA, SLA16N y SLA24N con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

Hay disponible al menos una interfaz a/b libre (placa base OCCM o módulo periférico SLAD4, SLAD8, SLAD16, 4SLA, 8SLA, 16SLA, SLA16N (solo OpenScape Business X5W) o SLA24N (solo OpenScape Business X5W)).

Paso a paso

- 1) Conecte la conexión a/b deseada con el teléfono analógico o el dispositivo analógico que desee conectar (fax, módem, TFE-S, etc.).

Elija una de estas opciones:

- Si la conexión se va a establecer a través del distribuidor principal externo MDFU, conecte el cable de conexión con el teléfono analógico o con el aparato analógico en la regleta divisora/de clasificación deseada del MDFU.

Consejo:

Solo para OpenScape Business X5W: si se utilizan interfaces a/b de los módulos periféricos SLA16N y SLA24N, la conexión solo se puede realizar a través de un distribuidor principal externo.

- Si desea realizar la conexión directamente con el sistema de comunicación (es decir, mediante un CABLU con bornes atornillables Wieland), inserte el cable de conexión con el teléfono analógico o con el dispositivo analógico en la toma RJ45 deseada del CABLU.

Consejo:

Siga las indicaciones de las instrucciones de instalación del teléfono o dispositivo que desea conectar.

- 2) Si lo desea, conecte más teléfonos o equipos analógicos con el sistema de comunicación siguiendo el mismo procedimiento.

5.8 Emisiones de interferencias

Para atenerse a los límites de emisiones de interferencias que permiten las especificaciones EMC Clase B, es preciso acoplar casquillos de ferrita a ciertas líneas del sistema de comunicación.

Cable de alimentación

Para reducir al mínimo las emisiones de interferencias, el conductor de alimentación debe pasarse tendido a través del casquillo de ferrita C39022-

Z7000-C7 incluido con el paquete de complementos del sistema de comunicación.

Cables periféricos

Para reducir al mínimo las emisiones de interferencias, los cables periféricos deben estar equipados con casquillos de ferrita. Utilice con ese fin los cinco casquillos de ferrita C39022-Z7000-C6 incluidos en el paquete del sistema de comunicación.

Siempre que sea posible, los casquillos de ferrita deben instalarse dentro de la canaleta del cable. Si el número de líneas con el que trabaja lo hace imposible, fije el casquillo de ferrita instalándolo directamente en la canaleta o el conducto del cable.

Si el número de casquillos de ferrita incluido no es suficiente para todos los conductores de conexión, puede adquirir más: L30460-X1358-X incluye cinco casquillos de ferrita C39022-Z7000-C6.

- OpenScape Business X3W
 - OCCM, OCCMA y OCCMB (placa base)

Los conductores de conexión de todas las interfaces $U_{P0/E}$, a/b y S_0 deben estar equipados con casquillo de ferrita C39022-Z7000-C6.

Los conductores de conexión deben pasar de nuevo a través del casquillo de ferrita, atravesándolo dos veces, es decir, formando un bucle. Cada casquillo de ferrita admite un máximo de tres conductores de conexión.
 - Todos los módulos de línea de extensión, líneas urbanas y líneas directas

Los conductores de conexión de todas las interfaces deben estar equipados con casquillo de ferrita C39022-Z7000-C6.

Los conductores de conexión deben pasar de nuevo a través del casquillo de ferrita, atravesándolo dos veces, es decir, formando un bucle. Cada casquillo de ferrita admite un máximo de tres conductores de conexión.
- OpenScape Business X5W
 - OCCM, OCCMA y OCCMB (placa base)

Los conductores de conexión de todas las interfaces $U_{P0/E}$, a/b y S_0 deben estar equipados con casquillo de ferrita C39022-Z7000-C6.

Los conductores de conexión deben pasar de nuevo a través del casquillo de ferrita, atravesándolo dos veces, es decir, formando un bucle. Cada casquillo de ferrita admite un máximo de tres conductores de conexión.
 - Todos los módulos de línea de extensión, inalámbricos (cordless), líneas urbanas y líneas directas

Los conductores de conexión de todas las interfaces deben estar equipados con casquillo de ferrita C39022-Z7000-C6.

Los conductores de conexión deben pasar de nuevo a través del casquillo de ferrita, atravesándolo dos veces, es decir, formando un bucle. Cada casquillo de ferrita admite un máximo de tres conductores de conexión.

5.8.1 Cómo colocar una ferrita en la línea de conexión de red

Requisitos previos



Atención:

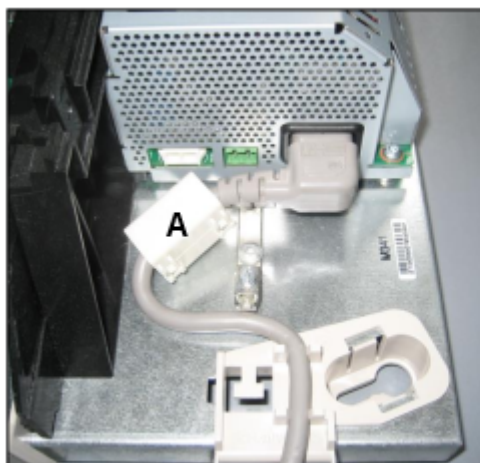
Descarga eléctrica al tocar los cables con tensión

Antes de la puesta en servicio, ponga a tierra el sistema de comunicación y los distribuidores principales que se pudieran estar utilizando con conductores de protección independientes.

La tapa de la carcasa del sistema de comunicación no está montada.

Paso a paso

- 1) Pase la línea de conexión de red por la ferrita incluida en el volumen de suministro del sistema de comunicación C39022-Z7000-C7.
- 2) Coloque la ferrita [A] como se muestra en la imagen siguiente para poder cerrar la tapa de la carcasa.



5.8.2 Cómo colocar ferritas en las líneas de conexión de periféricos

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de la puesta en servicio, ponga a tierra el sistema de comunicación y los distribuidores principales que se pudieran estar utilizando con conductores de protección independientes.

La tapa de la carcasa del sistema de comunicación no está montada.

Paso a paso

Seleccione el procedimiento en función del sistema de comunicación y del módulo.

Si		Entonces
Sistema de comunicación	Módulo	
OpenScape Business X3W	Placa base OCCM	Pase las líneas de conexión de todas las interfaces $U_{P0/E}$, a/b y S_0 por doble (en un lazo) por una ferrita C39022-Z7000-C6. Coloque la ferrita lo más dentro posible del canal de cable. Si no es posible hacerlo por el número de líneas, coloque la ferrita inmediatamente en la salida del canal de cable. Se pueden utilizar tres líneas de conexión como máximo por cada ferrita.
	Todos los módulos de línea urbana, de tráfico cruzado y de extensión	Pase las líneas de conexión de todas las interfaces por doble (en un lazo) por una ferrita C39022-Z7000-C6. Coloque la ferrita lo más dentro posible del canal de cable. Si no es posible hacerlo por el número de líneas, coloque la ferrita inmediatamente en la salida del canal de cable. Se pueden utilizar tres líneas de conexión como máximo por cada ferrita.
OpenScape Business X5W	Placa base OCCM	Pase las líneas de conexión de todas las interfaces $U_{P0/E}$, a/b y S_0 por doble (en un lazo) por una ferrita C39022-Z7000-C6. Coloque la ferrita lo más dentro posible del canal de cable. Si no es posible hacerlo por el número de líneas, coloque la ferrita inmediatamente en la salida del canal de cable. Se pueden utilizar tres líneas de conexión como máximo por cada ferrita.
	SLA16N SLC16N SLMO8	Pase el cable de conexión con el conector SIPAC 1 SU X8 del backplane por dos ferritas C39022-Z7000-C6. Coloque la ferrita lo más dentro posible de la carcasa.
	SLA24N SLMO24	Pase los dos cables de conexión con los conectores SIPAC 1 SU X8 y X9 del backplane por dos ferritas C39022-Z7000-C6. Coloque la ferrita lo más dentro posible de la carcasa.

Si		Entonces
Sistema de comunicación	Módulo	
	Todos los demás módulos de línea urbana, Cordless, de tráfico cruzado y de extensión	Pase las líneas de conexión de todas las interfaces por doble (en un lazo) por una ferrita C39022-Z7000-C6. Coloque la ferrita lo más dentro posible del canal de cable. Si no es posible hacerlo por el número de líneas, coloque la ferrita inmediatamente en la salida del canal de cable. Se pueden utilizar tres líneas de conexión como máximo por cada ferrita.

5.9 Tareas finales

Para finalizar el montaje hay que insertar la tarjeta SDHC, hacer una prueba visual, colocar la tapa de la carcasa y conectar el sistema a la red eléctrica.

A continuación se puede poner en servicio el sistema de comunicación con el OpenScape Business Assistant (gestión basada en web). Encontrará la descripción correspondiente en la ayuda en línea de la gestión basada en web o en el capítulo "Instalación inicial de OpenScape Business" de la documentación para el administrador.

Nota: En la puesta en servicio inicial del sistema de comunicación no está definido el estado de carga del acumulador en la placa base. Para conseguir una carga suficiente, el sistema debe estar al menos 2 días conectado con la red eléctrica. Si el sistema se desconecta de la red y el nivel de carga del acumulador es insuficiente, puede que se bloquee el periodo de activación por manipulación del tiempo.

5.9.1 Cómo insertar la tarjeta M.2 SSD o la tarjeta SDHC (sistema con OCCM)

La tarjeta M.2 SSD o la tarjeta SDHC contiene el software de comunicación OpenScape Business y deben montarse/insertarse antes de la puesta en servicio del sistema de comunicación.

Paso a paso

- 1) Compruebe que la protección contra escritura de la tarjeta SDHC esté desactivada (interruptor en dirección de los contactos metálicos).
- 2) Si todavía no lo ha hecho, inserte la tarjeta SDHC en el slot para tarjetas SDHC de la placa base, hasta que encaje. Los contactos metálicos de la tarjeta SDHC deben ir en dirección de la placa base.

5.9.2 Cómo efectuar la prueba visual

Antes de poner en servicio el sistema de comunicación hay que efectuar una prueba visual del hardware, del cableado y del suministro de tensión.

Requisitos previos



PELIGRO:

Descarga eléctrica al tocar los cables con tensión

Desconecte todos los circuitos de suministro del sistema de comunicación antes de comenzar con la prueba visual:

- Desconecte la tensión de acumulador, la tensión de alimentación (LUNA2) y la tensión de red de todos los powerbox OpenScape Business que pudiera haber conectados
- Si hay conectado un powerbox OpenScape Business, desconecte las líneas de conexión.
- Si hay un set de acumuladores conectores o un acumulador conectado, tienda las líneas de conexión.
- Extraiga el conector de red del sistema de comunicación.

Nota:

Al trabajar con módulos hay que llevar siempre puesto un brazalete de puesta a tierra.

Hay que respetar y seguir las medidas de protección contra descargas electrostáticas (consulte [Indicaciones de aviso: Nota](#)).

La tapa de la carcasa del sistema de comunicación no está montada.

Paso a paso

- 1) Desconecte todos los circuitos de corriente de suministro del sistema de comunicación.
- 2) Compruebe si el sistema de comunicación está sin tensión.
- 3) Compruebe si la tarjeta SDHC está bien encajada. La protección contra escritura de la tarjeta SDHC debe estar desactivada (interruptor en dirección de los contactos metálicos).
- 4) Compruebe que los módulos encajan perfectamente.

Si es necesario, compruebe que los módulos correspondientes están bien insertados (consulte [Cómo insertar un módulo](#)).

- 5) Compruebe que todos los cables de conexión están bien tendidos. Por ejemplo, ¿hay riesgo de tropezar?

Si es necesario, tienda correctamente los cables de conexión y de unión.

- 6) Compruebe si hay conectado un conductor de protección independiente en la conexión del conductor de protección del sistema de comunicación.

Si es necesario, realice una puesta a tierra de protección independiente del sistema de comunicación (consulte [Cómo conectar a tierra el sistema de comunicación y el distribuidor principal MDFU](#)).

- 7) Si se utilizan distribuidores principales, compruebe que están bien conectados con el conector de protección.

Si es necesario, realice una puesta a tierra de protección de todos los distribuidores principales (consulte [Cómo conectar a tierra el sistema de comunicación y el distribuidor principal MDFU](#)).

- 8) Compruebe si la tensión nominal del suministro de tensión de red coincide con la tensión nominal del sistema de comunicación (placa de características).

Pasos siguientes

Cierre el sistema de comunicación con la tapa de la carcasa (consulte [Cómo colocar la tapa de la carcasa](#)).

5.9.3 Cómo colocar la tapa de la carcasa

Paso a paso

- 1) Coloque la tapa de la carcasa sobre el sistema de comunicación. Para ello, coloque los dos pasadores de sujeción en los orificios correspondientes del soporte para módulos.



PRECAUCIÓN: Heridas por cortes provocados con los cantos afilados de la chapa de protección

Coja la tapa de carcasa siempre desde fuera. De lo contrario, existe peligro de sufrir cortes por la chapa protectora del interior de la carcasa, que podría tener cantos cortantes.



2) Fije la tapa de la carcasa con los dos tornillos de sujeción.

5.9.4 Cómo conectar el sistema a la red eléctrica

Paso a paso

Inserte el cable de conexión de red en la toma del suministro de corriente. El sistema de comunicación arranca.

Nota: Deje el sistema conectado a la red eléctrica durante 2 días al menos para que el acumulador de la placa base se cargue lo suficiente. Si la carga es insuficiente es posible que el periodo de activación se bloquee por manipulación del tiempo si se producen repetidos arranques.

6 Instalación de hardware por OpenScape Business X3R/X5R

Se describe el montaje estándar más realizado para los sistemas de comunicación OpenScape Business X3R y OpenScape Business X5R.

OpenScape Business X3R y OpenScape Business X5R son sistemas de comunicación con caja de rack de 19" que se pueden montar en un armario de 19", exentos (operación de escritorio) o en pared.



Atención:

Descarga eléctrica al tocar los cables con tensión

- Solo se puede trabajar con la carcasa abierta si el sistema está sin tensión.
- Antes de iniciar cualquier trabajo, compruebe si todos los circuitos de corriente están sin tensión. Jamás dé por sentado que al desconectar un fusible o un interruptor principal se han interrumpido efectivamente todos los circuitos de corriente.

6.1 Tipos de montaje

Los sistemas de comunicación OpenScape Business X3R y OpenScape Business X5R se pueden montar en un armario de 19 pulgadas, se pueden fijar en una pared o se pueden montar como sistemas autónomos (operación de escritorio).

6.1.1 Cómo montar OpenScape Business X3R en un armario de 19 pulgadas

Requisitos previos

Se han tenido en cuenta los requisitos para elegir el lugar de montaje (consulte [Requisitos para la instalación](#) en la página 31).

Hay disponibles tornillos específicos para el armario para fijar las escuadras de montaje al armario de 19 pulgadas (las suministra el proveedor del armario de 19").

Paso a paso

- 1) Fije las dos escuadras de sujeción incluidas en el volumen de suministro a los laterales del sistema de comunicación con dos tornillos.



Figura 8: OpenScape Business X3R – Escuadra de sujeción

- 2) Meta el sistema de comunicación en el armario de 19 pulgadas y fíjelo al armario de 19 pulgadas con las dos escuadras de sujeción [A] con los tornillos previstos para ello.



6.1.2 Cómo montar OpenScape Business X5R en un armario de 19"

Requisitos previos

Se han tenido en cuenta los requisitos para elegir el lugar de montaje (consulte [Requisitos para la instalación](#) en la página 31).

Hay disponibles tornillos específicos para el armario para fijar las escuadras de montaje y la escuadra de sujeción al armario de 19" (las suministra el proveedor del armario de 19").

Paso a paso

- 1) Fije las dos escuadras de sujeción incluidas en el volumen de suministro a los laterales del sistema de comunicación con dos tornillos.



Figura 9: OpenScape Business X5R – Escuadras de sujeción

- 2) Monte una escuadra de montaje derecha y una izquierda (incluidas en el kit de montaje para el montaje en armario de 19" (C39165-A7027-D1)) en el armario de 19" con los tornillos correspondientes.



Figura 10: OpenScape Business X5R – Escuadras de montaje

- 3) Meta el sistema de comunicación en el armario de 19 pulgadas y colóquelo sobre las dos escuadras de montaje [A]. Empuje el sistema de comunicación al interior del armario de 19", hasta que las dos escuadras de sujeción queden a ras del marco de 19" delantero.

- 4) Fije el sistema de comunicación al armario de 19" con las dos escuadras de sujeción [B] con los tornillos correspondientes.



6.1.3 Cómo fijar el sistema de comunicación a una pared

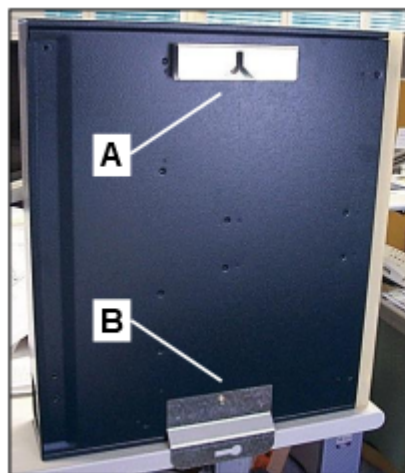
Requisitos previos

Se han tenido en cuenta los requisitos para elegir el lugar de montaje (consulte [Requisitos para la instalación](#) en la página 31).

Hay una pared con suficiente capacidad de carga para el montaje del sistema de comunicación.

Paso a paso

- 1) Monte las dos escuadras de sujeción [A] y [B] con los tornillos correspondientes en el fondo de la carcasa del sistema de comunicación.



- 2) Taladre un agujero para la escuadra de sujeción superior [A].

- 3) Meta un taco en el orificio e introduzca un tornillo dejando que sobresalga unos 2 mm.
- 4) Cuelgue el sistema de comunicación con la escuadra de sujeción superior [A].
- 5) Taladre un agujero para la escuadra de sujeción inferior [B].
- 6) Meta un taco en el orificio y fije la escuadra de sujeción inferior [B] con un tornillo.

6.2 Puesta a tierra de protección

La puesta a tierra de protección permite establecer una conexión segura con el potencial de masa para proteger el sistema de tensiones peligrosas en caso de error.



Atención:

Descarga eléctrica al tocar los cables con tensión

- Haga la puesta a tierra de los sistemas de comunicación OpenScape Business X3R y OpenScape Business X5R con un conductor de protección 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.
- Ha de procurarse un tendido con protección y una descarga de tracción del conductor de protección.

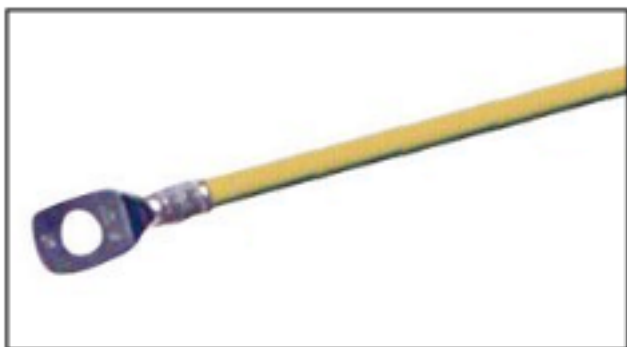
6.2.1 Puesta a tierra de protección con montaje en armario de 19"

La puesta a tierra de protección del sistema de comunicación se realiza mediante el embarrado equipotencial del armario de 19".

6.2.1.1 Cómo instalar una puesta a tierra de protección para el sistema de comunicación

Requisitos previos

Debe disponer de un conductor de puesta a tierra de protección con una sección transversal mínima de 12 AWG/2,5 mm² y un terminal de anilla (fíjese en la siguiente figura). Si no es posible proteger un conductor de puesta a tierra, se necesita una sección transversal mínima del conductor de 10 AWG/4 mm² para bloquear los efectos de factores externos.



Hay disponible una conexión de puesta a tierra de baja impedancia.

El armario de 19 pulgadas se conecta con la puesta a tierra a través de un conductor de puesta a tierra independiente (verde/amarillo). El armario de 19 pulgadas está equipado con una varilla de compensación de potencial, a la que se puede unir el sistema de comunicación por medio de una conexión de puesta a tierra separada.



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.



Atención:

Descarga eléctrica al tocar los cables con tensión

- Utilice conductores de conexión independientes para establecer la puesta a tierra de protección para los sistemas de comunicación OpenScape Business X3R y OpenScape Business X5R. 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.
- Asegúrese de que los conductores de protección de tierra colocados estén protegidos y no sufran tensiones.

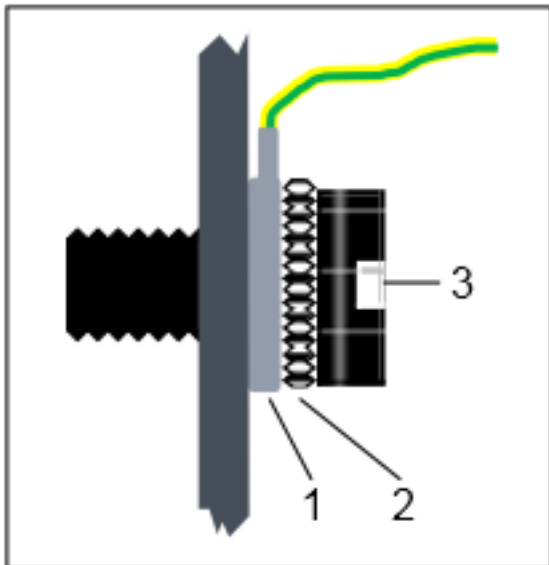
Es obligatorio cumplir las normas de implementación especificadas en las normativas IEC 60364, IEC 60950-1 e IEC 62368-1 durante la instalación.

Siga este procedimiento para garantizar una correcta puesta a tierra de protección:

Paso a paso

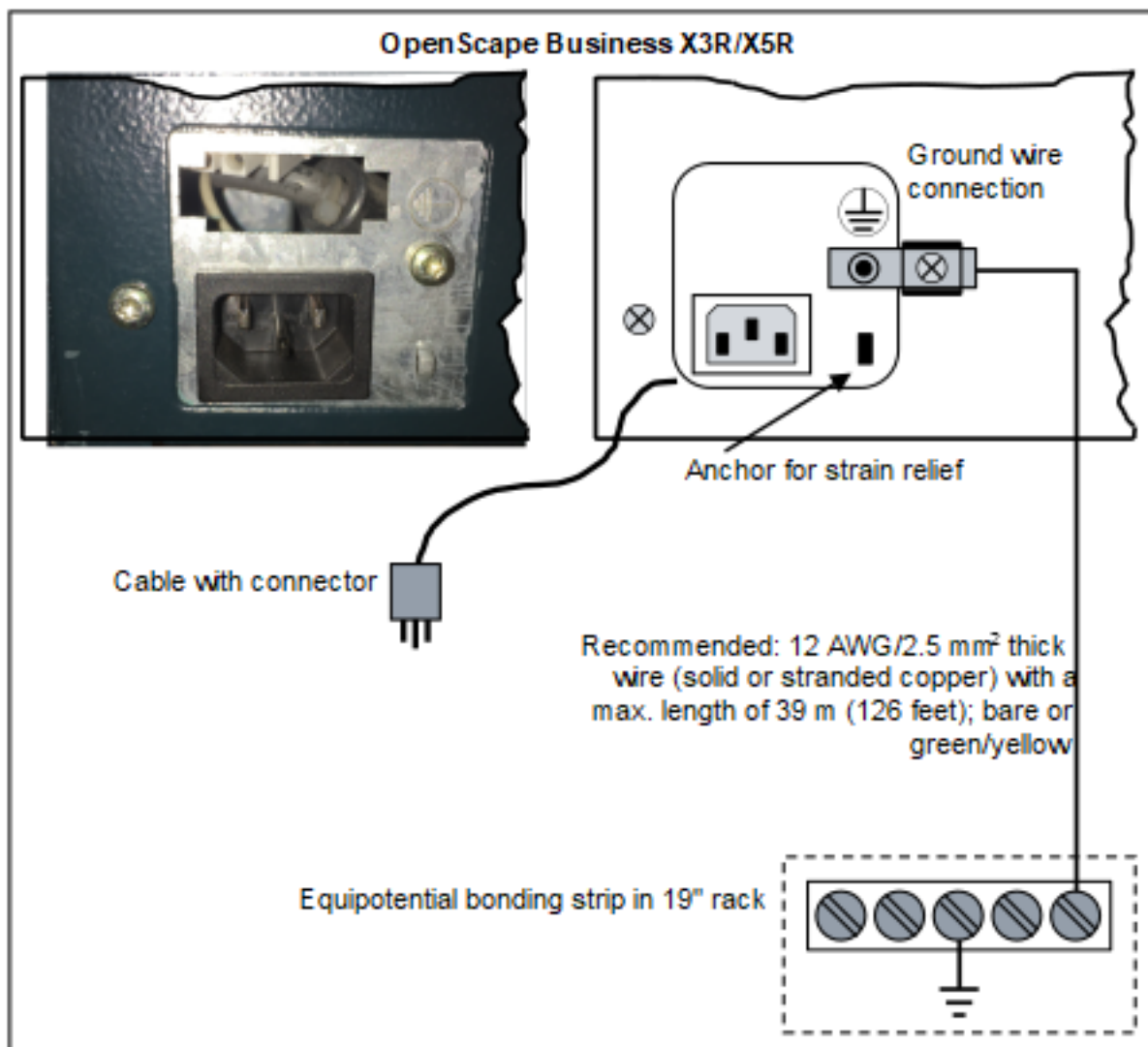
- 1) Instale el terminal de anilla [1] del conductor de puesta a tierra independiente como se indica en la figura, con la ayuda de una arandela de

seguridad [2] y un tornillo M4 [3] para fijarlo al conductor de protección del sistema de comunicación.



- 2) Fije el conductor de puesta a tierra al orificio apropiado para liberarlo de cualquier presión o tensión, con la ayuda de una brida.

- 3) Conecte el conductor de puesta a tierra con la varilla de compensación de potencial del armario de 19 pulgadas, tal y como muestra el diagrama conceptual en la figura a continuación.



Asegúrese de que el conductor de puesta a tierra colocado esté protegido y libre de tensiones (sección transversal mínima del conductor = 12 AWG/2,5 mm²). Si no es posible proteger un conductor de puesta a tierra, se necesita una sección transversal mínima del conductor de 10 AWG/4 mm² para bloquear los efectos de factores externos.

6.2.1.2 Cómo comprobar la puesta a tierra de protección

Requisitos previos

Ni el sistema de comunicación ni todos los demás dispositivos del armario de 19 pulgadas están conectados con la red de baja tensión mediante un cable de conexión de red.

La puesta a tierra de protección independiente del sistema de comunicación está conectada.

El armario de 19 pulgadas debe ponerse a tierra mediante un conductor de protección independiente (verde/amarillo).

Antes de la puesta en servicio, realice este test para garantizar una correcta puesta a tierra de protección del sistema de comunicación.

Paso a paso

Compruebe la resistencia óhmica del enlace del cable de protección con el sistema de comunicación:

- a) La primera medición se realiza entre el contacto de puesta a tierra de una caja de conexión de la red doméstica y el embarrado de equipotencialidad del armario de 19 pulgadas.
- b) La segunda medición se realiza entre el embarrado equipotencial del armario de 19 pulgadas y la carcasa del sistema de comunicación.

El resultado (valor nominal) de la medición debe ser claramente inferior a 10 ohmios.

Si en una medición se obtuviera otro resultado, póngase en contacto con un electricista profesional. Deberá comprobar la compensación de potencial de la instalación principal y garantizar el bajo ohmiaje del enlace de cable de protección.

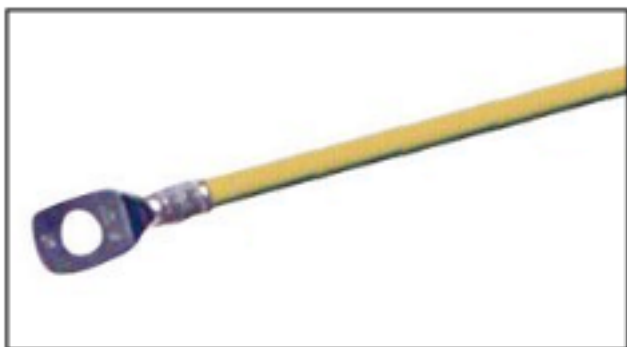
6.2.2 Toma de tierra en el montaje y con montaje autónomo

La toma de tierra del sistema de comunicación se realiza por ejemplo a través del embarrado de equipotencialidad del edificio, a través de una toma de conexión adicional con la red de baja tensión a través de una barra colectora de tierra principal o de un campo de puesta a tierra.

6.2.2.1 Cómo instalar una puesta a tierra de protección para el sistema de comunicación

Requisitos previos

Debe disponer de un conductor de puesta a tierra de protección con una sección transversal mínima de 12 AWG/2,5 mm² y un terminal de anilla (fíjese en la siguiente figura). Si no es posible proteger un conductor de puesta a tierra, se necesita una sección transversal mínima del conductor de 10 AWG/4 mm² para bloquear los efectos de factores externos. Si utiliza una caja de empalmes adicional para la conexión a la red de baja tensión, la sección transversal mínima de los conductores sería de 16 AWG/1,5 mm².



Hay disponible una conexión de puesta a tierra de baja impedancia.



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.



Atención:

Descarga eléctrica al tocar los cables con tensión

- Utilice conductores de conexión independientes para establecer la puesta a tierra de protección para los sistemas de comunicación OpenScape Business X3R y OpenScape Business X5R. 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.
- Asegúrese de que los conductores de protección de tierra colocados estén protegidos y no sufran tensiones.

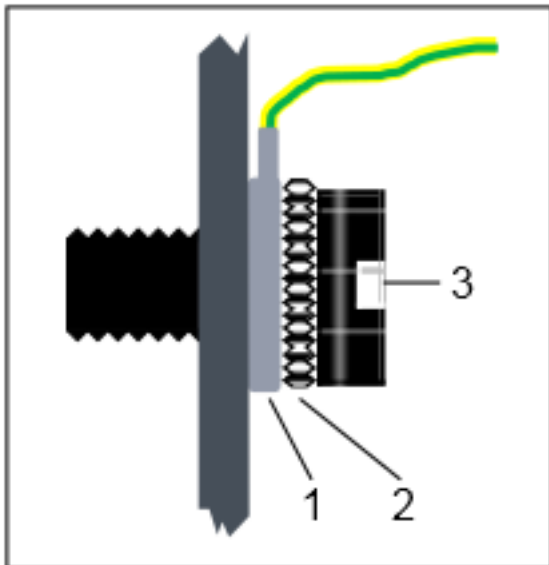
Es obligatorio cumplir las normas de implementación especificadas en las normativas IEC 60364, IEC 60950-1 e IEC 62368-1 durante la instalación.

Siga este procedimiento para garantizar una correcta puesta a tierra de protección:

Paso a paso

- 1) Instale el terminal de anilla [1] del conductor de puesta a tierra independiente como se indica en la figura, con la ayuda de una arandela de

seguridad [2] y un tornillo M4 [3] para fijarlo al conductor de protección del sistema de comunicación.

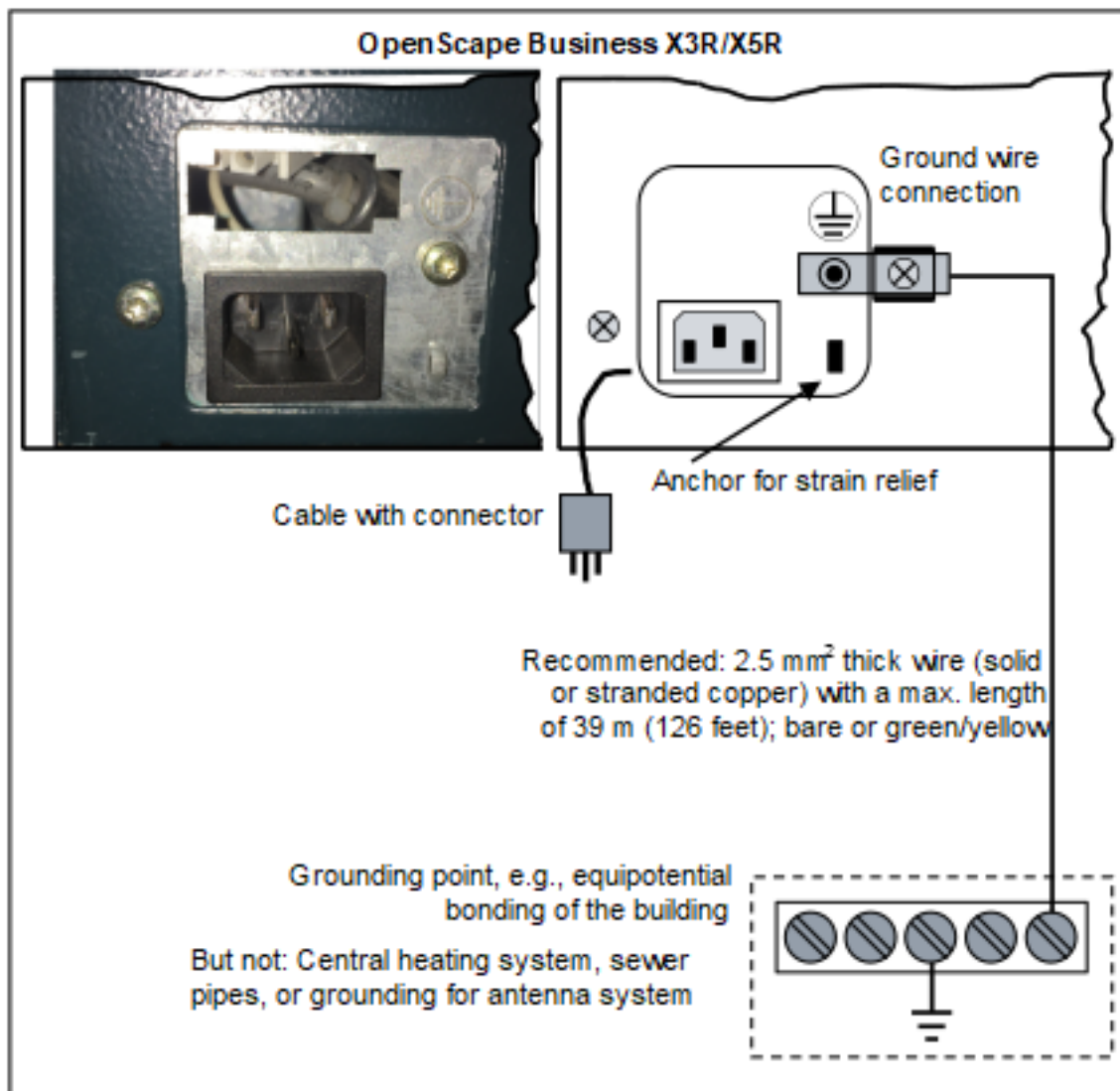


- 2) Fije el conductor de puesta a tierra al orificio apropiado para liberarlo de cualquier presión o tensión, con la ayuda de una brida.

3) Elija una de estas opciones:

- **No válido para EE. UU. y Canadá - Varilla de compensación de potencial**

Conecte el conductor de puesta a tierra independientes con el punto de toma de tierra (por ejemplo, la varilla de compensación de potencial del edificio) tal y como muestra el diagrama conceptual.

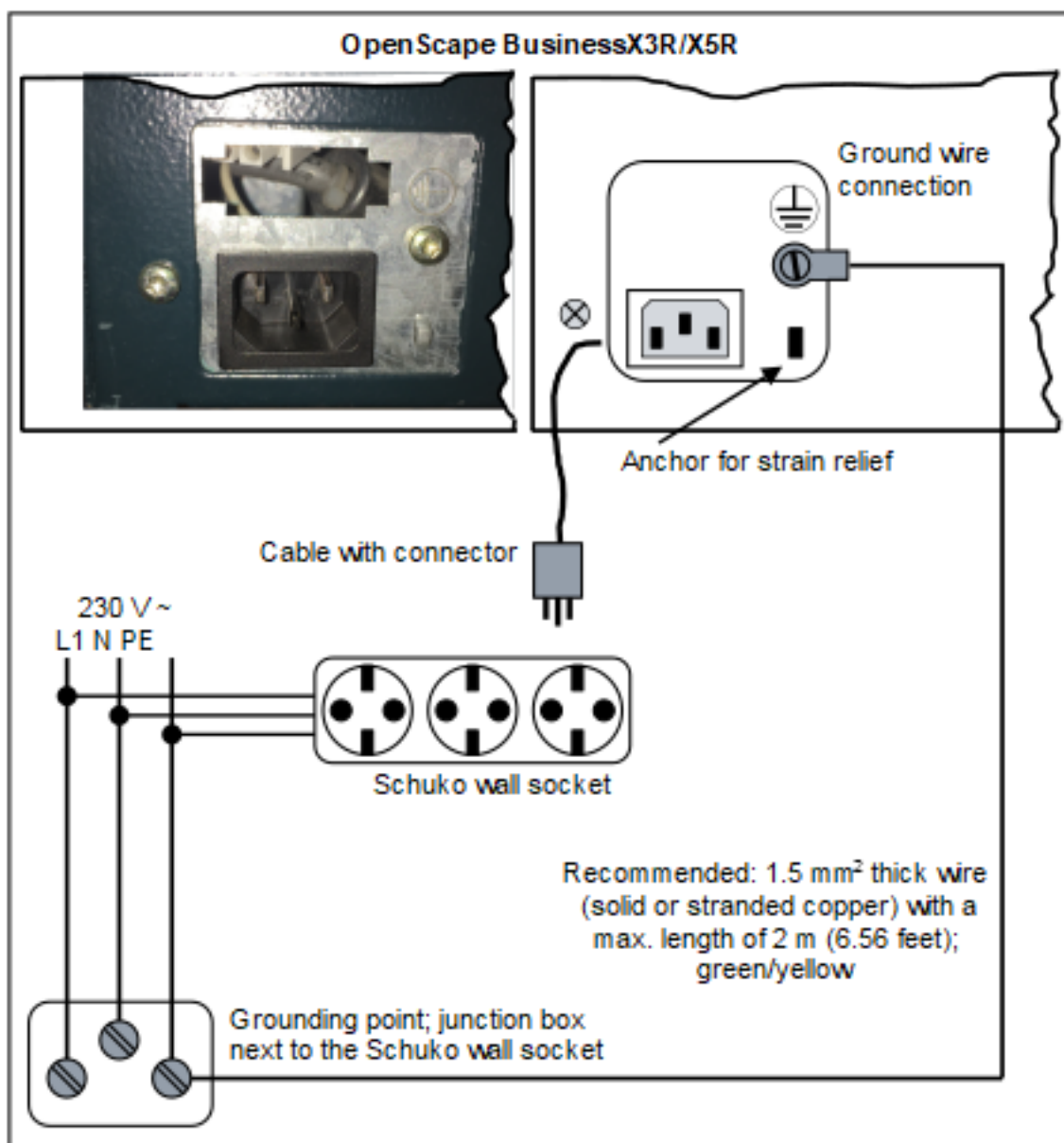


Asegúrese de que el conductor de protección de tierra colocado esté protegido y no sufra tensión ni presión. La sección transversal mínima de los conductores es de 12 AWG/2,5 mm²). Si no es posible proteger un conductor de puesta a tierra, se necesita una sección transversal mínima del conductor de 10 AWG/4 mm² para bloquear los efectos de factores externos.

- **No válido para EE. UU. y Canadá - Salida a la red de baja tensión**

Conecte una caja de empalmes a la red de baja tensión cerca de la toma Schuko de la pared a la cual esté enchufada el sistema de comunicación. Utilice un conductor de puesta a tierra independiente para establecer una

conexión fija a la caja de empalmes, como se muestra en el diagrama conceptual.

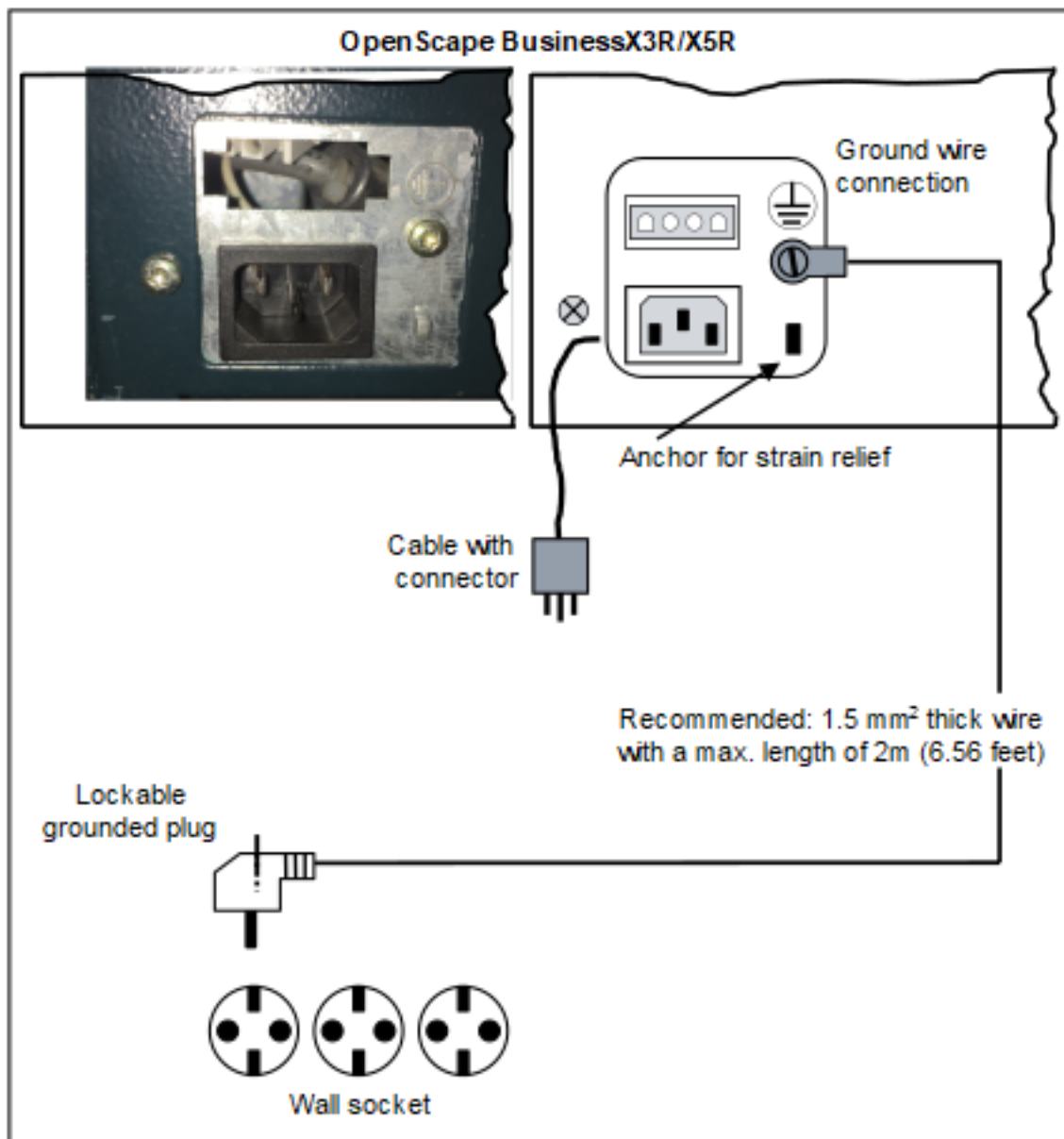


Asegúrese de que el conductor de protección de tierra colocado esté protegido y no sufra tensión ni presión. La sección transversal mínima de los conductores es de 16 AWG/1,5 mm².

- **No válido para EE. UU. y Canadá - Enchufe bloqueable con puesta a tierra para conexión a la red de baja tensión**

Inserte el enchufe bloqueable con puesta a tierra (un modelo de Schuko especial equipado con un conductor de toma de tierra de protección fijo) en una toma de pared de la red de baja tensión y bloquee el enchufe. Utilice el conductor de puesta a tierra conectado al enchufe para establecer una conexión fija al sistema de comunicación, como

se muestra en el diagrama conceptual. Utilice un segundo enchufe bloqueable con puesta a tierra si hay instalado un MDFU.

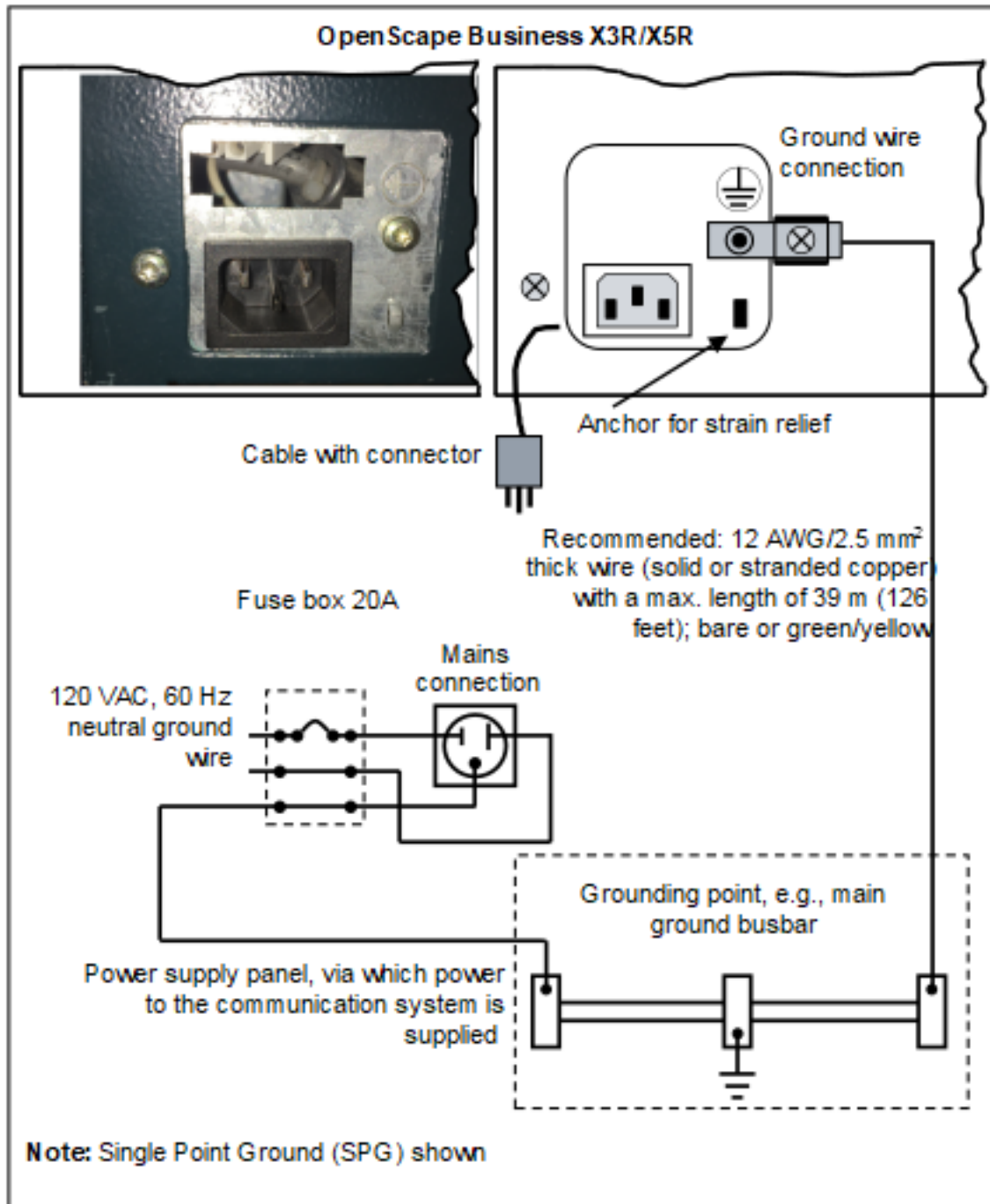


Asegúrese de que todos los conductores de protección de tierra colocados estén protegidos y sin tensión. La sección transversal mínima

del conductor es de 16 AWG/1,5 mm² hasta 2 metros y de al menos 12 AWG/2,5 mm² para 2 o más metros.

- **Solo para EE. UU. y Canadá: Barra principal de toma de tierra**

Conecte el conductor de puesta a tierra independiente con la toma de tierra (por ejemplo, la pica principal de toma de tierra o un electrodo de toma de tierra), tal y como muestra el diagrama conceptual.



Asegúrese de que todos los conductores de protección de tierra colocados estén protegidos y sin tensión. La sección transversal mínima de los conductores es de 12 AWG/2,5 mm². Si no es posible proteger un conductor de puesta a tierra, se necesita una sección transversal mínima

del conductor de 10 AWG/4 mm² para bloquear los efectos de factores externos.

6.2.2.2 Cómo comprobar la puesta a tierra de protección

Requisitos previos

El sistema de comunicación **aún** no está conectado con la red de baja tensión a través del cable de conexión de red.

La puesta a tierra de protección independiente del sistema de comunicación está conectada.

Antes de la puesta en servicio, realice este test para garantizar una correcta puesta a tierra de protección del sistema de comunicación.

Paso a paso

Compruebe la resistencia óhmica del enlace del cable de protección con el sistema de comunicación:

La medición se realiza entre el contacto de puesta a tierra de una caja de conexión de la red doméstica (en el lugar de conexión del sistema de comunicación) y la carcasa del sistema de comunicación.

El resultado (valor nominal) de la medición debe ser claramente inferior a 10 ohmios.

Si se obtuviera otro resultado, póngase en contacto con un técnico eléctrico cualificado. Deberá comprobar la compensación de potencial de la instalación principal y garantizar el bajo ohmiaje del enlace de cable de protección.

6.3 Indicaciones para la configuración

Las Indicaciones para la configuración incluyen información sobre los slots para módulos de los sistemas de comunicación OpenScape Business X3R y OpenScape Business X5R.

6.3.1 Slots de módulos en OpenScape Business X3R

OpenScape Business X3R incluye tres niveles de slots para el equipamiento con módulos y opciones.

- Nivel de slots 1: slots para dos módulos periféricos
- Nivel de slots 2: slot para la placa base OCCMR
- Nivel de slots 3: slots para tres opciones

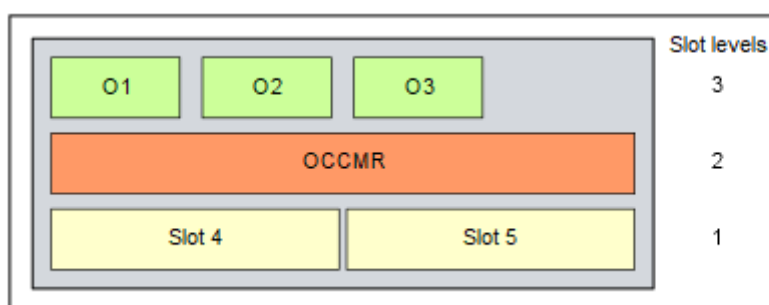


Figura 11: OpenScape Business X3R – Slots de módulos

6.3.2 Slots de módulos en OpenScape Business X5R

OpenScape Business X5R incluye cinco niveles de slots para la asignación con módulos y opciones.

- Niveles de slots 1 a 3: slots para dos módulos periféricos cada uno
- Nivel de slots 4: slot para la placa base OCCMR
- Nivel de slots 5: slots para tres opciones

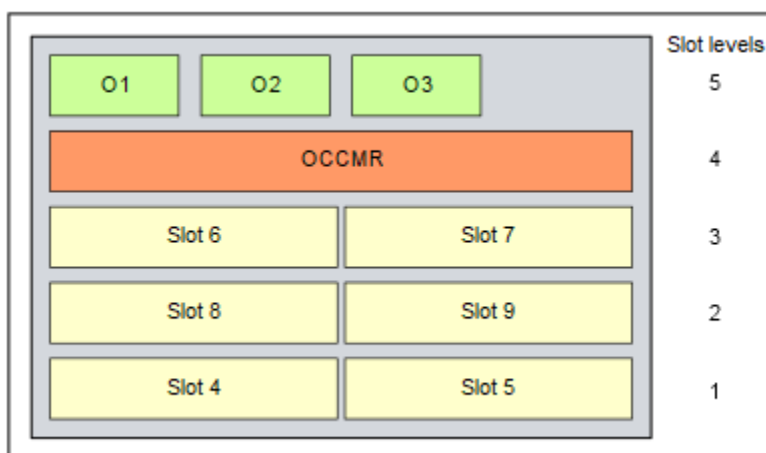


Figura 12: OpenScape Business X5R – Slots de módulos

6.3.3 Instalación de módulos

6.3.3.1 Cómo insertar un módulo

Requisitos previos

Hay disponible un slot para módulos libre.

Nota: Al trabajar con módulos hay que llevar siempre puesto un brazalet de puesta a tierra.

Hay que respetar y seguir las medidas de protección contra descargas electrostáticas (consulte [Indicaciones de aviso: Aviso](#) en la página 16)

Paso a paso

- 1) Suelte los dos tornillos de fijación de la placa de protección del slot para módulos deseado.
- 2) Retire la placa de protección.
- 3) Introduzca el módulo con ayuda de los rieles guía hasta el tope en el slot para módulos.
- 4) Fije el módulo con los dos tornillos de fijación a la carcasa.

6.3.3.2 Cómo retirar un módulo

Requisitos previos

Nota: Al trabajar con módulos hay que llevar siempre puesto un brazalete de puesta a tierra.

Hay que respetar y seguir las medidas de protección contra descargas electrostáticas (consulte [Indicaciones de aviso: Aviso](#) en la página 16)

Paso a paso

- 1) Suelte los dos tornillos de fijación de la placa frontal del módulo que desea retirar.
- 2) Extraiga el módulo del slots para módulos.

6.3.3.3 Cómo montar una placa de protección

Todos los slots para módulos que estén vacíos deben tener una placa de protección para garantizar un blindaje suficiente.

Paso a paso

- 1) Coloque la placa de protección en el slot para módulos vacío.
- 2) Fije la placa de protección a la carcasa con los dos tornillos de sujeción.

6.4 Conexión urbana

Los sistemas de comunicación OpenScape Business X3R y OpenScape Business X5R ofrecen diferentes opciones para la conexión urbana y, con ello, para acceder a la red de comunicación pública.

De entre las siguientes opciones, seleccione la conexión o conexiones de línea urbana requeridas para su sistema de comunicación:

- Conexión de centralita RDSI y acceso individual RDSI a través de una interfaz S₀ (no para EE. UU., Canadá)

- Solo para OpenScape Business X5R: conexión múltiplex primaria RDSI mediante interfaz S_{2M} (no para EE. UU. ni Canadá)
- Solo para OpenScape Business X5R: conexión múltiplex primara RDSI mediante interfaz T1 (solo para EE. UU. y Canadá)
- Solo para OpenScape Business X5R: conexión urbana con protocolo CAS mediante interfaz CAS (solo para algunos países)
- Conexión urbana analógica

6.4.1 No para EE. UU. ni Canadá: Cómo implementar una conexión de centralita RDSI o un acceso individual RDSI mediante una interfaz S_0

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra el sistema de comunicación con conductores de protección independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

Hay al menos una interfaz S_0 libre (placa base OCCMR o módulo periférico STLSX4R, STLS4R).

La interfaz S_0 utilizada se debe configurar como conexión de centralita RDSI o acceso individual RDSI al hacer la puesta en servicio.

Hay disponible una conexión de centralita RDSI o un acceso individual RDSI.

Paso a paso

Conecte la conexión S_0 deseada con el NTBA de la conexión de centralita RDSI o del acceso individual RDSI.

6.4.2 No para EE. UU. ni Canadá: Cómo realizar una conexión múltiplex primaria RDSI mediante la interfaz S_{2M} (solo para OpenScape Business X5R)

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra el sistema de comunicación con conductores de protección independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

OpenScape Business X5R equipa un módulo TS2RN.

Hay disponible una conexión múltiplex primaria RDSI.

Paso a paso

Conecte la interfaz S_{2M} con el NTPM de la conexión múltiplex primaria RDSI.

6.4.3 Solo para EE. UU. y Canadá: Cómo hacer una conexión múltiplex primaria RDSI mediante la interfaz T1 (solo para OpenScape Business X5R)

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra el sistema de comunicación con conductores de protección independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

OpenScape Business X5R equipa un módulo TST1R.

Hay disponible una CSU (Channel Service Unit) aprobada según FCC Parte 68 y que cumple con la directriz ANSI T1.403. La interfaz T1 no se puede conectar directamente a la PSTN (Public Switched Telephone Network). Es necesario activar una CSU entre el sistema de comunicación y la conexión urbana digital. Mediante la CSU, OpenScape Business X5R recibe estas características: aislamiento y protección de sobretensión del sistema de comunicación, opciones de diagnóstico en caso de error (como Signal Loop Back, Inserción de señales de prueba y patrones de prueba) y ajuste de la señal de salida de acuerdo a la longitud de línea especificada por el proveedor de red. Una CSU no es un componente de suministro del sistema de comunicación OpenScape Business X5R.

Hay disponible una conexión múltiplex primaria RDSI.

Paso a paso

Conecte la interfaz T1 con la CSU (Channel Service Unit).

6.4.4 Solo para algunos países: Cómo implementar una conexión de línea urbana mediante la interfaz E1-CAS (solo para OpenScape Business X5R)

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra el sistema de comunicación con conductores de protección independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

OpenScape Business X5R equipa un módulo TCASR-2.

Hay disponible una conexión de línea urbana con el protocolo CAS.

Paso a paso

Conecte la interfaz CAS deseada del módulo TCASR-2 con el NT de la conexión urbana.

6.4.5 Cómo realizar una conexión urbana analógica

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra el sistema de comunicación con conductores de protección independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos TLANI4R con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

El sistema de comunicación equipa al menos un módulo TLANI4R.

Solo para EE. UU., Canadá: hay disponible al menos un elemento de seguridad conforme a UL 497A o CSA C22.2 núm. 226. Las indicaciones de instalación exigen que la conexión de las líneas urbanas analógicas se realicen a través de elementos de seguridad conformes al UL 497A o CSA C22.2 N° 226.

Hay disponible una conexión urbana analógica con sistema de señalización de teléfonos principales (Ground Start/Arranque tierra o Loop Start/Arranque bucle).

Paso a paso

Conecte la conexión a/b deseada del módulo deseado con la toma de conexión TAE de la conexión urbana analógica.

6.5 Conexión de teléfonos y dispositivos

Los sistemas de comunicación OpenScape Business X3W y OpenScape Business X5W ofrecen diferentes opciones para la conexión de teléfonos y dispositivos.

Puede seleccionar las conexiones que requiera para su sistema de comunicación de entre las siguientes opciones:

- Conexión directa de teléfonos RDSI (excepto EE. UU. y Canadá)
- Conexión de teléfonos RDSI mediante el bus S_0 (excepto EE. UU. y Canadá)
- Conexión de teléfonos $U_{P0/E}$
- Conexión de teléfonos y dispositivos analógicos

Nota: Solo se puede conectar un dispositivo analógico a una interfaz a/b.

6.5.1 No para EE. UU., Canadá: cómo conectar directamente teléfonos RDSI

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra el sistema de comunicación con conductores de protección independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Solo para las interfaces que se utilizan para conexiones de extensión: Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos OCCMR, STLSX4R y STLS4R con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

Hay al menos una interfaz S_0 libre (placa base OCCMR o módulo periférico STLSX4R, STLS4R).

Las interfaces S_0 utilizadas tienen que configurarse en la puesta en servicio como una conexión S_0 interna.

Los teléfonos RDSI a conectar deben disponer de alimentación propia, por ejemplo, con un alimentador enchufable. Los módulos OCCMR, STLSX4R y STLS4R no se pueden alimentar mediante las interfaces S_0 .

Paso a paso

1) Conecte la conexión S_0 deseada con el teléfono RDSI.

Consejo:

Siga las indicaciones de las instrucciones de instalación del teléfono que desea conectar.

- 2) Si lo desea, conecte más teléfonos RDSI con el sistema de comunicación siguiendo el mismo procedimiento.

6.5.2 No para EE. UU., Canadá: Cómo conectar teléfonos RDSI por bus S₀

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra el sistema de comunicación con conductores de protección independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Solo para las interfaces que se utilizan para conexiones de extensión: Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos OCCMR, STLSX4R y STLS4R con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

Hay al menos una interfaz S₀ libre (placa base OCCMR o módulo periférico STLSX4R, STLS4R).

Las interfaces S₀ utilizadas tienen que configurarse en la puesta en servicio como una conexión S₀ interna.

Los teléfonos RDSI a conectar deben disponer de alimentación propia, por ejemplo, con un alimentador enchufable. Los módulos OCCMR, STLSX4R y STLS4R no se pueden alimentar mediante las interfaces S₀.

Todos los teléfonos RDSI (extensiones RDSI) deben tener asignado un MSN (Multiple Subscriber Number) único. Esta asignación se realiza en el menú de configuración de la extensión RDSI.

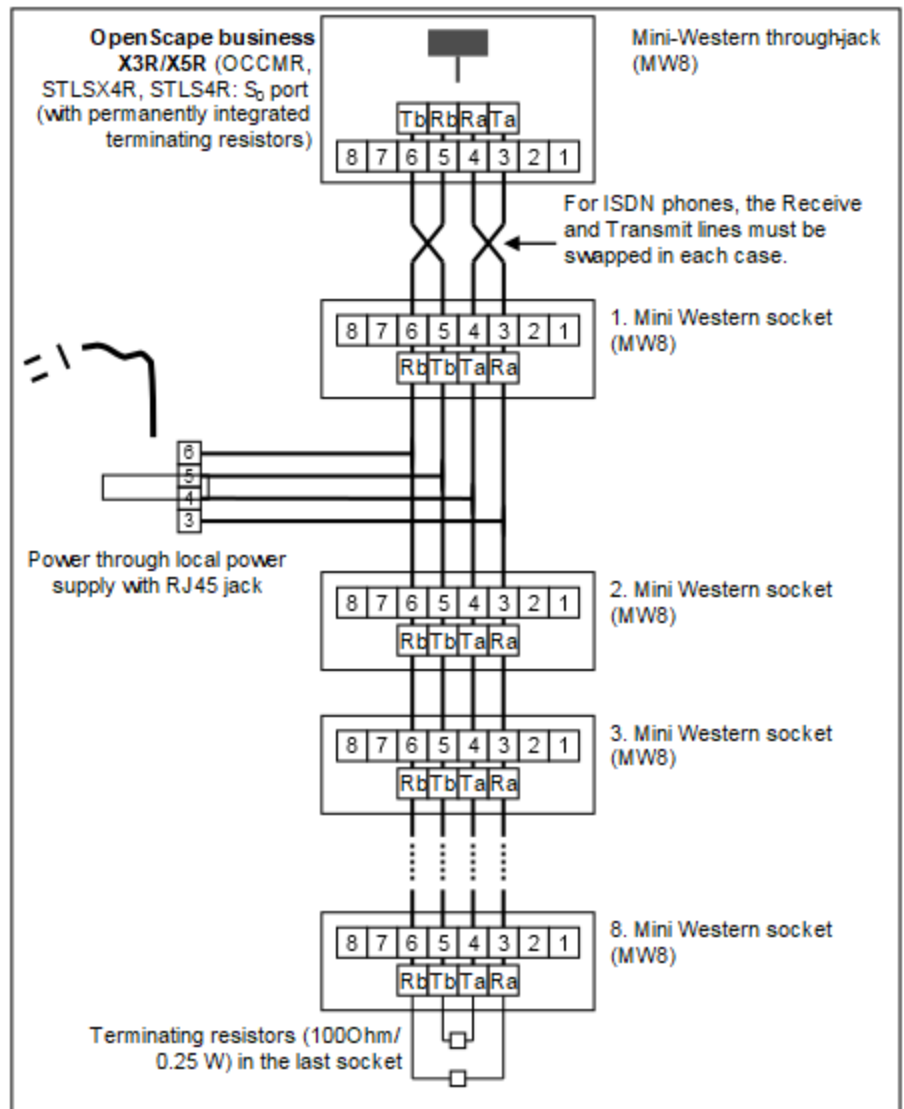
Paso a paso

- 1) Conecte la conexión S_0 deseada con la toma de paso Mini-Western del bus S_0 .

Consejo:

Siga las indicaciones de las instrucciones de instalación del teléfono que desea conectar.

- 2) Para realizar el resto del cableado, siga las indicaciones de la imagen siguiente.



- 3) Instale resistencias de terminación (100 Ohmios/0,25 W) en la última caja de conexión del bus S_0 .

- 4) Asegúrese de que solo hay resistencias de terminación en los dos extremos del bus S_0 . Las demás cajas de conexión del bus S_0 no necesitan resistencias de terminación.

Consejo:

Como las resistencias de terminación ya están integradas en OpenScape Business X3R y en OpenScape Business X5R, el sistema de comunicación constituye uno de los extremos de un bus S_3 .

Consejo:

Siga las indicaciones de las instrucciones de instalación del teléfono que desea conectar.

6.5.3 Cómo conectar teléfonos $U_{P0/E}$

Requisitos previos

**Atención:**

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra el sistema de comunicación con conductores de protección independientes.

**PRECAUCIÓN:**

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos OCCMR y SLU8R con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

Hay al menos una interfaz $U_{P0/E}$ libre (placa base OCCMR o módulo periférico SLU8R).

Paso a paso

- 1) Conecte la conexión $U_{P0/E}$ deseada con el teléfono $U_{P0/E}$.

Consejo:

Siga las indicaciones de las instrucciones de instalación del teléfono que desea conectar.

- 2) Si lo desea, conecte más teléfonos $U_{P0/E}$ con el sistema de comunicación siguiendo el mismo procedimiento.

6.5.4 Cómo conectar dispositivos y teléfonos analógicos

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra el sistema de comunicación con conductores de protección independientes.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos OCCMR, SLAD8R y 8SLAR con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

Hay disponible al menos una interfaz a/b libre (placa base OCCMR o módulos periféricos SLAD8R, 8SLAR).

Paso a paso

- 1) Conecte la conexión a/b deseada con el teléfono analógico o el dispositivo analógico que desee conectar (fax, módem, TFE-S, etc.).

Consejo:

Siga las indicaciones de las instrucciones de instalación del teléfono o dispositivo que desea conectar.

- 2) Si lo desea, conecte más teléfonos o equipos analógicos con el sistema de comunicación siguiendo el mismo procedimiento.

6.6 Tareas finales

Para finalizar el montaje hay que insertar la tarjeta SDHC, hacer una prueba visual y conectar el sistema a la red eléctrica.

A continuación se puede poner en servicio el sistema de comunicación con el OpenScape Business Assistant (gestión basada en web). Encontrará la descripción correspondiente en la ayuda en línea de la gestión basada en web o en el capítulo "Instalación inicial de OpenScape Business" de la documentación para el administrador.

Nota: En la puesta en servicio inicial del sistema de comunicación no está definido el estado de carga del acumulador en la placa base. Para conseguir una carga suficiente, el sistema debe estar al menos 2 días conectado con la red eléctrica. Si el sistema se desconecta de la red y el nivel de carga del acumulador es insuficiente, puede que se bloquee el periodo de activación por manipulación del tiempo.

6.6.1 Cómo insertar la tarjeta M.2 SSD o la tarjeta SDHC (sistema con OCCM)

La tarjeta M.2 SSD o la tarjeta SDHC contiene el software de comunicación OpenScape Business y deben montarse/insertarse antes de la puesta en servicio del sistema de comunicación.

Paso a paso

- 1) Compruebe que la protección contra escritura de la tarjeta SDHC esté desactivada (interruptor en dirección de los contactos metálicos).
- 2) Si todavía no lo ha hecho, inserte la tarjeta SDHC en el slot para tarjetas SDHC de la placa base, hasta que encaje. Los contactos metálicos de la tarjeta SDHC deben ir en dirección de la placa base.

6.6.2 Cómo efectuar la prueba visual

Antes de poner en servicio el sistema de comunicación hay que efectuar una prueba visual del hardware, del cableado y del suministro de tensión.

Requisitos previos



PELIGRO:

Descarga eléctrica al tocar los cables con tensión

Desconecte todos los circuitos de suministro del sistema de comunicación antes de comenzar con la prueba visual:

- Desconecte la tensión de acumulador, la tensión de alimentación (LUNA2) y la tensión de red de todos los powerbox OpenScape Business que pudiera haber conectados
 - Si hay conectado un powerbox OpenScape Business, desconecte las líneas de conexión.
 - Si hay un set de acumuladores conectores o un acumulador conectado, tienda las líneas de conexión.
 - Extraiga el conector de red del sistema de comunicación.
-

Nota:

Al trabajar con módulos hay que llevar siempre puesto un brazalete de puesta a tierra.

Hay que respetar y seguir las medidas de protección contra descargas electrostáticas (consulte [Indicaciones de aviso: Aviso](#) en la página 16).

Paso a paso

- 1) Desconecte todos los circuitos de corriente de suministro del sistema de comunicación.
- 2) Compruebe si el sistema de comunicación está sin tensión.
- 3) Compruebe si la tarjeta SDHC está bien encajada. La protección contra escritura de la tarjeta SDHC debe estar desactivada (interruptor en dirección de los contactos metálicos).
- 4) Compruebe que los módulos encajan perfectamente.
Si es necesario, compruebe que los módulos correspondientes están bien insertados (consulte [Cómo insertar un módulo](#)).
- 5) Compruebe si hay placas de protección en slots de módulos vacíos.
Si es necesario, monte las placas de protección que falten (consulte [Cómo montar una placa de protección](#)).
- 6) Compruebe que todos los cables de conexión están bien tendidos. Por ejemplo, ¿hay riesgo de tropezar?
Si es necesario, tienda correctamente los cables de conexión y de unión.
- 7) Compruebe si hay conectado un conductor de protección independiente en la conexión del conductor de protección del sistema de comunicación.
Si es necesario, realice la puesta a tierra de protección independiente del sistema de comunicación (véase [Puesta a tierra de protección con montaje en armario de 19 pulgadas](#) y [Puesta a tierra de protección con montaje mural e independiente](#)).

- 8) Compruebe si la tensión nominal del suministro de tensión de red coincide con la tensión nominal del sistema de comunicación (placa de características).

6.6.3 Cómo conectar el sistema a la red eléctrica

Paso a paso

Inserte el cable de conexión de red en la toma del suministro de corriente. El sistema de comunicación arranca.

Nota: Deje el sistema conectado a la red eléctrica durante 2 días al menos para que el acumulador de la placa base se cargue lo suficiente. Si la carga es insuficiente es posible que el periodo de activación se bloquee por manipulación del tiempo si se producen repetidos arranques.

7 Instalación de hardware por OpenScape Business X8

Se describe el montaje estándar más frecuente del sistema de comunicación OpenScape Business X8.

OpenScape Business X8 es un sistema de comunicación modular que se puede utilizar como sistema de box único (armario básico) o como sistema de box doble (armario básico + armario de ampliación). OpenScape Business X se puede montar de forma autónoma o en un armario de 19 pulgadas.



Atención:

Descarga eléctrica al tocar los cables con tensión

- Solo se puede trabajar con la carcasa abierta si el sistema está sin tensión.
- Antes de iniciar cualquier trabajo, compruebe si todos los circuitos de corriente están sin tensión. Jamás dé por sentado que al desconectar un fusible o un interruptor principal se han interrumpido efectivamente todos los circuitos de corriente.

7.1 Tipos de montaje

OpenScape Business X se puede montar de forma autónoma o en un armario de 19 pulgadas.

7.1.1 Montaje autónomo

OpenScape Business X8 es un sistema de comunicación modular que se puede utilizar como sistema de box único (armario básico) o como sistema de box doble (armario básico + armario de ampliación). En un armario de doble box, los armarios del sistema se pueden montar sobrepuestos o uno al lado del otro.

7.1.1.1 Cómo montar un sistema de box único

Requisitos previos

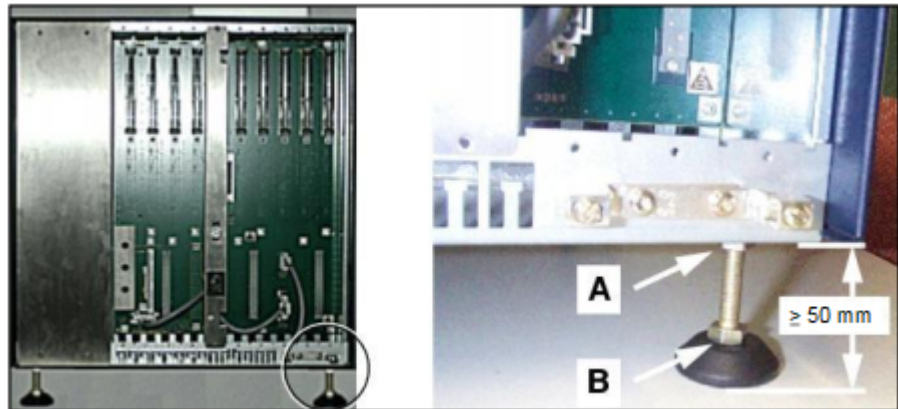
Se han atendido los requisitos para elegir el lugar de montaje autónomo (consulte [Requisitos para la instalación](#) en la página 31).

La cubierta de plástico delantera y trasera del armario del sistema no están montadas.

Paso a paso

- 1) Coloque el armario del sistema en el lugar de montaje y asegúrese de que el lugar elegido es estable y no presenta desniveles.
- 2) Verifique que la distancia entre el borde inferior del armario del sistema y el suelo no es inferior a la distancia mínima de 50 mm.

- 3) Si es necesario, oriente el armario del sistema del siguiente modo:
- Suelte la contratuerca [A] de una pata con ayuda de una llave de boca (ancho de llave = 13 mm).
 - Modifique la altura de la pata girando la tuerca de rosca [B] de forma que el armario del sistema quede recto y se mantenga la distancia mínima.
 - Fije la pata apretando la contratuerca [A].
 - Si es necesario, repita los pasos de a-c para las demás patas, hasta que el armario del sistema esté recto y se respete la distancia mínima.



7.1.1.2 Sistema de box doble: Cómo montar superpuestos los armarios del sistema

Requisitos previos

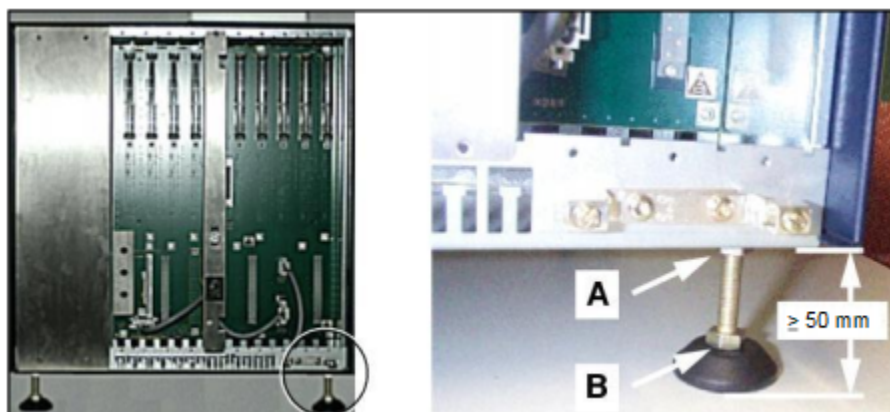
Se han atendido los requisitos para elegir el lugar de montaje autónomo (consulte [Requisitos para la instalación](#) en la página 31).

La cubierta de plástico delantera y trasera de los armarios del sistema no están montadas.

Paso a paso

- Coloque el armario básico en el lugar de montaje y asegúrese de que el lugar elegido es estable y no presenta desniveles.
- Verifique que la distancia mínima de 50 mm entre el borde inferior del armario básico y el suelo no es inferior.

- 3) Si es necesario, oriente el armario básico del siguiente modo:
- Suelte la contratuerca [A] de una pata con ayuda de una llave de boca (ancho de llave = 13 mm).
 - Modifique la altura de la pata girando la tuerca de rosca [B] de forma que el armario básico quede recto y se mantenga la distancia mínima.
 - Fije la pata apretando la contratuerca [A].
 - Si es necesario, repita los pasos a-c para las demás patas, hasta que el armario básico quede recto y se mantenga la distancia mínima.



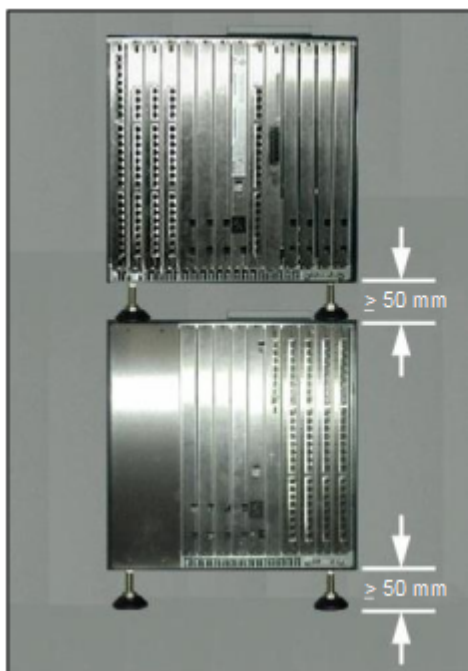
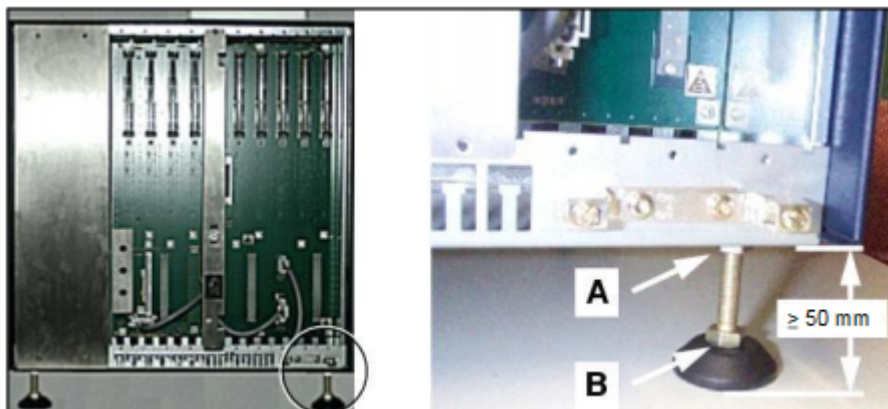
- 4) Coloque el armario de ampliación sobre el armario básico.

Las patas de los armarios del sistema están provistas de hendiduras. Al colocar el armario de ampliación, asegúrese de que estas hendiduras queden justamente en las cabezas de los tornillos de las cuatro esquinas del armario básico.



- 5) Verifique que la distancia entre el armario de ampliación y el armario básico no es inferior a la distancia mínima de 50 mm.

- 6) Si es necesario, oriente el armario de ampliación del siguiente modo:
- Suelte la contratuerca [A] de una pata con ayuda de una llave de boca (ancho de llave = 13 mm).
 - Modifique la altura de la pata girando la tuerca de rosca [B] de forma que el armario de ampliación quede recto y se mantenga la distancia mínima.
 - Fije la pata apretando la contratuerca [A].
 - Si es necesario, repita los pasos a-c para las demás patas, hasta que el armario básico quede recto y se mantenga la distancia mínima con el armario básico.



7.1.1.3 Sistema de doble box: Cómo montar armarios del sistema superpuestos

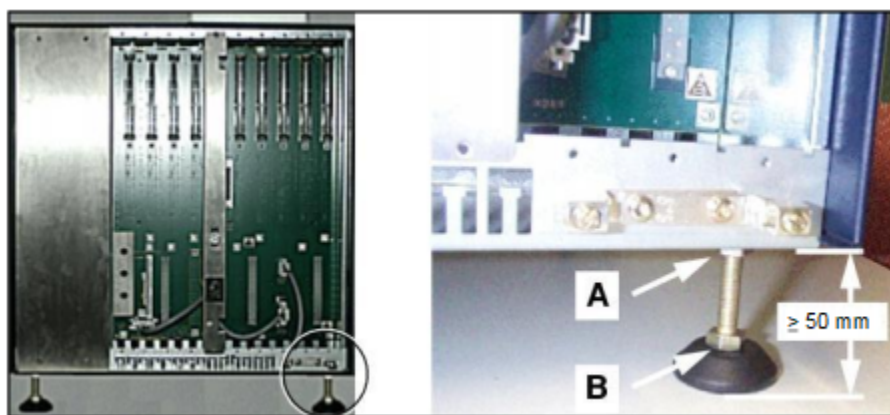
Requisitos previos

Se han atendido los requisitos para elegir el lugar de montaje autónomo (consulte [Requisitos para la instalación](#) en la página 31).

La cubierta de plástico delantera y trasera de los armarios del sistema no están montadas.

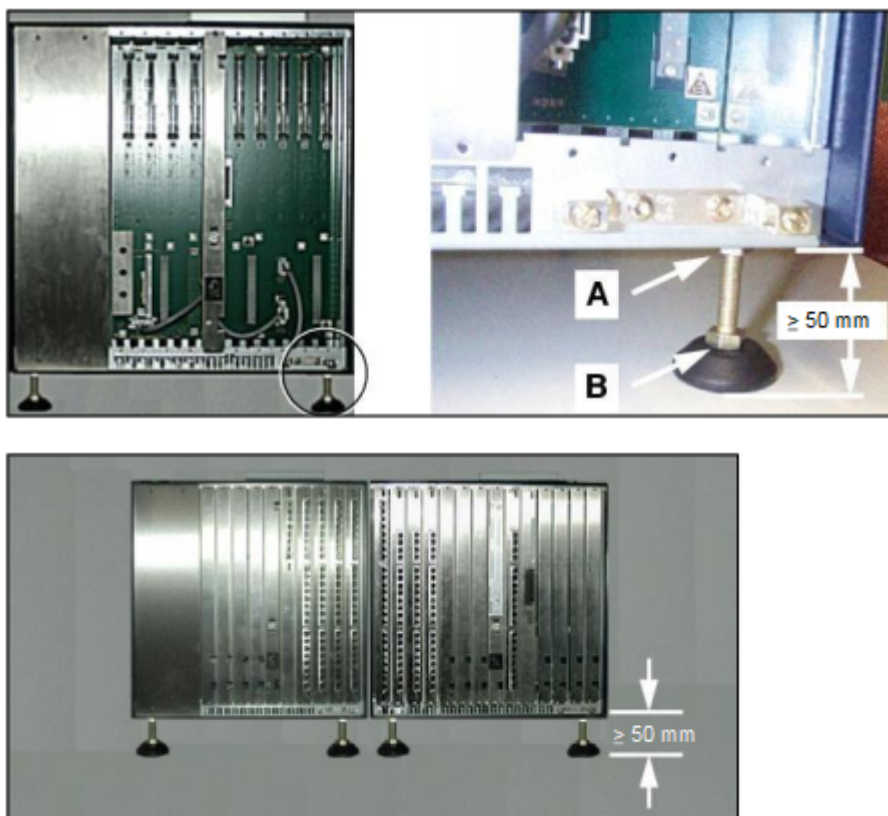
Paso a paso

- 1) Coloque el armario básico en el lugar de montaje y asegúrese de que el lugar elegido es estable y no presenta desniveles.
- 2) Verifique que la distancia mínima de 50 mm entre el borde inferior del armario básico y el suelo no es inferior.
- 3) Si es necesario, oriente el armario básico del siguiente modo:
 - a) Suelte la contratuerca [A] de una pata con ayuda de una llave de boca (ancho de llave = 13 mm).
 - b) Modifique la altura de la pata girando la tuerca de rosca [B] de forma que el armario básico quede recto y se mantenga la distancia mínima.
 - c) Fije la pata apretando la contratuerca [A].
 - d) Si es necesario, repita los pasos a-c para las demás patas, hasta que el armario básico quede recto y se mantenga la distancia mínima.



- 4) Coloque el armario de ampliación junto al armario básico.
- 5) Verifique que la distancia mínima de 50 mm entre el borde inferior del armario de ampliación y el suelo no es inferior.

- 6) Si es necesario, oriente el armario de ampliación del siguiente modo:
- Suelte la contratuerca [A] de una pata con ayuda de una llave de boca (ancho de llave = 13 mm).
 - Modifique la altura de la pata girando la tuerca de rosca [B] de forma que el armario de ampliación quede recto y se mantenga la distancia mínima.
 - Fije la pata apretando la contratuerca [A].
 - Si es necesario, repita los pasos a-c para las demás patas, hasta que el armario de ampliación quede recto y se mantenga la distancia mínima.



7.1.2 Montaje en armario de 19 pulgadas

OpenScape Business X8 es un sistema de comunicación modular que se puede montar como sistema de box único (armario básico) o de box doble (armario básico + armario de ampliación) en un armario de 19 pulgadas.

7.1.2.1 Cómo montar un armario de sistema en un rack de 19 pulgadas

Requisitos previos

Los requisitos previos para seleccionar el lugar de montaje para una instalación con rack de 19 pulgadas se han tenido en cuenta (véase [Requisitos para la instalación](#) en la página 31).

Las cubiertas de plástico delantera y trasera no están puestas en el armario del sistema.

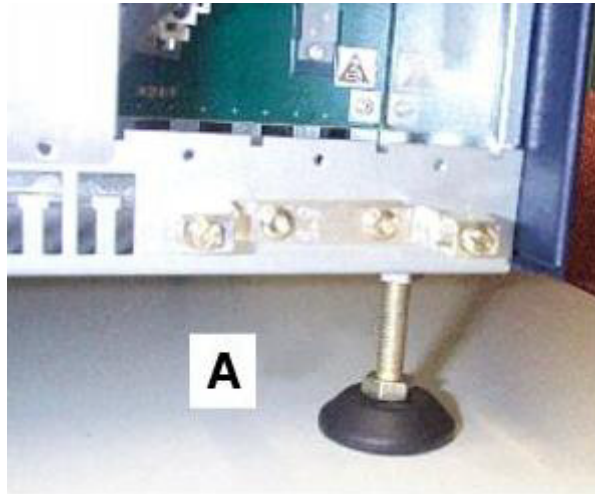
Hay disponibles dos soportes de montaje específicos para el armario (con una carga máxima > 40 kg). Debe incluirlos entre el material el propio proveedor del armario de 19 pulgadas.

Nota: No está permitido utilizar suelos en los armarios, para prevenir el sobrecalentamiento.

Se dispone de los tornillos específicos para el armario, que unirán los ángulos y los soportes de montaje al bastidor o rack de 19 pulgadas.

Paso a paso

- 1) Retire las cuatro patas del armario del sistema:
 - a) Desenrosque la tuerca [A] de una de las patas con una llave de boca abierta (tamaño de la llave = 13 mm).
 - b) Desenrosque la pata por completo.
 - c) Repita los pasos a y b para las otras tres patas del armario.



- 2) Fije los dos soportes angulares incluidos [B] a los laterales de la caja del sistema con los tornillos también incluidos.

Instalación de hardware por OpenScape Business X8

Paneles de interconexión (opcional)

- 3) Fije un soporte de montaje derecho y otro izquierdo [C] al bastidor de 19 pulgadas, con los tornillos incluidos.



- 4) Levante la caja del sistema hasta situarla en el bastidor de 19 pulgadas y colóquela sobre los dos soportes de montaje [C]. Deslice la caja del sistema por el bastidor de 19 pulgadas hasta que el borde delantero de la misma quede a ras con la parte delantera del bastidor de 19 pulgadas.



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

No intente levantar una caja de sistema para instalarla en el bastidor de 19 pulgadas sin ayuda.

- 5) Utilice los dos soportes angulares [B] y los tornillos incluidos para fijar la caja del sistema al bastidor de 19 pulgadas.
- 6) Si desea instalar un armario de ampliación, repita los pasos 1 a 6.

7.2 Paneles de interconexión (opcional)

Para una instalación con montaje en armario de 19 pulgadas del sistema de comunicación OpenScape Business X8, los teléfonos, las líneas, etc. se pueden conectar a través del panel de interconexión externo.

Panel de interconexión S30807-K6143-X

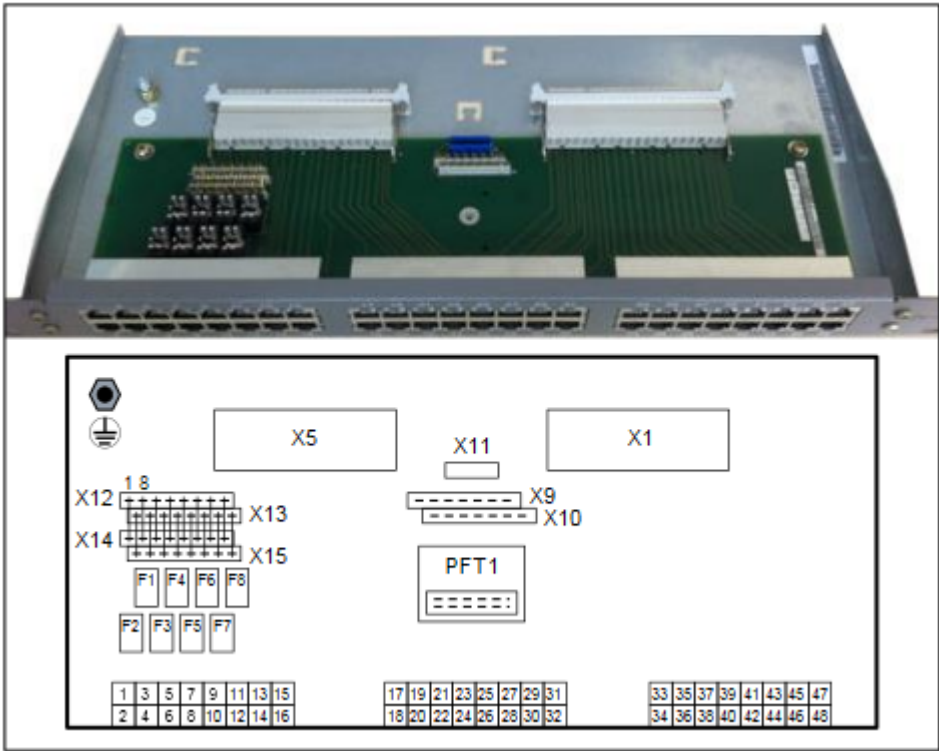


Figura 13: Panel de interconexión S30807-K6143-X

Características principales

- Dos conectores SIVAPAC (X1, X5) para la conexión al backplane del sistema de comunicación mediante unidades CABLU (unidades de cableado preconfeccionadas de fábrica)

Es preciso insertar puentes entre las regletas de terminales X12 y X14, y también entre las regletas de terminales X13 y X15, utilizando cable jumper de puente. El contacto entre el conector SIVAPAC X5 y las 8 primeras tomas RJ45 solamente se establece cuando hay presentes cables de puente.

A la hora de conectar teléfonos, líneas urbanas, etc. mediante puentes directamente a las regletas de terminales X12 y X13, no hacen falta puentes de cable.

- 48 tomas RJ45 (1 a 48) para la conexión de teléfonos, líneas urbanas, etc.

Tabla 1: Panel de interconexión S30807-K6143-X - Asignación de las tomas RJ45

Pin	Señal
4	a
5	b

Las tomas RJ45 están ocupadas con dos hilos.

- Ocho slots para conductores de descarga de sobretensión (F1 a F8)

Nota:

Peligro de incendio por sobretensión

Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos analógicos y de línea de usuario digital con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza instalando conductores de descarga de sobretensión (con gas) en el panel de interconexión.

Consejo: X9, X10, X11 y PFT1 no se usan con OpenScape Business.

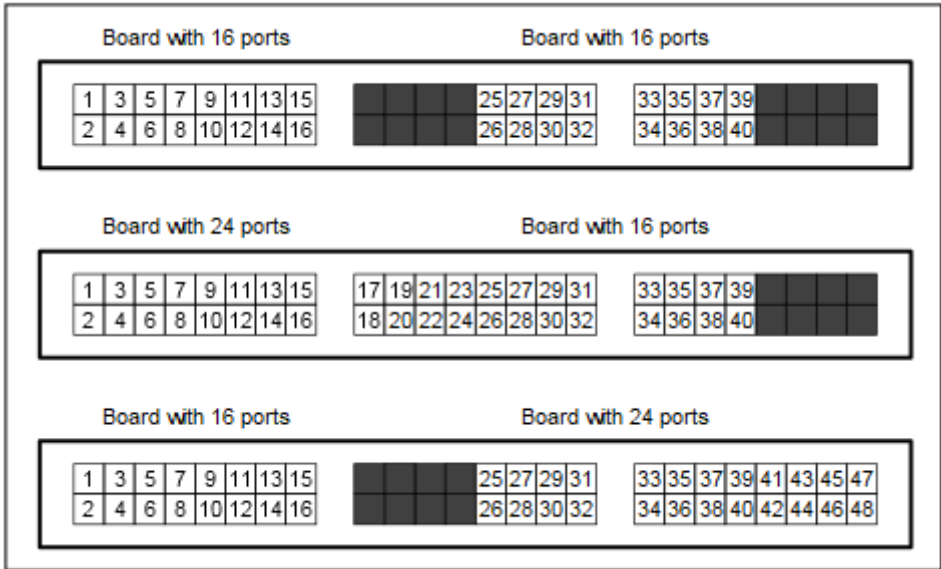


Figura 14: Panel de interconexión S30807-K6143-X – Uso de las 48 tomas RJ45

La figura anterior muestra el uso de las 48 tomas RJ45, dependiendo del número de interfaces de los módulos periféricos conectados.

Panel de interconexión S₀ C39104-Z7001-B3

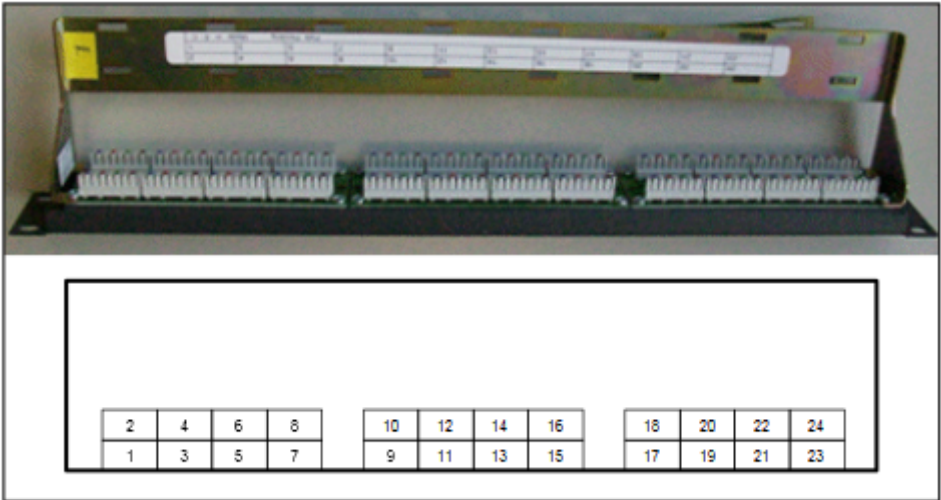


Figura 15: Panel de interconexión S₀ C39104-Z7001-B3

Características principales

- 24 tomas RJ45 (1 a 24) para la conexión de teléfonos RDSI, líneas urbanas RDSI, etc.

La conexión al backplane del sistema de comunicación se realiza mediante cables de extremo abierto que deben fijarse manualmente al panel de interconexión S₀.

Tabla 2: Panel de interconexión S₀ C39104-Z7001-B3 - Asignación de las tomas RJ45

Pin	Señal	
	Conexión de línea urbana/Interconexión	Conexión de extensión
3	Enviar +	Recibir +
4	Recibir +	Enviar +
5	Recibir –	Enviar –
6	Enviar –	Recibir –

Cada una de las tomas RJ45 debe tener cuatro hilos.

Nota: Si utiliza paneles de interconexión de otro proveedor, debe respetar las instrucciones de instalación y puesta a tierra de protección que facilite el fabricante.

7.2.1 Cómo montar un panel de interconexión en un armario de 19 pulgadas

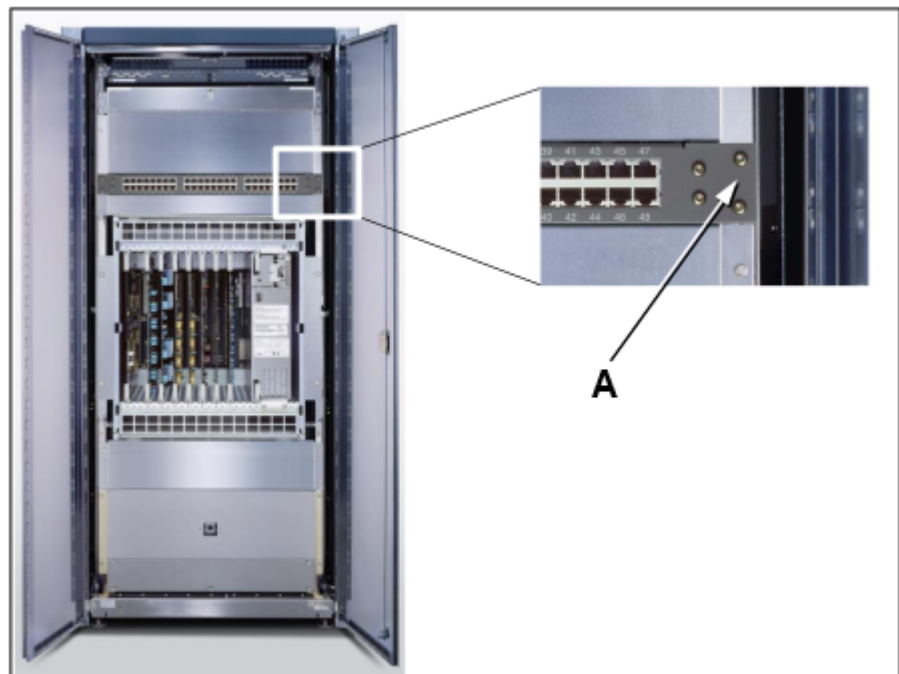
Requisitos previos

Se han tenido en cuenta los requisitos para elegir el lugar de montaje en un armario de 19 pulgadas (consulte [Requisitos para la instalación](#) en la página 31).

Hay tornillos especiales para el armario para fijar el panel de interconexión en el armario de 19 pulgadas.

Paso a paso

Meta el panel de interconexión en el armario de 19 pulgadas y fíjelo con los tornillos previstos para ellos [A] a dicho armario.



7.3 Puesta a tierra de protección

La puesta a tierra de protección permite establecer una conexión segura con el potencial de masa para proteger el sistema de tensiones peligrosas en caso de error.



Atención:

Descarga eléctrica al tocar los cables con tensión

- Ponga a tierra los armarios del sistema de comunicación OpenScape Business X8 y los distribuidores principales y los paneles de interconexión que se pudieran estar utilizando con conductores de protección independientes. Antes de poner en servicio y de conectar los teléfonos y las líneas, conecte los armarios

del sistema de su sistema de comunicación, el distribuidor principal y los paneles de interconexión con el conductor de protección.

- Ha de procurarse un tendido con protección y una descarga de tracción del conductor de protección (sección mínima del conductor = 12 AWG/2,5 mm²). Si puede haber influencias externas sobre un conductor de protección y no se puede realizar un tendido con protección, el conductor de protección deberá tener una sección de 10 AWG/4 mm².

7.3.1 Puesta a tierra de protección con montaje autónomo

La puesta a tierra de protección de los armarios del sistema del sistema de comunicación y de los distribuidores principales que se pudieran estar utilizando se realiza, por ejemplo, a través del embarrado equipotencial del edificio, de una barra colectora de tierra principal o de un campo de puesta a tierra).

7.3.1.1 Cómo establecer una puesta a tierra de protección para el MDFU del distribuidor principal

Requisitos previos

Hay una conexión de puesta a tierra con una resistencia de menos de 2 ohmios. Ejemplos: varilla de compensación de potencial del edificio, pica de toma de tierra principal, electrodo de toma de tierra



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.



Atención:

Descarga eléctrica al tocar los cables con tensión

- Utilice conductores de protección de tierra independientes para establecer una puesta a tierra de protección para los armarios de sistema del sistema de comunicación OpenScape Business X8 y para los distribuidores principales que se puedan estar utilizando. Conecte los armarios de sistema del sistema de comunicación y el distribuidor principal al cable de puesta a tierra antes de poner en servicio el sistema y conectar los teléfonos y líneas.
- Asegúrese de que los conductores de puesta a tierra colocados estén protegidos y sin tensión (sección transversal mínima del conductor = 12 AWG/2,5 mm²). Si no es posible proteger un conductor de puesta a tierra, se necesita una sección transversal

mínima del conductor de 10 AWG/4 mm² para bloquear los efectos de factores externos.

La puesta a tierra de los armarios del sistema debe ejecutarse desde el punto de puesta a tierra, en configuración de estrella.

Es obligatorio cumplir las normas de implementación especificadas en las normativas IEC 60364, IEC 60950-1 e IEC 62368-1 durante la instalación.

Siga este procedimiento para garantizar una correcta puesta a tierra de protección:

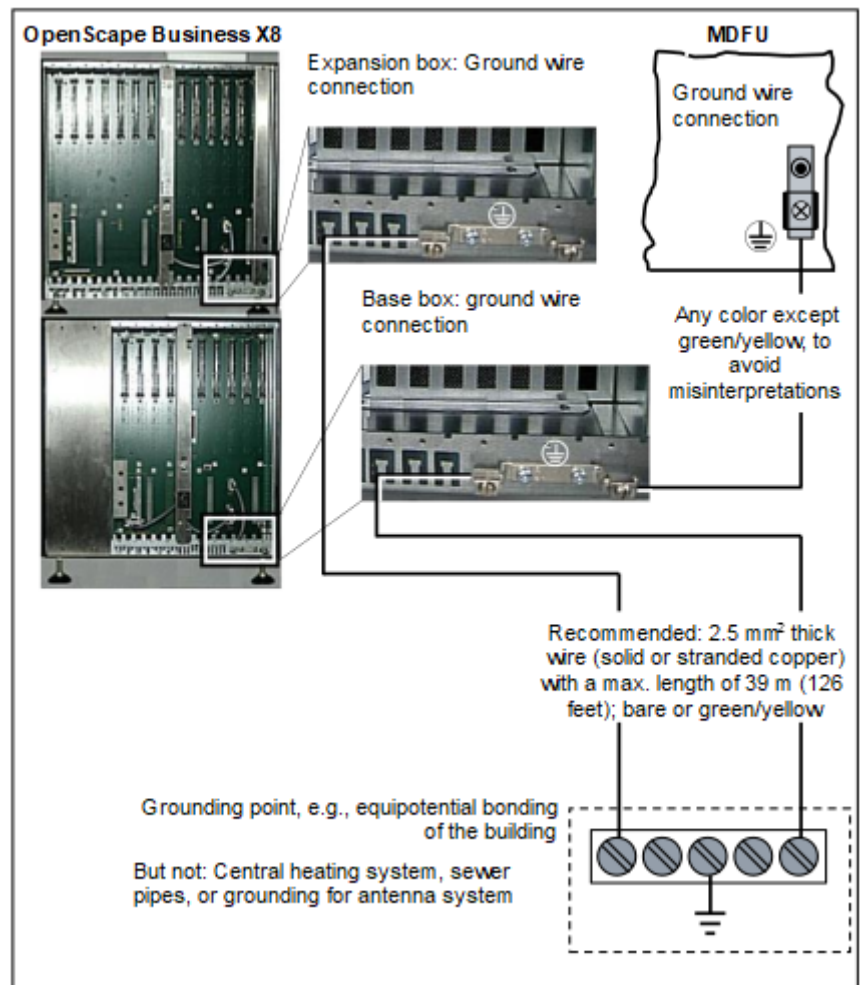
Paso a paso

- 1) Fije un conductor de puesta a tierra independiente al terminal de tierra del armario básico del sistema de comunicación, según se indica en la siguiente figura.



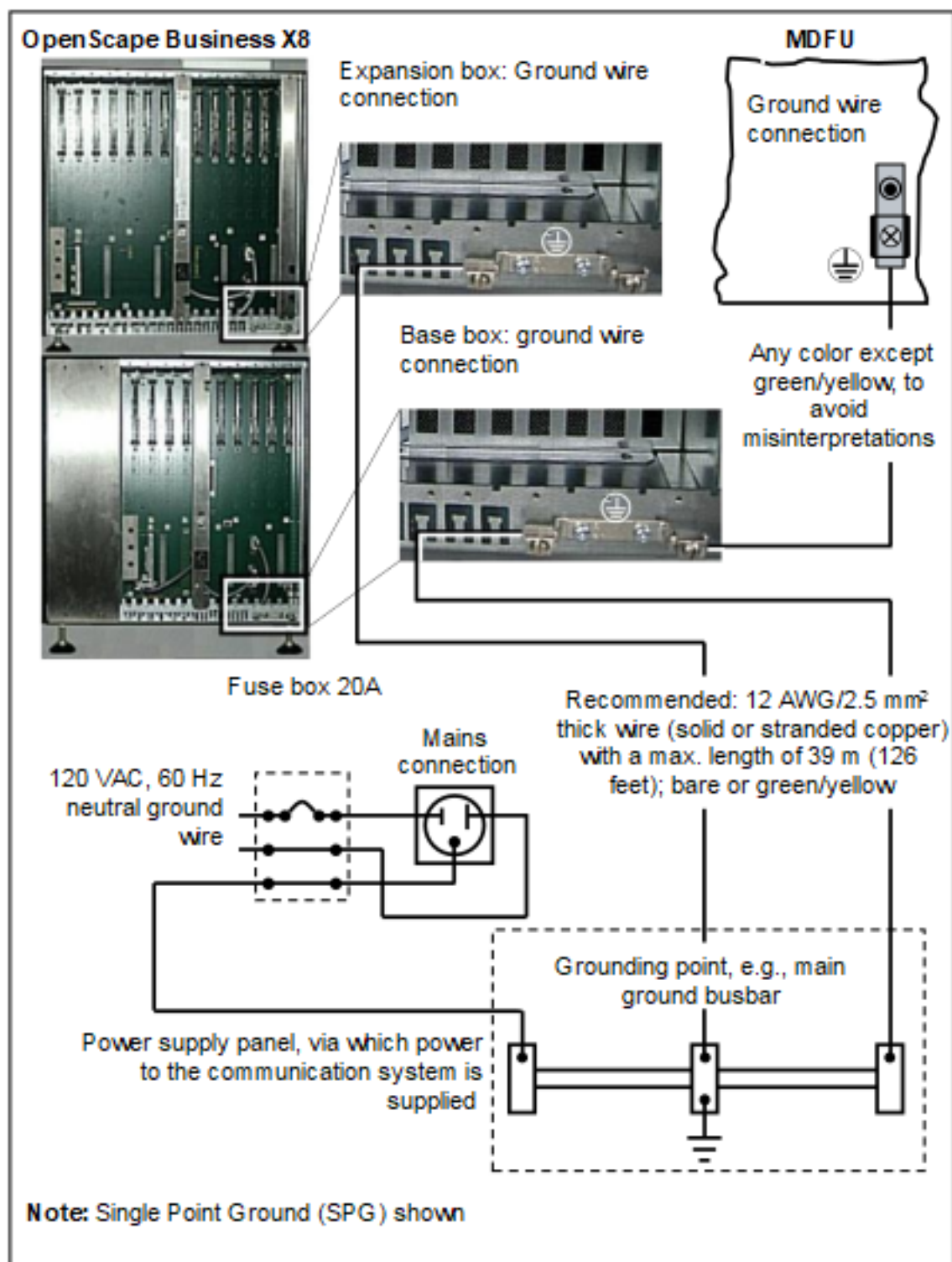
- 2) Utilice una brida para fijar el conductor de puesta a tierra al armario básico y librarlo de cualquier tensión.
- 3) Utilice un conductor de 12 AWG/2,5 mm² de grosor (macizo o de cobre trenzado) con una longitud máxima de 39 metros (126 pies) para conectar el terminal de puesta a tierra del armario básico con el terminal de puesta a tierra del distribuidor principal externo. Para evitar posibles confusiones, puede utilizar cualquier color salvo el verde/amarillo.
- 4) Si hay presente un armario de ampliación: Fije un conductor de puesta a tierra independiente al terminal de tierra del armario básico del sistema de comunicación.
- 5) Si hay presente un armario de ampliación: Utilice una brida para fijar el conductor de puesta a tierra al armario de ampliación y librarlo de cualquier tensión.
- 6) Elija una de estas opciones:
 - **No válido para EE. UU. y Canadá:** Conecte los conductores de puesta a tierra independientes de los armarios del sistema con la toma de tierra (por ejemplo, la varilla de compensación de potencial del edificio), tal y como muestra el diagrama conceptual en la figura a continuación.

Asegúrese de que todos los conductores de protección de tierra colocados estén protegidos y sin tensión.



- **Solo para EE. UU. y Canadá:** Conecte los conductores de puesta a tierra independientes de los armarios del sistema con la toma de tierra (por ejemplo, la pica de toma de tierra principal o un electrodo de toma de tierra), tal y como muestra el diagrama conceptual en la figura a

continuación. Asegúrese de que todos los conductores de protección de tierra colocados estén protegidos y sin tensión.



7.3.1.2 Cómo comprobar la puesta a tierra de protección

Requisitos previos

El armario o armarios del sistema del sistema de comunicación todavía no están conectados a la red de baja tensión con un cable de red.

Se ha conectado la puesta a tierra de protección de cada armario del sistema del sistema de comunicación y de los distribuidores principales que se estén utilizando.

Antes de la puesta en servicio, realice este test para garantizar una correcta puesta a tierra de protección del sistema de comunicación y del distribuidor principal utilizado.

Paso a paso

- 1) Compruebe la resistencia óhmica del enlace del cable de protección con el sistema de comunicación:

La medición se realiza entre el contacto de puesta a tierra de una caja de conexión de la red doméstica (en el lugar de conexión del sistema de comunicación) y un armario del sistema del sistema de comunicación.

- 2) Repita la medición en todos los demás armarios del sistema del sistema de comunicación.

- 3) Compruebe la resistencia óhmica entre los armarios del sistema del sistema de comunicación y los distribuidores principales.

El resultado (valor nominal) de la medición debe ser claramente inferior a 10 ohmios.

Si en una medición se obtuviera otro resultado, póngase en contacto con un electricista profesional. Deberá comprobar la compensación de potencial de la instalación principal y garantizar el bajo ohmiaje del enlace de cable de protección.

7.3.2 Puesta a tierra de protección con montaje en armario de 19"

La puesta a tierra de protección de los armarios del sistema del sistema de comunicación y de los paneles de interconexión que se pudieran estar utilizando se realiza mediante el embarrado equipotencial del armario de 19 pulgadas.

7.3.2.1 Cómo instalar una puesta a tierra de protección para el sistema de comunicación y el panel de interconexión

Requisitos previos

Hay una conexión de puesta a tierra con una resistencia de menos de 2 ohmios. Ejemplos: varilla de compensación de potencial del edificio, pica de toma de tierra principal, electrodo de toma de tierra

El armario de 19 pulgadas se conecta con la puesta a tierra a través de un conductor de puesta a tierra independiente (verde/amarillo). El armario de 19

pulgadas está equipado con una varilla de compensación de potencial, a la que pueden conectarse los armarios de sistema del sistema de comunicación y los paneles de interconexión de forma independiente.



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.



Atención:

Descarga eléctrica al tocar los cables con tensión

- Utilice conductores de protección de tierra independientes para establecer una puesta a tierra de protección para los armarios de sistema del sistema de comunicación OpenScape Business X8 y para los paneles de interconexión que se puedan estar utilizando. Conecte los armarios de sistema del sistema de comunicación y los paneles de interconexión al cable de puesta a tierra antes de poner en servicio el sistema y conectar los teléfonos y líneas.
- Asegúrese de que los conductores de puesta a tierra colocados estén protegidos y sin tensión (sección transversal mínima del conductor = 12 AWG/2,5 mm²). Si no es posible proteger un conductor de puesta a tierra, se necesita una sección transversal mínima del conductor de 10 AWG/4 mm² para bloquear los efectos de factores externos.

La puesta a tierra de los armarios del sistema debe ejecutarse desde el punto de puesta a tierra, en configuración de estrella.

Es obligatorio cumplir las normas de implementación especificadas en las normativas IEC 60364, IEC 60950-1 e IEC 62368-1 durante la instalación.

Nota:

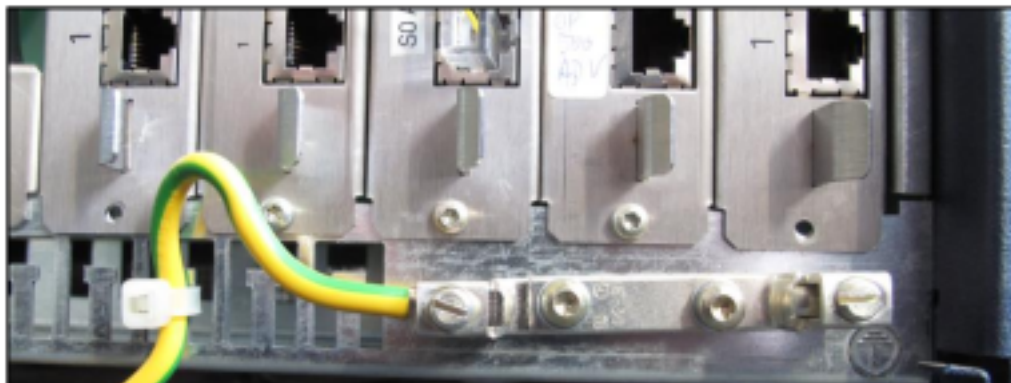
Los requisitos enumerados son aplicables si utiliza paneles de interconexión de otro proveedor.

No es necesaria una puesta a tierra de protección del panel de interconexión S₀ (C39104-Z7001-B3).

Siga este procedimiento para garantizar una correcta puesta a tierra de protección:

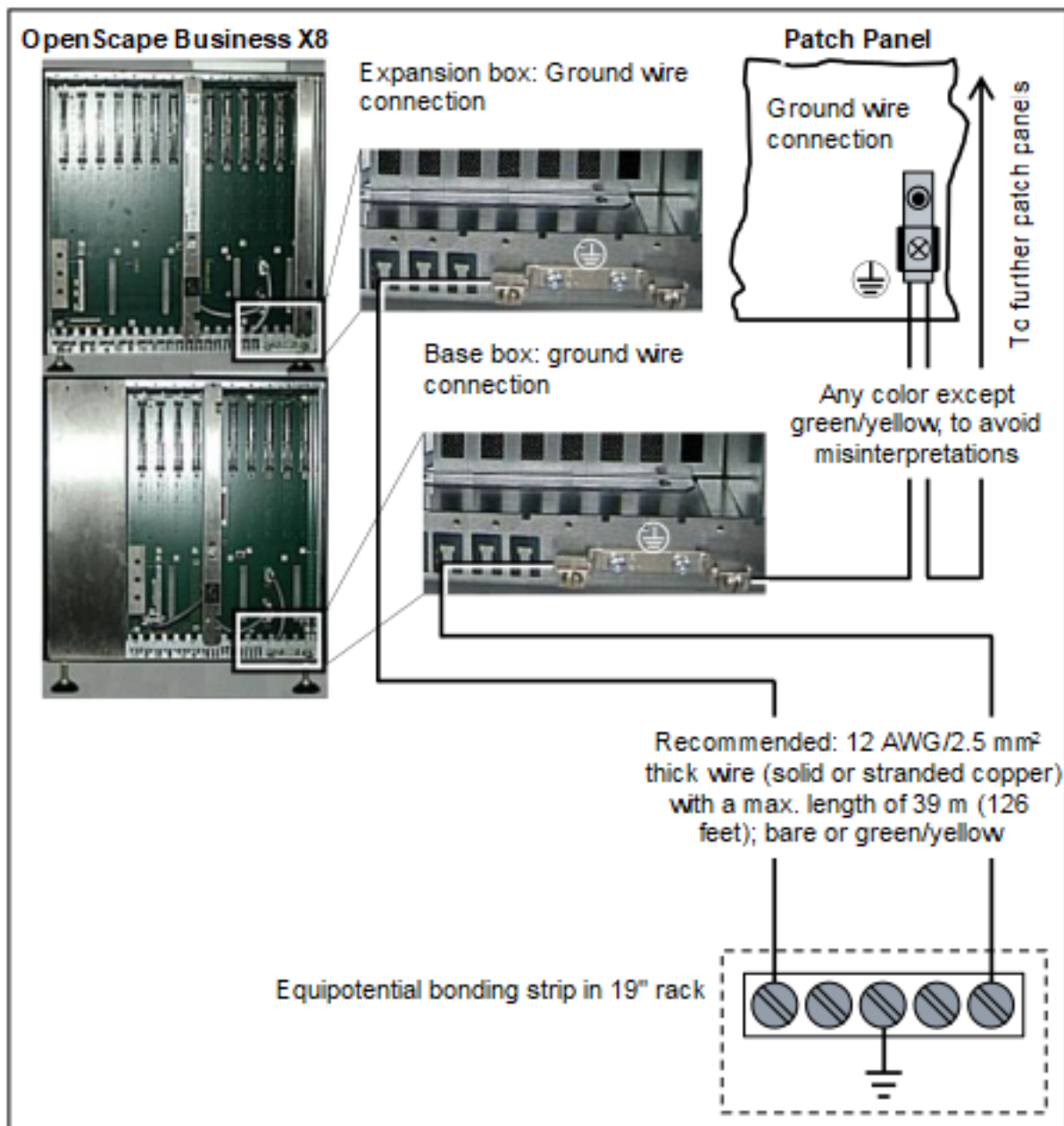
Paso a paso

- 1) Fije un conductor de puesta a tierra independiente al terminal de tierra del armario básico del sistema de comunicación, según se indica en la siguiente figura.



- 2) Utilice una brida para fijar el conductor de puesta a tierra al armario básico y librarlo de cualquier tensión.
- 3) Utilice un conductor de 12 AWG/2,5 mm² de grosor (macizo o de cobre trenzado) con una longitud máxima de 39 metros (126 pies) para conectar el terminal de puesta a tierra del armario básico con el terminal de puesta a tierra del panel de interconexión (S30807-K6143-X). Para evitar posibles confusiones, puede utilizar cualquier color salvo el verde/amarillo.
- 4) Si hay presente un panel de interconexión adicional (S30807-K6143-X): Utilice un conductor de 12 AWG/2,5 mm² de grosor (macizo o de cobre trenzado) con una longitud máxima de 39 metros (126 pies) para conectar los terminales de puesta a tierra de los paneles de interconexión entre sí. Para evitar posibles confusiones, puede utilizar cualquier color salvo el verde/amarillo.
- 5) Si hay presente un armario de ampliación: Fije un conductor de puesta a tierra independiente al terminal de tierra del armario básico del sistema de comunicación.
- 6) Si hay presente un armario de ampliación: Utilice una brida para fijar el conductor de puesta a tierra al armario de ampliación y librarlo de cualquier tensión.
- 7) Conecte los conductores de puesta a tierra independientes de los armarios del sistema con la varilla de compensación de potencial del armario de 19 pulgadas, tal y como muestra el diagrama conceptual en la figura a

continuación. Asegúrese de que todos los conductores de protección de tierra colocados estén protegidos y sin tensión.



7.3.2.2 Cómo comprobar la puesta a tierra de protección

Requisitos previos

Los armarios del sistema del sistema de comunicación y todos los demás dispositivos del armario de 19 pulgadas no están conectados con la red de baja tensión mediante el cable de conexión de red.

La puesta a tierra independiente de cada armario del sistema del sistema de comunicación o del panel de interconexión utilizado está conectada.

El armario de 19 pulgadas debe ponerse a tierra mediante un conductor de protección independiente (verde/amarillo).

Antes de la puesta en servicio, realice este test para garantizar una correcta puesta a tierra de protección del sistema de comunicación y del panel de interconexión utilizado.

Paso a paso

- 1) Compruebe la resistencia óhmica del enlace del cable de protección con el sistema de comunicación:
 - a) La primera medición se realiza entre el contacto de puesta a tierra de una caja de conexión de la red doméstica y el embarrado de equipotencialidad del armario de 19 pulgadas.
 - b) La segunda medición se realiza entre el embarrado de equipotencialidad del armario de 19 pulgadas y un armario del sistema de comunicación.
 - c) Repita la segunda medición con todos los demás armarios del sistema del sistema de comunicación.
- 2) Compruebe la resistencia óhmica entre los armarios del sistema del sistema de comunicación y los paneles de interconexión.

El resultado (valor nominal) de la medición debe ser claramente inferior a 10 ohmios.

Si en una medición se obtuviera otro resultado, póngase en contacto con un electricista profesional. Deberá comprobar la compensación de potencial de la instalación principal y garantizar el bajo ohmiaje del enlace de cable de protección.

7.4 Notas de configuración

Las notas de configuración incluyen información sobre los slots de módulos del armario básico y del armario de ampliación, la puesta en servicio de los módulos, la distribución de las líneas múltiplex PCM del armario básico y del armario de ampliación, así como sobre la instalación de módulos.

7.4.1 Slots de módulos del armario básico

El módulo básico dispone de 9 slots para módulos periféricos (slots 1 a 5 y 7 a 10). Un slot fijo está asignado a la placa base OCCL u OCCLA (slot 6). Según lo requiera, puede utilizar hasta tres fuentes de alimentación LUNA2 en el armario básico.

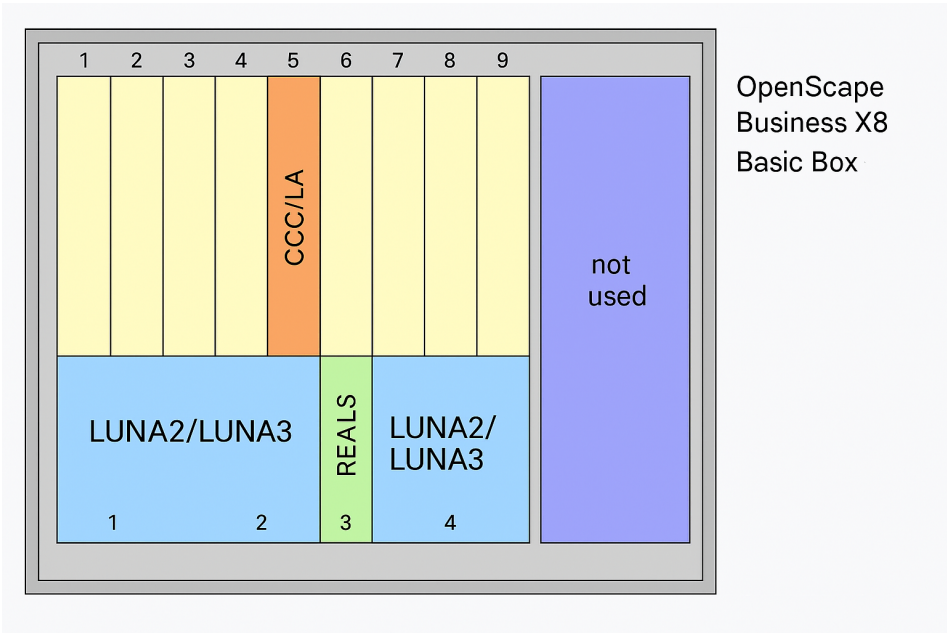


Figura 16: OpenScape Business X8 – Slots de módulos del armario básico

7.4.2 Slots de módulos en el armario de ampliación

En el armario de ampliación hay trece slots para módulos periféricos (slots 1 a 6 y 8 a 14). Según la necesidad, el suministro de corriente LUNA2 se puede utilizar hasta cuatro veces en el armario de ampliación.

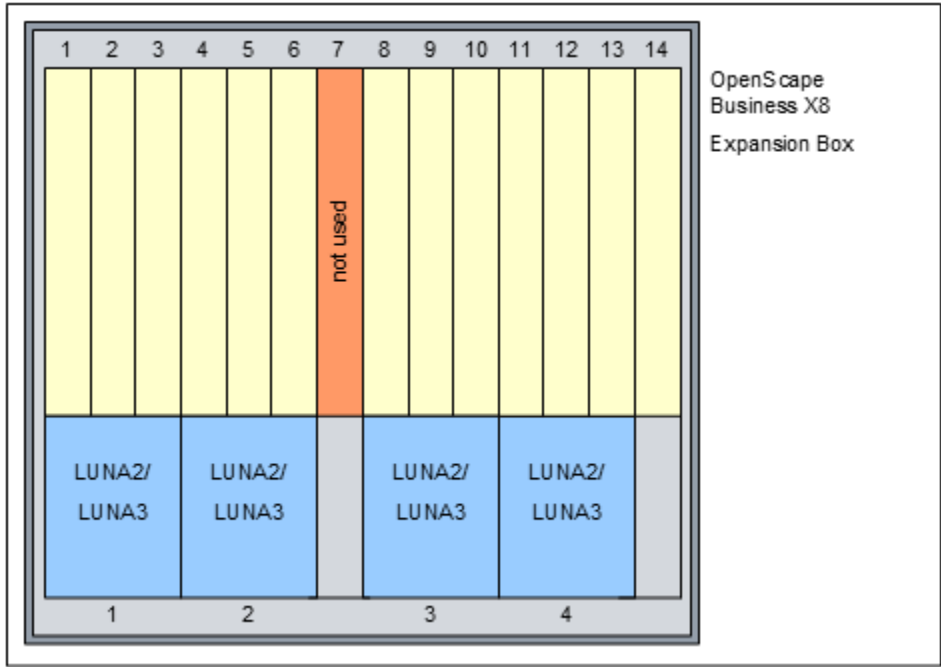


Figura 17: OpenScape Business X8 – Slots para módulos del armario de ampliación

7.4.3 Slots de módulos especiales

Los siguientes módulos se usan con slots especiales.

DBSAP

El módulo DBSAP forma parte del envío del armario de ampliación y se conecta en el conector de backplane correspondiente del armario de ampliación de fábrica.

LUNA2

Los slots para el LUNA2 se encuentran en la parte inferior del soporte para módulos de los armarios del sistema. En el armario básico hay tres slots y en el armario de ampliación, cuatro.

Nota:

El módulo LUNA2 solo puede insertarse o extraerse con el sistema desconectado (con el conmutador de alimentación en posición = DC-OFF).

Antes de poner en servicio el sistema de comunicación, los slots de las fuentes de alimentación deben cubrirse con paneles exteriores.

REALS

El slot para el REALS se encuentra en la parte inferior del soporte para módulos del armario básico.

Los slots de las fuentes de alimentación y el slot del módulo REALS deben cubrirse con paneles exteriores antes de arrancar el sistema de comunicación.

Si desea información detallada, consulte la descripción del módulo específico.

7.4.4 Inicialización de los módulos

En la puesta en servicio inicial, el software del sistema reconoce e inicializa los módulos en sentido ascendente empezando por el slot más bajo.

Las interfaces de los módulos se ponen en servicio según la dirección de la flecha de la imagen siguiente.

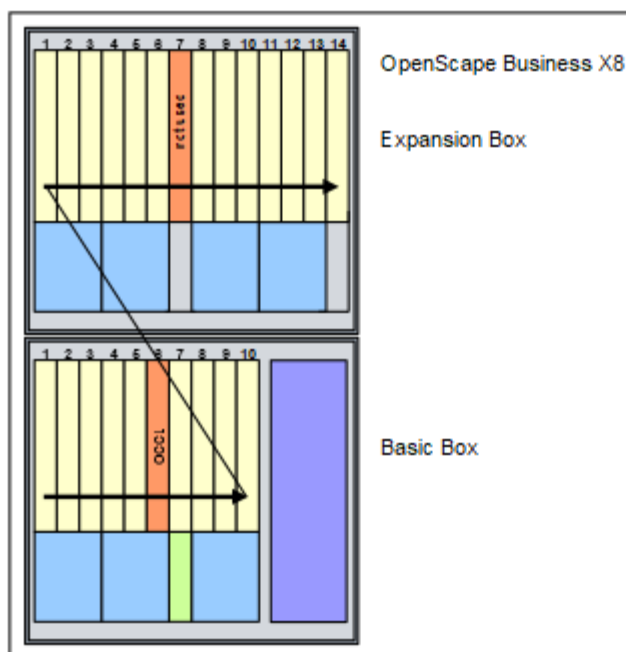


Figura 18: OpenScape Business X8 – Inicialización de los módulos

Todos los módulos enchufados se ponen en servicio cuando

- Todavía no se alcanzado la expansión máxima del sistema de comunicación.

Escaneando en secuencias los slots, el software del sistema comprueba si se ha sobrepasado la cantidad máxima de extensiones o líneas. De ser así, el módulo queda fuera de servicio.

- Con módulos de línea urbana, hay disponible al menos un canal B para el lugar de montaje.

Solo se pone en servicio el número de canales B disponibles del sistema de comunicación.

7.4.5 Distribución de las líneas múltiplex PCM en el armario básico

El armario básico ofrece dos haces de líneas múltiplex PCM con 2 x 4 líneas múltiplex PCM cada uno para los slots de módulos periféricos. Por cada línea múltiplex PCM se dispone de 32 canales múltiplex de tiempo respectivamente. Si están ocupados, no se pueden ejecutar más solicitudes de conversación.

Para garantizar un funcionamiento sin bloqueos, al realizar la instalación de los módulos deberá procurarse que los módulos periféricos de una sección PCM no requieran más que los canales múltiplex de tiempo disponibles.

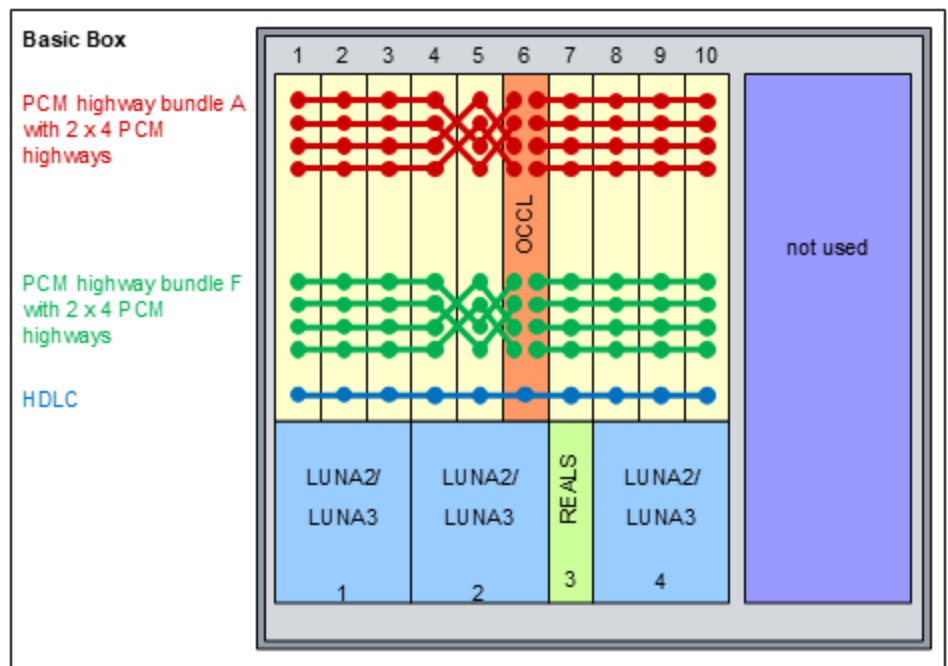


Figura 19: OpenScape Business X8 – Líneas múltiplex PCM en el armario básico

La utilización de los haces de líneas múltiplex PCM del armario básico por módulos periféricos tiene lugar según las siguientes reglas:

- Sistema de box único
 - Haz de líneas múltiplex PCM A

Excepto los módulos DIUT2, DIUN2 y DIU2U, los módulos periféricos solo utilizan las líneas múltiplex PCM del haz A.

Hay disponibles 128 canales múltiplex de tiempo (4 líneas múltiplex PCM) en la sección PCM para los slots para módulos 1 a 5 y en la sección PCM para los slots para módulos 7 a 10.
 - Haz de líneas múltiplex PCM F

Los módulos periféricos DIUT2, DIUN2 y DIU2U utilizan las líneas múltiplex PCM del haz F.

De esta forma, para estos módulos hay disponibles 128 canales múltiplex de tiempo en la sección PCM para los slots de módulos 1 a 5 y en la sección PCM para los slots de módulos 7 a 10.

Si debido al equipamiento con estos módulos, se requieren más de los 2 x 128 canales múltiplex de tiempo del haz de líneas múltiplex PCM F, el sistema de comunicación recurre automáticamente a los canales múltiplex de tiempo del haz de líneas múltiplex PCM A. No obstante, se conectan únicamente módulos completos a la otra troncal. Los demás canales múltiplex de tiempo del haz de líneas múltiplex PCM F permanecen libres.
- Sistema de box doble

Todos los módulos periféricos utilizan exclusivamente las líneas múltiplex PCM del haz A.

7.4.6 Distribución de las líneas múltiplex en el armario de ampliación

El armario de ampliación ofrece un haz de líneas múltiplex PCM con 2 x 4 líneas múltiplex PCM para los slots para módulos periféricos. Por cada línea múltiplex PCM se dispone de 32 canales múltiplex de tiempo respectivamente. Si están ocupados, no se pueden ejecutar más solicitudes de conversación.

Para garantizar un funcionamiento sin bloqueos, al realizar la instalación de los módulos deberá procurarse que los módulos periféricos de una sección PCM no requieran más que los canales múltiplex de tiempo disponibles.

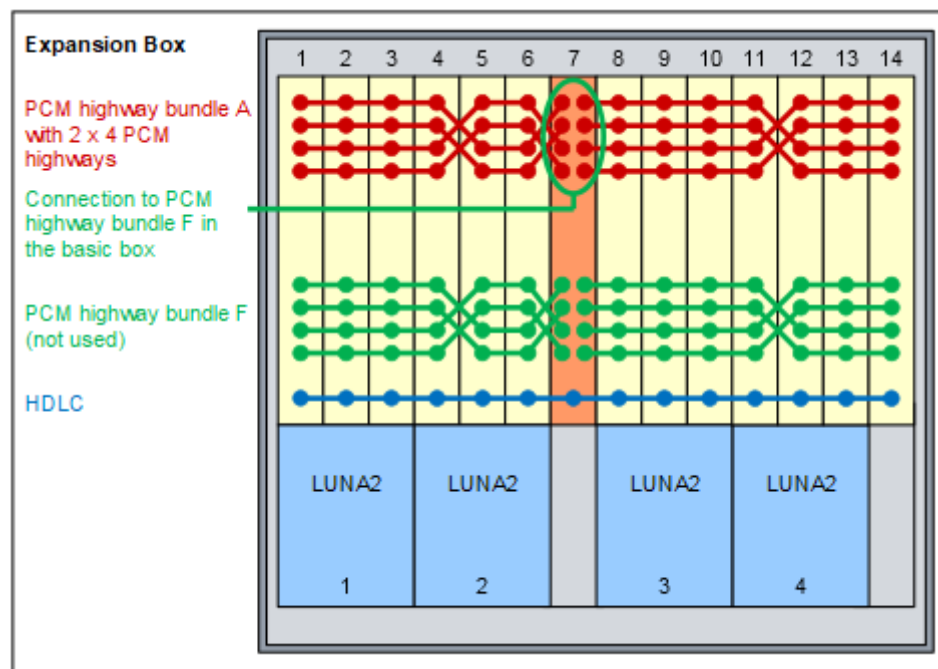


Figura 20: OpenScape Business X8 – Líneas múltiplex PCM en el armario de ampliación

Todos los módulos periféricos de un armario de ampliación utilizan exclusivamente las líneas múltiplex PCM del haz A.

Hay disponibles 128 canales múltiplex de tiempo (4 líneas múltiplex PCM) en la sección PCM para los slots para módulos 1 a 6 y en la sección PCM para los slots para módulos 8 a 14.

El haz de líneas múltiplex PCM F no se utiliza.

7.4.7 Canales múltiplex de tiempo de los módulos periféricos

Para ejecutar solicitudes de llamada, los módulos periféricos requieren un número diferente de canales múltiplex de tiempo. OpenScape Business X8 ofrece estos canales múltiplex de tiempo mediante líneas múltiplex PCM.

OpenScape Business X8 ofrece haces de líneas múltiplex PCM con 2 x 4 líneas múltiplex PCM cada uno para los slots de módulos periféricos. Por cada línea múltiplex PCM se dispone de 32 canales múltiplex de tiempo respectivamente. Si están ocupados, no se pueden ejecutar más solicitudes de conversación. Para garantizar un funcionamiento sin bloqueos del sistema de comunicación, al realizar la instalación de los módulos deberá procurarse que

los módulos periféricos de una sección PCM no requieran más que los canales múltiplex de tiempo disponibles.

En la asignación de canales múltiplex de tiempo mediante módulos periféricos, se distingue entre:

- Asignación estática

En módulos de línea urbana y de tráfico cruzado se realiza una asignación estática de los canales múltiplex de tiempo. De este modo queda garantizado el procesamiento de todas las llamadas.

Nota: El módulo TMDID utiliza exclusivamente la primera mitad de una sección PCM. Con ello, por cada sección PCM se dispone de como máximo 64 canales para canales múltiplex de tiempo estáticos del TMDID. Para garantizar un servicio sin bloqueos del sistema de comunicación en la operación del TMDID, los módulos utilizados en una sección PCM no pueden requerir más de 64 canales múltiplex de tiempo estáticos.

Ejemplos de una sección PCM:

2 x TMDID + 1 x DIU2U = 64 canales múltiplex de tiempo estáticos = configuración admisible

1 x TMDID + 1 x TMANI + 1 x DIUT2 = 76 canales múltiplex de tiempo estáticos = configuración inadmisble

1 x TMDID + 2 x SLMO2 = 8 canales múltiplex de tiempo estáticos y 96 dinámicos = configuración admisible

- Asignación dinámica

En el caso de módulos de líneas de extensión tiene lugar una ocupación dinámica de los canales múltiplex de tiempo. Los canales se ocupan con cada llamada y vuelven a liberarse al finalizar la llamada. La cantidad efectiva de canales múltiplex de tiempo necesarios depende de la cantidad de extensiones activas.

- Asignación estática/dinámica

En módulos con interfaces S_0 , la asignación de los canales múltiplex de tiempo se realiza en función del uso de las distintas interfaces S_0 . La asignación estática se realiza cuando se utiliza una interfaz S_0 para la conexión de línea urbana RDSI (línea urbana RDSI). La asignación dinámica se realiza con el uso de una interfaz S_0 para la conexión de extensión RDSI.

Para consultar información sobre la cantidad de canales múltiplex de tiempo que requieren los diferentes módulos periféricos, véase *OpenScape Business X3/X5/X8, Documentación de servicio; Anexo - Ampliación de hardware*.

7.4.8 Instalación de módulos

Los módulos periféricos se pueden insertar y extraer con la alimentación conectada (sin necesidad de desconectarla). Utilice siempre la llave de módulos para extraer e introducir módulos.

La placa base (OCCL u OCCLA) no se debe extraer mientras el sistema esté conectado a la alimentación. En este caso, es preciso desconectar primero el sistema de la alimentación eléctrica.

7.4.8.1 Cómo insertar un módulo

Requisitos previos

La cubierta de plástico delantera del armario de sistema no está puesta.

Hay disponible un slot libre para el módulo.

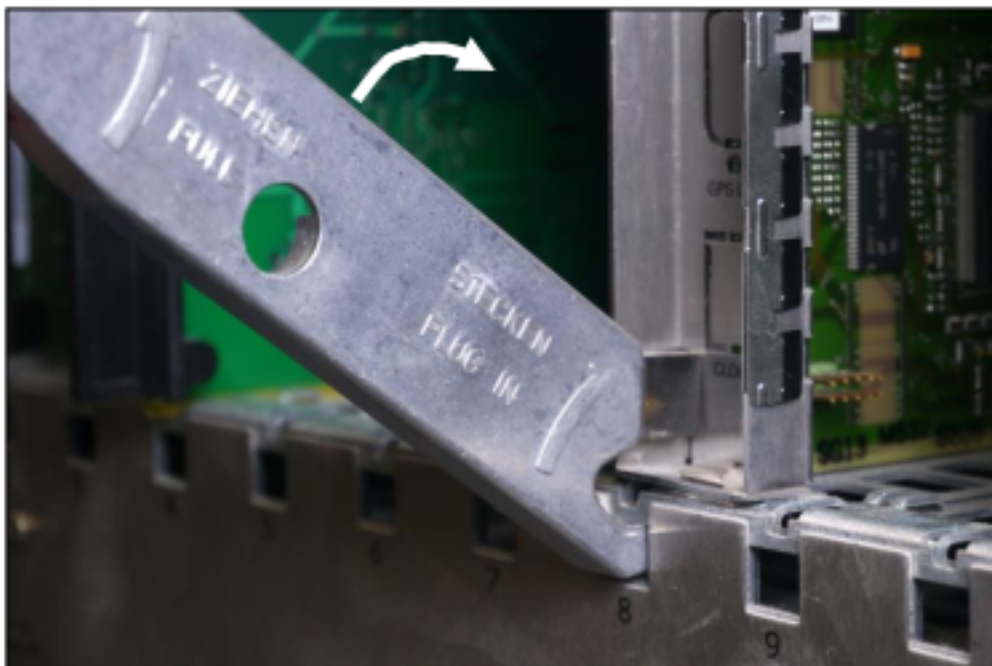
Debe tener en cuenta las especificaciones del distribuidor de líneas múltiplex PCM de los armarios del sistema.

Nota: Siempre que vaya a manipular módulos, debe llevar puesta una pulsera antiestática.

Es obligatorio conocer y respetar las medidas de prevención contra componentes sometidos a cargas electrostáticas (véase [Indicaciones de aviso: Aviso](#) en la página 16).

Paso a paso

- 1) Utilice los rieles guía para introducir el módulo en el armario del sistema deslizándolo hasta que haga tope.
- 2) Introduzca la punta marcada con "Plug In" de la llave de módulos en la ranura inferior de la tapa frontal del módulo.
- 3) Empuje la llave de módulos hacia arriba para hacer palanca e introducir el módulo en el soporte del armario del sistema.



7.4.8.2 Cómo extraer un módulo

Requisitos previos

La cubierta de plástico delantera del armario de sistema no está puesta.

Nota: Siempre que vaya a manipular módulos, debe llevar puesta una pulsera antiestática.

Es obligatorio conocer y respetar las medidas de prevención contra componentes sometidos a cargas electrostáticas (véase [Indicaciones de aviso: Aviso](#) en la página 16).

Paso a paso

- 1) Introduzca la punta marcada con "Pull" de la llave de módulos en la ranura superior de la cubierta frontal del módulo que pretenda extraer.
- 2) Haga palanca para extraer el módulo del soporte del armario del sistema. Para ello, empuje hacia arriba la llave de módulos.



- 3) Extraiga el módulo del armario del sistema deslizándolo sobre los rieles guía.

7.4.8.3 Cómo instalar cubiertas de blindaje

La instalación de una cubierta de blindaje permite asegurar de apantallar de forma segura los slots de módulos no utilizados o aquellos equipados con módulos periféricos que solamente tengan cubiertas de plástico. Esto afecta a los siguientes módulos: STMD3, TMDID, TMEW2, SLMU, SLMAV8N, SLMAV24N.

Instalación de hardware por OpenScape Business X8

Backplanes de los armarios del sistema

Requisitos previos

La cubierta de plástico delantera no está puesta en el armario del sistema.

Paso a paso

- 1) Inserte los dos pasadores inferiores de la cubierta de blindaje en las aberturas que presenta el soporte de módulos para este fin.
- 2) Empuje la cubierta de blindaje hacia el soporte de módulos hasta que encaje en su sitio con un chasquido.



7.5 Backplanes de los armarios del sistema

Los backplanes establecen la conexión entre el control central OCCL, los módulos periféricos y los suministros de corriente LUNA2 y permiten conectar teléfonos, líneas urbanas, etc.

7.5.1 Backplane del armario básico

El backplane del armario básico proporciona la conexión entre la placa de control central OCCLA, los módulos periféricos y las fuentes de alimentación LUNA2. También dispone de conectores para teléfonos, líneas urbanas, etc.

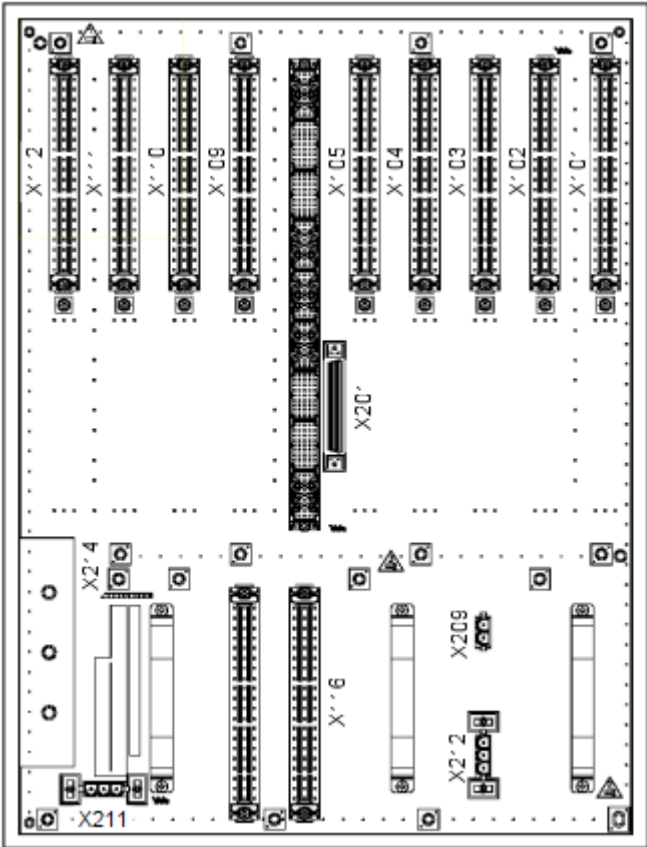


Figura 21: OpenScape Business X8 – Backplane del armario básico

Tabla 3: OpenScape Business X8 – Conexiones en el backplane del armario básico

Conexión	Función
X101 a X105, X109 a X112	Conectores SIVAPAC para recibir las señales de los módulos periféricos instalados en los slots 1 a 5 y 9 a 12 Hay un distribuidor principal externo o paneles de interconexión conectados mediante unidades CABLU (Cabling Units = unidades de cableado preconfeccionadas de fábrica) o cables de extremo abierto. La conexión del panel de interconexión S_0 se realiza a través de un cable de extremo abierto. Es posible conectar los siguientes paneles de conectores a los conectores SIVAPAC: - Panel de conexión con toma CHAMP para conectar un distribuidor principal externo o un panel de interconexión mediante unidades CABLU. - Paneles de conexión con 8 y 24 tomas RJ45 para la conexión directa de teléfonos, líneas urbanas, etc.

Conexión	Función
X116	Conectores SIVAPAC para recibir las señales del módulo REALS Un distribuidor principal externo o paneles de interconexión están conectados a través de un cable de extremo abierto (24 DA): • S30267-Z196-A100: 10 m de longitud • S30267-Z196-A250: 25 m de longitud
X201	Toma DB68 de 68 patillas para conectar el cable al armario de ampliación (es decir, al módulo DBSAP)
X209	Puerto DC
X211, X212	Alimentación CA

7.5.2 Backplane del armario de ampliación

El backplane del armario de ampliación proporciona la conexión entre los módulos periféricos y las fuentes de alimentación LUNA2. También dispone conectores para teléfonos, líneas urbanas, etc.

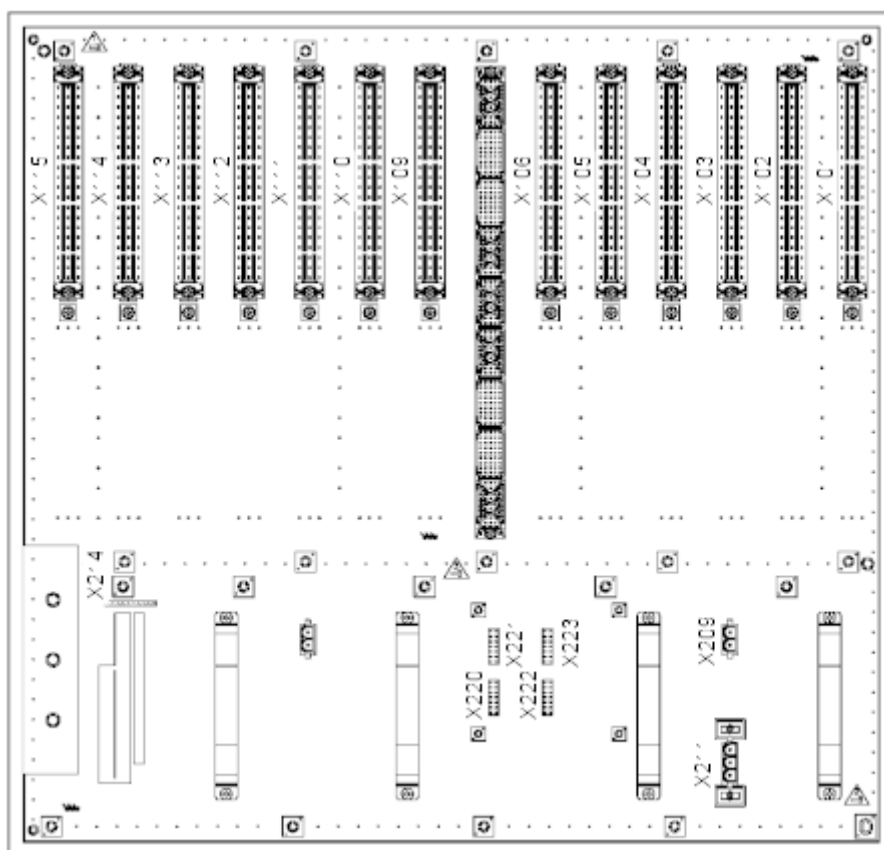


Figura 22: OpenScape Business X8 – Backplane del armario de ampliación

Tabla 4: OpenScape Business X8 – Conexiones en el backplane del armario de ampliación

Conexión	Función
X101 a X106, X109 a X115	Conectores SIVAPAC para recibir las señales de los módulos periféricos instalados en los slots 1 a 6 y 9 a 15 Hay un distribuidor principal externo o paneles de interconexión conectados mediante unidades CABLU (Cabling Units = unidades de cableado preconfeccionadas de fábrica) o cables de extremo abierto. La conexión del panel de interconexión S₀ se realiza a través de un cable de extremo abierto. Es posible conectar los siguientes paneles de conectores a los conectores SIVAPAC: - Panel de conexión con toma CHAMP para conectar un distribuidor principal externo o un panel de interconexión mediante unidades CABLU. - Paneles de conexión con 8 y 24 tomas RJ45 para la conexión directa de teléfonos, líneas urbanas, etc.
X209	Puerto DC
X211	Alimentación CA
X220 a X223	Conexiones para conectar al módulo DBSAP El módulo DBSAP posee una toma DB-68 de 68 patillas para conectar el cable conductor de conexión al armario básico (X201).

7.5.3 Paneles de conexión y de blindaje para backplanes

En el conector SIVAPAC de los backplanes del armario básico y de ampliación se pueden insertar paneles de conexión con toma CHAMP (para conectar el distribuidor principal MDFU-E o un panel de interconexión mediante CABLU) y paneles de conexión con tomas RJ45 (para la conexión directa de teléfonos, líneas urbanas, etc.). El montaje de paneles de blindaje garantiza una protección suficiente del backplane si se utilizan módulos cuyas señales no se pueden detectar mediante paneles de conexión.

Panel de conexión con toma CHAMP (NPPSC, S30807-Q6626-X)



Panel de conexión con 24 tomas RJ45 (NPPAB, S30807-Q6622-X)

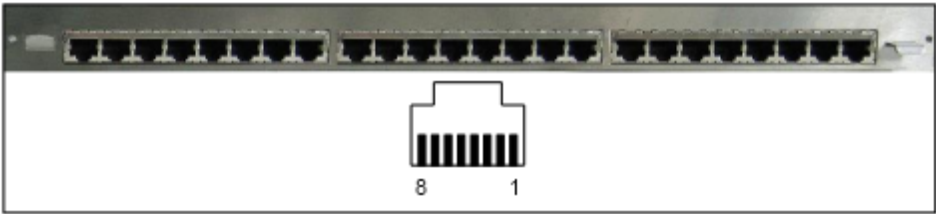


Tabla 5: Panel de conexión con 24 tomas RJ45 – Asignación de las tomas RJ45

Pin	Señal
4	a
5	b
Las tomas RJ45 están ocupadas con dos hilos.	

Panel de conexión con 8 tomas RJ45 (NPPS0, S30807-Q6624-X)

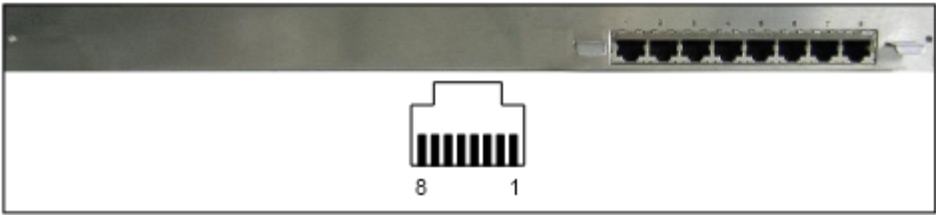


Tabla 6: Panel de conexión con 8 tomas RJ45 – Asignación de las tomas RJ45

Pin	Señal	
	Conexión de línea urbana/ Interconexión	Conexión de extensión
3	Enviar +	Recibir +
4	Recibir +	Enviar +
5	Recibir –	Enviar –
6	Enviar –	Recibir –
Las tomas RJ45 están ocupadas con cuatro hilos.		

Panel de blindaje (C39165-A7075-C44)



7.5.3.1 Cómo montar paneles de conexión o de blindaje

Requisitos previos

La cubierta de plástico trasera del armario del sistema no está montada.

Paso a paso

Elija una de estas opciones:

- Si desea montar un panel de conexión, empújelo en el conector SIVAPAC deseado del backplane.

Fije el panel de conexión al armario del sistema con los dos tornillos incluidos en el volumen de suministro.

- Si desea montar un panel de blindaje, pase los CABLU que pudiera haber por los pasos de cable.

Fije el panel de blindaje al armario del sistema con los dos tornillos incluidos en la entrega.

7.5.4 Conexión en backplanes

Los backplanes del armario básico y de ampliación permiten conectar teléfonos, líneas urbanas, etc. La conexión se puede realizar mediante un distribuidor principal externo o mediante un panel de interconexión externo. La conexión directa con el backplane se puede realizar mediante paneles de conexión con tomas RJ45.

7.5.4.1 Cómo conectar el conductor de conexión entre el armario básico y el armario de ampliación (opcional)

El cable de conexión (C39195-Z7611-A10) se encarga de conducir las señales HDLC, PCM y de temporización desde el armario básico hasta el armario de ampliación.

Requisitos previos

Las cubiertas de plástico de los armarios del sistema no están puestas.

El módulo DBSAP (S30807-Q6722-X) está instalado en el backplane del armario de ampliación.

Paso a paso

- 1) Enchufe uno de los conectores del cable en el conector DB68 de 68 patillas modelo X201 del armario básico.
- 2) Enchufe el otro conector del cable en el conector DB68 de 68 patillas del módulo DBSAP.
- 3) Utilice bridas para fijar ambos extremos del cable de conexión a los armarios del sistema.

7.5.4.2 Cómo instalar un conductor de conexión al distribuidor principal externo (opcional)

Hay varias opciones disponibles para conectar el backplane al distribuidor principal o a cualquier otro distribuidor principal externo. Dependen de qué módulos periféricos ocupen qué slots y de los paneles de conectores utilizados.

Requisitos previos



Atención: Descarga eléctrica al tocar los cables con tensión

Utilice cables conductores independientes para establecer la puesta a tierra de protección de los armarios del sistema del sistema de comunicación y todos los distribuidores principales antes de conectar teléfonos y líneas.

La cubierta de plástico trasera no está puesta en el armario del sistema.

Paso a paso

- 1) Seleccione el conductor de conexión apropiado, dependiendo del módulo periférico y del panel de conectores que utilice.

Si		entonces
Mód. periférico	Panel de conectores	Conductor de conexión
STMD3 TMANI TMDID TMEW2 SLMAV8N	—	Conexión al MDFU-E u otro distribuidor principal externo: cable de extremo abierto (24 DA) con toma SIVAPAC (backplane): • S30267-Z196-A100: 10 m de longitud • S30267-Z196-A250: 25 m de longitud
	Panel de conectores con conector CHAMP	Conexión a distribuidor principal externo: cable con conector CHAMP
SLMU SLMAV24N	—	Conexión al distribuidor principal externo: cable de extremo abierto (24 DA) con toma SIVAPAC (backplane): • S30267-Z196-A100: 10 m de longitud • S30267-Z196-A250: 25 m de longitud
	Panel de conectores con conector CHAMP	Conexión a distribuidor principal externo: cable con conector CHAMP

- 2) Enchufe el cable de conexión al conector del backplane deseado.
- 3) Fije el cable al armario del sistema mediante bridas.

- 4) Seleccione una de las siguientes opciones para establecer la conexión con cualquier distribuidor principal externo:
 - Si utiliza un distribuidor principal externo y un cable de extremo abierto, conecte el cable a la regleta divisora o de clasificación del distribuidor principal externo.
 - Si utiliza un distribuidor principal externo con conectores CHAMP y un cable CHAMP, inserte el conector macho en el conector hembra CHAMP que quiera usar del distribuidor principal externo.
- 5) Fije el cable de conexión al distribuidor principal externo mediante bridas.

7.5.4.3 Cómo conectar los cables de conexión con el panel de interconexión (opcional)

Para la conexión del backplane con el panel de interconexión hay disponibles CABLU (24 DA) con conectores SIVAPAC de 2 m (S30267-Z333-A20) y 5 m (S30267-Z333-A50).

Requisitos previos



Atención: Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra los armarios del sistema del sistema de comunicación y de todos los paneles de interconexión con conectores de protección independientes.

La cubierta de plástico trasera del armario del sistema deseado no está montada.

Paso a paso

- 1) Introduzca el cable de conexión en la conexión de backplane deseada.
- 2) Fije el cable de conexión con bridas al armario del sistema.
- 3) Inserte el cable de conexión en la conexión deseada del panel de interconexión.

Para obtener información sobre la asignación de las tomas RJ45 del panel de interconexión S30807-K6143-X, consulte [Paneles de interconexión \(opcional\)](#) en la página 110.

- 4) Fije el cable de conexión con bridas al panel de interconexión.

7.5.4.4 Cómo conectar el cable de conexión con el panel de interconexión S₀ (opcional)

Para conectar el backplane (Conector SIVAPAC) con el panel de interconexión S₀ hay disponibles cables Open-End (24 DA) de 10 m (S30267-Z196-A100) y 25 m (S30267-Z196-A250)

Requisitos previos



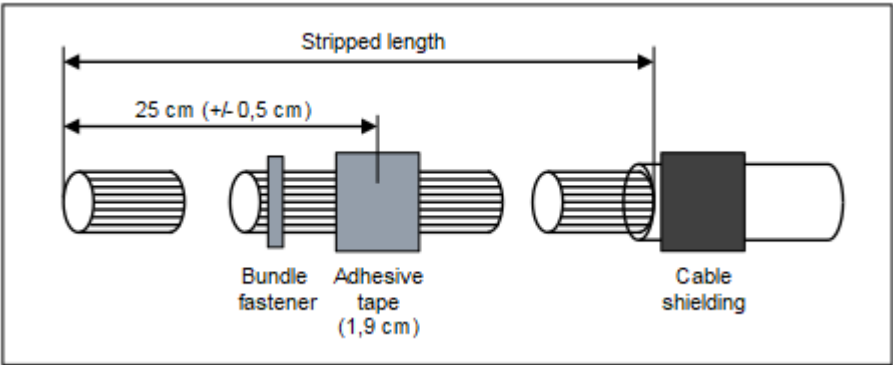
Atención: Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra los armarios del sistema del sistema de comunicación con conductores de protección independientes.

La cubierta de plástico trasera del armario del sistema deseado no está montada.

Paso a paso

- 1) Introduzca el cable de conexión en la conexión de backplane deseada.
- 2) Fije el cable de conexión con bridas al armario del sistema.
- 3) Deje libres los hilos del cable (pelado = 60 cm (+/- 0,5 cm)).



- 4) Pele unos 3 cm el blindaje del cable. Acorte el hilo de drenaje a unos 2,5 cm y fíjelo al blindaje del cable enrollándolo con cinta adhesiva (al menos 1,5 vueltas).
- 5) Tienda los hilos del cable con una herramienta de perforación estándar en el panel de interconexión S₀. Los hilos deben trenzarse antes del tendido (consulte la imagen siguiente).

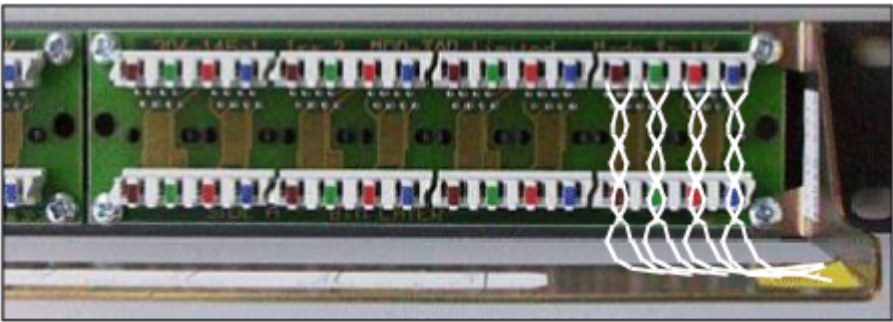


Tabla 7: Código de colores de los cables Open-End

Grupo de colores	Par	Hilo a	Hilo b
1	1	blanco/azul	azul/blanco
	2	blanco/naranja	naranja/blanco
	3	blanco/verde	

Grupo de colores	Par	Hilo a	Hilo b
	4	blanco/marrón	verde/blanco
			marrón/blanco
	5	blanco/gris	
			gris/blanco
2	6	rojo/azul	
			azul/rojo
	7	rojo/naranja	
			naranja/rojo
	8	rojo/verde	
			verde/rojo
	9	rojo/marrón	
			marrón/rojo
	10	rojo/gris	
			gris/rojo
3	11	negro/azul	
			azul/negro
	12	negro/naranja	
			naranja/negro
	13	negro/verde	
			verde/negro
	14	negro/marrón	
			marrón/negro
	15	negro/gris	
			gris/negro
4	16	amarillo/azul	
			azul/amarillo
	17	amarillo/naranja	
			naranja/amarillo
	18	amarillo/verde	
			vd/am
	19	amarillo/marrón	
			marrón/amarillo
	20	amarillo/gris	
			gris/amarillo

Grupo de colores	Par	Hilo a	Hilo b
5	21	violeta/azul	
			azul/violeta
	22	violeta/naranja	
			naranja/violeta
	23	violeta/verde	
			verde/violeta
	24	violeta/marrón	
			marrón/violeta

Para obtener información sobre la asignación de las tomas RJ45 del panel de interconexión S₀ C39104-Z7001-B3 para la conexión de extensiones y para la conexión de línea urbana, consulte [Paneles de interconexión \(opcional\)](#).

6) Fije el cable de conexión con bridas al panel de interconexión S₀.

7.6 Conexión de línea urbana

El sistema de comunicación Openscape Business X8 ofrece diferentes opciones para conexiones de líneas urbanas y con ellas, distintas opciones para acceder a la red de comunicación pública.

Puede seleccionar la conexión o conexiones de línea urbana que requiera para su sistema de comunicación de entre las siguientes opciones:

- conexión de centralita RDSI y conexión de acceso individual RDSI mediante interfaz S₀ (no válido para EE. UU. y Canadá)
- interfaz de línea múltiplex primaria de RDSI mediante interfaz S_{2M} (no válido para EE. UU. y Canadá)
- interfaz de línea múltiplex primaria de RDSI mediante interfaz T1 (no válido para EE. UU. y Canadá)
- conexión de línea urbana con protocolo CAS mediante interfaz CAS (solo para determinados países)
- conexiones de línea urbana analógica

7.6.1 Cómo configurar una conexión de centralita RDSI o una conexión de acceso individual RDSI mediante un puerto S₀ (no válido para EE. UU. y Canadá)

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Utilice cables conductores independientes para establecer la puesta a tierra de protección de los armarios del sistema del sistema de

comunicación y los distribuidores principales y paneles de interconexión antes de conectar teléfonos y líneas.

No es necesaria una puesta a tierra de protección del panel de interconexión S_0 (C39104-Z7001-B3).



PRECAUCIÓN: Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm. (AWG 26) o mayor.

OpenScape Business X8 está equipado al menos con un módulo STMD3.

Durante el arranque, se debe configurar la interfaz S_0 como conexión de centralita RDSI o conexión de acceso individual RDSI.

Hay disponible una conexión de centralita o de acceso individual RDSI.

Paso a paso

Conecte el puerto S_0 deseado con el NTBA de la conexión de centralita o de acceso individual RDSI.

Elija una de estas opciones:

- Si la conexión va a realizarse a través del MDFU del distribuidor principal externo, conecte el conductor de conexión del NTBA a la regleta divisora o regleta de clasificación deseada en el MDFU-E.
- Si la conexión va a realizarse a través del panel de interconexión S_0 externo, conecte el conductor de conexión del NTBA a la toma RJ45 deseada del panel de interconexión S_0 .
- Si la conexión va a realizarse a través del backplane de un armario de sistema (es decir, a través de un panel de conectores con 8 tomas RJ45), conecte el conductor de conexión del NTBA a la toma RJ45 deseada del panel de conectores que quiera.

7.6.2 Cómo configurar la interfaz de línea múltiplex primaria de RDSI mediante un puerto S_{2M} (no válido para EE. UU. y Canadá)

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Utilice cables conductores independientes para establecer la puesta a tierra de protección de los armarios del sistema del sistema de comunicación y los distribuidores principales y paneles de interconexión antes de conectar teléfonos y líneas.



PRECAUCIÓN: Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm. (AWG 26) o mayor.

OpenScape Business X8 está equipado al menos con un módulo DIUT2.

Hay disponible una interfaz de línea múltiplex primaria de RDSI.

Paso a paso

Conecte el conector sub-D deseado del panel delantero del módulo deseado con la NTPM de la interfaz de línea múltiplex primaria de RDSI.

7.6.3 Cómo configurar la interfaz de línea múltiplex primaria de RDSI mediante una interfaz T1 (solo para EE. UU. y Canadá)

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Utilice cables conductores independientes para establecer la puesta a tierra de protección de los armarios del sistema del sistema de comunicación y los distribuidores principales y paneles de interconexión antes de conectar teléfonos y líneas.



PRECAUCIÓN: Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm. (AWG 26) o mayor.

OpenScape Business X8 está equipado al menos con un módulo DIUT2.

Hay disponible una unidad de servicio de canal (Channel Service Unit, CSU) homologada según la normativa Part 68 y que cumple con la norma ANSI T1.403. La interfaz T1 no se puede conectar directamente a la PSTN (Public Switched Telephone Network). Es fundamental que se instale una CSU entre el sistema de comunicación y la conexión de línea digital. La CSU le proporciona las siguientes características a OpenScape Business X8: aislamiento y protección de sobretensión del sistema de comunicación, opciones de diagnóstico en caso de error (como Signal Loop Back, Inserción de señales de prueba y patrones de prueba) y ajuste de la señal de salida de acuerdo a la longitud de línea especificada por el proveedor de red. Una CSU no constituye un componente de entrega del sistema de comunicación OpenScape Business X8.

Hay disponible una interfaz de línea múltiplex primaria de RDSI.

Paso a paso

Conecte el conector sub-D deseado del panel delantero del módulo deseado con la unidad de servicio de canal (Channel Service Unit, CSU).

7.6.4 Solo para algunos países: Cómo hacer una conexión de línea urbana mediante una interfaz E1-CAS

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Antes de conectar los teléfonos y las líneas, ponga a tierra los armarios del sistema de su sistema de comunicación y todos los distribuidores principales y paneles de interconexión con conductores de protección independientes.



PRECAUCIÓN: Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm (AWG 26) o mayor.

OpenScape Business X8 equipa al menos un módulo TMCAS2 o TMCAS.

Hay disponible una conexión de línea urbana con el protocolo CAS.

Paso a paso

Conecte la interfaz CAS deseada de la placa frontal del módulo deseado con el NT de la conexión de línea urbana.

7.6.5 Cómo configurar una conexión con línea analógica

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Utilice cables conductores independientes para establecer la puesta a tierra de protección de los armarios del sistema del sistema de comunicación y los distribuidores principales y paneles de interconexión antes de conectar teléfonos y líneas.



PRECAUCIÓN: Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm. (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos TMANI y TMDID con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

OpenScape Business X8 está equipado al menos con un módulo TMANI o TMDID.

Solo para EE. UU. y Canadá: Hay disponible un protector según UL 497A o CSA C22.2 núm. 226. Por las indicaciones de instalación, la conexión de líneas urbanas analógicas se debe realizar a través de elementos de protección conformes a las normas UL 497A o CSA C22.2 núm. 226.

Está disponible una conexión de línea analógica con HKZ (interfaz de extensión principal) señalizando procedimiento (señalización de arranque por tierra y arranque por bucle).

Paso a paso

Conecte el puerto a/b deseado del módulo que desee con la toma TAE de la conexión de línea analógica.

Elija una de estas opciones:

- Si la conexión va a realizarse a través del MDFU del distribuidor principal externo, conecte el conductor de conexión TAE a la regleta divisora o regleta de clasificación deseada en el MDFU.
- Si la conexión va a realizarse a través del panel de interconexión externo, conecte el conductor de conexión TAE a la toma RJ45 del panel de interconexión.
- Si la conexión va a realizarse a través del backplane de un armario de sistema (es decir, a través de un panel de conectores con 24 tomas RJ45), conecte el conductor de conexión TAE a la toma RJ45 deseada del panel de conectores que quiera.

7.7 Conexión de teléfonos y dispositivos

El sistema de comunicación OpenScape Business X8 ofrece varias opciones para conectar teléfonos y dispositivos.

Puede seleccionar las conexiones que requiera para su sistema de comunicación de entre las siguientes opciones:

- Conexión directa de teléfonos RDSI (excepto EE. UU. y Canadá)
- Conexión de teléfonos RDSI mediante el bus S_0 (excepto EE. UU. y Canadá)
- Conexión de teléfonos $U_{P0/E}$
- Conexión de teléfonos y dispositivos analógicos

Nota: Solo se puede conectar un dispositivo analógico a una interfaz a/b.

7.7.1 Cómo conectar teléfonos RDSI directamente (no válido para EE. UU. y Canadá)

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Utilice cables conductores independientes para establecer la puesta a tierra de protección de los armarios del sistema de comunicación y los distribuidores principales y paneles de interconexión antes de conectar teléfonos y líneas.

No es necesaria una puesta a tierra de protección del panel de interconexión S₀ (C39104-Z7001-B3).



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm. (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Tan solo para las interfaces de conexión de extensiones:

Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger el módulo STMD3 con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

OpenScape Business X8 está equipado al menos con un módulo STMD3.

Los puertos S₀ utilizados deben configurarse en el arranque como una conexión S₀ interna.

Los teléfonos RDSI por conectar deben disponer de alimentación propia, por ejemplo, con un alimentador enchufable. No puede haber alimentación a través de los puertos S₀ del módulo STMD3.

Paso a paso

1) Conecte el puerto S_0 deseado con el teléfono RDSI.

Elija una de estas opciones:

- Si la conexión va a realizarse a través del MDFU-E del distribuidor principal externo, conecte el conductor de conexión del teléfono RDSI a la regleta divisora deseada en el MDFU-E.
- Si la conexión va a realizarse a través del panel de interconexión externo S_0 , conecte el conductor de conexión del teléfono RDSI a la toma RJ45 del panel de interconexión S_0 .
- Si la conexión va a realizarse a través del backplane de un armario de sistema (es decir, a través de un panel de conectores con 8 tomas RJ45), conecte el conductor de conexión del teléfono RDSI a la toma RJ45 deseada del panel de conectores que quiera.

Consejo: Consulte las instrucciones de instalación del teléfono que pretenda conectar.

2) Si hay algún otro teléfono RDSI presente, conéctelos al sistema de comunicación siguiendo este mismo método.

7.7.2 Cómo conectar teléfonos RDSI mediante el bus S_0 (no válido para EE. UU. y Canadá)

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Utilice cables conductores independientes para establecer la puesta a tierra de protección de los armarios del sistema del sistema de comunicación y los distribuidores principales y paneles de interconexión antes de conectar teléfonos y líneas.

No es necesaria una puesta a tierra de protección del panel de interconexión S_0 (C39104-Z7001-B3).



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm. (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Tan solo para las interfaces de conexión de extensiones:
Con líneas que midan más de 500 m y líneas que salgan del

edificio, hay que proteger el módulo STMD3 con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

OpenScape Business X8 está equipado al menos con un módulo STMD3.

Los puertos S_0 utilizados deben configurarse en el arranque como una conexión S_0 interna.

Los teléfonos RDSI por conectar deben disponer de alimentación propia, por ejemplo, con un alimentador enchufable. No puede haber alimentación a través de los puertos S_0 del módulo STMD3.

Es obligatorio asignar a cada teléfono RDSI individual (extensiones RDSI) un número de usuario múltiple (MSN = Multiple Subscriber Number). Esta asignación se realiza en el menú de configuración de la extensión RDSI.

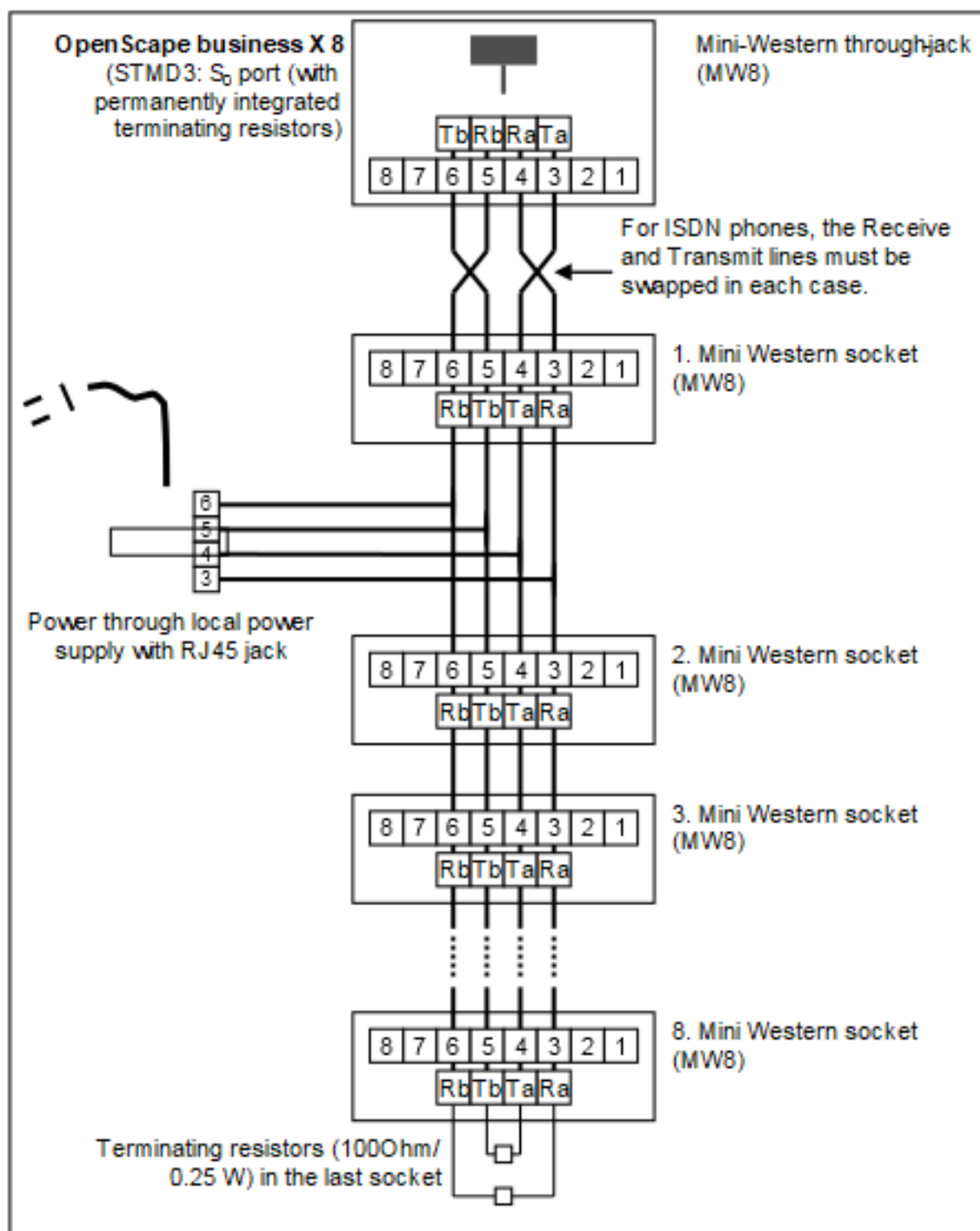
Paso a paso

- 1) Conecte el puerto S_0 deseado con el conector hembra Mini Western del bus S_0 .

Elija una de estas opciones:

- Si la conexión va a realizarse a través del MDFU del distribuidor principal externo, conecte el conductor de conexión del conector hembra Mini Western del bus S_0 a la regleta divisora deseada del MDFU.
- Si la conexión va a realizarse a través del panel de interconexión externo S_0 , conecte el conductor de conexión del conector hembra Mini Western del bus S_0 a la toma RJ45 del panel de interconexión S_0 .
- Si la conexión va a realizarse a través del backplane de un armario de sistema (es decir, a través de un panel de conectores con 8 tomas RJ45), conecte el conductor de conexión del conector hembra Mini Western del bus S_0 a la toma RJ45 deseada del panel de conectores que quiera.

2) Complete el cableado según se indica en el siguiente diagrama.



3) Instale resistencias terminales (100 ohmios/0,25 W) en la última toma del bus S₀.

- 4) Compruebe que las resistencias terminales solamente se conecten a los dos extremos del bus S_0 . No son necesarias resistencias terminales para las demás tomas del bus S_0 .

Consejo: Dado que las resistencias terminales ya están integradas en OpenScape Business X8, el sistema de comunicación conforma un extremo de un bus S_0 .

Consejo: Consulte las instrucciones de instalación del teléfono que pretenda conectar.

7.7.3 Cómo conectar teléfonos $U_{P0/E}$

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Utilice cables conductores independientes para establecer la puesta a tierra de protección de los armarios del sistema del sistema de comunicación y los distribuidores principales y paneles de interconexión antes de conectar teléfonos y líneas.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm. (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos SLMO2 y SLMO8 con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

OpenScape Business X8 está equipado al menos con un módulo SLMU.

Paso a paso

1) Conecte el puerto $U_{P0/E}$ deseado con el teléfono $U_{P0/E}$.

Elija una de estas opciones:

- Si la conexión va a realizarse a través del MDFU del distribuidor principal externo, conecte el conductor de conexión del teléfono $U_{P0/E}$ a la regleta divisora o regleta de clasificación deseada en el MDFU.
- Si la conexión va a realizarse a través del panel de interconexión externo, conecte el conductor de conexión del teléfono $U_{P0/E}$ a la toma RJ45 deseada del panel de interconexión.
- Si la conexión va a realizarse a través del backplane de un armario de sistema (es decir, a través de un panel de conectores con 24 tomas RJ45), conecte el conductor de conexión del teléfono $U_{P0/E}$ a la toma RJ45 deseada del panel de conectores que quiera.

Consejo: Consulte las instrucciones de instalación del teléfono que pretenda conectar.

2) Si hay algún otro teléfono $U_{P0/E}$ presente, conéctelos al sistema de comunicación siguiendo este mismo método.

7.7.4 Cómo conectar teléfonos y dispositivos analógicos

Requisitos previos



Atención:

Descarga eléctrica al tocar los cables con tensión

Utilice cables conductores independientes para establecer la puesta a tierra de protección de los armarios del sistema del sistema de comunicación y los distribuidores principales y paneles de interconexión antes de conectar teléfonos y líneas.



PRECAUCIÓN:

Peligro de incendio

Para reducir el riesgo de incendio, solo se deberían utilizar líneas de comunicación con un diámetro mínimo de 0,4 mm. (AWG 26) o mayor.

Nota:

Peligro de incendio por sobretensión

Con líneas que midan más de 500 m y líneas que salgan del edificio, hay que proteger los módulos SLMAV8N y SLMAV24N con una protección antirrayos externa.

Este tipo de protección contra descargas (antirrayos) se denomina protección primaria adicional. La protección primaria adicional se garantiza mediante el montaje 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.

OpenScape Business X8 está equipado al menos con una placa SLMAV8N o SLMAV24N.

Paso a paso

- 1) Conecte el puerto a/b que desee utilizar al dispositivo analógico (teléfono, fax, módem, altavoz, etc.).

Elija una de estas opciones:

- Si la conexión va a realizarse a través del MDFU del distribuidor principal externo, conecte el conductor de conexión del teléfono o dispositivo analógico a la regleta divisora o regleta de clasificación deseada en el MDFU.
 - Si la conexión va a realizarse a través del panel de interconexión externo, conecte el conductor de conexión del dispositivo o teléfono analógico a la toma RJ45 deseada del panel de interconexión.
 - Si la conexión va a realizarse a través del backplane de un armario de sistema (es decir, a través de un panel de conectores con 24 tomas RJ45), conecte el conductor de conexión del teléfono o dispositivo analógico a la toma RJ45 deseada del panel de conectores que quiera.
- 2) Si hay algún otro teléfono o dispositivo analógico más presente, conéctelos al sistema de comunicación siguiendo este mismo método.

7.8 Tareas finales

Para completar la instalación, debe insertar la tarjeta M.2 SSD o SDHC y debe realizar una inspección visual. Además, para montajes autónomos, cierre todos los armarios de sistema del sistema de comunicación con las cubiertas de plástico proporcionadas para tal fin. Por último, debe conectar el sistema a la red de alimentación.

A continuación, el sistema de comunicación puede entrar en funcionamiento con OpenScape Business Assistant (WBM). La descripción de este último elemento la encontrará en la ayuda online de WBM (Gestión basada en web) o en el capítulo de Documentación para el administrador de la sección "Instalación inicial de OpenScape Business".

Nota: Durante la puesta en servicio inicial del sistema de comunicación, no está definido el nivel de carga de la batería de la placa base. Para conseguir una carga suficiente, el sistema debe estar al menos 2 días conectado a la fuente de alimentación de la red eléctrica. Si se desconecta el sistema del suministro de alimentación de la red, la batería podría no disponer de carga suficiente y podría provocar que se bloquee el período de activación debido a una manipulación del tiempo.

7.8.1 Cómo insertar la tarjeta M.2 SSD o la tarjeta SDHC (sistema con OCCM)

La tarjeta M.2 SSD o la tarjeta SDHC contiene el software de comunicación OpenScape Business y deben montarse/insertarse antes de la puesta en servicio del sistema de comunicación.

Paso a paso

- 1) Compruebe que la protección contra escritura de la tarjeta SDHC esté desactivada (interruptor en dirección de los contactos metálicos).
- 2) Si todavía no lo ha hecho, inserte la tarjeta SDHC en el slot para tarjetas SDHC de la placa base, hasta que encaje. Los contactos metálicos de la tarjeta SDHC deben ir en dirección de la placa base.

7.8.2 Cómo realizar una inspección visual

Antes de arrancar el sistema de comunicación, es obligatorio realizar una inspección visual del hardware, el cableado y el suministro de alimentación.

Requisitos previos



PELIGRO:

Descarga eléctrica al tocar los cables con tensión

Desconecte todos los circuitos de corriente de suministro del sistema de comunicación antes de comenzar la inspección visual.

- Desconecte la tensión de la batería, la tensión de alimentación (LUNA2) y la tensión de línea.
- Desconecte las líneas de conexión de los acumuladores o los sets de acumuladores que pudiera haber conectados.
- Tienda todos los conectores de red del sistema de comunicación.

Nota:

Siempre que vaya a manipular módulos, debe llevar puesta una pulsera antiestática.

Es obligatorio conocer y respetar las medidas de prevención contra componentes sometidos a cargas electrostáticas (véase [Advertencias: Aviso](#)).

Las cubiertas de plástico delantera y trasera no deben estar puestas en los armarios del sistema.

Paso a paso

- 1) Desconecte todos los circuitos de corriente de suministro del sistema de comunicación.
- 2) Compruebe que el sistema de comunicación esté sin tensión.

- 3) Compruebe que la tarjeta M.2 SSD o SDHC esté insertada correctamente. La protección contra escritura de la tarjeta SDHC debe desactivarse (con el interruptor en dirección de los contactos metálicos).
- 4) Revise que todos los módulos estén en buen estado y bien instalados.
Si es necesario, compruebe que los módulos correspondientes se hayan insertado correctamente (véase [Cómo insertar un módulo](#)).
- 5) Asegúrese de que todos los cables de conexión estén bien tendidos y fijados. Por ejemplo, ¿hay algún riesgo de tropezar con un cable o pisarlo?
Si es necesario, compruebe que los cables de conexión están correctamente instalados.
- 6) Revise que las cubiertas de blindaje estén bien instaladas para proteger los slots de módulos o slots que no se utilicen o aquellos slots equipados con módulos periféricos que solamente dispongan de cubiertas de plástico.
Si es necesario, instale las cubiertas de blindaje que faltan (véase [Cómo instalar cubiertas de blindaje](#)).
- 7) Verifique que los slots de alimentación de LUNA2 y el módulo REALS situados en el armario básico están cubiertos por un panel exterior.
Si es preciso, instale el panel exterior.
- 8) Verifique que los slots de alimentación de LUNA2 y del módulo REALS situados dentro del armario de ampliación (si es que hay uno) están cubiertos por un panel exterior.
Si es preciso, instale el panel exterior.
- 9) Revise si están instalados los paneles de blindaje de la parte trasera para aquellos módulos que no tienen paneles de conectores.
Si es necesario, instale los paneles de blindaje que faltan (véase [Cómo instalar paneles de blindaje o paneles de conectores](#)).
- 10) Compruebe si hay un cable de toma de tierra específico conectado al terminal de tierra de cada armario del sistema.
Si es necesario, establezca la puesta a tierra de todos los armarios de sistema por separado (véase [Puesta a tierra de protección para instalaciones independientes](#) y [Puesta a tierra de protección para instalaciones de montaje en armarios de 19 pulgadas](#)).
- 11) Asegúrese de que los distribuidores principales o paneles de interconexión que haya en uso estén correctamente conectados al cable de puesta a tierra.
Si es necesario, establezca la puesta a tierra de todos los distribuidores principales o paneles de interconexión por separado (véase [Puesta a tierra de protección para instalaciones independientes](#) y [Puesta a tierra de protección para instalaciones de montaje en armarios de 19 pulgadas](#)).
- 12) Compruebe que la tensión nominal de la red de alimentación coincida con la tensión nominal del sistema de comunicación (placa de características).

Pasos siguientes

Tan solo para montajes autónomos: cierre todos los armarios de sistema del sistema de comunicación con las cubiertas de plástico proporcionadas para tal fin (véase [Solo con montaje autónomo: Cómo montar las cubiertas de plástico de un armario del sistema](#) en la página 156).

7.8.3 Solo con montaje autónomo: Cómo montar las cubiertas de plástico de un armario del sistema

En caso de montaje autónomo, todos los armarios de sistema se deben cerrar con las cubiertas de plástico previstas para ello antes de poner en marcha el sistema de comunicación.

Paso a paso

- 1) Coloque las espigas del borde inferior de una cubierta de plástico en la ranura guía de la parte delantera del armario básico.
- 2) Empuje la cubierta de plástico hacia el armario básico hasta que encaje.



- 3) Repita los pasos 1 y 2, para montar la cubierta de plástico en el lado trasero del armario básico.
- 4) Si hay un armario de ampliación, repita los pasos 1 bis 3 para montar las cubiertas de plástico correspondientes.

7.8.4 Cómo conectar el sistema a la red eléctrica

Paso a paso

Inserte el cable de conexión de red en la toma del suministro de corriente. El sistema de comunicación arranca.

Nota: Deje el sistema conectado a la red eléctrica durante 2 días al menos para que el acumulador de la placa base se cargue lo suficiente. Si la carga es insuficiente es posible que el periodo de activación se bloquee por manipulación del tiempo si se producen repetidos arranques.

8 Instalación del servidor Linux

Para OpenScape Business S y OpenScape Business UC Booster Server, el software de comunicación OpenScape Business está instalado en un sistema operativo Linux. El software de comunicación puede ejecutarse directamente en un servidor Linux o en un entorno virtual con VMware vSphere o Microsoft Hyper-V.

Nota: En lo sucesivo, cuando una descripción se aplique tanto a OpenScape Business S como al servidor UC OpenScape Business Booster, se utilizará el término genérico OpenScape Business por simplicidad.

Debe instalarse la versión regular SLES 15 SP6/SP7 de 64 bits optimizada por el fabricante del servidor como sistema operativo Linux.

Estas instrucciones de instalación describen el arranque inicial del servidor Linux. Esto depende de si el servidor Linux utiliza o no un RAID por software. La instalación del software de comunicación OpenScape Business y la posterior configuración de OpenScape Business se describen en la *documentación del administrador de OpenScape Business*.

El arranque inicial del servidor Linux que se describe aquí se basa en la interfaz de usuario en inglés. La instalación y configuración también pueden realizarse, por supuesto, en un idioma de interfaz diferente.

8.1 Requisitos previos

A continuación se describen los requisitos previos y las restricciones generales para el funcionamiento de OpenScape Business en el servidor Linux (el PC servidor).

Requisitos mínimos de hardware

El PC servidor debe cumplir los siguientes requisitos mínimos:

- Compatible con 64 bits
- Equipado para funcionar 24 horas al día, 7 días a la semana
- Certificado por el fabricante del PC para SLES 15 SP6/SP7 de 64 bits
- El software de comunicación para OpenScape Business debe ser la única aplicación en ejecución (excluyendo los escáneres de virus)
- Conexión LAN con velocidad mínima de 100 Mbps
- teclado, ratón, USB 2.0, unidad de DVD
- Resolución de pantalla: 1024x768 o superior
- Familias de CPU recomendadas:
 - Procesadores Intel Core i: CPU Xeon de sexta generación y superiores correspondientes
 - Procesadores AMD Ryzen

La categoría del servidor (*Básico, Estándar, Avanzado*) se define por el *número máximo de usuarios* que cada uno soporta.

	Servidor básico	Servidor estándar	Servidor avanzado
Número máximo de usuarios	hasta 50	hasta 500	hasta 1500
Núcleos de procesador / velocidad de reloj base por núcleo	2/2,5 GHz o 4/2 GHz	2/3 GHz o 4/2,5 GHz	4/3,5 GHz o 6/3 GHz
RAM	4GB	6GB	8GB
HDD / SSD	60GB	200GB	500GB

Tenga en cuenta que si se utiliza el Centro de contacto multimedia, siempre se deberá utilizar el Servidor avanzado.

Además, si se utiliza la opción de fax, la configuración del servidor estándar es el requisito mínimo.

La instalación puede realizarse incluso si no se cumplen los requisitos mínimos; sin embargo, esto podría ocasionar problemas durante el funcionamiento.

Software

Para instalar el sistema operativo Linux en el PC servidor, se requiere la versión de Linux de 64 bits SLES 15 SP6/SP7.

Al adquirir el software de comunicación OpenScape Business, puede comprar un archivo .ISO con esta versión de Linux. Este archivo .ISO solo se puede utilizar junto con el software de comunicación.

Algunos fabricantes de PC ofrecen sus propios discos de instalación de Linux optimizados para sus modelos de PC servidor. Estos se pueden utilizar si admiten la versión de Linux SLES 15 SP6 de 64 bits.

Mantenga el archivo .ISO de Linux a mano durante la instalación del software de comunicación OpenScape Business, ya que es posible que algunos paquetes de software (RPM) necesarios para el software de comunicación deban instalarse más adelante desde este archivo .ISO.

Certificación SLES 15 SP6/SP7 de 64 bits

El servidor debe estar certificado para SLES 15 SP6/SP7 de 64 bits.

Novell ofrece a los fabricantes de PC un programa de certificación llamado "YES" para la certificación de sus PC servidor. Los resultados se pueden encontrar en Internet en:

<https://www.suse.com/yessearch/Search.jsp>

Si no hay certificación disponible, se debe preguntar al fabricante del PC si el servidor es compatible con SLES 15 SP6/SP7 de 64 bits. Si se instala algún hardware adicional (por ejemplo, una tarjeta de red o gráfica) que sea incompatible con SLES 15 SP6/SP7 de 64 bits, se debe obtener un controlador adecuado del proveedor de la tarjeta, independientemente de la certificación. Si no hay ningún controlador disponible, la tarjeta correspondiente debe ser reemplazada por un modelo que sea compatible con SLES 15 SP6/SP7 de 64 bits.

Registrarse en Novell

Aunque la instalación y el funcionamiento de SLES 15 SP6/SP7 de 64 bits es posible sin registrarse en Novell, el registro en Novell es necesario para obtener parches de seguridad y actualizaciones de software. Para ello, deberá crear una cuenta de cliente con Novell con la ayuda del código de activación (consulte también [Actualizaciones en la página 179](#)). Se recomienda que la cuenta del cliente se configure antes de la instalación de Linux.

Se puede obtener un código de activación de Novell (código de registro) a través del elemento de pedido "Clave de actualización de OpenScape Business SLES".

Infraestructura

La red interna debe satisfacer las siguientes condiciones:

- LAN con al menos 100 Mbps e IPv4
- Base de tiempo uniforme (por ejemplo, a través de un servidor NTP)
- Dirección IP fija para el PC servidor

Acceso a Internet

El PC servidor debe tener acceso a Internet para:

- Registrarse en Novell
- Parches de seguridad y actualizaciones generales de software de Linux

OpenScape Business requiere una conexión a Internet para:

- Actualizaciones del software OpenScape Business
- Funciones de OpenScape Business como la telefonía por Internet, por ejemplo
- Servicio remoto (SSDP)/RSP.servicelink

Configuración de la red

Durante la instalación de Linux, se le solicitarán los detalles de configuración de la red. Por lo tanto, es aconsejable crear un esquema de direcciones IP que contenga todos los componentes de la red y sus direcciones IP antes de la configuración de la red.

El siguiente es un ejemplo de un esquema de dirección IP con el rango de direcciones IP 192.168.5.x: Los parámetros que se muestran en negrita son las especificaciones mínimas obligatorias requeridas durante la instalación de Linux.

Parámetros	Valores de muestra
Servidor DHCP externo o servidor DHCP de Linux	Servidor DHCP del enrutador de Internet (externo)
rango de direcciones DHCP	192.168.5.50 a 192.168.5.254
Máscara de subred de la red o segmento de red	255.255.255.0
Dirección IP fija del servidor Linux Esta dirección IP debe estar fuera del rango DHCP.	192.168.5.10
Enrutador de Internet	192.168.5.1

Parámetros	Valores de muestra
Servidor con dirección IP fija (opcional), por ejemplo, servidor de correo electrónico	192.168.5.20
Clientes con dirección IP fija (opcional) Esta dirección IP debe estar fuera del rango DHCP.	192.168.5.1 a 192.168.5.49
Gateway predeterminado , es decir, el enrutador de Internet en el ejemplo	192.168.5.1
Servidor DNS (i.e., el enrutador de Internet en el ejemplo)	192.168.5.1
Nombre de dominio al utilizar un servidor DNS (por ejemplo, el nombre de dominio de Internet)	customer.com
Nombre de host de OpenScape Business El nombre puede elegirse libremente, pero debe coordinarse con el administrador de la red.	comm_server

Si los datos de red reales no están disponibles en el momento de la instalación, la red debe configurarse con los datos de esta red de muestra.

Después de la instalación exitosa de Linux, los datos de la red se pueden editar en cualquier momento con YaST y adaptarlos a la red.

Nota: No se recomienda omitir la configuración de la red, ya que la instalación posterior de OpenScape Business no se puede completar con éxito sin una red completamente configurada.

8.2 Instalación en un entorno virtual

El software de comunicación puede ejecutarse en un entorno virtual.

Para configurar un entorno virtual, primero se debe instalar y configurar el software de virtualización (sistema operativo anfitrión) en el PC servidor. Posteriormente, se instala Linux como sistema operativo invitado. Finalmente, el software de comunicación se instala dentro del sistema operativo Linux.

Para la concesión de licencias en un entorno virtual, se genera y utiliza un ID de bloqueo avanzado para el softswitch en lugar de la dirección MAC del PC servidor.

Se ha publicado el siguiente software de virtualización:

- En las notas de lanzamiento de OpenScape Business encontrará información detallada sobre las versiones publicadas de VMware vSphere, incluidos los últimos parches.

Para obtener detalles sobre los requisitos de hardware del servidor físico, consulte la "Guía de compatibilidad de VMware" y la "Guía de recursos de administración de VMware" en www.vmware.com.

Para determinar los requisitos de hardware del servidor físico, VMware ofrece una función de búsqueda en línea de hardware certificado y probado en la sección "Guías de compatibilidad" de su página web: <http://www.vmware.com/guides>

Las directrices de aprovisionamiento de discos se pueden encontrar en https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc_50%2FGUID-81629CAB-72FA-42F0-9F8FD0DE39E57.html

- Windows Server (2008 R2, 2012, 2012 R2) Hyper-V, incluyendo los últimos parches.

Para obtener detalles sobre los requisitos de hardware del servidor físico, consulte technet.microsoft.com.

Encontrará toda la información necesaria sobre Hyper-V en la sección Biblioteca -> Windows Server 2012 R2 (o su sistema Windows Server actual) -> Roles y tecnologías del servidor -> Hyper-V en la página de Microsoft TechNet.

La descripción de la instalación y configuración del software de virtualización no forma parte de esta documentación. La instalación de Linux y del software de comunicación en un entorno virtual es exactamente la misma que para una instalación directa en el servidor.

En el entorno virtual, deben configurarse los siguientes requisitos mínimos para Linux y el software de comunicación:

Parámetros	Configuración de VM
Sistema operativo invitado	SLES 15 SP6/SP7 de 64 bits
Capacidad de VM HD	Hasta 50 usuarios: 60 GB o más Hasta 100 usuarios: 100 GB o más Hasta 500 usuarios: 200 GB o más OpenScape Business Contact Center: 200 GB o más Con 500 usuarios: 500 GB o más
Modo de disco virtual	Por defecto
Tipo de formato de disco virtual	Aprovisionamiento ligero (capacidad HD dinámica) o Aprovisionamiento grueso (capacidad de disco duro fija)
vCPUs	2 4 para OpenScape Business Contact Center o más de 500 usuarios
Cuota de vCPU (Alta/Normal)	Alta
Reserva de vCPU	2 GHz
Límite de vCPU	Ilimitado

Parámetros	Configuración de VM
Memoria de VM	2 GB (se recomiendan 4 GB) 6 GB para: - Fax como PDF - OpenScape Business Contact Center 8 GB para: - Más de 500 usuarios
Recursos de memoria de VM (Alto/Normal)	Normal
Reserva de memoria de VM	4GB
Límite de memoria de VM	Ilimitado
Número de vNIC	1
Manual de VMware MAC utilizado	NO
Compatibilidad con adaptadores de red virtual	Sí, controlador vmxnet3
Instalación de VMware Tools	SI

La máquina virtual (VM) puede utilizar la CPU hasta un 70%; valores superiores a ese porcentaje pueden provocar un comportamiento errático.

Se admiten las siguientes características de VMware vSphere:

- Aprovisionamiento ligero
- Alta disponibilidad (HA)
- VMotion
- Recuperación de datos (VDR)
- DRS (VMotion automático)
- Almacenamiento VMotion

Las siguientes características de VMware vSphere no son compatibles:

- Tolerancia a fallos

Se admiten las siguientes características de Microsoft Hyper-V:

- Aprovisionamiento ligero
- Alta disponibilidad (HA)
- Migración en vivo
- Recuperación de datos

El protector de pantalla del entorno virtual debe estar desactivado.

8.2.1 Política de Calidad de Servicio y Residencia Compartida de VM

Esta Política de Calidad de Servicio y Residencia Compartida de VM proporciona las reglas que deben seguir los encargados de implementar máquinas virtuales (VM) Unify de gestionar el entorno virtual al implementar VM Unify con recursos de hardware y de red consolidados:

- Los encargados de implementar VM Unify y de gestionar el entorno virtual deben garantizar el cumplimiento de los criterios de rendimiento. La incertidumbre se puede reducir mediante pruebas previas a la implementación, líneas de base y siguiendo las reglas de la Guía de configuración y recursos de VM Unify, incluida esta política.
- Las máquinas virtuales con aplicaciones en tiempo real y críticas se deben proteger de otras aplicaciones en la red de encaminamiento y conmutación, para garantizar que el tráfico de red de voz/vídeo reciba el ancho de banda y la protección frente a retardo y jitter que necesita.
- Las máquinas virtuales con aplicaciones en tiempo real y críticas se deben proteger de otras aplicaciones cuando el host de virtualización comparte hardware de red, almacenamiento y computación entre varias máquinas virtuales de aplicación (por ejemplo, no puede programar en tiempo real Unify).
- Es necesario cumplir las reglas de configuración de recursos y de virtualización de Unify (por ejemplo, tamaño de hardware físico/virtual, política de residencia compartida, etc.) para garantizar que las máquinas virtuales Unify reciban el rendimiento de red/almacenamiento, la capacidad de almacenamiento, la memoria y la CPU que necesitan.
- No aloje máquinas virtuales Unify en el mismo hardware con máquinas virtuales de terceros que tengan definidos requisitos de recursos incompletos.
- El hardware de host se debe supervisar ininterrumpidamente (por ejemplo, con vCenter) y debe utilizar como máximo el 80 % de la potencia de procesamiento de la CPU y un valor %RDY máximo del 5 %.
- Los valores totales de RAM, almacenamiento y NW (incluida red de almacenamiento) no debe superar la capacidad del hardware de host (no exceder la suscripción).
- Aun cuando el procesador de host tenga capacidad de subprocesamiento múltiple (Hyper-Threading) y tenga habilitada esta funcionalidad, los núcleos físicos solo se deben contar una vez.
- Las cuotas de vCPU se deben configurar para garantizar que las VM Unify críticas (incluidas las VM en tiempo real) no se queden nunca sin tiempo de CPU.
- Los clientes deben garantizar que se cumplen los requisitos, aunque la máquina virtual se traslade en el entorno, por ejemplo, modificando manualmente la configuración de las cuotas de CPU de una VM que se traslade a otro grupo de recursos u otro host de VM.
- Los planes de Recuperación ante desastres deben atender a los recursos adicionales necesarios al hacer la conmutación por error a la ubicación de conmutación por error (centro de datos 2).

8.2.2 Sincronización de hora del sistema operativo invitado Linux

Hay que desactivar la sincronización de hora (base temporal homogénea de fecha y hora) entre el sistema operativo invitado VMware vSphere o Microsoft Hyper-V y el sistema operativo Linux. La base temporal homogénea debe proceder del sistema operativo invitado a través de un servidor NTP.

8.2.2.1 Cómo onfigurar la sincronización horaria para el sistema operativo invitado Linux en VMWare

Paso a paso

- 1) Con el cliente VMware **vSphere Client**, haga clic con el botón secundario del ratón sobre el sistema operativo invitado Linux y seleccione la opción de menú **Edit Settings** (Editar ajustes).
- 2) En **Virtual Machine Properties** (Propiedades del equipo virtual) de la pestaña **Options** (Opciones) y en la entrada **VMware Tools** (Herramientas VMware) del área **Advanced** (Avanzado), seleccione la opción **Synchronize guest time with host** (Sincronizar hora de invitado con host).
- 3) Para el sistema operativo invitado Linux, modifique los ajustes NTP del archivo `./etc/ntp.conf` tal y como se muestra a continuación, utilizando los parámetros en negrita:

```
*****
```

```
...
```

```
tinker panic 0
```

```
# server 127.127.1.0
```

```
# local clock (LCL)
```

```
# fudge 127.127.1.0 stratum 10
```

```
# LCL is unsynchronized
```

```
...
```

```
server 0.de.pool.ntp.org iburst
```

```
restrict 0.de.pool.ntp.org
```

```
restrict 127.0.0.1
```

```
restrict default kod nomodify notrap
```

```
...
```

```
*****
```

Nota: El servidor NTP **de.pool.ntp.org** es un servidor de ejemplo y, en su caso, hay que sustituirlo por una dirección de servidor SNTP a la que se pueda acceder desde el sistema operativo invitado Linux.

8.3 Aspectos de seguridad de Linux y unión RAID

Si se observan los elementos de seguridad Linux y se usa una unión RAID aumenta la seguridad del servidor Linux.

Firewall

Si se establece conexión con Internet se requiere un firewall, a fin de impedir el acceso no autorizado desde el exterior. Después de instalar Linux, el firewall de Linux está activado. Con el programa de instalación del software de comunicación se ajusta el firewall de forma tal que permita el funcionamiento correcto del software de comunicación. Los puertos para el software de comunicación se abren y todos los demás se cierran. OCCM: conectores de tarjeta X11, consulte Cómo montar OCCB1 en placas base OCCM

Si en la red se utiliza un firewall externo, hay que desactivar el firewall de Linux; además, hay que abrir las direcciones y puertos que necesite utilizar el software de comunicación (véase [Puertos utilizados](#) en la página 279 en las instrucciones de instalación de OpenScape Business S o OpenScape Business UC Booster Server).

Explorador de virus

En la instalación de Linux no se incluye un antivirus. Se recomienda instalar un antivirus. Si es necesario, puede obtener más información en las notas de la versión del software de comunicación.

Para evitar posibles problemas de rendimiento por el uso de un antivirus, hay que programar las exploraciones del disco duro regulares en momentos en los que no se use el software de comunicación o tenga un uso reducido.

Intrusion Detection System (AppsArmor)

La rutina de instalación del servidor de aplicaciones no realiza ningún cambio en el sistema de detección de intrusiones de Linux, Linux Intrusion Detection System (AppsArmor). Se aplican los ajustes estándar de la instalación de Linux. Para trabajar con el software de comunicación no es necesario realizar más ajustes de configuración.

Durante la instalación el softswitch se actualiza y activa el sistema de detección de intrusiones de Linux, Linux Intrusion Detection System (AppsArmor). Para trabajar con el software de comunicación no es necesario realizar más ajustes de configuración.

Seguridad en caso de caída

Recomendaciones para aumentar la seguridad en caso de caída (redundancia):

- dos discos duros en la unión RAID1.
- segundo alimentador de tensión para el servidor Linux
- alimentación de tensión sin interrupciones

Al utilizar teléfonos IP hay que tener en cuenta que los conmutadores LAN y los teléfonos IP reciban una alimentación de tensión sin interrupciones.

Unión RAID1

En una unión RAID 1 el contenido del primer disco duro se duplica en el segundo. Si un disco duro tiene un error, el sistema continúa ejecutándose en el segundo disco duro.

Una unión RAID se puede implementar como RAID de software o como RAID de hardware (BIOS RAID o HW-RAID-Controller).

Para obtener información sobre las peculiaridades de la instalación con un RAID de software, consulte .

En numerosas ocasiones, un RAID de hardware requiere un controlador propio no incluido en el sistema operativo Linux. El fabricante es el encargado de ofrecer este controlador y se debe instalar siguiendo sus indicaciones. Si el controlador no es compatible con la versión de Linux o no se dispone de ningún operador, no se puede utilizar el RAID de hardware. Esta documentación no describe los sistemas RAID basados en hardware. En este caso, póngase en contacto con el fabricante para obtener información sobre la configuración y los controladores de Linux.

8.4 Arranque inicial sin RAID por software

El arranque inicial del servidor Linux sin RAID por software incluye la instalación y configuración de Linux, al tener en cuenta que no se está utilizando RAID por software.

Los ajustes necesarios para el programa de comunicación se realizan durante la instalación y la configuración.

Particiones de Linux

El disco duro debe particionarse durante la puesta en marcha inicial de la siguiente manera:

Partición	Tipo	Tamaño	Sistema de archivos	Montaje	Nota
Partición 1	Partición primaria	2GB	Intercambio	intercambio	corresponde al tamaño de la memoria de trabajo
Partición 2	Partición primaria	20GB	Ext4	/	para el sistema operativo Linux
Partición 3	Partición primaria	Resto ¹	Ext4	/hogar	Para el programa de comunicación

Nota: El procedimiento de instalación del programa de comunicación comprueba estos tamaños de partición y puede impedir la instalación.

Nota: Algunos equipos servidor exigen una partición de arranque complementaria. Si Linux sugiere una partición de arranque, el tamaño propuesto debe admitirse.

¹ Hasta 50 usuarios: mín. 40 GB - Hasta 100 usuarios: mín. 80 GB - Más de 500 usuarios: mín. 180 GB - Con OpenScape Business Contact Center: mín. 180 GB - Más de 500 usuarios: mín. 480 GB

8.4.1 Cómo instalar y configurar SLES 15 SP6/SP7 sin RAID por software

Requisitos previos

La configuración de la BIOS del servidor Linux está establecida para que el servidor arranque desde el archivo .ISO en la memoria USB.

Para registrarse en Novell, se requiere acceso a Internet y el código de activación.

Paso a paso

- 1) Inserte el archivo .ISO de SLES 15 en una memoria USB en un puerto USB e inicie el sistema desde el archivo .ISO.
Aparece la ventana de inicio de la instalación de Linux.
- 2) Seleccione **Instalación** y presione Enter.
- 3) En la ventana **Idioma, teclado y selección de productos**, seleccione la configuración de país para el sistema operativo Linux:
 - a) Seleccione **Inglés (EE. UU.)** como el idioma de la interfaz de usuario de la lista desplegable **idioma**.
 - b) Seleccione la distribución del teclado para el país deseado en la lista desplegable **Distribución del teclado**.
 - c) Seleccione **SUSE Linux Enterprise Server 15 SP6 o SP7** como producto para instalar.
- 4) Lea el acuerdo de licencia y acepte los términos de la licencia marcando la casilla de verificación **Acepto los términos de la licencia** y luego haga clic en **Siguiente**.
- 5) Aparece la **configuración de red**. En caso contrario, seleccione **Configuración de red** en la ventana de **Registro**.
Si desea configurar la red más tarde, haga clic en **Siguiente**.
- 6) En la ventana **Configuración de red**, configure la tarjeta de red.
 - a) Seleccione la tarjeta de red deseada en la ventana **Descripción general**. La dirección MAC de la tarjeta de red seleccionada aquí se asigna más tarde en el proceso de licencia a las licencias individuales. Haga clic en **Editar**.
 - b) Habilite el botón de opción **Dirección IP asignada estáticamente**.
 - c) Bajo la dirección IP, ingrese la dirección IP asignada del servidor Linux (por ejemplo, 192.168.5.10).
La dirección IP debe ajustarse al esquema de direcciones IP de su red interna y no debe haber sido asignada a ningún otro cliente de la red, ya que de lo contrario esto generaría un conflicto de direcciones IP.
 - d) En **Máscara de subred**, ingrese la máscara de subred asignada del servidor Linux (por ejemplo, 255.255.255.0).
La máscara de subred debe coincidir con el esquema de dirección IP de su red interna.
 - e) En **Nombre de host**, ingrese el nombre de host asignado del servidor Linux (por ejemplo, OSBiz-Booster).



Aviso: El nombre de host debe ajustarse al esquema de nombres de host de su red interna y no debe asignarse a ningún cliente de red, ya que esto provocaría un conflicto de nombres de host. El nombre de host predeterminado "localhost" no se puede utilizar con OSBiz S / Booster Server y debe cambiarse.

El nombre de host configurado en los ajustes de red también debe estar configurado en la configuración de la tarjeta de red.

- f) Haga clic en **Continuar**.
- 7) Especifique el servidor DNS y el gateway predeterminado.
 - a) En la ventana **Configuración de red**, haga clic en la pestaña **Nombre de host/DNS**.
 - b) Introduzca el nombre de host del servidor DNS en **Nombre de host estático**.

El nombre de host debe ajustarse al esquema de nombres de host de su red interna y no debe asignarse a otros clientes de la red, ya que esto provocaría un conflicto de nombres de host. El nombre de host predeterminado "localhost" no se puede utilizar con OSBIZ S / Booster Server y debe cambiarse.

En caso de que el campo permanezca vacío o sea un localhost, "sles15_OSBIZS" se agrega automáticamente como nombre de host estático predeterminado durante el proceso de instalación de OSBIZ S. Este valor se puede cambiar más adelante durante el inicio de OSBIZ S a través de YaST en la pestaña **Configuración de red > Nombre de host/DNS**.
 - c) Introduzca el nombre de dominio del servidor DNS en **Nombre de dominio**.

El nombre de dominio debe ser único, ya que de lo contrario esto podría generar un conflicto de nombre de dominio.
 - d) Introduzca la dirección IP del servidor DNS en **Servidor de nombre 1**.

Si no hay ningún servidor DNS disponible en la red interna, ingrese la dirección IP del enrutador de Internet (por ejemplo, 192.168.5.1).
 - e) En la ventana **Configuración de red**, haga clic en la pestaña **Enrutamiento**.
 - f) Seleccione **Agregar** y en **Gateway predeterminado** ingrese la dirección IP del enrutador de Internet (por ejemplo, 192.168.5.1) y seleccione el dispositivo Ethernet de la lista desplegable.
- 8) Haga clic en **Continuar**.
- 9) En la ventana de **Registro**, seleccione **Registrar sistema en ia scc.suse.com**, ingrese su dirección de correo electrónico y código de registro y haga clic en **Siguiente**.
- 10) En la ventana **selección de Extensiones y módulos** seleccione las siguientes extensiones y módulos: Módulo del sistema base, Módulo de contenedores, Módulo de aplicaciones de escritorio, Módulo de herramientas de desarrollo, Módulo heredado, Módulo de aplicaciones de servidor
- 11) Haga clic en **Continuar**.
- 12) En la ventana **Rol del sistema**, seleccione **SLES con GNOME** y haga clic en **Siguiente**.
- 13) En la ventana **Particionado sugerido** se propone ejecutar primero el Asistente guiado para crear particiones de arranque y de intercambio automáticamente. Para ello, seleccione **Configuración guiada**.
- 14) En la ventana **Seleccionar disco(s) duro(s)**, seleccione **Quitar incluso si no es necesario** para ambas selecciones y haga clic en **Siguiente**.
- 15) En el **tipo de sistema de archivos**, seleccione **Ext4** como sistema de archivos tanto para la partición raíz como para la partición de inicio.

Habilite las opciones **Proponer particiones de intercambio separadas** y **Ampliar el tamaño de RAM para Suspend** y haga clic en **Siguiente**.

- 16) Se propone un nuevo diseño en la ventana **Particiones sugeridas**. Haga clic en **Particionador experto > Iniciar con la propuesta actual**.
Eliminar únicamente las particiones raíz (/) y de inicio (/home). Conservar únicamente las particiones de intercambio y de arranque. Seleccione la partición que desea eliminar, haga clic en **Eliminar** y confirme la operación de eliminación haciendo clic en **Sí**.
- 17) Cree la partición para el sistema operativo Linux.
 - a) Haga clic en el dispositivo `/dev/sda` y seleccione **Agregar partición**.
 - b) En **Tamaño personalizado**, ingrese el tamaño de la partición 20 GB y haga clic en **Siguiente**.
El tamaño mínimo de la partición del sistema operativo Linux es de 15 GB y el recomendado es de 20 GB.
 - c) En la ventana **Agregar rol de partición**, seleccione el rol de **Sistema operativo** y haga clic en **Siguiente**.
 - d) Seleccione **Ext4** en **Formatear dispositivo**, seleccione `/` en **Montar dispositivo** y haga clic en **Siguiente**.
- 18) Cree la partición para el software de comunicación.
 - a) Haga clic en el dispositivo `/dev/sda` y seleccione **Agregar partición**.
 - b) Seleccione **Tamaño máximo** si prefiere utilizar el espacio restante del disco duro o en **Tamaño personalizado** para ingresar el tamaño de la partición y haga clic en **Siguiente**.
El tamaño mínimo de la partición del software de comunicación es de 40 GB.
 - c) En la ventana **Agregar partición en /dev/sda**, seleccione la función **Datos y aplicaciones ISV** y haga clic en **Siguiente**.
 - d) Seleccione **Ext4** en **Formatear dispositivo**, seleccione `/home` en **Montar dispositivo** y haga clic en **Siguiente** y **Aceptar**.
- 19) En la ventana **Reloj y zona horaria**, seleccione la región y la zona horaria correctas.
Para ajustar la fecha y la hora o configurar un servidor NTP (para una base horaria uniforme), haga clic en el botón **Otros ajustes**. Haga clic en **Siguiente** cuando termine.
- 20) En la ventana **Usuarios locales**, agregue un usuario y una contraseña y haga clic en **Siguiente**.
- 21) En la ventana **Contraseña para el administrador del sistema "root"**, ingrese la contraseña del administrador del sistema con perfil "root" en los campos **Contraseña para el usuario root** y **Confirmar contraseña** y luego haga clic en **Siguiente**.
La contraseña debe cumplir con las políticas de seguridad convencionales. Debe tener al menos 8 caracteres, al menos una letra minúscula, al menos una letra mayúscula, al menos un número y al menos un carácter especial.

- 22) En la ventana **Configuración de instalación**, haga clic en **Software**.
- a) Habilitar **entorno de ejecución de 32 bits**.
 - b) Habilitar **DHCP y servidor DNS**.
 - c) Haga clic en **Detalles** y luego en el campo **Buscar** escriba `tcpdump` y seleccione el paquete `tcpdump`.
 - d) Haga clic en **Detalles** y en el campo de búsqueda escriba `docker`. Seleccione los paquetes: **docker**, **docker-bash-completion**, **docker-rootless-extras**
 - e) Haga clic en **Aceptar**.

Nota: Los paquetes anteriores son obligatorios para una instalación exitosa de SLES 15 SP6/SP7, excepto los paquetes docker (paso 22d) que son obligatorios solo para SLES 15 SP7. Es necesario instalar el paquete de **servidor DHCP y DNS**, incluso cuando no se utilizan como servidores en OpenScape Business S.

- 23) Para abrir el puerto SSH (el puerto SSH está cerrado de forma predeterminada por motivos de seguridad), en la ventana de **Configuración de instalación**, en la sección **Seguridad**, haga clic en **Abrir** en el campo **El puerto SSH estará bloqueado**.
- 24) Haga clic en **Instalar** nuevamente para confirmar la instalación.
- La ventana **Configuración de instalación** es una descripción general de los componentes que se instalarán. Antes de completar la instalación, puede realizar los cambios necesarios desde esta ventana.
- Una vez finalizada la instalación, la computadora se reinicia en el sistema instalado.

8.4.2 Cómo actualizar de SLES 12 SP5 a SLES 15 SP6/SP7

Requisitos previos

Última versión del sistema OpenScape Business V3R4. Si OpenScape Business no está actualizado a la última versión V3R4, proceda a una actualización de software.

Se instaló el sistema OpenScape Business en un SLES 12 SP5.

Si se utiliza una versión anterior, primero es necesario actualizar a SLES 12 SP5. Este capítulo describe la actualización de un sistema OpenScape Business completamente operativo instalado en SLES 12 SP 5 a SLES 15 SP6/SP7.

Nota: Se recomienda encarecidamente, siguiendo las recomendaciones de la Guía de actualización de SUSE SLES 15, realizar una instalación limpia/nueva en lugar de utilizar el mecanismo de actualización.

Con una instalación nueva, aún podrá restaurar su copia de seguridad de OpenScape Business existente de la versión anterior en los nuevos sistemas instalados basados en SLES 15 SP6/SP7.

Se ha observado que el mecanismo de actualización puede causar problemas en algunas configuraciones de Linux, que pueden ser críticas para la funcionalidad de OpenScape Business.

Si se utiliza una máquina virtual (por ejemplo, ESXi), se recomienda crear una nueva máquina virtual en lugar de utilizar la máquina virtual utilizada como SLES 12 SP5. De lo contrario, pueden existir problemas adicionales cuando el sistema operativo anfitrión (por ejemplo, ESCi) se queja de la versión de Linux instalada en el sistema invitado (la máquina virtual se creó inicialmente para SLES 12 y ahora ejecutará SLES 15).

En una opción de instalación limpia/nueva en una máquina virtual, se cambiará el ALI (ID de bloqueo) del sistema y será obligatorio volver a alojar la licencia anterior.

Paso a paso

- 1) Realice una actualización de software de OpenScape Business a la versión V3R4.
- 2) Realice una copia de seguridad de todos los datos de OpenScape Business Server o UC Booster Server. Para ello, siga las instrucciones en [Cómo realizar una copia de seguridad de datos](#).
- 3) Desinstale OpenScape Business Server o UC Booster Server. Para ello, siga las instrucciones en [Cómo desinstalar el software de comunicación](#).
- 4) Inserte la unidad USB de instalación de SLES 15 SP6/SP7 y arranque.
- 5) Realice una instalación limpia de SLES 15 SP6/SP7.
- 6) Después de actualizar el sistema a SLES 15 SP6/SP7, instale la versión de OpenScape Business Server que sea compatible con SLES 15 SP6/SP7.

Nota: Utilice la misma partición que en SLES 12 SP5. Además, el sistema de archivos debe ser el mismo para SLES 12 y SLES 15; de lo contrario, no se podrá importar la copia de seguridad.

- 7) Restaure todos los datos de OpenScape Business Server.

8.4.3 Cómo actualizar de SLES 15 SP6 a SLES 15 SP7

Requisitos previos

Última versión del sistema OpenScape Business V3R4. Si OpenScape Business no está actualizado a la última versión V3R4, proceda a una actualización de software.

Se instaló el sistema OpenScape Business en un SLES 15 SP6. La actualización a SLES 15 es obligatoria ya que SLES 12 no es compatible con la versión OpenScape Business V3R4 FR3.

Nota: La actualización a SP7 es fluida, lo que significa que ya no es necesario realizar una copia de seguridad de OpenScape Business S.

Paso a paso

- 1) Realice una actualización de software de OpenScape Business a la última versión V3R4.
- 2) Inserte la memoria USB con el archivo *.iso de SLES 15 SP7.
- 3) Reinicie la máquina SLES y seleccione el inicio de la máquina a través de la memoria USB.
- 4) Seleccione **Actualizar**.
- 5) Siga las instrucciones exactas que se describen en el capítulo [Cómo instalar y configurar SLES 15 SP6/SP7 sin RAID por software](#).

Nota: Durante el proceso de actualización, aparece una notificación sobre la utilidad *rsyslog*. OpenScape Business utiliza *syslog-ng* utilidad para registros. Por lo tanto, seleccione la opción de desinstalar este paquete y proceda con la actualización.

8.5 Arranque inicial con un RAID por software

El arranque inicial del servidor Linux con un RAID por software incluye la instalación y configuración de Linux, teniendo en cuenta que se está utilizando un RAID por software.

Proceder de la siguiente manera:

- 1) Desactive el RAID de la BIOS (opcional)
Si se va a configurar una matriz RAID mediante RAID por software, primero se debe deshabilitar en la BIOS cualquier BIOS RAID integrada que pueda estar presente en la placa base del servidor.
- 2) Instalar y configurar SLES 15 SP6/SP7 con un RAID por software
Los ajustes necesarios para el software de comunicación se realizan durante la instalación y configuración.

Particiones de Linux

El disco duro debe particionarse durante el arranque inicial de la siguiente manera:

Partición	Tipo	Tamaño	Sistema de archivos	Montaje	Nota
Partición 1	Partición primaria	2GB	Intercambiar	intercambiar	corresponde al tamaño de la memoria de trabajo
Partición 2	Partición primaria	20GB	Ext4	/	para el sistema operativo Linux

Partición	Tipo	Tamaño	Sistema de archivos	Montaje	Nota
Partición 3	Partición primaria	El resto ²	Ext4	/home	Para el software de comunicación

Los puntos de montaje se asignan después del particionamiento al configurar el sistema RAID.

Nota: La rutina de instalación del software de comunicación comprueba el tamaño de estas particiones y puede rechazar la instalación.

Nota: Algunos servidores requieren una partición de arranque adicional. Si Linux sugiere una partición de arranque durante la instalación, debe aceptarse con el tamaño propuesto.

8.5.1 Cómo desactivar el RAID de la BIOS

Requisitos previos

La placa base del PC dispone de un controlador RAID integrado (BIOS RAID).

Paso a paso

- 1) Reinicie el equipo. Durante el arranque, podrá comprobar si se ha activado el RAID de la BIOS. Si el RAID de la BIOS no está activado, vaya al paso 3.
- 2) Deshabilite el RAID activo de la BIOS:
 - a) Pulse la combinación de teclas correspondiente en el momento adecuado durante el arranque para poder acceder a la configuración RAID de la BIOS. La combinación se le mostrará durante el arranque (por ejemplo, CTRL M para LSI MegaRAID BIOS).
 - b) Borre la configuración RAID de la BIOS. Ejemplo para LSI MegaRAID BIOS: Menú Gestión > Configurar > Menú Configuración > Borrar configuración.
 - c) Salga de la configuración del RAID de la BIOS y reinicie el equipo.
- 3) Desactive la configuración RAID SATA en la configuración de la BIOS de su ordenador:
 - a) Pulse la tecla correspondiente (por ejemplo, F2 o Supr) en el momento adecuado durante el arranque para entrar en la configuración de la BIOS del equipo.
 - b) Desactive el RAID SATA. Ejemplo para una BIOS Phoenix: Avanzado > Configuración avanzada del sistema > RAID SATA Desactivado.
 - c) Guarde los cambios y salga de la configuración de la BIOS de su PC (con la tecla F10, por ejemplo).
- 4) Reinicie el equipo.

² hasta 50 usuarios: mín. 40 GB - Hasta 100 usuarios: mín. 80 GB - Más de 500 usuarios: mín. 180 GB - Con OpenScape Business Contact Center: mín. 180 GB - Más de 500 usuarios: mín. 480 GB

Pasos siguientes

Instale y configure SLES 15 con un RAID que funcione mediante un programa informático.

8.5.2 Cómo instalar y configurar SLES 15 SP6/SP7 con un RAID por software

Requisitos previos

Cualquier RAID por hardware que pudiera existir queda desactivado.

La configuración de la BIOS del servidor Linux está establecida para que el servidor arranque desde el archivo .ISO.

Para registrarse en Novell, se requiere acceso a Internet y el código de activación.

Paso a paso

- 1) Inserte el archivo .ISO de SLES 15 en una memoria USB en un puerto USB e inicie el sistema desde el archivo .ISO. Aparece la ventana de inicio de la instalación de Linux.
- 2) Seleccione la opción de menú **Instalación** y confírmelo pulsando la tecla Enter.
- 3) En la ventana **Acuerdo de idioma, teclado y licencia**, seleccione la configuración de país para el sistema operativo Linux:
 - a) Seleccione **Inglés (EE. UU.)** como idioma de la interfaz de usuario en la lista desplegable **Idioma**.
 - b) Seleccione la distribución del teclado para el país deseado en la lista desplegable **Distribución del teclado**.
- 4) Lea el acuerdo de licencia y acepte los términos de la licencia marcando la casilla **Acepto los términos de la licencia**. Luego haga clic en **Siguiente**.
- 5) En la ventana de **registro**, seleccione **Registrar sistema a través de scc.suse.com**, ingrese su dirección de correo electrónico y código de registro y haga clic en **Siguiente**.

: Si desea omitir el registro, seleccione **Omitir registro**, luego haga clic en **Aceptar** en la ventana de **advertencia** que aparece y, finalmente, haga clic en **Siguiente**. Si omite el registro, no podrá acceder a los repositorios de actualizaciones. Sin embargo, puede registrarse después de la instalación o visitar el servicio de atención al cliente.

- 6) En la ventana de **productos complementarios**, haga clic en **Configuración de red**.

Nota: Si desea configurar la red más tarde, haga clic en **Siguiente**.

- 7) En la ventana **Configuración de red**, configure la tarjeta de red.
 - a) Seleccione la tarjeta de red deseada en la ventana **Descripción general**. La dirección MAC de la tarjeta de red seleccionada aquí se

asigna más tarde en el proceso de licencia a las licencias individuales. Haga clic en **Editar**.

- b) Habilite el botón de opción **Dirección IP asignada estáticamente**.
- c) En **Dirección IP**, ingrese la dirección IP asignada al servidor Linux (por ejemplo, 192.168.5.10).

La dirección IP debe ajustarse al esquema de direcciones IP de su red interna y no debe haber sido asignada a ningún cliente de red, ya que de lo contrario esto resultaría en un conflicto de direcciones IP.

- d) En **Nombre de host**, ingrese el nombre de host asignado del servidor Linux (por ejemplo, OSBiz-Booster).

El nombre de host debe ajustarse al esquema de nombre de host de su red interna y no debe haber sido asignado a ningún otro cliente de red, ya que de lo contrario esto generaría un conflicto de nombre de host.

- e) En **Máscara de subred**, ingrese la máscara de subred asignada del servidor Linux (por ejemplo, 255.255.255.0).

La máscara de subred debe coincidir con el esquema de dirección IP de su red interna.

- f) Luego haga clic en **Siguiente**.

8) Especifique el servidor DNS y el gateway predeterminado.

- a) En la ventana de **Configuración de red**, haga clic en la pestaña **Nombre de host/DNS**.

- b) Introduzca el nombre de host del servidor DNS en **Nombre de host**.

El nombre de host debe ajustarse al esquema de nombre de host de su red interna y no debe haber sido asignado a ningún otro cliente de red, ya que de lo contrario esto generaría un conflicto de nombre de host.

- c) Introduzca el nombre de dominio del servidor DNS en **Nombre de dominio**.

El nombre de dominio debe ser único, ya que de lo contrario esto podría generar un conflicto de nombre de dominio.

- d) Introduzca la dirección IP del servidor DNS en **Servidor de nombre 1**.

Si no hay ningún servidor DNS disponible en la red interna, introduzca la dirección IP del router de Internet (por ejemplo, 192.168.5.1).

- e) En la ventana **Configuración de red**, haga clic en la pestaña **Enrutamiento**.

- f) En **Gateway predeterminado**, ingrese la dirección IP del enrutador de Internet (por ejemplo, 192.168.5.1).

9) Haga clic en Siguiente.

10) En la ventana de producto adicional, haga clic en Siguiente.

11) En la ventana Rol del sistema, seleccione Sistema predeterminado y haga clic en Siguiente.

12) En la ventana de Particionamiento sugerido, seleccione Particionador experto...

13) Particiona los dos discos duros:

- a) Navegue en el árbol de menús de **Vista del sistema** hasta **Discos duros > sda** (primer disco duro del RAID por software).
- b) Elimine todas las particiones preasignadas (sda1, sda2, etc.) marcando la partición, haciendo clic en **Eliminar** y luego confirmando la operación de eliminación con **Sí**.
- c) Particione el primer disco duro utilizando el botón **Agregar partición**.

Utilice los siguientes datos para la partición:

Partición 1	Partición primaria	2GB	Papel: Intercambiar Cambio de formato Punto de montaje = intercambio, Opción fstab = Nombre del dispositivo
Partición 2	Partición primaria	0,5GB	Papel: Sistema operativo Formato Ext4 Punto de montaje = /boot Nota: Esta partición debe crearse únicamente en la primera unidad.
Partición 3	Partición primaria	20GB	Papel: Sistema operativo Formato Ext4 /
Partición 4	Partición primaria	Resto	Papel: Datos y aplicaciones de proveedores de software independientes (ISV) Formato Ext4 /home

- d) Navegue en el árbol de menús de **Vista del sistema** hasta **Discos duros > sdb** (segundo disco duro del RAID por software).
- e) Complete también los pasos 13b y 13c para el segundo disco duro.

Nota: No es necesario crear ninguna partición de arranque en el segundo disco duro.

- 14) Especifique la configuración RAID por software:
 - a) Seleccione la opción de menú **RAID** y haga clic en **Agregar RAID**.
 - b) Seleccione **RAID 1 (Espejo)**.
 - c) Seleccione las dos particiones sda3 y sdb2 en el área **Dispositivos disponibles** a la izquierda y transfíralas con **Agregar** al área **Dispositivos seleccionados** a la derecha.
 - d) Haga clic en **Siguiente**.
 - e) Confirme el valor predeterminado para el tamaño del fragmento con **Siguiente**.
 - f) En la siguiente ventana, seleccione **Sistema operativo** y haga clic en **Siguiente**.
 - g) En la siguiente ventana, seleccione **Ext4** como formato y el punto de montaje "/" para el primer dispositivo RAID (/dev/md0) y haga clic en **Finalizar**.
 - h) Luego, haga clic en **Añadir RAID** de nuevo.
 - i) Seleccione **RAID 1 (Espejo)**.
 - j) Seleccione las dos particiones sda4 y sdb3 en el área **Dispositivos disponibles** a la izquierda y transfíralas con **Agregar** al área **Dispositivos seleccionados** a la derecha.
 - k) Haga clic en **Siguiente**.
 - l) Confirme el valor predeterminado para el tamaño del fragmento con **Siguiente**.
 - m) En la siguiente ventana, seleccione **Datos y aplicaciones ISV** y haga clic en **Siguiente**.
 - n) En la siguiente ventana, seleccione **Ext4** como formato y el punto de montaje "/home" para el segundo dispositivo RAID (/dev/md1) y haga clic en **Finalizar**.
- 15) Haga clic en **Aceptar y Siguiente**.

Los datos de particionamiento se guardan; el particionamiento real del disco duro se realiza posteriormente.
- 16) En la ventana **Reloj y zona horaria**, seleccione la región y la zona horaria correctas.

Para ajustar la fecha y la hora o configurar un servidor NTP (para una base horaria uniforme), haga clic en el botón **Otros ajustes**. Haga clic en **Siguiente** cuando termine.
- 17) En la ventana **Usuarios locales**, agregue un usuario y una contraseña y haga clic en **Siguiente**.
- 18) En la ventana **Contraseña para el administrador del sistema "root"**, ingrese la contraseña del administrador del sistema con el perfil "root" en los campos **Contraseña para el usuario root** y **Confirmar contraseña** y luego haga clic en **Siguiente**.

La contraseña debe cumplir con las políticas de seguridad convencionales. Debe tener al menos 8 caracteres, al menos una letra minúscula, al menos una letra mayúscula, al menos un número y al menos un carácter especial.
- 19) En la ventana de **Configuración de instalación**, haga clic en **Instalar** y confirme la instalación haciendo clic de nuevo en **Instalar**.

La ventana **Configuración de instalación** es una descripción general de los componentes que se instalarán. Antes de finalizar la instalación, puede realizar aquí los cambios necesarios.

Una vez finalizado el proceso de instalación, el ordenador se reinicia con el sistema instalado.

Para seleccionar una resolución de pantalla adecuada:

- Haga clic en **Aplicaciones** en la barra de tareas.
- Luego, en el árbol del menú, haga clic en **Configuración > Pantallas**.
- En la ventana **Pantallas**, haga clic en **Pantalla desconocida**
- En la ventana emergente **Pantalla desconocida** que aparece, seleccione la resolución adecuada de la lista desplegable **Resolución** y, a continuación, haga clic en **Aplicar**.
- Finalmente, en la ventana emergente de confirmación que aparece, haga clic en **Guardar cambios**.

8.6 Configuración de una base temporal uniforme

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 ofrece por un servidor SNTP.

Se pueden utilizar como base temporal las siguientes variantes:

- **Servidor SNTP de la red interna (recomendado)**

Si es posible, se debe utilizar un servidor SNTP que esté presente en la red interna. En este caso, se requiere la dirección IP, la URL o el nombre DNS del servidor SNTP.

- **Servidor SNTP de Internet**

Si hay disponible acceso a Internet y está configurado, también se puede utilizar un servidor SNTP de Internet. En este caso se necesita la URL o el nombre DNS del servidor SNTP.

- **OpenScape Business X3/X5/X8 como servidor SNTP**

Como alternativa, el sistema de comunicación OpenScape Business X3/X5/X8 se puede utilizar como servidor SNTP. Para ello es necesario que OpenScape Business X3/X5/X8 esté conectado a la línea urbana mediante líneas RDSI y que la línea urbana aplique la hora del sistema. En este caso, OpenScape Business X3/X5/X8 debe configurarse como servidor SNTP (consulte la Documentación para el administrador); a continuación, la dirección IP del OpenScape Business X3/X5/X8 debe introducirse como servidor SNTP en Linux.

Los teléfonos IP reciben la fecha y la hora automáticamente del softswitch OpenScape Business S o, en el caso del OpenScape Business UC Booster Server, del sistema de comunicación OpenScape Business X3/X5/X8. La fecha y la hora de los PC cliente en que están instalados los clientes de comunicación OpenScape Business deben estar sincronizadas con el softswitch OpenScape Business S o con el sistema de comunicación OpenScape Business X3/X5/X8 (consulte las instrucciones del sistema operativo de los PC cliente para obtener información detallada).

8.6.1 Cómo configurar el servidor SNTP

Paso a paso

- 1) En la barra de tareas, haga clic en **Aplicaciones**.
- 2) En el grupo de menús, haga clic en **Herramientas > YaST**.
- 3) Introduzca la contraseña del usuario "root" y haga clic en **Continuar**. Se abre el YaST Control Center.
- 4) En el grupo de menús, haga clic en **Sistema**.
- 5) En la sección **Sistema**, haga clic en **Fecha y hora**.
- 6) Haga clic en **Cambiar**.
- 7) Active la opción **Sincronizar con servidor NTP**.
- 8) Introduzca un servidor NTP:
 - **Servidor SNTP de la red interna** (recomendado)
Introduzca la dirección IP, la URL o el nombre DNS del servidor SNTP directamente en el campo de lista.
 - **Servidor SNTP de Internet**
Seleccione el servidor SNTP deseado en la lista **Dirección de servidor NTP** o introduzca la URL o el nombre DNS del servidor SNTP directamente en el campo de lista.
 - **OpenScape Business X3/X5/X8 como servidor SNTP (solo para OpenScape Business UC Booster Server)**
Introduzca la dirección IP del sistema de comunicación OpenScape Business X3/X5/X8 directamente en el cuadro de lista.
- 9) Active la casilla de verificación **Guardar configuración NTP**.
- 10) Haga clic en **Configurar**.
- 11) Active la opción **Ahora y al arrancar**.
- 12) Haga clic en **OK** y, a continuación, en **Aceptar**.
- 13) Cierre la ventana con **OK**.
- 14) Cierre el **YaST2Control Center**.

8.7 Actualizaciones

Para recibir actualizaciones, es necesario registrarse directamente con Novell.

La instalación y el funcionamiento de la versión comercial SLES 15 SP6/SP7 de 64 bits es posible sin registro. Sin embargo, sigue siendo importante registrarse en Novell para obtener parches de seguridad y actualizaciones de software.

Se puede obtener un código de activación de Novell (código de registro) a través del elemento de pedido "Clave de actualización de OpenScape Business SLES". Al realizar el pedido, recibirá una LAC (Clave de Activación de Licencia). Utilizando este LAC, puede descargar el código de activación en el CLS (Servidor Central de Licencias), con el cual luego podrá crear una cuenta con Novell. Se recomienda que la cuenta del cliente se configure antes de la instalación de Linux.

Son posibles las siguientes variantes de actualización: Es requisito previo registrarse en Novell.

- **Actualizaciones durante la instalación de Linux (recomendado)**

Durante la instalación de Linux, las actualizaciones y los parches se pueden descargar en línea desde el servidor de descargas de Novell.

Excepción: Es posible que no se instalen los Service Packs.

- **Actualizaciones posteriores a la instalación de Linux y anteriores a la instalación del software de comunicación**

Tras la instalación de Linux, las actualizaciones y parches se pueden descargar manualmente desde el servidor de descargas de Novell utilizando YaST (Software - Actualizaciones en línea).

Excepción: Es posible que no se instalen los Service Packs.

- **Actualizaciones tras la instalación del software de comunicación**

Tras la instalación del software de comunicación, las actualizaciones y los parches se pueden descargar automáticamente desde el servidor de descargas de Novell. Al realizar estas actualizaciones, deben omitirse todas las actualizaciones y parches que requieran reiniciar el servidor Linux (actualizaciones interactivas). Después de cada 2 o 3 procesos de actualización, se recomienda iniciar una actualización manual para que también se instalen las actualizaciones interactivas omitidas.

Los ajustes correspondientes se realizan mediante YaST (Software - Actualizaciones en línea).

Es posible que existan desviaciones de las variantes mencionadas anteriormente, las cuales se describen en el Aviso de Lanzamiento del software de comunicación.

Nota: Durante una actualización en línea de SLES, la herramienta de administración Yast de Linux solicita eliminar rsyslog o syslog-ng. Solo debe eliminar el paquete rsyslog, ya que el paquete syslog-ng se utiliza en la función de seguimiento de OpenScape Business S.

8.7.1 Cómo activar las actualizaciones automáticas en línea

Paso a paso

- 1) En la barra de tareas, haga clic en **Aplicaciones**.
- 2) En el árbol de menús, haga clic en **Herramientas del sistema > YaST**.
- 3) Introduzca la contraseña del usuario "root" y haga clic en **Continuar**. Se abre la ventana **Configuración de administrador**.
- 4) Haga clic en **Configuración de actualización en línea**.
- 5) Active la casilla de verificación **Actualización en línea automática** y seleccione **diario**, **semanal** o **mensual** como intervalo.
- 6) Seleccione la casilla de verificación **Omitir parches interactivos**.
- 7) Haga clic en **Aceptar**.
- 8) Cierre la **Configuración de administrador**.

8.7.2 Cómo activar manualmente las actualizaciones online

Paso a paso

- 1) En la barra de tareas, haga clic en **Aplicaciones**.
- 2) En el árbol de menús, haga clic en **Herramientas del sistema > YaST**.
- 3) Introduzca la contraseña del usuario "root" y haga clic en **Continuar**. Se abre la ventana **Configuración de administrador**.
- 4) Haga clic en **Actualización online** y verá una lista de los parches disponibles (**Parches necesarios**) necesarios en la sección **Resumen**. Si ya tiene instalados todos los últimos parches, esta lista estará vacía; en caso contrario, seleccione todas las casillas que aparecen.
- 5) Haga clic en **Aceptar** para iniciar la actualización manual. Después de la actualización, la ventana se cierra automáticamente.
- 6) Cierre la **Configuración de administrador**.

8.7.3 Cómo configurar SLES 15 SP6/SP7 Yast2-Yast Online Update

Durante el procedimiento de actualización en línea, se deben seguir dos reglas para mantener la estabilidad del sistema de comunicación.

Configuración de repositorios

Ejecuta los siguientes comandos a través de PuTTY y verifica que se hayan ejecutado correctamente. Estos comandos añaden módulos SLES específicos a la lista de repositorios.

```
suseconnect -p sle-module-desktop-applications/15.6/x86_64
suseconnect -p sle-module-development-tools/15.6/x86_64
suseconnect -p sle-module-legacy/15.6/x86_64
```

Paquetes de actualización en línea

El mecanismo de actualización en línea recopila paquetes y parches a través de los repositorios de SUSE. Cuando se producen conflictos con los paquetes, YaST2 Online Update muestra advertencias.

En una instalación limpia de OpenScape Business, algunos paquetes están bloqueados para garantizar la estabilidad del sistema.

No actualice ni elimine estos paquetes bloqueados.

Si una advertencia le solicita que elimine un paquete bloqueado, seleccione **No instalar parche** en la ventana de resolución de conflictos.

Nota: Para obtener más información sobre las actualizaciones de SLES Online, consulte la documentación correspondiente de SUSE: *Guía de administración de servidores SUSE Linux Enterprise, capítulo 7 "Actualización en línea de YaST"*.

8.8 Copia de seguridad y recuperación de software de servidor

Hay que hacer una copia de seguridad del sistema operativo Linux para poder restablecerlo en caso de emergencia.

Después de la puesta en servicio inicial y antes de cada actualización manual se recomienda encarecidamente hacer una copia de seguridad completa del PC de servidor o de las particiones correspondientes con una herramienta adecuada. Si, por ejemplo, después de una actualización se produce un error grave, hay que restablecer completamente el PC de servidor.

En un entorno virtualizado se puede copiar toda la máquina virtual.

Si se hace una copia de seguridad de todo el PC de servidor, esa copia de seguridad incluirá los datos del software de comunicación. Si solo se hace una copia de seguridad del sistema operativo, también hay que hacer con regularidad una copia de seguridad de los datos del software de comunicación.

9 Puesta en servicio inicial por OpenScape Business X

Se describe la puesta en servicio inicial de OpenScape Business X1/X3/X5/X8. El sistema de comunicación y los componentes correspondientes se integran en una estructura previa integrada por una LAN de clientes y una red de telefonía TDM. Se configuran el acceso a Internet y la conexión de línea urbana y se configura la extensión conectada.

La puesta en servicio inicial de OpenScape Business X1/X3/X5/X8 (el "sistema de comunicación") se realiza con el programa de administración OpenScape Business Assistant (la "Gestión basada en Web" o "WBM").

Aquí se describe la configuración inicial estándar de componentes de uso habitual. Los pasos de instalación dependen del sistema de comunicación y de los componentes (p.ej. UC Booster Card) en cuestión. Durante la configuración inicial, puede que tenga que elegir entre varias opciones en algunos puntos u omitir ajustes por completo. También es posible que los pasos de instalación que aquí se describen no aparezcan en su sistema de comunicación.

En los siguientes capítulos encontrará información detallada sobre la configuración 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.

Estos son los pasos de instalación más importantes:

- Configuración de direcciones IP y DHCP
- Configuración de país y hora
- Números de teléfono del sistema e interconexión
- Configuración RDSI
- Acceso a Internet
- Telefonía Internet
- Configuración de extensiones
- Registro de licencia
- Almacenamiento de datos

9.1 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 S₀.
- 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 *Documentación para el administrador, Instalación inicial de X3/X5/X8*).
- Hay disponible, y se conoce, un plan de numeración (véase *Documentación para el administrador, Instalación inicial de X3/X5/X8*).

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.

9.2 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.

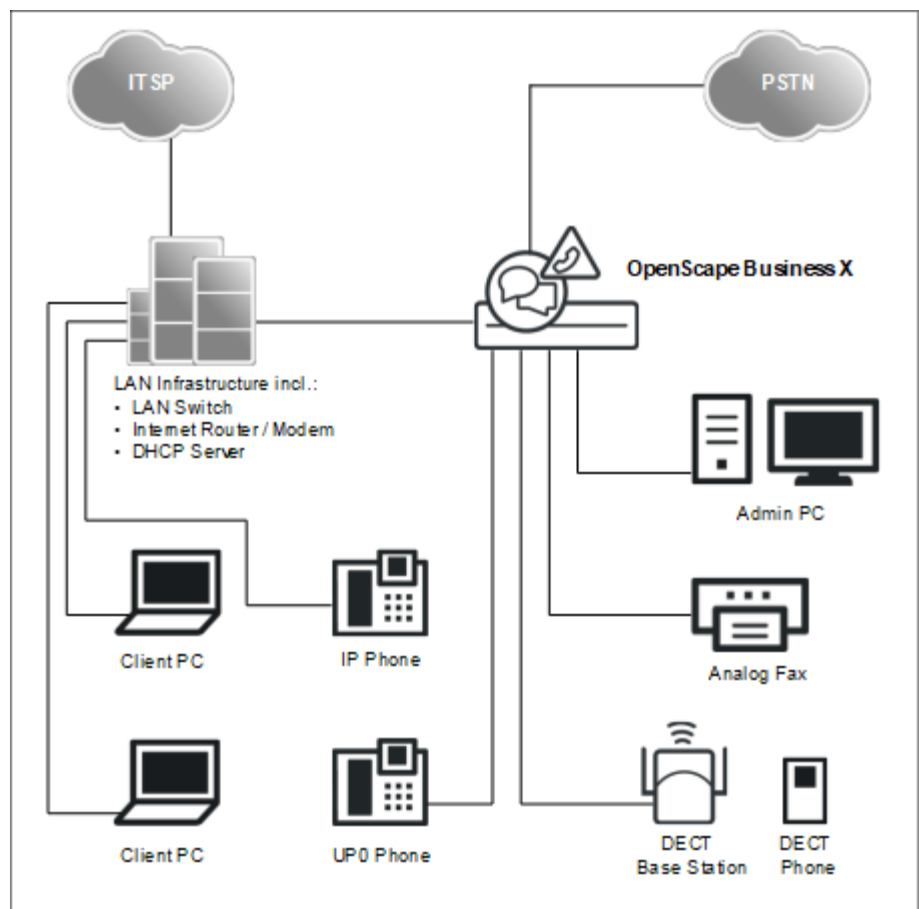
- Extensiones analógicas

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.



9.3 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
Códigos de ruta (códigos externos):		
Ruta 1 (línea urbana RDSI, analógica)	0 = Mundial / 9 = EE. UU.	0 = Mundial / 9 = EE. UU.
Ruta 8 (UC Suite)	-	851
Ruta 12-15 (línea urbana, ITSP)	sin preasignar	855-858
Ruta 16 (interconexión)	sin preasignar	859
Número de teléfono para el acceso remoto	sin preasignar	sin preasignar
Número de teléfono para mensajes de voz	351	351
UC Smart	-	sin preasignar
UC Suite		

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.

9.4 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 rango de direcciones IP 192.168.1.0 -x:

Área direcc. IP	Clientes
192.168.1.1 hasta 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
192.168.1.50 hasta 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 remoto
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 consultar en la Gestión basada en Web (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: Máscara de 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)

Puesta en servicio inicial por OpenScape Business X

Puesta en servicio inicial

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: Máscara de red
- 192.169.3.2: dirección IP interna del sistema de comunicación

Se puede modificar mediante **Modo Experto > Telefonía > Payload > Módulos hardware > Editar ajustes DSP**

- 192.170.2.1: dirección IP de la interfaz LAN3 (puerto de administración)

Se puede modificar mediante **Modo Experto > Telefonía > Interfaces de red > Placa base > LAN 3 (Admin)**

9.5 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 X1/X3W/X5W solo se puede encender si la caja 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.

9.5.1 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).

9.5.2 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).

9.5.3 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.

9.6 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.

9.6.1 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.

9.6.2 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. Está 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](#) en la página 187).

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

Requisitos previos

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

System Settings	
Display Logo:	OSBiz
Brand:	OpenScape Business
OpenScape Business	
OpenScape Business - IP address:	192.168.186.13
OpenScape Business - Netmask:	255.255.255.0
OpenScape Business - Default Routing via:	LAN
OpenScape Business - IP Address of Default Router:	192.168.186.22
Application Board	
Application Board - IP address:	192.168.1.3
Application Board - Netmask:	255.255.255.0
Application Board - IP Address of Default Router:	192.168.186.22

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.

9.6.2.2 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**.

The screenshot shows a web-based configuration interface titled 'Setup - Wizards - Basic Installation - Initial Installation'. It features a 'System Settings' section with two expandable panels: 'OpenScape Business' and 'Application Board'. The 'OpenScape Business' panel contains fields for 'IP address' (192.168.186.13), 'Netmask' (255.255.255.0), 'Default Routing via' (LAN), and 'IP Address of Default Router' (192.168.186.22). The 'Application Board' panel contains fields for 'IP address' (192.168.1.3), 'Netmask' (255.255.255.0), and 'IP Address of Default Router' (192.168.186.22).

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.

9.6.2.3 Cómo especificar el nombre de dispositivo

Requisitos previos

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

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.

9.6.3 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 (*Documentación para el administrador, Deployment Service (DLI y DLS)*). El servidor DHCP debe conocer la dirección IP del DLI integrado o del servidor DLS externo.

Dispone de 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 (*Documentación para el administrador, 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.

9.6.3.1 Cómo desactivar el servidor DHCP interno

Requisitos previos

En la red interna, hay activo un servidor DHCP externo (por ejemplo, el servidor DHCP del router Internet).

Se encuentra en la ventana **Ajustes globales DHCP**.

Paso a paso

- 1) Desactive la casilla de verificación **Act. servidor DHCP**.
- 2) Haga clic en **OK & Continuar**.

Pasos siguientes

Configure los ajustes de país y hora.

9.6.3.2 Cómo activar y configurar el servidor DHCP interno

Requisitos previos

En la red interna, el servidor DHCP externo (por ejemplo, el servidor DHCP del router Internet) está desactivado.

Se encuentra en la ventana **Ajustes globales DHCP**.

The screenshot shows the 'DHCP Global Settings' window. At the top, there is a blue header bar with the text 'Setup - Wizards - Network / Internet - Network Configuration'. Below the header, the title 'DHCP Global Settings' is centered. A red warning message states: 'In Expert Mode, DHCP was set to Relay Agent. If you now switch the DHCP server on, the IP addresses HiPath OpenOffice will be distributed. Network problems may occur as a result.' The settings are organized into sections: 'Enable DHCP Server' (checked), 'Netmask' (255.255.255.0), 'Broadcast Address' (0.0.0.0 optional), 'Default Gateway' (Preferred Gateway: 192.168.1.2), 'DNS Server' (Domain Name, Preferred Server: 192.168.1.2), 'Lease time in hours (0 infinite): 1', and 'Enable Dynamic DNS Update' (unchecked).

Paso a paso

- 1) Deje activada la casilla de verificación **Act. servidor DHCP**.
- 2) En el campo **Máscara de red** ajuste la máscara de red a su rango de direcciones IP (p. ej. 255.255.255.0).
- 3) En el campo **Gateway favorito**, introduzca la dirección IP del router de Internet (por ejemplo, 192.168.1.1).
- 4) En el campo **Servidor favorito**, introduzca la dirección IP del servidor DNS (por ejemplo, la dirección IP del router Internet, 192.168.1.1).
- 5) Haga clic en **OK & Continuar**. Se muestra la ventana **Pool de direcciones DHCP**.

The screenshot shows the 'DHCP Address Pool' window. It has a blue header bar with 'Setup - Wizards - Network / Internet - Network Configuration'. The title 'DHCP Address Pool' is centered. The settings include 'Subnet address' (192.168.1.0), 'Subnet mask' (255.255.255.0), and 'Address range 1' (192.168.1.50 - 192.168.1.254).

- 6) En los campos **Dirección de subred**, **Máscara de red** y **Área direcciones 1** defina el rango de direcciones IP que va a administrar el servidor DHCP interno.

Si en la red interna se utilizan direcciones IP fijas (por ejemplo, para un servidor de impresora) se debe seleccionar el área de direcciones IP (pool

de direcciones DHCP) de forma que las direcciones IP fijas no estén dentro del área de direcciones IP.

Ejemplo:

Router Internet: 192.168.1.1

OpenScape Business: 192.168.1.2

UC Booster Card: 192.168.1.3

Dirección de subred: 192.168.1.0

Máscara de red: 255.255.255.0

Servidor de impresora: 192.168.1.10

Pool de direcciones DHCP: 192.168.1.50 bis 192.168.1.254

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

Pasos siguientes

Configure los ajustes de país y hora.

9.6.4 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).

9.6.4.1 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 del registro de incidencias del cliente**, introduzca el idioma en el que se mostrarán los registros de eventos (registros de eventos del sistema, registros de 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.

9.6.4.2 Cómo introducir la identificación del sistema DECT

Requisitos previos

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

Puesta en servicio inicial por OpenScape Business X

Setup - Wizards - Basic Installation - Initial Installation

Basic Configuration

Language settings

System Country Code: Germany

Language for Customer Trace Log: English

Time settings

Date and Time: Day: 03, Month: 03, Year: 2023, hh:mm:ss: 10:40:00

Timezone: (UTC +02:00) Athens, Beirut, Istanbul, Minsk

Detect date and time via an SNTP server

Date and Time via an external SNTP Server: ☒

IP Address / DNS Name of External Time Server: 192.168.142.49

Poll Interval for External Time Server: Continuous

CMI data

System ID: 00000000

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.

9.6.4.3 Configuración manual de fecha y hora

Requisitos previos

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

Setup - Wizards - Basic Installation - Initial Installation

Basic Configuration

Language settings

System Country Code: Germany

Language for Customer Trace Log: English

Time settings

Date and Time: Day: 03, Month: 03, Year: 2023, hh:mm:ss: 10:40:00

Timezone: (UTC +02:00) Athens, Beirut, Istanbul, Minsk

Detect date and time via an SNTP server

Date and Time via an external SNTP Server: ☒

IP Address / DNS Name of External Time Server: 192.168.142.49

Poll Interval for External Time Server: Continuous

CMI data

System ID: 00000000

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.

9.6.4.4 Obtención de la fecha y hora de un servidor SNTP**Requisitos previos**

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

The screenshot shows the 'Basic Configuration' window with the following settings:

- Language settings:** System Country Code: Germany, Language for Customer Trace Log: English.
- Time settings:** Date and Time: Day 03, Month 03, Year 2023, hh:mm:ss 10:40:00. Timezone: (UTC +02:00) Athens, Beirut, Istanbul, Minsk.
- Detect date and time via an SNTP server:** Date and Time via an external SNTP Server: ☒. IP Address / DNS Name of External Time Server: 192.168.142.49. Poll Interval for External Time Server: Continuous.
- CMi data:** System ID: 00000000.

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.

9.6.5 Solución UC

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

Dispone de 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**

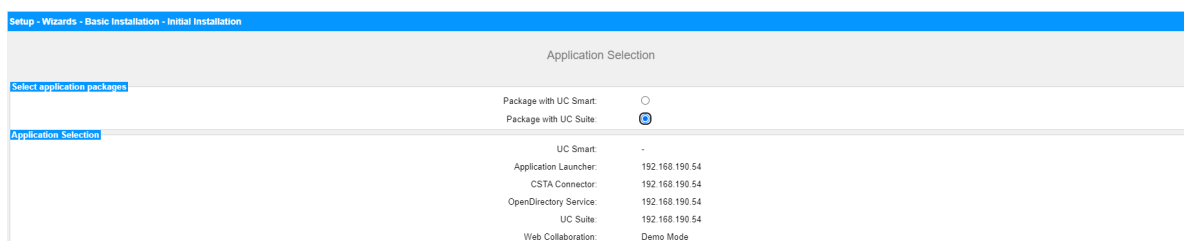
La solución de Comunicaciones Unificadas UC Suite está integrada en el servidor Linux externo "OpenScape Business UC Booster Server".

9.6.5.1 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 **Modificar 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.

9.6.6 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.

9.6.6.1 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.

9.7 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.

9.7.1 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.

9.7.2 Números de teléfono del sistema e interconexión

En la ventana **Resumen**, indique los números de teléfono del sistema (número 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 o 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.

9.7.2.1 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 **Descripción general del sistema**.

Setup - Wizards - Basic Installation - Basic Installation

1 System Overview 2 Central Functions for Stations 3 Provider configuration and activation for Internet Telephony 4 Select a station 5 Configured Stations 6 Automatic Configuration of Application Suite 7 Configure MeetLife Conference 8 Configure E-Mail Forwarding

Note: changes done in expert mode must be reviewed/repeated after running through the wizard.
Note: At least the configuration of the 'Country code' is needed for features such as 'Internet telephony' and 'MeetLife conference'.
If you want your OpenScape Business in "OpenScape Business Network Integration" you should select the "Network Integration" check box and enter a node ID. In this case, make sure that this node ID is unique within the whole network integration.
Normally, this integration is done by a Service Technician.
For a standalone OpenScape Business clear the "Network Integration" check box.

PABX number

Country code: 00 (49) (mandatory)
Local area code: 0 (186) (optional)
PABX number: (27) (optional)

General

International Prefix: (00)

Network Parameters

Network Integration: ☐
Node ID: (2)

Upstream of your internet connection

Upstream up to (Kbps): (2048)

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.

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

Requisitos previos

Tiene un acceso individual.

Se encuentra en la ventana **Descripción general del sistema**.

Puesta en servicio inicial por OpenScape Business X

Setup - Wizards - Basic Installation - Basic Installation

1 System Overview 2 Central Functions for Stations 3 Provider configuration and activation for Internet Telephony 4 Select a station 5 Configured Stations 6 Automatic Configuration of Application Suite 7 Configure MeetMe Conference 8 Configure E-Mail Forwarding

Note: changes done in expert mode must be reviewed/repeated after running through the wizard.
Note: At least the configuration of the 'Country code' is needed for features such as 'Internet telephony' and 'MeetMe conference'.
If you want your OpenScape Business in "OpenScape Business Network Integration" you should select the "Network Integration" check box and enter a node ID. In this case, make sure that this node ID is unique within the whole network integration.
Normally, this integration is done by a Service Technician.
For a standalone OpenScape Business clear the 'Network Integration' check box.

PABX number

Country code: 00 49 (mandatory)
Local area code: 0 186 (optional)
PABX number: 27 (optional)

General

International Prefix: 00

Network Parameters

Network Integration: ☐
Node ID: 2

Upstream of your internet connection

Upstream up to (Kbps): 2048

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.

9.7.2.3 Cómo activar o desactivar la interconexión

Requisitos previos

Se encuentra en la ventana **Descripción general del sistema**.

Setup - Wizards - Basic Installation - Basic Installation

1 System Overview 2 Central Functions for Stations 3 Provider configuration and activation for Internet Telephony 4 Select a station 5 Configured Stations 6 Automatic Configuration of Application Suite 7 Configure MeetMe Conference 8 Configure E-Mail Forwarding

Note: changes done in expert mode must be reviewed/repeated after running through the wizard.
Note: At least the configuration of the 'Country code' is needed for features such as 'Internet telephony' and 'MeetMe conference'.
If you want your OpenScape Business in "OpenScape Business Network Integration" you should select the "Network Integration" check box and enter a node ID. In this case, make sure that this node ID is unique within the whole network integration.
Normally, this integration is done by a Service Technician.
For a standalone OpenScape Business clear the 'Network Integration' check box.

PABX number

Country code: 00 49 (mandatory)
Local area code: 0 186 (optional)
PABX number: 27 (optional)

General

International Prefix: 00

Network Parameters

Network Integration: ☐
Node ID: 2

Upstream of your internet connection

Upstream up to (Kbps): 2048

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.

9.7.3 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.

Dispone de 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 **modifica los números de llamada preconfigurados**, hay que revisar o repetir la configuración personalizada que se hubiera hecho en la 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.

9.7.3.1 Cómo mostrar los datos de extensión

Requisitos previos

Se encuentra en la ventana **Funciones centrales para extensiones**.

Paso a paso

- 1) Active el campo de opción **Mostrar configuración de extensiones**.

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

- 3) Haga clic en **Aceptar**. Regresa a la ventana **Funciones centrales para extensiones**.
- 4) Si no quiere modificar ningún dato de extensión, haga clic en **OK & Continuar**.

9.7.3.2 Cómo borrar todos los números de llamada

Requisitos previos

Se encuentra en la ventana **Funciones centrales para extensiones**.

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**. Se borran todos los números de teléfono preasignados. A continuación aparece la ventana **Cambiar números de función y de llamada preconfigurados**.

Change preconfigured call and functional numbers			
- The Internet Telephony numbers must be available. It is not possible to delete these numbers. - Please keep in mind that these numbers are not available for station or group dialing use. - Automatic changes may be applied. Please check LCR dial plan and correct if necessary.			
Preconfiguration for Internet Telephony			
Announcement Player	659999		
Voicemail call number (Smart VM)			
Autoattendant call number (Smart VM)			
Attendant code			
Remote Admin call number	659995		
Licensing call number	659994		
Functional numbers for Conferencing	-	-	-
Functional number for MeetMe Conferencing	-		

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

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

Requisitos previos

Se encuentra en la ventana **Funciones centrales para extensiones**.

Paso a paso

- 1) Active la 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 haga clic a continuación en **Aceptar**. Regresa a la ventana **Funciones centrales para extensiones**.
- 4) Si no desea modificar más datos de extensión, haga clic en **OK & Continuar**.

9.7.3.4 Cómo importar los datos de extensión mediante un archivo XML

Requisitos previos

Se encuentra en la ventana **Funciones centrales para extensiones**.

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) Active la opción **Importar archivo CSV para extensiones**.
- 2) Haga clic en **Ejecutar función**.
- 3) Mediante **Examinar** seleccione el archivo XML que ha creado y haga clic en **Abrir**.
- 4) A continuación, haga clic en **Aceptar**. Se importan los datos de extensión.
- 5) Haga clic en **OK & Continuar**.

9.7.3.5 Cómo mostrar datos de Mass

Requisitos previos

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

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: Prueba de consistencia de front-end y Prueba de consistencia 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 consistencia 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 modificar los datos y la ventana vuelve al modo de edición. El modo de edición restringida garantiza 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 el módulo al 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 a cabo.

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.

9.7.4 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 S₀.

Dispone de 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 conexiones S_0 internas.

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.

9.7.4.1 Cómo configurar la conexión de extensiones RDSI

Requisitos previos

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

Box	Slot	S0-Port	Board Type	Point-to-point connection	Point-to-multipoint connection	Internal S0 connection	Settings configured in expert mode
1	1	1	STLS2N	☐	☐	☒	
1	1	2	STLS2N	☐	☐	☒	

Paso a paso

- 1) Deje desactivada la casilla de verificación **Sin comunicación a través de la 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.

9.7.4.2 Cómo configurar la conexión de centralita RDSI

Requisitos previos

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

Box	Slot	S0-Port	Board Type	Point-to-point connection	Point-to-multipoint connection	Internal S0 connection
1	1	1	STLS2N	☒	☐	☐
1	1	2	STLS2N	☐	☐	☒

Paso a paso

- 1) Para configurar la conexión urbana RDSI, deje desactivada la casilla de verificación **Sin comunicación a través de la lín. urbana RDSI (S0)**.
- 2) En la conexión S₀ deseada, active el campo de opción **Conexión de centralita**.
- 3) Haga clic en **OK & Continuar**.

9.7.4.3 Cómo configurar el acceso individual RDSI

Requisitos previos

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

Box	Slot	S0-Port	Board Type	Point-to-point connection	Point-to-multipoint connection	Internal S0 connection
1	1	1	STLS2N	☐	☒	☐
1	1	2	STLS2N	☐	☐	☒

Paso a paso

- 1) Para configurar la conexión urbana RDSI, deje desactivada la casilla de verificación **Sin comunicación a través de la lín. urbana RDSI (S0)**.
- 2) Junto a la conexión S₀ deseada, active el campo de opción **Acceso individual RDSI**.
- 3) Haga clic en **OK & Continuar**.

Box	Slot	S0-Port	ISDN Multiple Subscriber Numbers
1	1	1	
1	1	2	
1	1	3	
1	1	4	
1	1	5	
1	1	6	
1	1	7	
1	1	8	
1	1	9	
1	1	10	

- 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 puede indicar 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**.

9.7.4.4 Cómo desactivar la configuración RDSI

Requisitos previos

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

Paso a paso

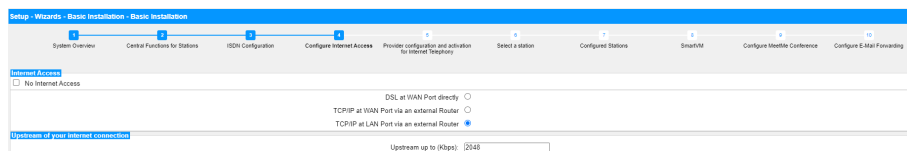
- 1) Desactive la casilla de verificación **Sin telefonía a través de la lín. urbana RDSI (S0)**.

Nota: También se pueden realizar llamadas a través de un ITSP (Internet Telephony Service Provider), véase .

- 2) Haga clic en **OK & Continuar**.

9.7.5 Acceso a Internet

En la ventana **Configuración de Acceso a Internet** puede configurar el 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).

Solo hay que elegir una de las opciones presentadas.

- 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.



Dispone de 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.

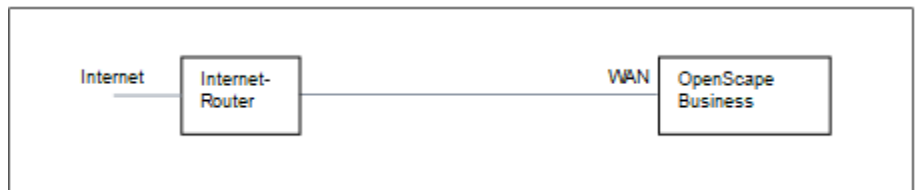
- Acceso a Internet a través de un router de Internet externo

Desea operar el sistema de comunicación en un router Internet externo. El proveedor de servicios de Internet ya está configurado en el router Internet.

Dispone de 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)

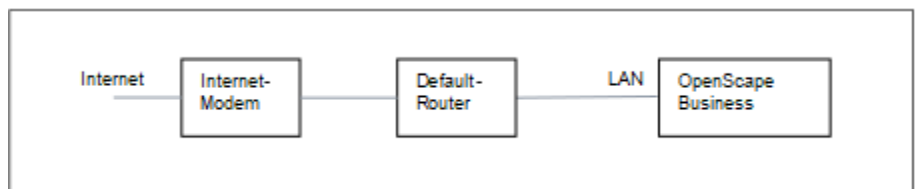


Para ello, utilice la conexión WAN del sistema de comunicación.

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.

9.7.5.1 Cómo configurar el acceso a Internet a través de un router de Internet externo mediante la conexión LAN

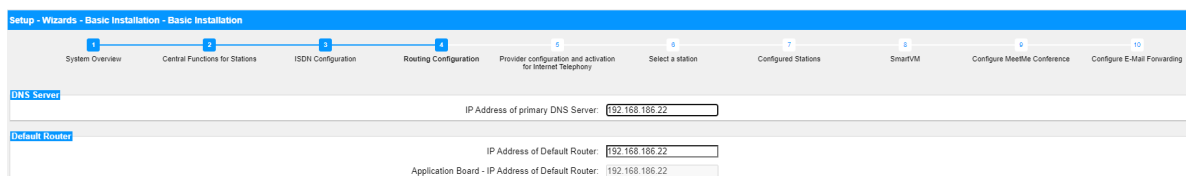
Requisitos previos

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 **Configuración de Acceso a Internet**.

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 & 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**.

9.7.5.2 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 **Configuración de Acceso a Internet**.

Paso a paso

- 1) Desactive la casilla de verificación **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 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**.
- 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) Active la casilla de verificación **Traducción dirección 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 Kbit/s para la descarga o para la carga. El valor le será suministrado por su ISP.
- 8) Haga clic en **OK & Continuar**.

9.7.5.3 Cómo configurar el acceso a Internet a través de un ISP preconfigurado

Requisitos previos

Se encuentra en la ventana **Configuración de Acceso a Internet**.

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: Conoce los datos de una cuenta DynDNS (nombre, contraseña, nombre host, nombre de dominio del proveedor DynDNS)

Paso a paso

- 1) Desactive la casilla de verificación **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 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 campo **Cortar automáticamente tras (segundos)**, indique el tiempo de inactividad tras el cual deberá interrumpirse la conexión (por ejemplo, 60 segundos).
- 6) 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%).
- 7) Haga clic en **OK & Continuar**. 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, 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**.
- 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 **OK & Continuar**.

9.7.5.4 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)		
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.	
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 autenticación 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		

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.	

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 **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 campo **Cortar automáticamente tras (segundos)**, indique el tiempo de inactividad tras el cual deberá interrumpirse 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.
 - 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. El estándar habitual es el modo de autenticación **Cliente CHAP**.
 - El ISP no solicita autenticación: asegúrese de que la casilla de verificación **Autenticación PPP** está 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 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%).

- 9) Haga clic en **OK & Continuar**. 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=<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**.
- 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) Clic **OK & Cont.**

9.7.5.5 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.	

Campo	Descripción	Valor del ISP
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 autenticación 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.**

9.7.5.6 Cómo desactivar el acceso a Internet

Requisitos previos

Se encuentra en la ventana **Configuración de Acceso a Internet**.

Paso a paso

- 1) Desactive la casilla de verificación **Sin acceso a Internet**.
- 2) Haga clic en **OK & Continuar**.

9.7.6 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.

Dispone de 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 *Documentación para el administrador, 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 rango de números de teléfono (p.ej. (+49) 89 7007-100 a (+49) 89 7007-147). Los números de teléfono de ese margen 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.

n.º llam. interno	Nombre	N.º llam. marc. 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).

9.7.6.1 Cómo configurar un ITSP predefinido

Requisitos previos

Se encuentra en la ventana **Configuración y activación de proveedor para telefonía Internet**.

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) Desactive **Sin teléf. a través 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. Luego, haga clic en **Aceptar**.
- 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 **OK y Continuar**.
- 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 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 de teléfono estándar**, introduzca el número de teléfono que se utilizará en caso de llamadas salientes para las extensiones que no tengan un número propio.
- 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 telefonía por Internet - Opción 2:
Usar número interno (Nº llam) / Entradas individuales: Dispone de una conexión de telefonía por Internet y ha recibido números de llamada individuales como números de teléfono de telefonía por Internet (por ejemplo, 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 telefonía por Internet - Opción 3:

Usar número interno (n.º llamada) / Intervalo: 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) Introduzca el intervalo de números DID deseado para la estación de telefonía por Internet en los campos **De** y **A** después del Rango de marcación entrante directa. Por defecto están registrados los valores 100 - 147.

14) Haga clic en **OK y Continuar**.

15) Si desea configurar más cuentas con los números de telefonía Internet correspondientes, repita los pasos del 7 al 14.

16) Haga clic en **OK y Continuar**. 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**.

Name of Internet Telephony Station	Internet Telephony Phone Number	Internal Call Number	Use as PABX number for outgoing calls
0186136	755555555	-	☐

- a) En la línea correspondiente de la lista desplegable **N.º 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 **OK y Continuar**. 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 **OK y Continuar**.

- 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.

- 21) Haga clic en **OK y Continuar**.
- 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 **Desconexión forzosa a las (hrs:min)**, establezca hora para desconectar Internet (por ejemplo, 04:59).
- c) Haga clic en **OK y Continuar**.
- 23) En la columna **Cifras marcadas** introduzca los números de teléfono especiales deseados.

Special phone number	Dialed digits	Dial over Provider
1	0C112	Sipgate
2	0C110	Sipgate
3	0C0137Z	Sipgate
4	0C0136Z	Sipgate
5	0C0900Z	Sipgate
6	0C118Z	Sipgate
7	0C116Z	Sipgate
8	0C115	Sipgate
9	0C010Z	Sipgate

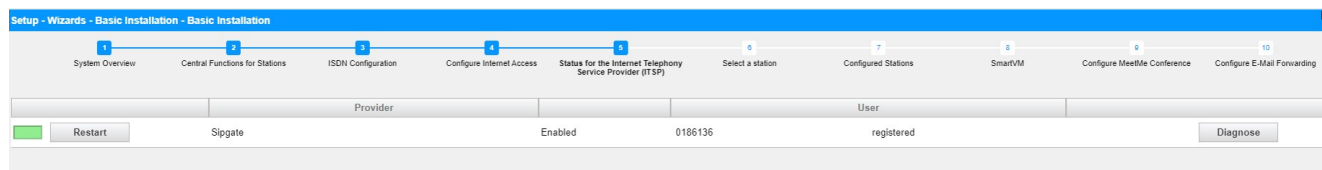
Son válidas estas entradas de número de teléfono:

- 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 marcación simulado (se puede introducir 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 **OK** y **Continuar**. 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 **Cont.** y luego en **Salir**.

9.7.6.2 Cómo desactivar telefonía Internet

Requisitos previos

Se encuentra en la ventana **Configuración y activación de proveedor para telefonía Internet**.

Paso a paso

- 1) Deje activada la casilla de verificación **Sin telefonía a través de Internet**.
- 2) Haga clic dos veces en **OK & Continuar**.

9.7.7 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 *Documentación para el administrador, Configuración de la solución Cordless integrada*

5) Configurar extensiones IP y SIP

Son extensiones IP y SIP, por ejemplo, teléfonos LAN y teléfonos WLAN.

9.7.7.1 Cómo configurar extensiones RDSI

Requisitos previos

Se encuentra en la ventana **Seleccionar extensión - Terminales RDSI** del asistente **Configuración básica**.

Las conexiones S₀ a las que están conectados los teléfonos RDSI, deben estar configuradas como conexiones S₀ internas.

Box	Slot	SD-Port	Callno	First Name	Last Name	Display	DID	Fax Callno	Fax DID	Class of service	Call pickup
1	1	1								International	-
1	1	2								International	-

Paso a paso

- 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.
- 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.
- 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.º 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**.

The screenshot shows the 'Setup - Wizards - Telephones / Subscribers - RDSN Devices' window. The 'Station' tab is selected, displaying fields for 'First Name', 'Last Name', 'Display (for Subscriber)', 'Call number', and 'Direct inward dialing (Number for Direct Inward Dialing)'. The 'Parameter' tab is also visible, showing fields for 'Device Type', 'Clip/Lin', 'Access', 'Extension Type', 'Language', 'Call signaling internal', 'Call signaling external', and 'ITSP Loc-ID'. The 'Voicemail' tab is at the bottom, showing fields for 'UC Smart Mailbox type', 'Recording', 'Greeting', and 'Password Reset'.

- b) En el campo **Clip/Lin** indique un número de teléfono (número de marcación directa o MSN) que aparecerá en el display del usuario llamado en lugar del número de teléfono en sí 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, modif. flags ext. Para consultar una descripción de los flags de extensión, véase *Documentación para el administrador, Extensión > Extensión > Parámetros de extensión*.
- i) Clic **OK & Cont.**
- 8) Si desea configurar más extensiones RDSI, haga clic en **Guardar datos y repita los pasos 1 a 7**.
- 9) Clic **OK & Cont.**

9.7.7.2 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.

Box	Slot	a/b-Port	Callno	First Name	Last Name	Display	DID	Fax Callno	Fax DID	Class of service	Call pickup
1	3	1								International	-
1	3	2								International	-
1	3	3								International	-
1	3	4								International	-

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.º 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:
- En la línea de la extensión analógica deseada, haga clic en el símbolo en forma de lápiz **Editar**.

- En **Clip/Lin** indique número teléfono (número 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.

- En la lista desplegable **Tipo de ext.** seleccione el tipo del terminal analógico (p. ej. Fax).
- 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 **Mar. dir. para telefonía Internet** si la telefonía Internet no está configurada o no hay activado ningún ITSP.

- 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, modif. flags ext. Para consultar una descripción de los flags de extensión, véase *Documentación para el administrador*, **Extensión > Extensión > Parámetros de extensión**.
 - i) Clic **OK & Cont.**
- 8) Si desea configurar otra extensión analógica más, haga clic en **Guardar datos** y repita los pasos 1 a 7.
 - 9) Clic **OK & Cont.**

9.7.7.3 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.

Box	Slot	UP0-Port	Callno	First Name	Last Name	Display	DID	Fax Callno	Fax DID	Class of service	Call pickup
1	2	1 M								International	-
1	2	2 M								International	-
1	2	3 M								International	-
1	2	4 M								International	-
1	2	5 M								International	-
1	2	6 M								International	-
1	2	7 M								International	-
1	2	8 M								International	-
1	2	1 S								International	-
1	2	2 S								International	-

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.º 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 línea extensión deseada, haga clic en símbolo lápiz **Editar**.

b) En **Clip/Lin** indique número teléfono (número 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 **Marc. 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 ha 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, modif. flags ext. Para consultar una descripción de los flags de extensión, véase *Documentación para el administrador*, **Extensión > Extensión > Parámetros de extensión**.
 - j) Clic **OK & Cont.**
- 8) Si quiere configurar otra extensión UP0, haga clic en **Guardar datos** y repita los pasos 1 a 7.
 - 9) Clic **OK & Cont.**

9.7.7.4 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 (consulte la *Documentación del administrador*, *Configuración de extensiones*).

Box	Slot	Callno	First Name	Last Name	Display	DID	Type	Fax Callno	Fax DID	Class of service	Call pickup
1	0	-	ppc0	x651000	x651000, ppc0	-	System Client	-	-	International	-
1	0	-	651001	hfa1	hfa1, 651001	-	System Client	-	-	International	-
1	0	-	651002	hfa2	hfa2, 651002	-	System Client	-	-	International	-
1	0	-	651003	hfa3	hfa3, 651003	-	System Client	-	-	International	-
1	0	-	651004	hfa4	hfa4, 651004	-	System Client	-	-	International	-
1	0	-	651005	hfa5	hfa5, 651005	-	System Client	-	-	International	-
1	0	-	651007	hfa7	hfa7, 651007	-	System Client	-	-	International	-
1	0	-	651009	hfa9	hfa9, 651009	-	System Client	-	-	International	-
-	-	-	-	-	-	-	No Port	-	-	International	-
-	-	-	-	-	-	-	No Port	-	-	International	-

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.º 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:
- En la línea de la extensión deseada, haga clic en el símbolo en forma de lápiz **Editar**.

- 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.

- En la lista desplegable **Tipo de ext.**, haga clic en el tipo de terminal inalámbrico.
- En la lista desplegable **Idioma** deje la selección predeterminada. Esta configuración no es importante para los terminales inalámbricos.
- En la sección **Marc. 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.

- 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 obtener una descripción de los indicadores de extensión, consulte *Documentación del administrador*, **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**.

9.7.7.5 Cómo configurar extensiones IP y SIP

Requisitos previos

Se encuentra en la ventana **Seleccionar extensión - Teléfonos LAN**.

Para poder poner en servicio los teléfonos WLAN necesita una red LAN inalámbrica operativa.

Setup - Wizards - Telephones / Subscribers - IP Telephones

Select a station -LAN Phones/WLAN Phones

☒ Take DID from changed call number

Box	Slot	Callno	First Name	Last Name	Display	DID	Type	Fax Callno	Fax DID	Class of service	Call pickup
1	0	-	ppc0	x651000	x651000_ppc0	-	System Client	-	-	International	-
1	0	-	651001	hfa1	hfa1_651001	-	System Client	-	-	International	-
1	0	-	651002	hfa2	hfa2_651002	-	System Client	-	-	International	-
1	0	-	651003	hfa3	hfa3_651003	-	System Client	-	-	International	-
1	0	-	651004	hfa4	hfa4_651004	-	System Client	-	-	International	-
1	0	-	651005	hfa5	hfa5_651005	-	System Client	-	-	International	-
1	0	-	651007	hfa7	hfa7_651007	-	System Client	-	-	International	-
1	0	-	651009	hfa9	hfa9_651009	-	System Client	-	-	International	-
-	-	-	-	-	-	-	No Port	-	-	International	-
-	-	-	-	-	-	-	No Port	-	-	International	-

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.º 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.

Puesta en servicio inicial por OpenScape Business X

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 la *Documentación del administrador, 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: active la casilla de verificación **Autenticación activa**.
- h) Solo para teléfonos SIP: Introduzca la contraseña de autenticación en los campos **Contraseña** y **Confirmar contraseña**.
- i) Solo para teléfonos SIP: en el campo **ID de usuario SIP / Nombre usuario**, indique la identificación de usuario para la autenticación.
- j) Solo para teléfonos SIP: en el campo **Ámbito**, indique la zona correspondiente a la autenticación.
- k) Haga clic en **OK & Continuar**.
- l) Si es necesario, modifique los flags de extensión. Para obtener una descripción de los indicadores de extensión, consulte *Documentación del administrador*, **Extensión > Extensión > Parámetros de extensión**.
- m) 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**.

9.7.8 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.

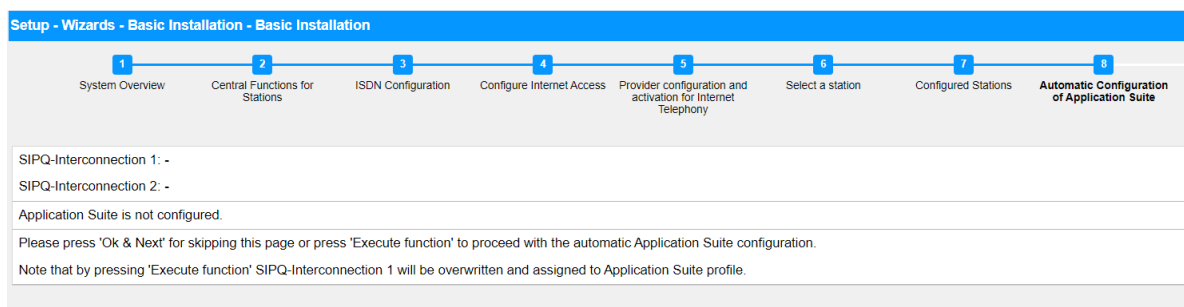
Nota: Esta ventana solo aparece si en el asistente **Instalación inicial** se ha seleccionado **Paquete con UC Suite** en la selección de aplicación.

9.7.8.1 Cómo configurar UC Suite

Requisitos previos

Se encuentra en la ventana **Configuración automática de la suite de aplicaciones**.

Puesta en servicio inicial por OpenScape Business X



Paso a paso

- 1) Si en el sistema de comunicación no hay integrada ninguna UC Booster Card, haga clic en **OK & Continuar**. Se omite la configuración.
- 2) Si la UC Booster Card está integrada en el sistema de comunicación, haga clic en **Ejecutar función**. La UC Suite se configura automáticamente. En cuanto la barra de progreso llegue al 100%, haga clic en **OK & Continuar**.

9.7.9 Configuración de los buzones de voz de UC Smart

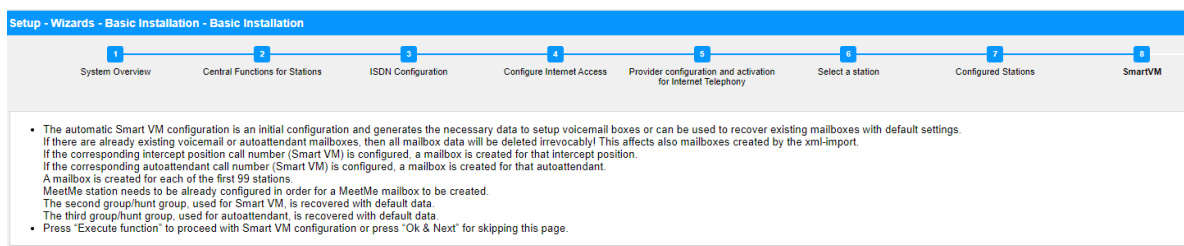
En la ventana **Configuración automática del Smart VM** puede hacer la configuración automática de los buzones de voz de UC Smart (Smart VM, Smart VoiceMail) si utiliza la solución de Comunicaciones Unificadas UC Smart.

Nota: Esta ventana solo aparece si en el asistente **Instalación inicial** se ha seleccionado **Paquete con UC Smart** en la selección de aplicación.

9.7.9.1 Cómo configurar los buzones de voz de UC Smart

Requisitos previos

Se encuentra en la ventana de **Configuración automática del Smart VM**.



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.

9.7.10 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.

9.7.10.1 Cómo modificar los ajustes del servidor de conferencias

Requisitos previos

Se encuentra en la ventana **Configurar conferencia Meet-Me**.

Paso a paso

- 1) En el campo **Número de teléfono**, indique un número de teléfono para la conferencia.
- 2) En el campo **Marcación directa**, establezca el número de acceso telefónico de la conferencia (Nº llam. marc. dir. de conferencia). A través de este número los participantes podrán acceder a una conferencia existente.
- 3) Haga clic en **OK & Continuar**.

9.7.11 Envío de correo electrónico (opcional)

En la ventana **Editar 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.

Dispone de 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.

9.7.11.1 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:

- 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 23: 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 usuario** cuenta correo, p. ej. `pepe.ejemplo`.
 - c) En **Contraseña y Repetir clave**, 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 250 (**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.

9.8 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 *Documentación del administrador, 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.

9.8.1 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:

- En la barra de navegación, haga clic en **Configuración**.
- En el árbol de navegación, haga clic en **Asistentes > Configuración básica**.
- Haga clic en **Editar** para iniciar el asistente **Registro de licencia**.

- En el campo **Código de autorización de licencia (LAC)** indique el LAC.
- Active la casilla de verificación **Tengo el nombre de usuario y la contraseña para el servidor de licencias y quiero iniciar sesión**.
- Introduzca el **Nombre de usuario** y la **Contraseña** para iniciar sesión en el servidor de licencia.
- 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:

- En la barra de navegación, haga clic en **Administración de licencias**.
- 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 la línea de la extensión deseada, active la casilla de verificación de la columna **Licencia de usuario** (primera columna con casillas de verificación).

System in network! Synchronization status: ● administrator@system Logoff

Home Administrators Setup Expert mode Data Backup **License Management** Service Center Networking

License Management

License Information

▼ Additional Products

OpenScape Personal Edition

▼ Local User licenses

Overview

IP User

TDM User

Mobility User

Deskshare User

CO Trunks

System Licenses

▼ License Profiles

Create Profiles

Assign Profiles

Registration

Activate License Online

Activate CLS Connect

Activate License File

Settings

IP User

Call number Display

Access	Call number	Display									
Remaining licenses			0	2	0	5*	2	4	2	6	0
LAN 0-SYS-1	x651000, ppc0		☒	☒	☐	☒	☐	☒	☐	☐	☐
LAN 0-SYS-2	hfa1, 651001		☒	☒	☐	☒	☐	☐	☐	☐	☐
LAN 0-SYS-3	hfa2, 651002		☒	☒	☐	☒	☐	☐	☐	☐	☐
LAN 0-SYS-4	hfa3, 651003		☒	☒	☐	☒	☐	☐	☐	☐	☐
LAN 0-SYS-5	hfa4, 651004		☒	☒	☐	☒	☐	☐	☐	☐	☐
LAN 0-SYS-6	hfa5, 651005		☒	☒	☐	☒	☐	☐	☐	☐	☐
LAN 0-SYS-7	hfa7, 651007		☐	☒	☒	☒	☒	☒	☒	☒	☒
LAN 0-SYS-8	hfa9, 651009		☒	☒	☐	☒	☐	☐	☐	☐	☐
LAN 0-SIP-3	Sip, justle		☒	☒	☐	☒	☐	☐	☐	☐	☐
LAN 0-SYS-9	WebRTC, justle		☒	☒	☐	☒	☐	☐	☐	☐	☐

Page 1 of 1

Items per page 10 25 50 100

Only configured users are displayed and can be licensed.

☒ Successfully licensed
 ☒ Not licensed
 ☐ License demand configurable
 ☐ License demand not configurable

☒ Unserved license release
 ☒ Unserved license demand release
 ☒ Unserved license demand

Abort Apply

- 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).

- 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.

- Si faltan licencias, las casillas de verificación tendrán fondo rojo. Corrija los fallos y repita el paso e.

3) Asignar licencias a las líneas:

- En el árbol de navegación, haga clic en **Líneas urbanas**. En el área **Líneas urbanas** aparece el número de licencias de línea adquiridas.
- 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 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 **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.

9.8.2 Cómo proporcionar el cliente UC Smart para la instalación

Requisitos previos

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

Está disponible el hardware y el software para usar la UC Smart.

Nota: Para utilizar el cliente UC Smart myPortal 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 Smart** y guarde el archivo de instalación en una unidad de red habilitada.
- 4) Haga clic en el símbolo de enlace de **Adobe AIR** y descargue el archivo de instalación en una unidad de red habilitada.
- 5) Envíe a los usuarios de myPortal Smart los dos archivos de instalación.
- 6) Como alternativa, también puede enviar enlaces a los usuarios de myPortal Smart para que puedan acceder directamente a los archivos de instalación:

`https://<Dirección IP del sistema de comunicación>/management/downloads/SmartClient.air`

`http://www.adobe.com/air`

9.8.3 Cómo preparar los clientes de UC Suite para la instalación

Requisitos previos

Ha iniciado sesión en Gestión basada en Web (WBM) con el perfil **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 > Envío de correo electrónico**.

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
```

9.8.4 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 *Documentación para el administrador, 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 *Documentación para el administrador, Actualización del sistema de comunicación*).

9.9 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.

9.9.1 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 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.

9.9.2 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.

10 Configuración inicial de OpenScape Business UC Booster

Se describen la instalación y la configuración iniciales del OpenScape Business UC Booster en el sistema de comunicación X3/X5/X8 de OpenScape Business. Hay que distinguir si para usar las funciones de UC Booster se utiliza la OpenScape Business UC Booster Card o el OpenScape Business UC Booster Server.

La configuración inicial de OpenScape Business UC Booster se realiza con el programa de administración OpenScape Business Assistant (la "Gestión basada en Web" o "WBM").

En los siguientes capítulos encontrará información detallada sobre la administración de las prestaciones no incluidas en la configuración inicial.

Configuración inicial de la OpenScape Business UC Booster Card

La OpenScape Business UC Booster Card se monta en el sistema de comunicación X3/X5/X8 de OpenScape Business y se configura para el servicio. A continuación se configuran las funciones de OpenScape Business UC Booster.

Los pasos de la configuración inicial son diferentes si la UC Booster Card se pondrá por primera vez en servicio junto con el sistema de comunicación X3/X5/X8 de OpenScape Business o si se va a integrar en un sistema de comunicación X3/X5/X8 de OpenScape Business ya configurado.

Visión general de los pasos de instalación para las dos 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 en la página 267
Montaje de la UC Booster Card La UC Booster Card se monta en el sistema de comunicación X3/X5/X8 de OpenScape Business. Para una descripción, véase <i>Para una descripción, véase OpenScape Business, Documentación de servicio, Montaje del hardware - Descripción de los módulos.</i>	Montaje de la UC Booster Card La UC Booster Card se monta en el sistema de comunicación X3/X5/X8 de OpenScape Business. Para una descripción, véase <i>Para una descripción, véase OpenScape Business, Documentación de servicio, Montaje del hardware - Descripción de los módulos.</i>
Configuración de la UC Booster Card La UC Booster Card se configura durante la instalación inicial del sistema de comunicación X3/X5/X8 de OpenScape Business. Para consultar una descripción, véase Integración en la LAN de clientes en la página 192.	Configuración de la UC Booster Card La UC Booster Card se configura con posterioridad en un sistema de comunicación X3/X5/X8 de OpenScape Business ya configurado. Para consultar una descripción, véase Integración en la LAN de clientes en la página 192. Si desea consultar los detalles específicos de la configuración, véase Configuración de la UC Booster Card en la página 269

Integración en un nuevo sistema de comunicación	Integración en un sistema de comunicación existente
Configuración básica La configuración básica se realiza en el momento de la instalación inicial del sistema de comunicación X3/X5/X8 de OpenScape Business. Para consultar una descripción, véase Configuración básica en la página 203.	Configuración básica La configuración básica se realiza con posterioridad en un sistema de comunicación X3/X5/X8 de OpenScape Business ya configurado. Para consultar una descripción, véase Configuración básica en la página 203. Para conocer las características especiales de la configuración básica, véase Configuración básica en la página 276
Tareas finales Las tareas finales (incluyendo el registro de licencia de los clientes de UC) se realizan durante la instalación inicial del sistema de comunicación X3/X5/X8 de OpenScape Business. Para consultar una descripción, véase Tareas finales en la página 251.	Tareas finales Las tareas finales (incluyendo el registro de licencia de los clientes de UC) se realizan durante la instalación inicial del sistema de comunicación X3/X5/X8 de OpenScape Business. Para consultar una descripción, véase Tareas finales en la página 251. Para conocer las características especiales de las actividades finales, véase Tareas finales en la página 277

Instalación inicial del OpenScape Business UC Booster Server

El OpenScape Business UC Booster Server es integrado en la LAN de clientes junto con el sistema de comunicación X3/X5/X8 de OpenScape Business.

El software de comunicación OpenScape Business para OpenScape Business UC Booster Server, que proporciona la funcionalidad OpenScape Business UC Booster, se instala en el sistema operativo Linux SLES 12 SP5 de 64 bits. El software de comunicación puede operar directamente con 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*.

El OpenScape Business UC Booster Server tiene una Gestión basada en Web (WBM) propia. Esta Gestión basada en Web se utiliza para la actualización de software, para hacer copias de seguridad de datos de configuración y para el diagnóstico del OpenScape Business UC Booster Server. La instalación inicial del OpenScape Business UC Booster Server se realiza con la Gestión basada en Web (WBM) del sistema de configuración.

Los pasos de la instalación inicial son diferentes si el UC Booster Server se pone en servicio por primera vez junto con el sistema de comunicación X3/X5/X8 de OpenScape Business o si se integra posteriormente en un sistema de comunicación X3/X5/X8 de OpenScape Business ya configurado.

Visión general de los pasos de instalación para las dos opciones:

Configuración inicial de OpenScape Business UC Booster

Requisitos para la puesta en servicio inicial

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 del servidor Linux La instalación del servidor Linux se describe en las instrucciones de instalación del servidor Linux de OpenScape Business.	Instalación del servidor Linux La instalación del servidor Linux se describe en las instrucciones de instalación del servidor Linux de OpenScape Business.
Instalación del software de comunicación	Instalación del software de comunicación
Configuración del UC Booster Server El UC Booster Server se configura durante la instalación inicial del sistema de comunicación X3/X5/X8 de OpenScape Business. Para consultar una descripción, véase Integración en la LAN de clientes en la página 192.	Configuración del UC Booster Server El UC Booster Server se configura posteriormente en un sistema de comunicación X3/X5/X8 de OpenScape Business ya configurado. Para consultar una descripción, véase Integración en la LAN de clientes en la página 192. Si desea consultar los detalles específicos de la configuración, véase Configuración del UC Booster Server en la página 273
Configuración básica La configuración básica se realiza en el momento de la instalación inicial del sistema de comunicación X3/X5/X8 de OpenScape Business. Para consultar una descripción, véase Configuración básica en la página 203.	Configuración básica La configuración básica se realiza con posterioridad en un sistema de comunicación X3/X5/X8 de OpenScape Business ya configurado. Para consultar una descripción, véase Configuración básica en la página 203. Para conocer las características especiales de la configuración básica, véase Configuración básica en la página 276
Tareas finales Las tareas finales (incluyendo el registro de licencia de los clientes de UC) se realizan durante la instalación inicial del sistema de comunicación X3/X5/X8 de OpenScape Business. Para consultar una descripción, véase Tareas finales en la página 251.	Tareas finales Las tareas finales (incluyendo el registro de licencia de los clientes de UC) se realizan durante la instalación inicial del sistema de comunicación X3/X5/X8 de OpenScape Business. Para consultar una descripción, véase Tareas finales en la página 251. Para conocer las características especiales de las actividades finales, véase Tareas finales en la página 277

10.1 Requisitos para la puesta en servicio inicial

Si se cumplen los requisitos para la puesta en servicio inicial, se garantiza el funcionamiento correcto del OpenScape Business UC Booster.

General

En función del hardware utilizado (teléfonos, etc.) y de la infraestructura existente, se aplican los siguientes requisitos generales:

- El sistema de comunicación X3/X5/X8 de OpenScape Business está configurado y operativo.
- La infraestructura LAN (router Internet, conmutadores, etc.) está disponible y se puede utilizar.
- Los teléfonos IP están conectados con la LAN de clientes.
- Se recomienda un acceso a Internet de banda ancha para la actualización de software y el acceso remoto.
- Se tienen todas las licencias necesarias para el OpenScape Business UC Booster (p.ej., Clientes de UC, Gate View, Directory Services, etc.). Si se hace una integración en un sistema de comunicación con licencia, no hay un periodo de activación.
- Hay disponible, y se conoce, un esquema de direcciones IP.
- Hay disponible, y se conoce, un plan de numeración.

Para UC Booster Card

Para el servicio de la UC Booster Card deben cumplirse los siguientes requisitos.

- Hardware de OpenScape Business:

Se ha instalado la UC Booster Card.

- Switch:

El conmutador (o switch) que se utiliza para conectar la UC Booster Card con el sistema de comunicación debe ser compatible con IPv6, para que la UC Booster Card reciba una dirección IP durante la puesta en servicio inicial.

Si el switch no es compatible con IPv6, el LED rojo del sistema de comunicación parpadea. En este caso, el puerto de administración del sistema se debe conectar con el segundo puerto LAN de la UC Booster Card mediante un cable Ethernet adicional. De esta forma, la UC Booster Card recibe automáticamente una dirección IP IPv4 mediante el protocolo IPv6. En cuanto la tarjeta UC Booster Card esté accesible a través de IP, se apaga el LED rojo del sistema de comunicación. A continuación, se puede introducir la dirección IP deseada para UC Booster Card durante la puesta en servicio inicial. La comunicación entre el sistema y la UC Booster Card se realiza ahora a través de la conexión IPv4 del conmutador.

Nota: Si se reinicia o recarga el sistema, no hay que desconectar el cable Ethernet adicional.

- Kit de ventilador:

La UC Booster Card requiere un ventilador adicional. El kit de ventiladores depende del sistema de comunicación.

- Tapa de la carcasa:

Con OpenScape Business X3W se requiere una tapa de la carcasa nueva para el kit de ventiladores para la UC Booster Card.

Con la migración de sistemas HiPath 3000, para OpenScape Business X3W/X5W y X3R/X5R se requieren nuevas tapas de la carcasa para el kit de ventiladores para la UC Booster Card.

- Software de comunicación:

El software del sistema de comunicación debe estar actualizado con la última versión de software publicada. Hay que tener cuidado de utilizar la imagen que incluya el software de la UC Booster Card.

- Navegador Web:

Para la puesta en servicio inicial de la UC Booster Card con el OpenScape Business Assistant (Gestión basada en Web, WBM) se utiliza el PC de administración. La Gestión basada en Web (WBM) se basa en navegador, por lo que es independiente del sistema operativo. Se necesita una resolución de pantalla de 1024x768 o superior.

Son compatibles los siguientes navegadores web con HTML 5:

- Microsoft Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Para consultar qué versiones de los navegadores Web son compatibles, véase las *Notas de la versión de software*. Si hay instalada una versión anterior del navegador Web, hay que instalar la actual para poder comenzar la puesta en servicio inicial.

Nota: Entre la placa base y la tarjeta UC Booster se requiere acceso directo a la red.

Para UC Booster Server

Para el servicio del UC Booster Server hay que cumplir los siguientes requisitos.

- Linux Server:

El servidor Linux necesario para OpenScape Business S se ha instalado siguiendo las *Instrucciones de instalación del servidor Linux de OpenScape Business*, está operativo y está integrado en la LAN de clientes.

- Software de comunicación OpenScape Business:

Se dispone del DVD de instalación con el software de comunicación OpenScape Business. Una vez finalizada la instalación del software hay que actualizar el software del sistema de comunicación y el software del sistema de comunicación del UC Booster Server, por separado, a la última versión de software publicada. La versión debe ser la misma en ambos casos.

- DVD con sistema operativo Linux SLES 12 SP5 de 64 bits

El DVD de Linux también puede ser necesario en la instalación del software de comunicación OpenScape Business si hay que instalar posteriormente los paquetes de software (RPM) necesarios para el software de comunicación.

- Navegador Web:

Para la puesta en servicio inicial del UC Booster Server con el OpenScape Business Assistant (Gestión basada en Web, WBM) se puede utilizar el servidor Linux o el PC de administración. La Gestión basada en Web (WBM)

se basa en navegador, por lo que es independiente del sistema operativo. Se necesita una resolución de pantalla de 1024x768 o superior.

Son compatibles los siguientes navegadores web con HTML 5:

- Microsoft Internet Explorer (PC de administración).
- Microsoft Edge
- Mozilla Firefox (servidor Linux/PC de administración)
- Google Chrome

Para consultar qué versiones de los navegadores Web se deben utilizar, véase las *Notas de la versión de software*. Si hay instalada una versión anterior del navegador Web, hay que instalar la actual para poder comenzar la puesta en servicio inicial.

- Firewall:

Si se establece conexión con Internet se requiere un firewall para el servidor Linux, a fin de impedir el acceso no autorizado desde el exterior. Después de instalar Linux, el firewall de Linux está activado. Con el programa de instalación del software de comunicación se ajusta el firewall de forma tal que permita el funcionamiento correcto del software de comunicación. Los puertos para el software de comunicación se abren y todos los demás se cierran.

Si en la red se utiliza un firewall externo, hay que desactivar el firewall Linux y liberar los puertos y las direcciones necesarios para el software de comunicación (véase [Puertos utilizados](#) en la página 279).

10.2 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 (como por ejemplo un soporte USB o una unidad de red).

10.2.1 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.

10.3 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.

10.3.1 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.

10.3.2 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.

10.3.3 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).

10.3.3.1 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 **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** > **Actualización a través de Internet**. Se muestra la versión de software instalada actualmente.

- 3) Haga clic en **OK & 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 & Continuar**.
- 6) Active el campo de opción **Iniciar acción - Inmediatamente / inmed. tras transmisión**.
- 7) Haga clic en **OK & 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**.

10.4 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.

10.4.1 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 las *Instrucciones de instalación de OpenScape Business, Linux Server* para informarse en profundidad).

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>).

10.4.1.1 Cómo instalar el software de comunicación en un servidor Linux o en un entorno virtual

Requisitos previos

- El sistema operativo SLES 15 SP6/SP7 se ha instalado y ejecutado correctamente en el servidor Linux.
- Archivo .ISO con el software de comunicación OpenScape Business.
- Archivo .ISO con el sistema operativo Linux SLES 15 SP6/SP7 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 administrador.
- 2) Inserte el archivo .ISO de OpenScape Business.
- 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 en inglés.
- 5) Seleccione el producto deseado 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 en caso de incumplimientos menores de los requisitos. Tras la confirmación haciendo clic en **Continuar**, se puede continuar con la instalación. En 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, posteriormente deberá volver al archivo .ISO de SLES 15.
- 7) Aparece 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 existe un servidor DHCP en la LAN del cliente (por ejemplo, el servidor DHCP del router de Internet), detenga aquí la configuración del servidor DHCP de Linux 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 utilice un servidor DHCP externo, tiene dos opciones:

a) La dirección IP del servidor Linux debe ingresarse como la 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/log/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 del Gateway predeterminado; por regla general, la dirección IP del enrutador de Internet, por ejemplo, 192.168.5.1.
 - **Dominio** (opcional): el dominio especificado durante la instalación de Linux, por ejemplo, <customer>.com
 - **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 (por ejemplo, 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 (por ejemplo: 192.168.5.10).
- **Subred:** subred apropiada para el rango de direcciones IP, por ejemplo: 192.168.5.0.
- **Máscara de red:** Máscara de subred del servidor Linux que se especificó durante la instalación de Linux, por ejemplo: 255.255.255.0.
- **Inicio del rango de IP y el final del rango de IP:** Rango de direcciones IP desde el cual el servidor DHCP puede asignar direcciones IP, por ejemplo: 192.168.5.100 a 192.168.5.254.

- 11) Haga clic en **Continuar**.
- 12) Tras la instalación, es necesario reiniciar el sistema operativo Linux. Seleccione la casilla de verificación **Reiniciar PC** y confirme con **Continuar**.
- 13) Si es necesario instalar paquetes RPM adicionales, se le pedirá que inserte el archivo .ISO de SLES 15. Inserte el archivo .ISO y confirme con **Continuar**. Tras la instalación correcta de los paquetes RPM, vuelva a insertar el archivo .ISO de OpenScape Business y confirme con **Continuar**., seguido de **Ejecutar**.
- 14) El software de comunicación OpenScape Business está instalado. El sistema operativo entonces realiza un reinicio automático.
- 15) Tras el reinicio, inicie sesión con la cuenta de usuario que configuró anteriormente durante la instalación de Linux.

Nota: Toma unos minutos hasta que todos los componentes del software de comunicación OpenScape Business estén activos.

10.4.2 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.

10.4.2.1 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@sisistema` 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@sisistema` 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**.

10.4.3 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).

10.5 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.

10.6 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.

10.7 Desinstalación del software de comunicación

El software de comunicación se puede desinstalar mediante una consola de texto.

10.7.1 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.

10.8 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 *Instalación inicial de OpenScape Business UC Booster - 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 OpenScape Business X3/X5/X8 - Integración en la LAN de clientes - 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 *Configuración de OpenScape Business X3/X5/X8 - Integración en la LAN de clientes - 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 inicial de OpenScape Business UC Booster - Puesta en servicio inicial del UC Booster Server - 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 *Instalación inicial del OpenScape Business UC Booster - Puesta en servicio inicial del UC Booster Server - 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 *Mantenimiento - Restart, Reload, Shutdown - 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 *Mantenimiento - Actualización*.

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 *Mantenimiento - Guardar y Recuperar - Recuperar*.

10.9 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>).

Configuración inicial de OpenScape Business UC Booster

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
CAR Update Registration	X		12061	X		X	
CAR Update Server	X		12063	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
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			

Configuración inicial de OpenScape Business UC Booster

Descripción	TCP	UDP	Número de puerto	OpenScape Business X	Tarjeta de refuerzo UC	OpenScape Business S	UC Booster Server
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	
SIP TLS Subscriber (servidor)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (capturas)		X	162	X		X	
TFTP		X	69		O	O	O
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.

11 Componentes retirados de producción

Esta sección contiene información relativa a componentes retirados de producción, que se incluyen aquí solamente para consulta.

11.1 Distribuidor principal MDFU (opcional)

La conexión de teléfonos, líneas urbanas y demás al OpenScape Business X3W y al OpenScape Business X5W se puede realizar directamente a los módulos de los sistemas de comunicación o mediante el distribuidor principal externo MDFU.

El distribuidor principal MDFU (Main Distribution Frame Universal) ofrece nueve slots para regletas de división y de clasificación.

Dimensiones:

- Altura = 367,0 mm
- Anchura = 328,8 mm
- Profundidad = 125,4 mm

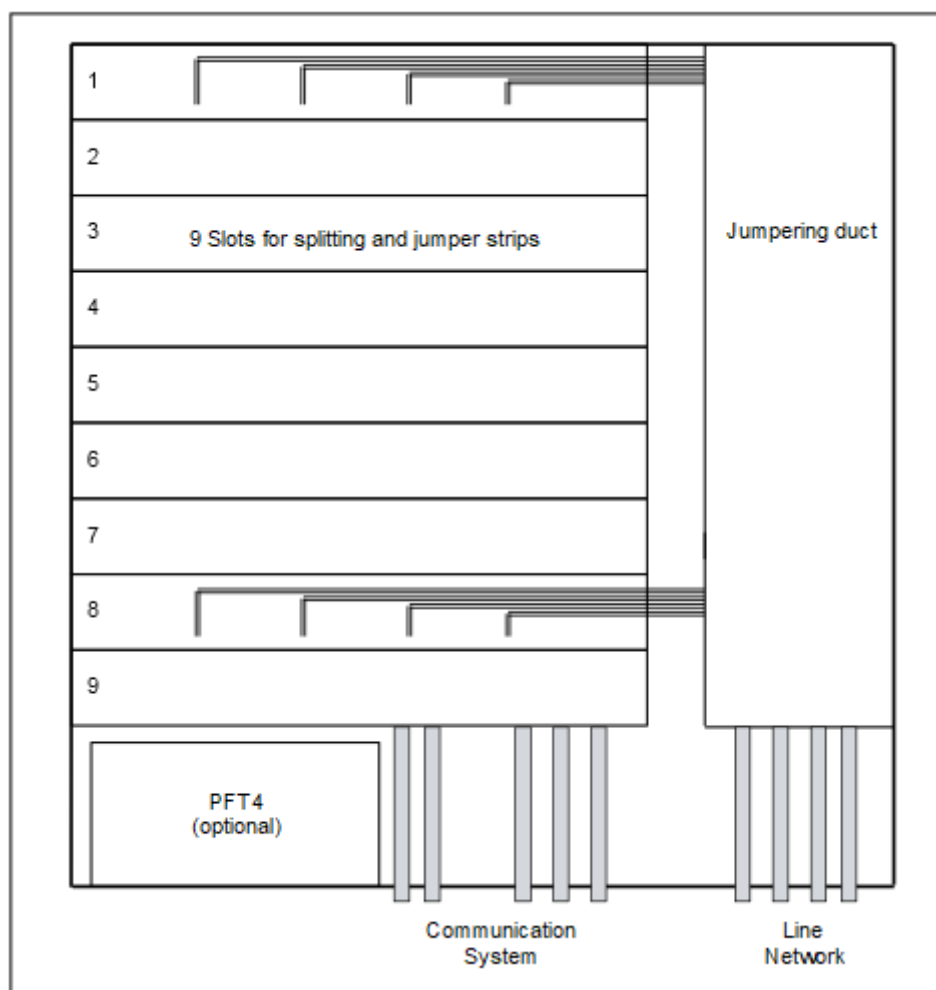


Figura 24: Distribuidor principal MDFU

Nota: Si no utiliza el MDFU sino un distribuidor principal de otro fabricante, observe y siga las indicaciones del fabricante sobre el montaje y la toma de tierra.

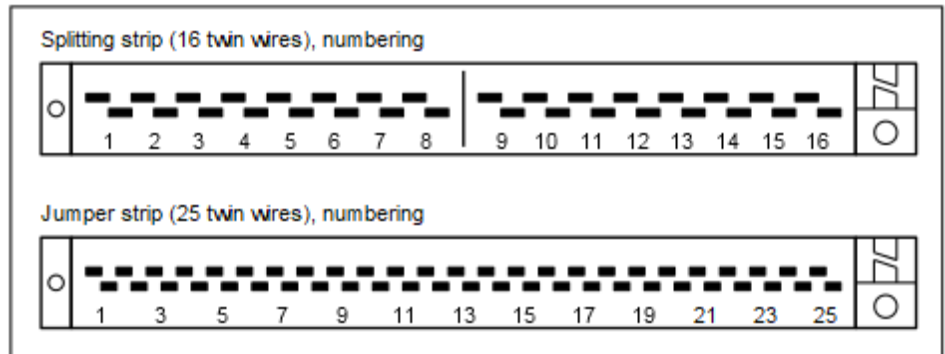


Figura 25: Regleta divisora y de clasificación – Numeración de las conexiones

11.1.1 Cómo fijar a una pared el distribuidor principal MDFU

Requisitos previos

Hay una pared con capacidad de carga y con espacio suficiente para montar el distribuidor principal MDFU.

Paso a paso

- 1) Fije las plantillas para taladro suministradas en el lugar de montaje deseado.
- 2) Haga los agujeros.
- 3) Inserte los tacos en los agujeros del taladro y fije los tornillos dejándolos sobresalir unos 5 mm.
- 4) Retire la tapa de la carcasa del MDFU.
- 5) Suspenda el MDFU en los soportes y alinéelo.
- 6) Apriete los tornillos.

11.2 Cable de conexión con el distribuidor principal externo (opcional)

Los teléfonos, líneas urbanas, etc. se pueden conectar con el OpenScape Business X3W y OpenScape Business X5W a través del distribuidor principal MDFU o de otro distribuidor principal externo. Hay diferentes opciones para conectar el sistema de comunicación con un distribuidor principal.

CABLU S30269-Z41-A30

CABLU (24 DA) con

- seis bornes atornillables Wieland para la conexión directa en los conectores de tarjeta de los módulos de los sistemas de comunicación OpenScape Business X3W y OpenScape Business X5W

- Regleta de clasificación para el montaje en el MDFU

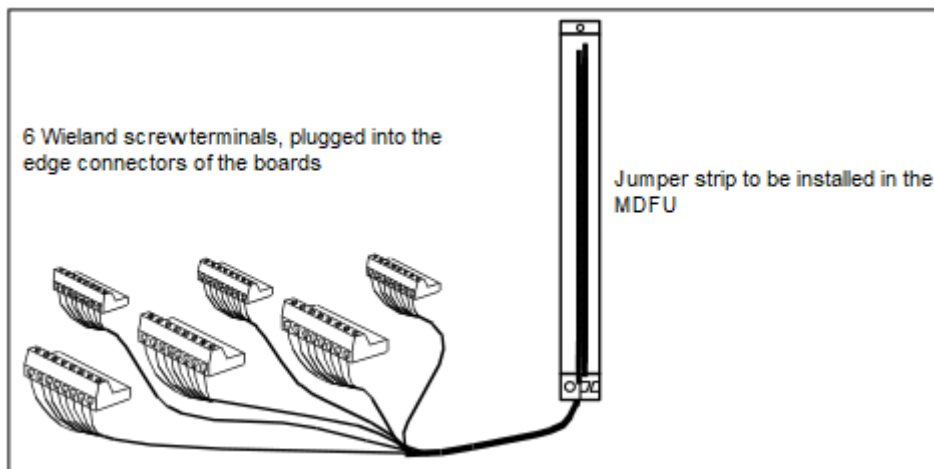


Figura 26: CABLU S30269-Z41-A30

Cable Open-End S30267-Z322-Axxx

Cable Open-End (24 DA) con seis bornes atornillables Wieland para la conexión directa con los conectores de tarjeta de los módulos de los sistemas de comunicación OpenScape Business X3W y OpenScape Business X5W. El cable debe tenderse manualmente en una regleta divisora o de clasificación del MDFU o en otro distribuidor principal externo.

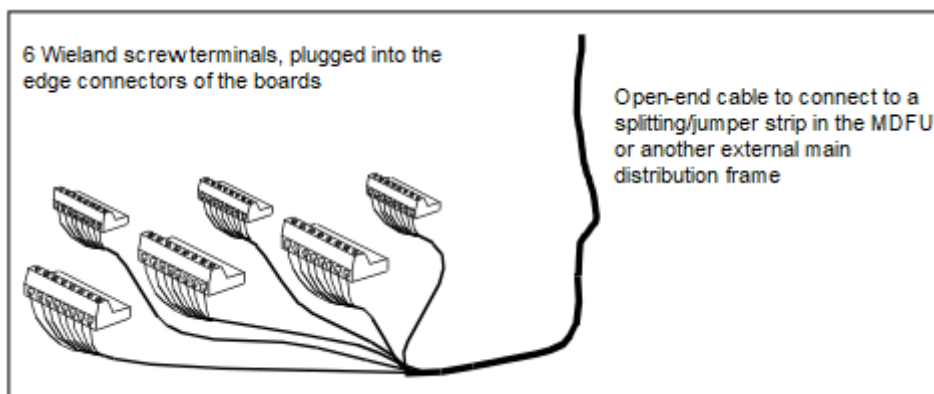


Figura 27: Cable Open-End S30267-Z322-Axxx

CABLU S30269-Z100-A11/-A21

CABLU (16 DA) con

- una toma SIPAC 1 SU para conectar en el conector de backplane X8 del sistema de comunicación OpenScape Business X5W
- Regleta divisora para el montaje en el MDFU

CABLU S30269-Z100-A14/-A24

CABLU (24 DA) con

- dos tomas SIPAC 1 SU para conectar en los conectores de backplane X8 y X9 del sistema de comunicación OpenScape Business X5W
- Regleta de clasificación para el montaje en el MDFU

CABLU S30267-Z346-A30

CABLU con

- una toma SIPAC 1 SU para conectar en el conector de backplane X8 del sistema de comunicación OpenScape Business X5W
- Conector CHAMP para la conexión de un distribuidor principal externo

CABLU S30267-Z365-A30

CABLU con

- dos tomas SIPAC 1 SU para conectar en los conectores de backplane X8 y X9 del sistema de comunicación OpenScape Business X5W
- Conector CHAMP para la conexión de un distribuidor principal externo

11.2.1 Cómo conectar un conductor de conexión al distribuidor principal externo (opcional)

Requisitos previos**Atención:**

Descarga eléctrica al tocar los cables con tensión

Utilice cables conductores independientes para establecer la puesta a tierra de protección del sistema de comunicación y de todos los distribuidores principales antes de conectar teléfonos y líneas.

La tapa de la carcasa del sistema de comunicación no está puesta.

Paso a paso

- 1) Seleccione el conductor de conexión apropiado, de acuerdo con el sistema de comunicación y la placa.

Si		entonces
Sistema de comunicación	Módulo	Conductor de conexión
OpenScape Business X3W	Todos los módulos periféricos y la placa base OCCM, OCCMA y OCCMB	Conexión con el MDF externo: CABLU con seis bornes atornillables Wieland (para la conexión directa a los conectores de tarjeta) y una regleta de clasificación para 24 DA:
		• S30269-Z41-A30: 3 m de longitud
		Conexión al MDFU o a otro distribuidor principal externo: Cable de extremo abierto (24 DA) con seis bornes atornillables Wieland (para la conexión directa a los conectores de tarjeta):
		• S30267-Z322-A100: 10 m de longitud

Si		entonces
Sistema de comunicación	Módulo	Conductor de conexión
OpenScape Business X5W	Todos los módulos periféricos (excepto los módulos periféricos con formato SIPAC) y la placa base OCCM, OCCMA y OCCMB	Conexión con el MDFU: CABLU con seis bornes atornillables Wieland (para la conexión directa a los conectores de tarjeta) y una regleta de clasificación para 24 DA: - S30269-Z41-A30: 3 m de longitud Conexión al MDFU o a otro distribuidor principal externo: Cable de extremo abierto (24 DA) con seis bornes atornillables Wieland (para la conexión directa a los conectores de tarjeta): - S30267-Z322-A100: 10 m de longitud

2) Elija una de estas opciones de conectividad para el sistema de comunicación:

- Si utiliza una unidad CABLU con seis bornes atornillables Wieland, fije los bornes atornillables a los conectores de tarjeta que desee de los módulos elegidos.
- Si utiliza una unidad CABLU con una toma SIPAC 1 SU, conecte el cable al conector X8 del backplane.

3) Fije el conductor de conexión al sistema de comunicación mediante bridas.

4) Seleccione una de las siguientes opciones para establecer la conexión con el MDFU o cualquier otro distribuidor principal externo:

- Si utiliza el MDFU y una unidad CABLU con una regleta divisora o una regleta de clasificación, instale la regleta en el MDFU.

Para más información sobre las características esenciales del MDFU y sobre la numeración de las regletas divisoras y de clasificación, véase [Distribuidor principal externo MDFU \(opcional\)](#).

- Si utiliza el MDFU y un cable de extremo abierto, conecte el cable a la regleta divisora o de clasificación del MDFU.

Procedimiento:

Pele los hilos del cable conductor.

Retire el apantallamiento del cable por espacio de unos 3 cm. Corte el hilo de drenaje hasta unos 2,5 cm y fíjelo al apantallamiento del cable envolviéndolo en cinta (con al menos 1,5 vueltas).

Utilice una herramienta estándar para tender los cables.

Tabla 8: Códigos de colores para el cable de extremo abierto

Grupo de colores	Par	Hilo a	Hilo b
1	1	blanco/azul	
			azul/blanco
	2	blanco/naranja	

Componentes retirados de producción

Grupo de colores	Par	Hilo a	Hilo b
	3	blanco/verde	naranja/blanco
			verde/blanco
	4	blanco/marrón	
			marrón/blanco
	5	blanco/gris	
			gris/blanco
2	6	rojo/azul	
			azul/rojo
	7	rojo/naranja	
			naranja/rojo
	8	rojo/verde	
			verde/rojo
	9	rojo/marrón	
			marrón/rojo
	10	rojo/gris	
			gris/rojo
3	11	negro/azul	
			azul/negro
	12	negro/naranja	
			naranja/negro
	13	negro/verde	
			verde/negro
	14	negro/marrón	
			marrón/negro
	15	negro/gris	
			gris/negro
4	16	amarillo/azul	
			azul/amarillo
	17	amarillo/naranja	
			naranja/amarillo
	18	amarillo/verde	
			verde/amarillo
	19	amarillo/marrón	
			marrón/amarillo

Grupo de colores	Par	Hilo a	Hilo b
5	20	amarillo/gris	
			gris/amarillo
	21	violeta/azul	
			azul/violeta
	22	violeta/naranja	
			naranja/violeta
	23	violeta/verde	
			verde/violeta
	24	violeta/marrón	
			marrón/violeta

Para más información sobre las características esenciales del MDFU y sobre la numeración de las regletas divisoras y de clasificación, véase [Distribuidor principal externo MDFU \(opcional\)](#).

- Si utiliza un distribuidor principal externo con conectores CHAMP y un cable CHAMP, inserte el conector macho en el conector hembra CHAMP que quiera usar del distribuidor principal externo.
 - Si utiliza otro distribuidor principal externo y un cable de extremo abierto, conecte el cable a la regleta divisora o de clasificación del distribuidor principal externo.
- 5) Fije el conductor de conexión al MDFU o al distribuidor principal externo mediante bridas.

Índice

Caracteres Especiales

- Área de conexión
 - OpenScape Business S 24
 - OpenScape Business UC Booster Server 24

A

- acceso remoto
 - activar, a través de acceso a Internet con dirección IP fija 252, 254
- Acceso remoto
 - activar, a través de acceso a Internet con dirección IP fija 254, 256
- advertencias
 - atención 15

C

- cableado para conexiones LAN y WAN 24
- Canales múltiplex de tiempo 129
- Circuito de alimentación eléctrica y conexión
 - OpenScape Business S 24
 - OpenScape Business UC Booster Server 24
- Comportamiento en caso de emergencia 22, 22
- Concepto 12
- Condiciones de servicio (climáticas, mecánicas)
 - OpenScape Business S 30
 - OpenScape Business UC Booster Server 30
 - OpenScape Business X3, X5, X8 29
- conformidad
 - normas estadounidenses y canadienses 28
 - normas internacionales 28
- Conformidad CE 28
- Convenciones de representación 12
- Cubierta de blindaje para módulo 132

D

- Desempaquetar los componentes 36
- Distribuidor principal MDFU 282
- Distribuidor principal MDFU-E
 - puesta a tierra de protección 115
- Distribuidor principal MDFU:montaje mural 283

E

- eliminación 23
- Esquema de direcciones IP 187

I

- Indicaciones de aviso 13
 - advertencia 14

- aviso 16
- peligro 14
- Indicaciones de seguridad 13
- Indicaciones de seguridad para Australia 17
- Indicaciones de seguridad para Brasil 18
- Indicaciones de seguridad para Canadá 20
- Indicaciones de seguridad para EE. UU. 18
- Inicialización de los módulos 125
- instalación 262
- Instalación 183
- instalación de módulos
 - OpenScape Business X3R y X5R 89
 - OpenScape Business X3W y X5W 52
 - OpenScape Business X8 129
- Instrucciones de uso 12
- interferencias de radiofrecuencia 26
- interferencias electromagnéticas 26
- ITSP (Internet Telephony Service Provider) 224

J

- Java Runtime Environment (JRE) 184

L

- Líneas múltiplex PCM
 - armario básico 126
 - armario de ampliación 128

M

- MDFU 282
 - puesta a tierra de protección 41
- MDFU-E
 - puesta a tierra de protección 115
- MDFU:montaje mural 283

N

- normativa de protección antiincendios 25
- Notificar accidente 22

O

- OpenScape Business X3R
 - instalación de módulos 89
 - lugar de montaje 32
 - Montaje 73
 - montaje en armario de 19 pulgadas 73
 - placa de protección para módulos 90
- OpenScape Business X3R: conexión de teléfonos y dispositivos 94
- OpenScape Business X3R:conexión urbana 90
- OpenScape Business X3R:efectuar la prueba visual 101

OpenScape Business X3R: montaje mural [76](#)
OpenScape Business X3R: Slots de módulos [88](#)
OpenScape Business X3W
 emisiones de interferencias [65](#)
 Interfaz WAN [53](#)
 Puerto LAN [53](#)
OpenScape Business X3W
 cable de conexión [48](#)
 cable de conexión con el distribuidor principal externo [283](#)
 conexión de tensión de red (solo para EE. UU./Canadá) [35](#)
 herramientas y medios auxiliares [31](#)
 instalación de módulos [52](#)
 lugar de montaje [32](#)
 Montaje [40](#)
 montaje mural [40](#)
 slots de módulos [50](#)
OpenScape Business X3W: conexión de teléfonos y dispositivos [58](#)
OpenScape Business X3W: conexión urbana [54](#)
OpenScape Business X3W: efectuar prueba visual [70](#)
OpenScape Business X5R
 lugar de montaje [32](#)
 Montaje [73](#)
 montaje en armario de 19" [74](#)
 placa de protección para módulos [90](#)
OpenScape Business X5R: conexión de teléfonos y dispositivos [94](#)
OpenScape Business X5R: conexión urbana [90](#)
OpenScape Business X5R: efectuar la prueba visual [101](#)
OpenScape Business X5R: montaje mural [76](#)
OpenScape Business X5R: slots de módulos [89](#)
OpenScape Business X5W
 cable de conexión [48](#)
 cable de conexión con el distribuidor principal externo [283](#)
 conexión de tensión de red (solo para EE. UU./Canadá) [35](#)
 conexión urbana [54](#)
 emisiones de interferencias [65](#)
 herramientas y medios auxiliares [31](#)
 instalación de módulos [52](#)
 Interfaz WAN [53](#)
 lugar de montaje [32](#)
 Montaje [40](#)
 montaje mural [40](#)
 Puerto LAN [53](#)
 slots para módulos [50](#)
OpenScape Business X5W: conexión de teléfonos y dispositivos [58](#)
OpenScape Business X5W: efectuar prueba visual [70](#)
OpenScape Business X8
 conectar un conductor al MDFU-E [138](#)
 conexión de línea urbana [142](#)
OpenScape Business X8
 Backplane [132](#)
 cable de conexión con el panel de interconexión [139](#)

 cables de conexión con el panel de interconexión S0 [139](#)
 canales múltiplex de tiempo de los módulos periféricos [129](#)
 Cubierta de blindaje para módulo [132](#)
 instalación de módulos [129](#)
 líneas múltiplex PCM en el armario básico [126](#)
 líneas múltiplex PCM en el armario de ampliación [128](#)
 lugar de montaje con montaje autónomo [31](#), [33](#)
 lugar de montaje con montaje en armario de 19" [33](#)
 Montaje [103](#)
 montaje autónomo [103](#)
 montaje en armario de 19 pulgadas [108](#)
 Panel de conexión o de blindaje [135](#)
 puesta a tierra de protección [114](#)
 Realizar una inspección visual [154](#)
OpenScape Business X8: conexión de teléfonos y dispositivos [146](#)
OpenScape Business X8: cerrar el armario del sistema [156](#)
OpenScape X5R
 instalación para módulos [89](#)

P

Panel de conexión o de blindaje [135](#)
panel de interconexión [111](#)
Panel de interconexión
 montaje [114](#)
 puesta a tierra de protección [114](#)
Placa de protección para módulos [90](#)
Plan de numeración [186](#)
Protección de datos [27](#)
puesta a tierra de protección
 distribuidor principal MDFU [41](#)
 X3W [41](#)
 X5W [41](#)
Puesta a tierra de protección
 X3R [77](#)
 X5R [77](#)

R

reciclaje [23](#)
Requisitos de protección contra descargas [25](#)

S

seguridad de los datos [27](#)
Sello CE [26](#)
servidor de licencias (CLS)
 Editar la dirección IP [253](#)
slots del armario básico [123](#)
Slots del armario de ampliación [124](#)

T

Tipos de temas [12](#)

U

Uso adecuado de los sistemas de comunicación y servidores [22](#)

