A MITEL
PRODUCT
GUIDE

Mitel OpenScape Business

OpenScape Business V3

Documentazione per l'amministratore
11/2025

A31003-P3030-M100-63-76A9

Mitel

Notices

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

Trademarks

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

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Indice

1 Cronologia delle modifiche..... 39
1.1 Cronologia dei miglioramenti/risoluzioni..... 57

2 Introduzione e informazioni importanti..... 68
2.1 Con questa documentazione..... 68
2.1.1 Documentazione e destinatari..... 69
2.1.2 Struttura della documentazione per l'amministratore..... 70
2.1.3 Tipi di argomenti..... 72
2.1.4 Convenzioni di visualizzazione/rappresentazione..... 73
2.2 Avvertimenti di sicurezza e attenzione..... 73
2.2.1 Tipo di avvertimento: Pericolo..... 74
2.2.2 Tipo di avvertimento: Avvertenza..... 75
2.2.3 Avvertenze: Attenzione..... 76
2.2.4 Avvertimento: Avviso..... 77
2.2.5 Istruzioni di sicurezza specifiche del paese..... 77
2.2.5.1 Istruzioni di sicurezza per l'Australia..... 77
2.2.5.2 Istruzioni di sicurezza per Brasile..... 78
2.2.5.3 Istruzioni di sicurezza per USA..... 78
2.2.5.4 Istruzioni di sicurezza per Canada..... 81
2.3 Informazioni importanti..... 81
2.3.1 Comportamento in caso di emergenza..... 82
2.3.2 Uso previsto..... 83
2.3.3 Smaltimento e riciclaggio appropriati..... 83
2.3.4 Norme e linee guida per l'installazione..... 84
2.3.4.1 Collegamento di OpenScape Business X al circuito di alimentazione..... 84
2.3.4.2 Allacciamento di OpenScape Business S e OpenScape Business UC Booster Server al circuito di alimentazione..... 84
2.3.4.3 Cablaggio schermato per allacciamenti LAN e WAN di OpenScape Business X..... 85
2.3.4.4 Requisiti antincendio..... 85
2.3.4.5 Requisiti di protezione contro i fulmini..... 86
2.3.4.6 Identificativi di OpenScape Business X..... 86
2.3.5 Informazioni sull'emissione di interferenze e interferenze radio di OpenScape Business X..... 87
2.3.6 Protezione e sicurezza dei dati..... 87
2.3.7 Requisiti tecnici e conformità di OpenScape Business X..... 88
2.3.7.1 Conformità CE..... 88
2.3.7.2 Conformità alle norme degli Stati Uniti e del Canada..... 88
2.3.7.3 Conformità alle norme internazionali..... 89
2.3.8 Condizioni d'uso..... 89
2.3.8.1 Condizioni d'uso per OpenScape Business X..... 89
2.3.8.2 Condizioni d'uso - OpenScape Business S e OpenScape Business UC Booster Server..... 90

3 Panoramica..... 91
3.1 Punti salienti..... 91
3.2 Comunicazione unificata..... 91
3.2.1 Funzioni UC..... 92
3.2.2 Accesso dell'utente alle funzioni UC (client UC)..... 98
3.2.3 Integrazione in applicazioni commerciali..... 101
3.3 OpenScape Business - Modelli..... 102
3.3.1 Livelli di espansione disponibili presso il reparto commerciale..... 102
3.3.2 Modelli hardware UC..... 106
3.3.3 Hardware UC Booster..... 107

3.3.4 Modelli software UC (soft switch)..... 107
3.3.5 Struttura e condizioni ambientali..... 107
3.3.6 Telefoni supportati..... 108
3.4 Altre informazioni..... 109
3.4.1 Lingue supportate..... 109
3.4.2 Collegamenti Internet..... 112

4 Principi di base per l'amministrazione..... 113
4.1 OpenScape Business Assistant (WBM)..... 113
4.1.1 Requisiti per il WBM..... 113
4.1.2 Pagina iniziale di WBM..... 113
4.1.3 Introduzione su WBM..... 115
4.1.3.1 Come accedere al WBM..... 117
4.1.3.2 Come disconnettersi dal WBM..... 117
4.1.4 Gestione utenti WBM..... 117
4.1.4.1 Come aggiungere amministratori..... 121
4.1.4.2 Come modificare amministratori..... 121
4.1.4.3 Come modificare la propria password amministratore..... 121
4.1.4.4 Come cancellare amministratori..... 122
4.1.4.5 Come modificare una password di amministratore Manager E..... 122
4.1.5 Procedure guidate..... 122
4.1.5.1 Procedure guidate – Installazione di base..... 123
4.1.5.2 Procedure guidate – Rete / Internet..... 123
4.1.5.3 Procedure guidate - Telefoni/Abbonati..... 123
4.1.5.4 Procedure guidate – Telefonia centrale..... 124
4.1.5.5 Procedure guidate – Telefonia utenti..... 125
4.1.5.6 Procedure guidate – Sicurezza..... 126
4.1.5.7 Procedure guidate – UC Smart (solo con UC Smart)..... 126
4.1.5.8 Procedure guidate – UC Suite (solo con UC Suite)..... 126
4.1.5.9 Procedure guidate - Rubrica unificata..... 127
4.1.5.10 Procedure guidate - Servizi cloud..... 127
4.1.6 Centro assistenza..... 127
4.1.6.1 Centro assistenza – **Documenti**..... 128
4.1.6.2 Centro assistenza – **Software** 128
4.1.6.3 Centro assistenza – **Inventario** > **Sistema**..... 128
4.1.6.4 Centro assistenza – **Inventario** > **Numeri di telefono**..... 128
4.1.6.5 Centro assistenza – **Inventario** > **Descrizione rete**..... 129
4.1.6.6 Centro assistenza - **Aggiornamento del software**..... 129
4.1.6.7 Centro assistenza - **Inoltro e-mail**..... 129
4.1.6.8 Centro assistenza – **Accesso remoto**..... 129
4.1.6.9 Centro assistenza - **Riavvia/Ricarica**..... 129
4.1.6.10 Centro assistenza – **Diagnostica** > **Stato**..... 129
4.1.6.11 Centro assistenza – **Diagnostica** > **Visualizzatore eventi**..... 129
4.1.6.12 Centro assistenza – **Diagnostica** > **Traccia**..... 129
4.1.6.13 Centro assistenza – Diagnostica > Log servizi..... 130
4.1.7 Modalità esperti..... 130
4.1.8 Guida in linea..... 130
4.1.8.1 Come aprire la Guida in linea in modo sensibile al contesto..... 130
4.2 Manager E..... 131
4.2.1 Come caricare il CDB in Manager E..... 132
4.2.2 Come ripristinare il CDB nel sistema..... 132

5 Configurazione iniziale di OpenScape Business X..... 133
5.1 Requisiti richiesti per l'installazione iniziale..... 134
5.2 Componenti..... 135
5.3 Piano di composizione..... 136

5.4 Schema indirizzi IP....137
5.5 Prima messa in servizio....138
5.5.1 Come avviare il sistema di comunicazione....139
5.5.2 Come collegare il PC Admin al sistema di comunicazione....140
5.5.3 Come avviare WBM....141
5.6 Integrazione nella LAN del cliente....142
5.6.1 Come avviare la procedura guidata Prima installazione....143
5.6.2 Impostazioni di sistema....143
5.6.2.1 Come definire il logo sul display e la descrizione del prodotto....144
5.6.2.2 Come definire gli indirizzi IP (opzionale)....144
5.6.2.3 Come specificare il nome del dispositivo....145
5.6.3 Impostazioni DHCP....146
5.6.3.1 Come disabilitare il server DHCP interno....146
5.6.3.2 Come abilitare e configurare il server DHCP interno....147
5.6.3.3 Come abilitare il DHCP solo per i dispositivi Mitel/Unify....148
5.6.4 Impostazioni temporali e del paese....150
5.6.4.1 Come selezionare il prefisso nazionale e la lingua per i registri eventi....150
5.6.4.2 Come immettere l'ID di sistema (EIC) DECT....151
5.6.4.3 Come configurare manualmente data e ora....152
5.6.4.4 Come fare riferimento alla data e all'ora di un server SNTP....152
5.6.5 Soluzione UC....153
5.6.5.1 Come definire la soluzione UC....153
5.6.6 Connessione del sistema di comunicazione alla LAN del cliente....154
5.6.6.1 Come collegare il sistema di comunicazione alla LAN del cliente....154
5.7 Configurazione base....155
5.7.1 Come avviare la procedura guidata Installazione di base....155
5.7.2 Numeri di telefono completi e collegamento in rete....156
5.7.2.1 Come inserire i numeri di telefono completi per una connessione punto - punto....156
5.7.2.2 Come inserire i numeri di telefono completi per una connessione punto - multipunto....157
5.7.2.3 Come attivare o disattivare la connessione di rete....158
5.7.3 Dati dell'utente....159
5.7.3.1 Come visualizzare i dati utente....161
5.7.3.2 Come eliminare tutti i numeri di telefono....161
5.7.3.3 Modificare i numeri di telefono preconfigurati in base al piano di composizione specifico....161
5.7.3.4 Come importare i dati degli utenti tramite un file XML....162
5.7.3.5 Come visualizzare i dati di massa....162
5.7.4 Configurazione ISDN....164
5.7.4.1 Come configurare il collegamento di utenti ISDN....164
5.7.4.2 Come configurare la linea esterna punto - punto ISDN....165
5.7.4.3 Come configurare la linea esterna punto - multipunto ISDN....165
5.7.4.4 Come disattivare la configurazione ISDN....166
5.7.5 Accesso a Internet....166
5.7.5.1 Come configurare l'accesso a Internet tramite un router Internet esterno mediante una connessione LAN....169
5.7.5.2 Come configurare l'accesso a Internet con un router Internet esterno mediante una connessione WAN....170
5.7.5.3 Come configurare l'accesso a Internet tramite ISP preimpostato....171
5.7.5.4 Come configurare l'accesso a Internet tramite un ISP standard PPPoE....173
5.7.5.5 Come configurare l'accesso a Internet tramite un ISP standard PPTP....175
5.7.5.6 Come configurare l'accesso a Internet tramite un router Internet esterno sulla LAN con porta WAN dedicata all'ITSP....177
5.7.5.7 Come disattivare l'accesso a Internet....178
5.7.6 Telefonia Internet....179
5.7.6.1 Come configurare un ITSP predefinito....180
5.7.6.2 Come disattivare la telefonia Internet....185
5.7.7 Utenti....185

5.7.7.1 Come configurare gli utenti ISDN 186
5.7.7.2 Come configurare gli utenti analogici....188
5.7.7.3 Come configurare gli utenti UP0....191
5.7.7.4 Come configurare gli utenti DECT....194
5.7.7.5 Come configurare utenti IP e SIP....196
5.7.8 Configurazione della UC Suite....199
5.7.8.1 Come configurare la UC Suite....199
5.7.9 Configurazione delle caselle vocali UC Smart....200
5.7.9.1 Come configurare le caselle vocali UC Smart....200
5.7.10 Impostazioni del server conferenze....201
5.7.10.1 Come modificare le impostazioni server conferenza....201
5.7.11 Invio per e-mail (opzionale)....202
5.7.11.1 Come configurare l'invio di e-mail....202
5.8 Attività finali....205
5.8.1 Come attivare e assegnare le licenze....206
5.8.2 Come preparare i client UC Smart all'installazione....208
5.8.3 Come preparare i client UC Suite all'installazione....208
5.8.4 Come eseguire il backup dei dati....209
5.9 Messa in servizio dei telefoni IP....210
5.9.1 Come configurare il telefono IP....212
5.9.2 Come configurare un telefono SIP....213
5.10 Come raccogliere tracce diagnostiche per un evento di errore....215
5.11 Reflashing....216

6 Configurazione iniziale di OpenScape Business S....218
6.1 Requisiti richiesti per la configurazione iniziale....218
6.2 Componenti....221
6.3 Schema indirizzi IP....222
6.4 Piano di composizione....222
6.5 Installazione del software di comunicazione....223
6.5.1 Come installare il software di comunicazione....225
6.6 Messa in servizio....227
6.6.1 Come avviare la procedura guidata Prima installazione....227
6.6.2 Impostazioni di sistema....227
6.6.2.1 Come impostare il logo sul display e il nome del prodotto....228
6.6.2.2 Come selezionare il prefisso nazionale e la lingua per i registri di traccia....229
6.6.2.3 Come attivare una porta LAN aggiunta come interfaccia WAN....229
6.6.2.4 Come modificare il piano di composizione con numeri a 4 cifre....230
6.6.3 Soluzione UC....231
6.6.3.1 Come definire la soluzione UC....231
6.7 Configurazione base....232
6.7.1 Come avviare la procedura guidata Installazione di base....232
6.7.2 Numeri di telefono completi e collegamento in rete....233
6.7.2.1 Come inserire i numeri di telefono completi per una connessione punto - punto....233
6.7.2.2 Come inserire i numeri di telefono completi per una connessione punto - multipunto....234
6.7.2.3 Come attivare o disattivare la connessione di rete....235
6.7.2.4 Come configurare l'upstream della connessione a Internet....236
6.7.3 Dati dell'utente....236
6.7.3.1 Come visualizzare i dati utente....238
6.7.3.2 Come eliminare tutti i numeri di telefono....238
6.7.3.3 Modificare i numeri di telefono preconfigurati in base al piano di composizione specifico....238
6.7.3.4 Come importare i dati degli utenti tramite un file XML....239
6.7.4 Accesso a Internet....239
6.7.4.1 Come configurare l'accesso a Internet tramite un router Internet esterno sulla LAN con porta WAN dedicata all'ITSP....240
6.7.5 Telefonia Internet 241

6.7.5.1 Come configurare un ITSP predefinito....242
6.7.5.2 Come disattivare la telefonia Internet....247
6.7.6 Utenti....247
6.7.6.1 Come configurare utenti IP e SIP....247
6.7.7 Configurazione della UC Suite....250
6.7.7.1 Come configurare la UC Suite....250
6.7.8 Configurazione delle caselle vocali UC Smart....251
6.7.8.1 Come configurare le caselle vocali UC Smart....251
6.7.9 Impostazioni del server conferenze....252
6.7.9.1 Come modificare le impostazioni server conferenza....252
6.7.10 Invio per e-mail (opzionale)....253
6.7.10.1 Come configurare l'invio di e-mail....253
6.8 Attività finali....256
6.8.1 Come attivare e assegnare le licenze....257
6.8.2 Come preparare i client UC Smart all'installazione....259
6.8.3 Come preparare i client UC Suite all'installazione....259
6.8.4 Come eseguire il backup dei dati....260
6.9 Messa in servizio dei telefoni IP....261
6.9.1 Come configurare il telefono IP....262
6.9.2 Come configurare un telefono SIP....263
6.10 Disinstallazione del software di comunicazione....265
6.10.1 Come disinstallare il software di comunicazione....265
6.11 Porte usate....265
6.12 Come raccogliere tracce diagnostiche per un evento di errore....268
6.13 Reflashing....269

7 Configurazione iniziale di OpenScape Business UC Booster....271
7.1 Requisiti richiesti per la configurazione iniziale....273
7.2 Backup dei dati di configurazione del sistema di comunicazione....276
7.2.1 Come eseguire il backup dei dati....276
7.3 Messa in servizio della UC Booster Card....277
7.3.1 Montaggio della UC Booster Card....277
7.3.2 Configurazione della UC Booster Card....277
7.3.3 Aggiornamento software per la UC Booster Card....278
7.3.3.1 Come eseguire l'aggiornamento del software....278
7.4 Messa in servizio dell'UC Booster Server....279
7.4.1 Installazione del software di comunicazione....279
7.4.1.1 Come installare il software di comunicazione....280
7.4.2 Configurazione dell'UC Booster Server....282
7.4.2.1 Comunicazione dell'indirizzo IP del sistema di comunicazione....282
7.4.3 Aggiornamento software per l'UC Booster Server....284
7.5 Configurazione base....285
7.6 Attività finali....285
7.7 Disinstallazione del software di comunicazione....286
7.7.1 Come disinstallare il software di comunicazione....286
7.8 Aggiornamento da UC Booster Card a UC Booster Server....286
7.9 Porte usate....288

8 Concessione della licenza....291
8.1 Procedura per la concessione della licenza....292
8.2 Licenze....294
8.2.1 Licenza di base....295
8.2.2 Licenze utente....296
8.2.3 Licenze orientate all'utente....297
8.2.4 Licenze di sistema....299
8.2.5 Licenze dimostrative....301

8.2.6 Licenze di upgrade....303
8.2.7 Suggerimenti per combinazioni di licenze....303
8.3 Concessione della licenza di un sistema di comunicazione (indipendente)....306
8.3.1 CLS Connect....306
8.3.1.1 Come attivare CLS Connect....307
8.3.1.2 Passaggio da CLS connect....308
8.3.2 Attivazione licenza (sistema indipendente)....308
8.3.2.1 Come attivare le licenze online (indipendente)....309
8.3.2.2 Come attivare le licenze offline (indipendente)....310
8.3.3 Assegnazione della licenza (indipendente)....310
8.3.3.1 Come concedere licenze agli utenti (indipendente)....312
8.3.3.2 Come concedere licenze alle linee (indipendente)....315
8.4 Concessione della licenza in più sistemi di comunicazione (sistema di reti)....316
8.4.1 Attivazione licenza (sistema di reti)....318
8.4.1.1 Come attivare le licenze offline (sistema di reti)....318
8.4.1.2 Come unire più file di licenza in un file di licenza di rete....320
8.4.2 Assegnazione della licenza (sistema di reti)....321
8.4.2.1 Come concedere licenze agli utenti (sistema di reti)....323
8.4.2.2 Come concedere licenze alle linee (sistema di reti)....326
8.4.2.3 Come assegnare le licenze di sistema a un nodo....326
8.4.2.4 Come assegnare la licenza di sistema "Rete" a un nodo....327
8.5 Informazioni licenza....327
8.5.1 Informazioni sulle licenze in assenza di un sistema di reti (configurazione indipendente)....328
8.5.1.1 Come visualizzare le informazioni sulla licenza....328
8.5.2 Informazioni sulle licenze nel sistema di reti....328
8.5.2.1 Come visualizzare tutte le licenze del sistema di reti....329
8.5.2.2 Come visualizzare le licenze collegate a un nodo....329
8.5.2.3 Come visualizzare tutte le licenze condivise nel sistema di reti....330
8.5.2.4 Come visualizzare in base ai nodi le licenze apparecchio e orientate all'utente....330
8.6 Assegnazione del profilo licenza....330
8.6.1 Come aggiungere un profilo licenza....331
8.6.2 Come modificare un profilo licenza....331
8.6.3 Come assegnare un profilo licenza a un utente....332
8.6.4 Come eliminare un profilo licenza....333
8.7 Rehost dopo sostituzione dell'hardware....334
8.7.1 Come eseguire un rehost dopo una sostituzione dell'hardware....335
8.8 Server delle licenze (Central License Server, CLS)....335
8.8.1 Come interrogare o modificare l'indirizzo IP del server licenze....335
8.8.2 Come verificare la connessione al Central License Server (CLS)....336
8.9 Agente licenze (Customer License Agent, CLA)....336
8.9.1 Come configurare la connessione all'agente delle licenze locale....337
8.9.2 Come modificare la connessione all'agente delle licenze centrale....337
8.10 Locking ID e Advanced Locking ID....337
8.10.1 Come controllare il Locking ID del sistema di comunicazione....338
8.10.2 Come ottenere il Locking ID del soft switch....339
8.10.3 Come ottenere l'Advanced Locking ID dello soft switch....339
8.11 Come migrare dalla scheda madre V2 alla scheda madre V3 (sistema indipendente)....339
8.12 Come migrare il nodo master di un sistema connesso in rete dalla scheda madre V2 alla scheda madre V3....341
8.13 Come migrare il nodo slave di un sistema connesso in rete dalla scheda madre V2 alla scheda madre V3....342
8.14 Migrazione dei sistemi HiPath 3000 al software OSBiz V3 con scheda madre V3....342
8.15 Aggiornamento da V2 a V3 con **CLS Connect**....342
8.16 Aggiornamento da V2 a V3 senza **CLS Connect**....343

9 Integration nella rete dati interna (LAN)....344

9.1 Interfaccia LAN....344
9.1.1 Indirizzo IP e maschera di rete dell'interfaccia LAN....344
9.1.1.1 Come modificare l'indirizzo IP e la maschera di rete della piattaforma hardware....345
9.1.1.2 Come modificare l'indirizzo IP della UC Booster Card....345
9.1.1.3 Come modificare l'indirizzo IP e la maschera del soft switch....346
9.1.2 Intervallo di indirizzi IP interno dell'interfaccia LAN....347
9.1.2.1 Come modificare l'intervallo di indirizzi IP interni della piattaforma hardware....347
9.1.2.2 Come reimpostare l'intervallo di indirizzi IP interni della piattaforma hardware....347
9.2 DHCP....348
9.2.1 Agente di inoltro DHCP....348
9.2.1.1 Come configurare la piattaforma hardware come agente relè DHCP....348
9.2.2 Server DHCP....349
9.2.2.1 Come abilitare e configurare il server DHCP della piattaforma hardware....350
9.2.2.2 Come disabilitare il server DHCP della piattaforma hardware....352
9.2.2.3 Come attivare e configurare il server DHCP del soft switch....353
9.2.2.4 Come disattivare il server DHCP del soft switch....353
9.2.2.5 Come abilitare il DHCP solo per i dispositivi Mitel/Unify....354
9.3 DNS - Risoluzione dei nomi....355
9.3.1 Come impostare il server DNS esterno....356
9.4 Routing IP....357
9.4.1 Come attivare o disattivare il router predefinito....357
9.4.2 Come aggiungere la route statica....358
9.4.3 Come cancellare route statiche....359
9.5 Servizio di distribuzione (DLI e DLS)....359
9.5.1 Come configurare un server DLS esterno nel server DHCP interno....361
9.5.2 Come attivare il DLI interno....362
9.5.3 Come configurare il client del sistema di comunicazione come client di distribuzione e licenze....363

10 Connessione al provider di servizi....364
10.1 Accesso a Internet....364
10.1.1 Accesso a Internet tramite router esterno....366
10.1.1.1 Come configurare l'accesso a Internet tramite un router Internet esterno mediante una connessione LAN....366
10.1.1.2 Come configurare l'accesso a Internet con un router Internet esterno mediante una connessione WAN....367
10.1.1.3 Come configurare l'accesso a Internet tramite un router Internet esterno sulla LAN con porta WAN dedicata all'ITSP....368
10.1.2 Accesso a Internet tramite modem Internet....370
10.1.2.1 Come configurare l'accesso a Internet tramite ISP preimpostato....371
10.1.2.2 Come configurare l'accesso a Internet tramite un ISP standard PPPoE....373
10.1.2.3 Come configurare l'accesso a Internet tramite un ISP standard PPTP....375
10.1.3 Interfaccia WAN....378
10.1.4 DynDNS....378
10.1.4.1 Come configurare il servizio DynDNS....379
10.1.4.2 Come definire Mail Exchanger....381
10.2 Linea esterna tramite ITSP....381
10.2.1 Configurazione di un ITSP....383
10.2.1.1 Come configurare un ITSP predefinito....385
10.2.1.2 Come aggiungere un nuovo ITSP....391
10.2.1.3 Come configurare un multisito tramite ITSP....397
10.2.1.4 Come salvare un modello ITSP preconfigurato come un nuovo modello....398
10.2.1.5 Come modificare il modello ITSP preconfigurato....399
10.2.1.6 Come aggiornare manualmente il modello ITSP preconfigurato....399
10.2.2 STUN (Simple Traversal of UDP through NAT)....400
10.2.2.1 Come definire la modalità STUN....401
10.3 Accesso alla linea urbana tramite linee analogiche e digitali....401

10.3.1 Linee....401
10.3.1.1 Come configurare la linea esterna ISDN....403
10.3.1.2 Come configurare la linea esterna analogica....404
10.3.1.3 Come mostrare tutte le linee....405
10.3.1.4 Come visualizzare una singola linea....405
10.3.1.5 Come modificare il codice della linea....405
10.3.1.6 Come assegnare un MSN ad una linea....406
10.3.1.7 Come modificare il protocollo ISDN....406
10.3.1.8 Come modificare la modalità di impegno del canale B....406
10.3.1.9 Come modificare il tipo di selezione....407
10.3.2 Fasci....407
10.3.2.1 Come modificare l'assegnazione del fascio....410
10.3.2.2 Come modificare i nomi dei fasci....411
10.3.2.3 Come modificare i codici del fascio....411
10.3.2.4 Come configurare un fascio di overflow con la funzione LCR disattivata....411
10.3.2.5 Come configurare un fascio di overflow con la funzione LCR attivata....412
10.3.2.6 Come configurare il tipo di impegno....412
10.3.2.7 Come inserire il numero di telefono del sistema in entrata e in uscita....412
10.3.2.8 Come configurare il formato del numero di telefono trasmesso....413
10.3.2.9 Come configurare il tipo di numero di telefono trasmesso....413
10.3.2.10 Come configurare il prefisso del fascio....413
10.3.2.11 Come definire un fascio per la connessione di rete e inserire un secondo codice di linea urbana....414
10.3.3 Controllo del segnale di linea....414
10.3.3.1 Come configurare il ritardo per il controllo del segnale di linea....415
10.3.3.2 Come configurare il tempo di controllo del segnale di linea....416
10.3.3.3 Come configurare il tempo di selezione delle cifre....416
10.3.3.4 Come attivare o disattivare la valutazione del secondo tono di composizione....417
10.4 Assegnazione priorità accesso linea esterna con funzione LCR attivata....417
10.4.1 Come priorizzare l'accesso alla linea esterna....418

11 Utenti....419
11.1 Piano di composizione....419
11.1.1 Piano di composizione predefinito....420
11.1.2 Piano di composizione personalizzato....421
11.1.2.1 Come cancellare o modificare i numeri di telefono predefiniti....422
11.1.2.2 Come modificare i numeri di telefono predefiniti speciali....422
11.1.2.3 Come importare numeri di telefono e dati utente....423
11.2 Requisiti per la telefonia LAN....424
11.2.1 Codec audio....424
11.2.1.1 Come configurare i parametri Codec audio....425
11.2.1.2 Come assegnare i parametri codec audio a una destinazione....426
11.2.2 Trasmissione di toni secondo RFC2833....427
11.2.2.1 Come attivare o disattivare la trasmissione di toni fax/modem secondo RFC2833....427
11.2.2.2 Come attivare o disattivare la trasmissione DTMF secondo RFC2833....427
11.2.3 Quality of Service....428
11.2.3.1 Come configurare la Quality of Service....430
11.3 Utente IP....431
11.4 Stazioni SIP....432
11.5 Utenti UP0....434
11.6 Utenti DECT....435
11.7 Stazioni Mitel SIP DECT....435
11.8 Utenti ISDN....436
11.8.1 Come configurare l'interfaccia S_0 per utenti ISDN....438
11.8.2 Come consentire solo numeri configurati per MSN....438
11.9 Utenti analogici....439

11.10 Utenti virtuali....440
11.11 Programmazione dei tasti 441
11.11.1 Come programmare i tasti funzione nei telefoni del sistema....441
11.12 Profilo apparecchio....443
11.13 Configurazione degli utenti....443
11.13.1 Come configurare gli utenti IP 445
11.13.2 Come configurare gli utenti SIP....448
11.13.3 Come configurare le stazioni UP0....453
11.13.4 Come configurare gli utenti DECT....456
11.13.5 Come configurare le stazioni Mitel SIP DECT tramite provisioning....459
11.13.5.1 Come configurare le stazioni SIP in modalità Esperto....461
11.13.6 Come configurare gli utenti ISDN....462
11.13.7 Come configurare gli utenti analogici....465
11.13.8 Come modificare i nomi degli utenti....468
11.14 Configurazione dei profili apparecchio 469
11.14.1 Come creare un nuovo profilo apparecchio....469
11.14.2 Come visualizzare un profilo apparecchio e i relativi membri....470
11.14.3 Come aggiungere membri a un profilo apparecchio....471
11.14.4 Come cancellare i membri da un profilo apparecchio....471
11.14.5 Come importare o esportare i profili dei singoli utenti....472
11.14.6 Come modificare i valori e le impostazioni di un profilo apparecchio....473
11.14.7 Come importare o esportare i profili di tutti gli utenti....474
11.15 Configurazione dati di autenticazione nel telefono SIP....474
11.15.1 Come configurare i dati di autenticazione tramite il WBM del telefono SIP....475
11.15.2 Come configurare i dati di autenticazione sul display del telefono SIP....477
11.16 Esportazione dei dati degli utenti....478
11.16.1 Come esportare i dati degli utenti....478

12 UC Smart....480
12.1 Impostazioni di base per UC Smart....481
12.1.1 Come attivare UC Smart....481
12.1.2 Come configurare UC Smart....482
12.1.3 Come configurare le conferenze controllate da applicazioni....483
12.1.4 Come rilevare gli indirizzi IP dei componenti del sistema....484
12.1.5 Come controllare lo stato di UC Smart....484
12.2 Client UC Smart....485
12.2.1 myPortal @work....485
12.2.1.1 Requisiti richiesti per myPortal @work....487
12.2.1.2 Configurazione utente myPortal @work....489
12.2.1.3 Passaggi di configurazione per utilizzare myPortal @work via Internet....496
12.2.1.4 Altri suggerimenti & impostazioni di configurazione....497
12.2.1.5 Guida alla risoluzione dei problemi....499
12.2.1.6 Ulteriori suggerimenti....501
12.3 Utente di UC Smart....502
12.3.1 Come configurare un utente di UC Smart....503
12.3.2 Come modificare la password per un utente di UC Smart....503
12.4 Stato presenza (presenza)....504
12.5 Rubriche e diario....504
12.5.1 Rubriche....505
12.5.1.1 Come configurare le rubriche dei telefoni del sistema....505
12.5.2 Rubrica interna....506
12.5.2.1 Come attivare o disattivare un utente nella rubrica interna....507
12.5.3 Elenco dei Preferiti....507
12.5.4 Rubrica del sistema....507
12.5.5 Rubrica unificata....507
12.5.5.1 Caratteristiche....508

12.5.5.2 Regole e convenzioni..... 512
12.5.5.3 Capitolo 11.5.5.3 Limiti funzionali..... 512
12.5.5.4 Rubrica unificata nei sistemi di rete..... 513
12.5.6 Diario..... 514
12.6 Chiamate..... 514
12.6.1 Formati dei numeri di telefono..... 514
12.6.2 Requisiti per ricevere chiamate VoIP su myPortal to go utilizzando CallKit sull'iPhone..... 515
12.7 Conferenze..... 516
12.8 Web Collaboration..... 517
12.8.1 Come configurare la connessione al server di Web Collaboration (server pubblico)..... 518
12.8.2 Come disattivare la connessione al server di Web Collaboration..... 519
12.9 Invio messaggi immediato..... 519
12.9.1 Invio messaggi immediato..... 519
12.10 Casella vocale (SmartVM)..... 519
12.10.1 Configurazione della casella vocale (SmartVM) 522
12.10.1.1 Come attivare o disattivare la casella vocale..... 523
12.10.1.2 Come configurare la casella vocale (SmartVM)..... 523
12.10.1.3 Come aggiungere una mailbox standard per un utente..... 525
12.10.1.4 Come modificare il gruppo di abilitazione per la porta della casella vocale..... 525
12.10.1.5 Come modificare la struttura del menu del telefono per la casella vocale..... 526
12.10.1.6 Come caricare, salvare ed eliminare i singoli annunci di benvenuto..... 526
12.10.1.7 Come salvare e reimpostare gli annunci di benvenuto e i messaggi..... 527
12.10.2 Servizio informativo per nuovi messaggi..... 528
12.10.2.1 Come attivare o disattivare gli avvisi tramite e-mail..... 528

13 UC Suite..... 530
13.1 Impostazioni di base per UC Suite..... 530
13.1.1 Come attivare UC Suite..... 531
13.1.2 Come limitare l'abilitazione per le chiamate UC effettuate a livello di sistema..... 531
13.2 Client UC Suite..... 532
13.2.1 myPortal for Desktop..... 532
13.2.2 myPortal @work..... 533
13.2.3 myPortal for Outlook..... 533
13.2.4 Fax Printer..... 533
13.2.5 myAttendant..... 534
13.2.6 Requisiti richiesti per client PC della UC Suite..... 534
13.2.7 Installazione/disinstallazione Silent per client PC UC Suite..... 538
13.2.7.1 Come eseguire l'installazione Silent..... 539
13.2.7.2 Come eseguire la disinstallazione Silent..... 540
13.2.8 Aggiornamenti automatici..... 541
13.3 Utente e profilo utente della UC Suite..... 541
13.3.1 Utenti della..... 541
13.3.1.1 Come configurare gli utenti della UC Suite..... 544
13.3.1.2 Come reimpostare gli utenti della UC Suite..... 545
13.3.1.3 Come configurare un utente della UC Suite come agente (myAgent)..... 545
13.3.1.4 Come cambiare lo stato presenza per un utente della UC Suite..... 546
13.3.1.5 Come modificare la password per un utente della UC Suite..... 546
13.3.1.6 Come modificare la lunghezza della password per un utente della UC Suite..... 547
13.3.2 Profili utente della UC Suite..... 547
13.3.2.1 Come aggiungere un profilo utente della UC Suite..... 549
13.3.2.2 Come modificare un profilo utente della UC Suite..... 549
13.3.2.3 Come visualizzare il profilo utente della UC Suite..... 549
13.3.2.4 Come aggiungere membri a un profilo utente della UC Suite..... 550
13.3.2.5 Come eliminare i membri da un profilo utente della UC Suite..... 550
13.3.2.6 Come eliminare un profilo utente della UC Suite..... 550
13.4 Stato presenza e servizio CallMe..... 551

13.4.1 Stato presenza (presenza)....551
13.4.2 Servizio CallMe....553
13.4.3 Deviazione di chiamata in base allo stato....554
13.4.4 Inoltro di chiamata basato su regole....555
13.5 Rubriche e diario....556
13.5.1 Rubriche....556
13.5.1.1 Come configurare le rubriche dei telefoni del sistema....558
13.5.2 Rubrica interna....559
13.5.2.1 Come attivare o disattivare un utente analogico nella rubrica interna....559
13.5.2.2 Come abilitare o disabilitare la ricerca solo nella rubrica interna....560
13.5.3 Rubrica esterna....560
13.5.3.1 Come importare un file CSV dal file system locale nella rubrica esterna....562
13.5.3.2 Come aggiungere l'accesso a un database esterno per la rubrica esterna....563
13.5.3.3 Come esportare un file CSV dalla rubrica esterna....564
13.5.4 Rubrica esterna non in linea (LDAP)....564
13.5.4.1 Come aggiungere una rubrica esterna non in linea (LDAP) per client PC....565
13.5.4.2 Come eliminare la rubrica esterna non in linea (LDAP) per i client PC....566
13.5.4.3 Come aggiungere una rubrica esterna non in linea (LDAP) per i telefoni di sistema....566
13.5.5 Rubrica di sistema....567
13.5.6 Rubrica unificata....567
13.5.6.1 Caratteristiche....568
13.5.6.2 Regole e convenzioni....572
13.5.6.3 Capitolo 11.5.5.3 Limiti funzionali....572
13.5.6.4 Rubrica unificata nei sistemi di rete....573
13.5.6.5 Come importare i contatti nella directory unificata....574
13.5.6.6 Come modificare o aggiungere nuovi contatti alla directory unificata....575
13.5.7 Reparti....576
13.5.7.1 Come aggiungere un reparto....576
13.5.7.2 Come assegnare un reparto ad un utente....576
13.5.7.3 Come modificare un reparto....577
13.5.7.4 Come eliminare un reparto....577
13.5.8 Elenco dei Preferiti....577
13.5.9 Diario....578
13.5.9.1 Come modificare il tempo di conservazione massimo per il diario....579
13.6 Chiamate....580
13.6.1 Dialer sul desktop e dialer degli appunti....580
13.6.2 Finestre popup....580
13.6.3 Registrazione di chiamate....581
13.6.3.1 Come attivare e disattivare la registrazione di chiamate....581
13.6.3.2 Come attivare o disattivare l'annuncio relativo alla registrazione....582
13.6.3.3 Come attivare o disattivare il tono di avviso per la registrazione....582
13.7 Conferenze....583
13.7.1 Gestione conferenze....583
13.7.1.1 Come modificare il numero di accesso per sala conferenze virtuale....587
13.7.1.2 Come consentire o impedire la presenza di più partecipanti esterni alla conferenza....587
13.7.1.3 Come attivare/disattivare il tono di conferenza....587
13.7.1.4 Come modificare gli intervalli di tempo per la conclusione automatica delle conferenze....588
13.7.1.5 Come richiedere i dettagli di una conferenza memorizzata....588
13.7.1.6 Come eliminare una conferenza memorizzata....589
13.7.1.7 Come configurare la registrazione di conferenze....589
13.7.2 Conferenza AdHoc....589
13.7.3 Conferenza pianificata....590
13.7.4 Conferenza permanente....592
13.7.5 Apri conferenza....593
13.8 Web Collaboration....593
13.8.1 Come configurare la connessione al server di Web Collaboration (server personalizzato)....595

13.8.2 Come configurare la connessione al server di Web Collaboration (server pubblico)....596
13.8.3 Come disattivare la connessione al server di Web Collaboration....596
13.9 Invio messaggi immediato....597
13.9.1 Invio messaggi immediato....597
13.9.1.1 Come attivare o disattivare i messaggi istantanei....598
13.10 AutoAttendant....598
13.10.1 AutoAttendant personale....598
13.11 Messaggi vocali e fax....599
13.11.1 Casella vocale....599
13.11.1.1 Come configurare il numero di telefono per la casella vocale....601
13.11.1.2 Come configurare dell'inoltro chiamata alla casella vocale....601
13.11.1.3 Come configurare i parametri della casella vocale....602
13.11.1.4 Come configurare la durata di conservazione per messaggi vocali....602
13.11.1.5 Come attivare o disattivare la richiesta di immissione della password per la casella vocale....603
13.11.1.6 Come configurare le informazioni per i messaggi vocali ricevuti....603
13.11.1.7 Come configurare del tasto "Mailbox" per richiamare messaggi vocali....603
13.11.2 Annunci della casella vocale....604
13.11.2.1 Come importare gli annunci per la casella vocale....605
13.11.2.2 Come modificare la lingua per gli annunci della casella vocale....606
13.11.3 Casella fax....606
13.11.3.1 Come aggiungere una casella fax per gli utenti....607
13.11.3.2 Come configurare il tipo dati per i messaggi fax salvati (UC Suite)....607
13.11.4 Invio di messaggi fax con Fax Printer....608
13.11.4.1 Come aggiungere una copertina centralizzata....609
13.11.4.2 Come modificare la copertina centralizzata....609
13.11.4.3 Come aggiungere la riga di intestazione di Fax Printer....609
13.11.4.4 Come modificare la riga di intestazione di Fax Printer....610
13.11.4.5 Come cancellare la riga di intestazione di Fax Printer....610
13.11.5 Servizio informativo per nuovi messaggi (UC Suite)....611
13.11.6 Invio per e-mail....612
13.11.6.1 Come configurare l'invio di e-mail....612
13.11.7 Modello SMS....613
13.11.7.1 Come aggiungere un modello SMS....614
13.11.7.2 Come modificare un modello SMS....614
13.11.7.3 Come eliminare un modello SMS....615
13.11.8 Fax over IP (Fax T.38 / G.711)....615
13.11.8.1 Come attivare o disattivare Fax over IP (fax T.38)....616
13.12 Panoramica sull'integrazione di Microsoft Office 365....616
13.12.1 Come connettere il sistema OpenScape Business a Microsoft Office 365 tramite l'autenticazione base....617
13.12.2 How to connect OpenScape Business system to Microsoft Office 365 using Modern Authentication....623
13.12.3 Come verificare che le funzionalità di integrazione di Microsoft Office 365 siano configurate....623

14 Funzioni del telefono....625
14.1 Esegui chiamata....625
14.1.1 Composizione a cifre....625
14.1.2 Selezione in blocco....625
14.1.3 Selez. blocco tasti....625
14.1.4 Identificazione della fine della selezione....626
14.1.5 Modifica d.selez....626
14.1.5.1 Come attivare o disattivare Modifica d.selez....627
14.1.6 Ripetizione della selezione....627
14.1.6.1 Come attivare o disattivare la ripetizione automatica dell'ultimo nr. selez....628
14.1.7 Selezione breve del sistema....628
14.1.7.1 Come aggiungere una destinazione di selezione breve....630

14.1.7.2 Come importare destinazioni di selezione breve da un file XML..... 630
14.1.7.3 Come esportare le destinazioni di selezione breve in un file XML.....631
14.1.7.4 Come modificare le destinazioni di selezione breve..... 631
14.1.8 Selezione breve individuale (KWI).....632
14.1.9 Chiamata diretta.....632
14.1.10 Chiamata diretta / Risposta tramite altoparlante.....633
14.1.10.1 Come attivare/disattivare il rifiuto chiamata su altoparlante per utenti..... 634
14.1.11 Composizione associata.....634
14.1.12 Prenotazione linea.....634
14.1.12.1 Come attivare/disattivare la prenotazione della linea.....635
14.1.13 Linea privata.....636
14.2 Segnalazione della chiamata, visualizzazione del numero di telefono..... 636
14.2.1 Segnalazione delle chiamate diversificata.....636
14.2.2 Trasmissione del numero di telefono (CLIP = Calling Line Identification Presentation).....636
14.2.2.1 Come attivare o disattivare la funzione CLIP impostabile.....637
14.2.3 Disattivazione della visualizzazione del numero di telefono (CLIR = Calling Line Identification Restriction).....637
14.2.3.1 Come attivare o disattivare la visualizzazione del numero di telefono.....638
14.2.4 Presentazione dell'identificazione delle linee collegate (COLP).....639
14.2.4.1 Come attivare o disattivare la trasmissione del numero di telefono del chiamante.....639
14.2.5 Disattivazione della visualizzazione del numero di telefono del chiamato (COLR).....639
14.2.6 CLIP no screening (trasmissione di informazioni sul numero di telefono specifiche del cliente).....640
14.2.6.1 Come configurare CLIP no screening.....640
14.2.7 CLIP per dispositivi analogici.....641
14.2.8 Chiamata senza suoneria / Silenzio..... 641
14.2.9 Conversione del numero in nome nella selezione breve del sistema.....641
14.3 Funzioni disponibili durante la chiamata.....641
14.3.1 Metti in attesa.....641
14.3.2 Parcheggio.....642
14.3.3 Consultazione.....643
14.3.4 Richiamata alternata..... 643
14.3.5 Trasferisci..... 643
14.3.6 Richiamata.....644
14.3.7 Ascolto di una chiamata.....645
14.3.7.1 Come attivare/disattivare l'ascolto chiamate per un utente.....646
14.3.8 Chiamata altoparlante discreta..... 646
14.3.9 Registrazione delle chiamate (Voice Recording, registrazione vocale)..... 648
14.4 Controllo della reperibilità.....649
14.4.1 Inoltro di chiamata 649
14.4.1.1 Come configurare un inoltro di chiamata..... 651
14.4.2 Come attivare la deviazione di chiamata (AUL)..... 653
14.4.2.1 Come attivare o disattivare la deviazione di chiamata tramite linea urbana analogica.....654
14.4.2.2 Come attivare o disattivare la deviazione di chiamata dopo una deviazione verso una destinazione esterna..... 655
14.4.3 Deviazione di chiamata a tempo..... 655
14.4.4 Inoltro di chiamata nella linea urbana (Stati Uniti esclusi).....656
14.4.5 Assegnazione delle chiamate..... 656
14.4.5.1 Come configurare l'assegnazione delle chiamate.....657
14.4.6 Segnalazione delle chiamate..... 657
14.4.7 Rifiuto di chiamate..... 658
14.4.8 Rinvio di una chiamata..... 659
14.4.9 Non disturbare.....659
14.5 Ottimizzazione dell'accelerazione delle comunicazioni.....660
14.5.1 Richiamata.....660
14.5.2 Avviso di chiamata in attesa.....661
14.5.2.1 Come attivare o disattivare l'avviso di chiamata in attesa.....662

14.5.2.2 Come attivare o disattivare l'avviso di chiamata in attesa immediato tramite la console posto operatore ... 662
14.5.3 Inclusione (intrusione) ... 663
14.5.3.1 Come autorizzare un utente interno all'inclusione ... 664
14.5.3.2 Come abilitare il posto di rinvio per l'inclusione ... 664
14.5.4 Testi di assenza ... 665
14.5.4.1 Come modificare il testo di assenza ... 665
14.5.5 Messaggi ... 665
14.5.5.1 Come modificare il testo di un messaggio ... 666
14.5.6 Servizi associati ... 666
14.5.6.1 Come attivare/disattivare i vari servizi ... 667
14.5.7 DISA ... 667
14.5.7.1 Come attivare/disattivare l'abilitazione DISA per un utente ... 668
14.5.7.2 Come configurare il numero DISA ... 668
14.5.7.3 Come configurare la modalità di sicurezza DISA ... 669
14.5.8 Flex Call/PIN mobile ... 669
14.5.9 Trasferimento ... 670
14.5.9.1 Come eseguire il trasferimento/scambio numero a livello di sistema ... 670
14.5.10 Reimpostazione dei servizi attivati ... 670
14.5.11 Procedure ... 671
14.5.12 Promemoria e appuntamenti ... 672
14.6 Panoramica di funzioni e codici ... 673

15 Lavoro in team (Gruppi) ... 678
15.1 Gruppo di risposta per assente, chiamata di gruppo e gruppo di ricerca ... 678
15.1.1 Gruppo di risposta per assente ... 678
15.1.2 Chiamata di gruppo ... 680
15.1.3 Gruppo di ricerca ... 684
15.1.4 Configurazione di gruppi di risposta per assente, chiamate di gruppo e gruppi di ricerca tramite procedure guidate ... 687
15.1.4.1 Come configurare un gruppo di risposta per assente ... 688
15.1.4.2 Come aggiungere o cancellare un membro dal gruppo di risposta per assente ... 688
15.1.4.3 Come aggiungere una chiamata di gruppo (gruppo) ... 689
15.1.4.4 Come modificare una chiamata di gruppo (gruppo) ... 690
15.1.4.5 Come eliminare una chiamata di gruppo (gruppo) ... 691
15.1.4.6 Come aggiungere o cancellare membri dalle chiamate di gruppo (gruppo) ... 692
15.1.4.7 Come aggiungere un gruppo di ricerca ... 692
15.1.4.8 Come modificare un gruppo di ricerca ... 693
15.1.4.9 Come eliminare un gruppo di ricerca ... 694
15.1.4.10 Come aggiungere o cancellare membri dal gruppo di ricerca ... 695
15.1.5 Configurazione di gruppi di risposta per assente, chiamate di gruppo e gruppi di ricerca tramite la Modalità esperti ... 696
15.1.5.1 Come abilitare o disabilitare la visualizzazione del numero di telefono e del nome del chiamante ... 696
15.1.5.2 Come attivare o disattivare il tono di avviso ... 697
15.1.5.3 Come attivare o disattivare la risposta per assente di richiamate ... 697
15.1.5.4 Come aggiungere una chiamata di gruppo (Libero o Avviso di chiamata in attesa) ... 697
15.1.5.5 Come visualizzare o modificare una chiamata di gruppo (Libero o Avviso di chiamata in attesa) ... 698
15.1.5.6 Come cancellare una chiamata di gruppo (Libero o Avviso di chiamata in attesa) ... 699
15.1.5.7 Come aggiungere o eliminare un membro di una chiamata di gruppo (Libero o Avviso di chiamata in attesa) ... 699
15.1.5.8 Come disattivare o attivare il rifiuto dell'avviso di chiamata per i membri del gruppo ... 700
15.2 Configurazione team / Gruppo team e Direttore/Segretaria / Gruppo Top ... 700
15.2.1 Configurazione team / gruppo Team ... 701
15.2.2 Direttore/Segretaria / Gruppo Top ... 705

15.2.3 Impostazione di funzioni Configurazione team / Gruppo Team e Direttore/Segretaria / Gruppi Top tramite procedure guidate 709
15.2.3.1 Come aggiungere la configurazione team / gruppo Team..... 709
15.2.3.2 Come modificare la configurazione team / gruppo Team..... 711
15.2.3.3 Come eliminare la configurazione team / gruppo Team..... 711
15.2.3.4 Come aggiungere un gruppo Direttore/Segretaria / Top..... 712
15.2.3.5 Come modificare un gruppo Direttore/Segretaria / Top..... 713
15.2.3.6 Come eliminare un gruppo Direttore/Segretaria / Top..... 714
15.2.4 Impostazione di funzioni Configurazione team / Gruppo Team e Direttore/Segretaria / Gruppi Top tramite la Modalità esperti..... 715
15.2.4.1 Come aggiungere o cancellare un membro dalla configurazione team / gruppo Team..... 715
15.2.4.2 Come modificare un membro della configurazione team / gruppo Team..... 716
15.2.4.3 Come modificare le proprietà dei membri di un gruppo Team..... 716
15.2.4.4 Come modificare l'assegnazione tasti sul telefono per configurazione team / gruppo Team..... 717
15.2.4.5 Come aggiungere la casella fax alla configurazione team / gruppo Team..... 717
15.2.4.6 Come aggiungere o eliminare un membro dal gruppo Direttore/Segretaria / Top..... 718
15.2.4.7 Come modificare un membro di un gruppo Direttore/Segretaria / Top..... 718
15.2.4.8 Come modificare le proprietà dei membri di un gruppo Direttore/Segretaria / Top..... 719
15.2.4.9 Come aggiungere la casella fax a un gruppo Direttore/Segretaria / Top..... 719
15.3 Basic MULAP e Direttore MULAP..... 720
15.3.1 MULAP di base..... 720
15.3.2 Direttore MULAP..... 723
15.3.3 Configurazione di Basic MULAP e Direttore MULAP..... 725
15.3.3.1 Come aggiungere un Basic MULAP..... 725
15.3.3.2 Come visualizzare o modificare il Basic MULAP..... 726
15.3.3.3 Come cancellare il Basic MULAP..... 727
15.3.3.4 Come aggiungere o eliminare un membro da un Basic MULAP..... 727
15.3.3.5 Come modificare un membro in un gruppo Basic MULAP..... 728
15.3.3.6 Come aggiungere un Direttore MULAP..... 728
15.3.3.7 Come visualizzare o modificare il Direttore MULAP..... 729
15.3.3.8 Come cancellare il Direttore MULAP..... 729
15.3.3.9 Come aggiungere o eliminare un membro da un Direttore MULAP..... 729
15.3.3.10 Come modificare un membro di un Direttore MULAP..... 730
15.3.3.11 Come aggiungere un Basic MULAP in un gruppo..... 730
15.4 Gruppi casella vocale e gruppi fax..... 731
15.4.1 Gruppo Casella vocale..... 731
15.4.2 Gruppo Casella fax..... 732
15.4.3 Configurazione di gruppi casella vocale e gruppi casella fax..... 733
15.4.3.1 Come aggiungere un gruppo Casella vocale..... 733
15.4.3.2 Come visualizzare o modificare il gruppo Casella vocale..... 734
15.4.3.3 Come cancellare un gruppo Casella vocale..... 734
15.4.3.4 Come aggiungere o cancellare un membro dal gruppo Casella vocale..... 734
15.4.3.5 Come modificare un membro del gruppo Casella vocale..... 735
15.4.3.6 Come configurare un gruppo Casella fax..... 735
15.4.3.7 Visualizzare o modificare il gruppo Casella fax..... 736
15.4.3.8 Come cancellare un gruppo casella fax..... 737
15.4.3.9 Come aggiungere o cancellare un membro dal gruppo Casella fax..... 737
15.5 Chiamata diretta per gruppi..... 737
15.5.1 Paging interno al gruppo..... 738
15.5.2 Trasferta al gruppo con paging interno..... 738
15.6 UCD (Uniform Call Distribution)..... 739
15.6.1 Distribuzione delle chiamate / gruppo UCD..... 739
15.6.1.1 Come configurare la distribuzione delle chiamate / gruppi UCD..... 740
15.6.2 Agenti UCD..... 741
15.6.2.1 Come aggiungere / cancellare agenti UCD..... 742
15.6.3 Post-elaborazione..... 743

15.6.3.1 Come modificare il tempo di post-elaborazione....744
15.6.4 Assegnazione delle chiamate in base alla priorità....744
15.6.4.1 Come modificare la priorità delle chiamate....745
15.6.5 Accettazione automatica chiamate UCD....745
15.6.5.1 Come modificare l'accettazione automatica di chiamate UCD....745
15.6.6 Coda UCD....746
15.6.6.1 Come modificare la coda UCD....746
15.6.7 Overflow UCD....747
15.6.7.1 Come modificare overflow UCD....748
15.6.8 Servizio notte UCD....748
15.6.9 Annunci/ Musica su attesa per UCD....749
15.6.9.1 Come modificare gli annunci/ la musica su attesa per UCD....749
15.6.10 Trasferimento a gruppi UCD....750
15.6.10.1 Come modificare il tempo di richiamata per chiamate trasferite a gruppi UCD....750
15.6.11 Rilascio di chiamate UCD tramite linee analogiche....751
15.6.11.1 Come modificare il tempo di rilascio per chiamate UCD su linee analogiche....751

16 Routing delle chiamate....752
16.1 Autorizzazioni (controllo della composizione)....752
16.1.1 Gruppi di abilitazione e classi di servizio....752
16.1.1.1 Come modificare il nome di un gruppo di abilitazione....753
16.1.1.2 Come modificare le classi di abilitazione di un gruppo di abilitazione....753
16.1.1.3 Come visualizzare tutti gli utenti di un gruppo di abilitazione....754
16.1.2 Liste nr. permessi e vietati....754
16.1.2.1 Come creare un elenco dei numeri di emergenza....755
16.1.2.2 Come creare una lista nr. permessi e una lista nr. vietati....755
16.1.2.3 Come creare altri liste nr. permessi....756
16.1.2.4 Come creare altre liste nr. vietati....757
16.1.2.5 Come visualizzare tutti i numeri di telefono di una lista nr. vietati....757
16.1.2.6 Come visualizzare tutti i numeri di telefono di una lista nr. permessi....757
16.1.2.7 Come modificare i filtri di analisi per la lista dei numeri vietati....758
16.1.3 Lista nera....758
16.1.3.1 Come creare una lista nera per le chiamate in arrivo in Modalità esperti....759
16.1.3.2 Come modificare/eliminare numeri di telefono nella lista nera....760
16.1.3.3 Come visualizzare i numeri di telefono nella lista nera....761
16.1.3.4 Come creare una lista nera per le chiamate in arrivo in Configurazione....761
16.1.4 Servizio notturno....762
16.1.4.1 Come assegnare le abilitazioni per servizio notte manuale....763
16.1.4.2 Come eliminare le abilitazioni per servizio notte manuale....763
16.1.4.3 Come configurare il servizio notte pianificato....764
16.1.4.4 Come configurare un giorno speciale per il servizio notte pianificato....764
16.1.4.5 Come eliminare un giorno speciale per il servizio notte pianificato....765
16.1.5 Commutazione automatica COS a tempo....765
16.1.5.1 Pianificazione....766
16.1.6 VBZ (restrizioni di traffico)....767
16.1.6.1 Gruppi con restrizioni di traffico....767
16.1.6.2 Assegnazione dei numeri brevi del sistema a gruppi con restrizione di traffico....768
16.1.6.3 Come assegnare un utente ad un gruppo con restrizioni di traffico....768
16.1.6.4 Come assegnare una linea ad un gruppo con restrizioni di traffico....769
16.1.6.5 Come modificare la matrice VBZ....769
16.1.7 Chiave elettronica centrale/commutazione dell’abilitazione....769
16.1.8 Chiave elettronica individuale (blocco del telefono)....770
16.1.8.1 Come reimpostare le singole chiavi elettroniche....770
16.1.9 Rifiuto chiam.con add.al chiamante per linea esterna (solo per Brasile)....771
16.1.10 Rifiuto chiam.con add.al chiamante per utente (solo per Brasile)....771
16.2 LCR (Least Cost Routing, Instradamento a minor costo)....771

16.2.1 Funzionalità LCR....771
16.2.1.1 Come attivare LCR....774
16.2.2 Piano di composizione LCR....775
16.2.2.1 Come modificare il piano di composizione....776
16.2.3 Tabella delle rotte LCR....777
16.2.3.1 Come modificare tabelle delle rotte....777
16.2.4 Abilitazione LCR....778
16.2.4.1 Come assegnare e modificare l'abilitazione LCR....779
16.2.5 Regole di composizione LCR....779
16.2.5.1 Come modificare le regole di composizione....781
16.2.6 Gestore di rete....781
16.2.7 Impegno mirato delle linee urbane....783
16.2.7.1 Come configurare il codice per l'occupazione mirata delle linee urbane ISDN....783
16.2.7.2 Come visualizzare i codici di accesso diretto per l'impegno selettivo della linea esterna....783
16.3 Analisi del numero composto e routing delle chiamate....784
16.3.1 Panoramica Routing delle chiamate/LCR....785
16.3.2 Diagramma di flusso analisi della composizione....787
16.3.3 Call Routing e LCR nella rete....788
16.3.3.1 Gateway dedicato....790
16.3.4 Scenari: analisi della composizione e routing delle chiamate....791
16.3.4.1 L'utente A chiama l'utente B tramite numero di telefono interno....792
16.3.4.2 L'utente A chiama l'utente B tramite un numero della rete pubblica....794
16.3.4.3 L'utente A chiama un utente interno tramite linea urbana....797
16.3.4.4 La linea esterna ISDN chiama l'utente A....798
16.3.4.5 Configurazioni speciali....798
16.3.4.6 L'utente A chiama l'utente C tramite numero di telefono interno....801
16.3.4.7 L'utente A chiama l'utente C tramite il numero di telefono pubblico nel sistema di reti....802
16.3.4.8 La linea esterna ISDN chiama l'utente C....805
16.3.4.9 Il gateway 1 della linea esterna ISDN chiama l'utente D....806
16.3.4.10 L'utente D chiama un utente esterno tramite linea urbana....809
16.4 Chiamate di emergenza....811
16.4.1 Hotline a tempo / Hotline....812
16.4.1.1 Come configurare e modificare le destinazioni Hotline....813
16.4.1.2 Come modificare il tempo di ritardo Hotline....813
16.4.1.3 Come configurare A tempo o Hotline per un utente....814
16.4.2 Rilascio della linea per una chiamata di emergenza....814
16.4.2.1 Come attivare/disattivare l'interruzione della connessione per chiamata di emergenza....814
16.4.3 Solo per USA e Canada: servizio d'emergenza E911....815
16.4.3.1 Come modificare CLIP / Lin....815
16.4.4 Chiamate di emergenza in combinazione con Mobile Logon....816
16.4.4.1 Configurazione dello scenario di emergenza....816
16.4.5 E112 Servizio di chiamata di emergenza europeo....819
16.4.5.1 Come aggiungere un ID Loc ITSP a un utente....819
16.5 CAC (Call Admission Control)....819
16.5.1 Limitazione del numero di chiamate simultanee tramite ITSP....820
16.5.2 Limitazione della necessità di banda per le chiamate tramite gateway....820
16.5.3 Limitazione del numero di chiamate negli scenari di collegamento in rete....820
16.6 Sistema ad uso comune....821
16.6.1 Selezione breve del sistema negli impianti comuni....822

17 Attendant....824
17.1 AutoAttendant....824
17.1.1 Company AutoAttendant (UC Smart)....826
17.1.1.1 Come configurare un AutoAttendant aziendale impostato....827
17.1.1.2 Come configurare un nuovo Company AutoAttendant....828
17.1.2 Company AutoAttendant (UC Suite)....830

17.1.2.1 Pianificazioni ... 830
17.1.2.2 Modelli ... 839
17.2 OpenStage Attendant ... 840
17.3 OpenScape Business Attendant ... 841
17.3.1 OpenScape Business BLF ... 844
17.3.2 Esempi di configurazione per OpenScape Business Attendant e OpenScape Business BLF ... 845
17.3.2.1 Scenario 1: OpenScape Business Attendant collegato a un singolo sistema OpenScape Business ... 845
17.3.2.2 Scenario 2: Due o più OpenScape Business Attendant collegati a un singolo sistema OpenScape Business ... 850
17.3.2.3 Scenario 3: collegamento in rete di OpenScape Business con i propri OpenScape Business Attendant (BLF e stato presenza a livello di rete tramite WSI) ... 852
17.3.2.4 Scenario 4: collegamento in rete di OpenScape Business con OpenScape Business Attendant centrale (BLF e stato presenza a livello di rete tramite WSI) ... 852
17.3.2.5 Scenario 5: OpenScape Business BLF collegato a un singolo sistema OpenScape Business ... 853
17.3.2.6 Scenario 6: OpenScape Business BLF collegato a un sistema di reti OpenScape Business (stato BLF e Presenza tramite WSI) ... 855
17.4 myAttendant ... 855
17.4.1 Gestione utenti ... 857
17.4.2 Centro messaggi ... 857
17.4.3 Scenario 1: come configurare myAttendant collegato a un singolo sistema OpenScape Business ... 858
17.4.4 Scenario 2: come configurare due o più myAttendant collegati a un singolo sistema OpenScape Business ... 859
17.4.5 Scenario 3: come configurare un collegamento in rete di OpenScape Business con myAttendant centrale ... 860
17.5 Posto di rinvio ... 861
17.5.1 Come configurare il posto e i criteri di rinvio ... 863
17.5.2 Come configurare il posto di rinvio centrale ... 863
17.5.3 Come configurare il rinvio con chiave elettronica ... 864
17.5.4 Come configurare il rinvio con annuncio ... 864

18 Contact Center multimediale ... 865
18.1 Client del Contact Center ... 865
18.1.1 myAgent ... 866
18.1.2 Requisiti richiesti per l'uso di myAgent ... 867
18.1.3 myReports ... 869
18.1.3.1 Come reimpostare la password amministratore di myReports ... 871
18.1.4 Requisiti richiesti per l'uso di myReports ... 871
18.1.5 Note sull'utilizzo simultaneo di myAgent e client UC Suite ... 873
18.2 Agenti ... 874
18.2.1 Funzioni degli agenti indipendenti dal livello di autorizzazione ... 874
18.2.2 Agenti preferiti ... 875
18.2.3 Agente in più code d'attesa ... 876
18.2.4 Pause del Contact Center ... 876
18.2.5 Accesso/Disconnessione agente tramite telefono ... 876
18.3 Code d'attesa e pianificazioni ... 879
18.3.1 Code d'attesa ... 879
18.3.2 Pianificazioni ... 881
18.3.3 Elaborazione ... 891
18.3.4 Livello di servizio ... 891
18.3.5 Display a parete ... 892
18.3.6 Richiamata agente ... 892
18.4 Trattamento VIP ... 892
18.4.1 Priorità chiamante VIP ... 892
18.4.2 Elenco chiamate VIP ... 893
18.5 Soluzione secondaria (soluzione fallback) ... 893

18.6 Configurazione del Contact Center....897
18.6.1 Esempio per la configurazione di un Contact Center....897
18.6.1.1 Come configurare i gruppi UCD per il Contact Center di esempio....899
18.6.1.2 Come configurare la soluzione secondaria (soluzione fallback) per il Contact Center di esempio....900
18.6.1.3 Come configurare un utente come agente per il Contact Center di esempio....901
18.6.1.4 Come registrare annunci per il Contact Center di esempio....902
18.6.1.5 Come caricare annunci per il Contact Center di esempio....902
18.6.1.6 Come aggiungere una pianificazione XYZ per il Contact Center di esempio....903
18.6.1.7 Come aggiungere una pianificazione Hotline per il Contact Center di esempio....908
18.6.1.8 Come aggiungere code d'attesa per il Contact Center di esempio....909
18.6.1.9 Come assegnare gli agenti alle code d'attesa del Contact Center di esempio....911
18.6.2 Procedura di configurazione....913
18.6.2.1 Come configurare i gruppi UCD per il Contact Center....913
18.6.2.2 Come configurare un utente come agente....914
18.6.2.3 Come registrare singoli annunci per il Contact Center....915
18.6.2.4 Come caricare singoli annunci per il Contact Center....915
18.6.2.5 Come aggiungere pianificazioni....916
18.6.2.6 Come modificare la pianificazione....919
18.6.2.7 Come eliminare le pianificazioni....921
18.6.2.8 Come salvare una regola (CCV) come file PDF....921
18.6.2.9 How to Download a Rule (CCV) as a Backup File....921
18.6.2.10 How to Upload a Downloaded Rule (CCV) in a Backup File Format....922
18.6.2.11 Come aggiungere una coda d'attesa....922
18.6.2.12 Come modificare la coda d'attesa....926
18.6.2.13 Come attivare o disattivare la coda di attesa....928
18.6.2.14 Come configurare un pilota per i fax in arrivo nella coda di attesa....929
18.6.2.15 Come definire i valori soglia per il livello di servizio....929
18.6.2.16 Come definire la priorità del chiamante VIP....930
18.6.2.17 Come modificare l'elenco chiamate VIP....930
18.6.2.18 Come impostare l'agente preferito....931
18.6.2.19 Come eliminare l'agente preferito....932
18.6.2.20 Come aggiungere una pausa Contact Center....932
18.6.2.21 Come modificare una pausa del Contact Center....933
18.6.2.22 Come eliminare una pausa del Contact Center....933
18.6.2.23 Come aggiungere il motivo per l'elaborazione per "Elaborazione semplice"....933
18.6.2.24 Come modificare il motivo per l'elaborazione per "Elaborazione semplice"....934
18.6.2.25 Come eliminare il motivo per l'elaborazione per "Elaborazione semplice"....934
18.6.2.26 Come aggiungere il motivo per l'elaborazione per "Elaborazione multipla"....934
18.6.2.27 Come modificare il motivo per l'elaborazione per "Elaborazione multipla"....935
18.6.2.28 Come eliminare il motivo per l'elaborazione per "Elaborazione multipla"....936
18.6.2.29 Come assegnare un agente alla coda di attesa....936
18.6.2.30 Come eliminare un agente dalla coda di attesa....937
18.7 Istruzioni per l'uso del Contact Center....938
18.7.1 Limitazioni sull'uso del Contact Center....938
18.8 Note per l'uso dei telefoni DECT....941
18.9 Rapporti....942
18.9.1 Modelli di rapporti predefiniti....943

19 Mobilità....944
19.1 Soluzioni di mobilità integrata....944
19.2 Mobilità in viaggio....944
19.2.1 myPortal to go....945
19.2.1.1 Requisiti richiesti permyPortal to go....947
19.2.2 Mobility Entry....948
19.2.3 Confronto tra client mobile e Mobility Entry....950

19.2.4 Dipendenze per Mobility Client e Mobility Entry..... 952
19.2.5 Servizio One Number.....953
19.2.6 Telefonia dual mode.....954
19.2.7 Konfiguration von myPortal to go und Mobility Entry 954
19.2.7.1 Come integrare un cellulare GSM.....955
19.2.7.2 Come integrare un telefono dual mode (GSM/WLAN) con i client HFA o SIP..... 957
19.2.7.3 Come attivare l'interfaccia Web per telefoni mobili e i client Web.....958
19.2.7.4 Come eliminare l'integrazione numero cellulare.....959
19.3 Mobilità in ufficio.....960
19.3.1 Condivisione desk..... 960
19.3.2 Soluzione cordless integrata.....961
19.3.2.1 Panoramica..... 962
19.3.2.2 Collegamento di moduli cordless.....963
19.3.2.3 Configurazione del sistema..... 964
19.3.2.4 Cordless/Telefoni DECT.....965
19.3.2.5 Importanza dei risultati ottenuti dai test della gamma delle frequenze radio.....966
19.3.3 Configurazione della soluzione cordless integrata..... 968
19.3.3.1 Come inserire l'identificativo del sistema DECT e configurare eventuali parametri cordless aggiuntivi (dati a livello di sistema).....968
19.3.3.2 Come configurare le stazioni base cordless..... 969
19.3.3.3 Come effettuare la prima configurazione dei telefoni DECT..... 969
19.3.3.4 Come accedere al cordless di un telefono DECT (portatile OpenStage/Gigaset)..... 970
19.3.3.5 Come aggiungere altri telefoni DECT.....972
19.3.3.6 Come eliminare i telefoni DECT.....972
19.3.3.7 Come configurare i parametri Multi-SLC.....973
19.3.3.8 Come richiedere i dati sulle stazioni base.....973
19.3.3.9 Come attivare il tono di avviso dell'indicazione messaggio in attesa (MWI) per i telefoni DECT..... 974
19.3.3.10 Come controllare lo stato di connessione dei telefoni DECT..... 974
19.3.4 Cordless IP.....975
19.3.5 Telefoni WLAN e access point.....975
19.3.5.1 Requisiti per WLAN..... 975
19.4 Mobilità a casa..... 976
19.4.1 Configurazione della VPN.....977
19.4.2 Configurazione del Dispositivo SIP@Home.....977
19.4.3 Configurazione del DispositivoSistema@Home.....979
19.4.4 Come attivare Dispositivo@Home..... 981
19.4.5 Come aggiornare il software per il dispositivo di sistema (HFA) @Home..... 982
19.4.6 Come specificare il server STUN per Dispositivo@Home.....984

20 Sicurezza..... 985
20.1 Firewall.....985
20.1.1 Port handling..... 985
20.1.1.1 Abilitazione della porta.....986
20.1.1.2 Come configurare dell'abilitazione della porta.....986
20.1.1.3 Gestione della porta.....987
20.1.1.4 Come modificare le impostazioni globali della gestione delle porte..... 987
20.1.2 NAT.....988
20.1.2.1 Come configurare una regola NAT.....988
20.1.2.2 Come configurare più regole NAT con l'Editor tabelle NAT.....989
20.1.2.3 Come cancellare una regola NAT..... 990
20.1.3 Firewall applicaz.....990
20.1.3.1 Come visualizzare la configurazione del Firewall applicazioni.....991
20.1.3.2 Come limitare i servizi tramite il Firewall applicazioni..... 992
20.1.3.3 Come eliminare la configurazione del Firewall applicazioni..... 992
20.1.4 Gestione dei servizi (OpenScape Business S).....992

20.1.4.1 Come aggiungere o bloccare servizi....993
20.2 Crittografia segnalazione e payload (SPE)....993
20.2.1 Come attivare o disattivare il supporto SPE....995
20.2.2 Come modificare le impostazioni di protezione SPE....995
20.2.3 Come importare il certificato SPE e la chiave privata (file PKCS#12)....996
20.2.4 Come importare il certificato CA SPE....996
20.2.5 Come attivare o disattivare l'abilitazione SPE per un utente....997
20.3 Virtual Private Network, VPN 997
20.3.1 Requisiti per VPN....998
20.3.2 Connessione di operatori remoti tramite VPN....1000
20.3.2.1 Come configurare la connessione di operatori remoti tramite VPN....1001
20.3.2.2 Come esportare i dati degli operatori remoti....1003
20.3.3 Collegamento in rete di sistemi di comunicazione tramite VPN....1003
20.3.3.1 Come configurare la connessione di rete tramite VPN....1004
20.3.3.2 Come esportare e importare i dati relativi alla topologia di una rete VPN....1006
20.3.4 VPN - Meccanismi di protezione....1007
20.3.5 VPN - Certificati....1009
20.3.5.1 VPN - Come generare certificati CA Lightweight....1010
20.3.5.2 VPN - Gestione certificati - Come visualizzare un certificato....1011
20.3.5.3 VPN - Come importare un certificato CA attendibile (X.509)....1012
20.3.5.4 VPN - Certificati Peer - Come richiedere un certificato (CSR)....1012
20.3.5.5 VPN - Certificati Peer - Come creare un certificato (PKCS#12)....1013
20.3.5.6 VPN - Come importare un certificato Peer (PKCS#12)....1013
20.3.6 VPN - Client....1014
20.3.6.1 Impostazioni del client NCP VPN....1015
20.3.6.2 Come configurare un client NCP VPN....1017
20.3.6.3 Come configurare un client Shrew Soft VPN....1018
20.3.6.4 Come configurare un client iOS o Android VPN....1018
20.3.6.5 Come configurare un client VPN Mac OS X....1019
20.3.7 VPN - Servizi....1020
20.3.7.1 VPN - Servizi attivi - Come mostrare tutti i servizi IPsec....1020
20.3.7.2 VPN - Servizi attivi - Come mostrare un servizio IPsec speciale....1020
20.3.7.3 VPN - Servizi configurati - Come mostrare tutti i servizi IPsec....1020
20.3.7.4 VPN - Servizi configurati - Come modificare un servizio IPsec....1021
20.3.7.5 VPN - Servizi configurati - Come rinominare un servizio IPsec....1021
20.3.7.6 VPN - Servizi configurati - Come cancellare un servizio IPsec....1022
20.3.8 VPN - Tunnel....1022
20.3.8.1 VPN - Tunnel attivi - Come mostrare i dati generici dei tunnel....1022
20.3.8.2 VPN - Tunnel attivi - Come visualizzare le regole di tutti i tunnel....1023
20.3.8.3 VPN - Tunnel configurati - Come mostrare i dati generici dei tunnel....1023
20.3.8.4 VPN - Tunnel configurati - Come visualizzare le regole di tutti i tunnel....1023
20.3.8.5 VPN - Come aggiungere un tunnel configurato....1024
20.3.9 VPN - Regole....1025
20.3.9.1 VPN - Regole attive - Come mostrare tutte le regole....1026
20.3.9.2 VPN - Regole attive - Come mostrare una regola speciale....1026
20.3.9.3 VPN - Regole configurate - Come mostrare tutte le regole....1026
20.3.9.4 VPN - Regole configurate - Come aggiungere una regola....1027
20.3.9.5 VPN - Come modificare una regola....1028
20.3.9.6 VPN - Come aggiungere una regola per direzione opposta....1028
20.3.9.7 VPN - Come cancellare una regola....1029
20.3.10 Server PKI....1029
20.3.10.1 VPN - Come mostrare il server PKI....1029
20.3.10.2 VPN - Come aggiungere un server PKI....1029
20.4 Gestione dei certificati....1030
20.4.1 Introduzione....1031
20.4.2 Come generare un certificato CA....1032

20.4.3 Come creare un certificato autofirmato..... 1033
20.4.4 Come generare una richiesta di firma di un certificato (CSR)..... 1033
20.4.5 Come importare un certificato server (PKCS#12)..... 1035
20.4.6 Come importare i certificati server (PEM)..... 1035
20.4.7 Come visualizzare i certificati..... 1036
20.4.8 Come cancellare un certificato..... 1036
20.4.9 Come esportare un certificato (X.509)..... 1037
20.4.10 Come importare un certificato prorogato (X.509)..... 1037
20.4.11 Come attivare un certificato..... 1037
20.4.12 Gestione dei certificati per Booster Server..... 1038
20.5 Sicurezza Web..... 1039
20.5.1 Collegamenti al server Web..... 1039
20.5.1.1 Come configurare la connessione al server Web (UC Suite)..... 1039
20.5.1.2 Come configurare le connessioni al server Web (UC Smart)..... 1039
20.5.2 Registro Admin..... 1040
20.5.2.1 Come caricare il registro Admin..... 1040
20.5.2.2 Come modificare la Lingua registro Admin..... 1040
20.6 Sicurezza SQL..... 1041
20.6.1 Nodo singolo..... 1041
20.6.2 Multinodo..... 1041
20.6.3 Come configurare password per il database SQL..... 1042
20.7 Protezione da attacchi SIP..... 1043

21 Connessione in rete di OpenScape Business..... 1045
21.1 Piano di rete..... 1046
21.1.1 Reti omogenee ed eterogenee 1046
21.1.1.1 Come visualizzare una panoramica di tutti i nodi OpenScape Business..... 1047
21.1.2 Gateway singolo e multiplo..... 1047
21.2 Servizi di rete..... 1048
21.2.1 Servizi a livello di rete delle soluzioni UC..... 1048
21.2.2 Servizi voce a livello di rete..... 1051
21.3 Concessione della licenza di un sistema di reti..... 1052
21.4 Requisiti per la connessione in rete..... 1053
21.4.1 Requisiti della rete LAN..... 1053
21.4.2 Piano di composizione per rete..... 1055
21.4.2.1 Composizione di numeri di rete pubblica in rete..... 1056
21.5 Ottimizzazione delle rotte (Path Replacement)..... 1056
21.5.1 Come attivare o disattivare l'ottimizzazione delle rotte (Path Replacement)..... 1057
21.6 Scenari di connessione in rete..... 1058
21.6.1 Dipendenze e limitazioni..... 1058
21.6.2 Utilizzo di più OpenScape Business X..... 1059
21.6.2.1 Come configurare l'installazione di base per il nodo 1 (master)..... 1063
21.6.2.2 Come configurare la rete per il nodo 1 (master)..... 1064
21.6.2.3 Come configurare l'installazione di base per il nodo 2 (slave)..... 1065
21.6.2.4 Come configurare la rete per il nodo 2 (slave)..... 1066
21.6.2.5 Come controllare le funzioni di rete per il master..... 1066
21.6.2.6 Come configurare i fasci e i relativi parametri (linea ISDN per master)..... 1067
21.6.2.7 Come configurare i fasci e i relativi parametri (fascio 16) (master)..... 1067
21.6.2.8 Come configurare l'LCR per il collegamento in rete (master)..... 1068
21.6.2.9 Come configurare il fascio e i relativi parametri (slave)..... 1069
21.6.2.10 Come configurare l'LCR per il collegamento in rete (slave)..... 1069
21.6.3 Collegamento in rete di OpenScape Business X con OpenScape Business S (gateway singolo)..... 1070
21.6.3.1 Come configurare l'installazione di base per il nodo 1 (master)..... 1076
21.6.3.2 Come configurare la rete per il nodo 1 (master)..... 1077
21.6.3.3 Come configurare l'installazione di base per il nodo 2 (slave)..... 1078
21.6.3.4 Come configurare la rete per il nodo 2 (slave)..... 1079

21.6.3.5 Come configurare l'installazione di base per il nodo 3 (slave)..... 1079
21.6.3.6 Come controllare le funzioni di rete per il master..... 1080
21.6.3.7 Configurare il collegamento in rete per il nodo 3 (slave)..... 1081
21.6.3.8 Come configurare l'LCR per il collegamento in rete (nodi 3, slave)..... 1081
21.6.3.9 Come configurare l'LCR per il collegamento in rete (nodo 2)..... 1083
21.6.3.10 Come configurare i fasci e i relativi parametri (nodo 1, master)..... 1084
21.6.3.11 Come configurare i fasci e i relativi parametri (fascio 16) (nodo 1)..... 1085
21.6.3.12 Come configurare l'LCR per il collegamento in rete (nodo 1)..... 1085
21.6.4 Collegamento in rete di Open Scape Business X e OpenScape Business S (gateway multiplo)..... 1087
21.6.4.1 Come configurare l'installazione di base per il nodo 4 (OpenScape Business S, master)..... 1095
21.6.4.2 Come configurare la rete per il nodo 4 (master)..... 1096
21.6.4.3 Come configurare l'installazione di base per il nodo 1 (slave)..... 1097
21.6.4.4 Come configurare la rete per il nodo 1 (slave)..... 1098
21.6.4.5 Come configurare l'installazione di base per il nodo 2 (slave)..... 1098
21.6.4.6 Come configurare la rete per il nodo 2 (slave)..... 1099
21.6.4.7 Come configurare l'installazione di base per il nodo 3 (slave)..... 1100
21.6.4.8 Come configurare la rete per il nodo 3 (slave)..... 1101
21.6.4.9 Come controllare le funzioni di rete per il master..... 1101
21.6.4.10 Come configurare il gateway multiplo per il nodo 4 (master)..... 1102
21.6.4.11 Come configurare il fascio e i relativi parametri (nodo 1, slave)..... 1103
21.6.4.12 Come configurare l'LCR per il collegamento in rete (nodi 1, slave)..... 1103
21.6.4.13 Come configurare il fascio e i relativi parametri (nodo 2, slave)..... 1105
21.6.4.14 Come configurare l'LCR per il collegamento in rete (nodi 2, slave)..... 1106
21.6.4.15 Come configurare il fascio e i relativi parametri (nodo 3, slave)..... 1108
21.6.4.16 Come configurare l'LCR per il collegamento in rete (nodi 3, slave)..... 1108
21.6.4.17 Come configurare il fascio e i relativi parametri (nodo 4, master)..... 1111
21.6.4.18 Come configurare l'LCR per il collegamento in rete (nodo 4, master)..... 1111
21.6.5 Collegamento in rete di OpenScape Business in un ambiente di hosting..... 1114
21.6.6 Connessione in rete di OpenScape Business X e OpenScape 4000..... 1117
21.6.7 Collegamento in rete di OpenScape Business X e OpenScape Voice..... 1124
21.6.8 Collegamento di porte esterne a OpenScape Business tramite interconnessione SIP..... 1127
21.6.9 Numerazione aperta in OpenScape Business X - collegamento in rete..... 1128
21.6.9.1 Come configurare la numerazione aperta..... 1129
21.6.10 Collegamento in rete tramite ISDN..... 1131
21.6.11 Sistema di reti OpenScape Business con attacco di linea urbana ITSP centralizzato..... 1132
21.7 Posto di rinvio centrale nel sistema di reti (non per USA)..... 1134
21.7.1 Come configurare il posto di rinvio centrale nel sistema di reti MultiGateway..... 1135
21.8 Gestore presenze..... 1136
21.9 Stato sincronizzazione nel sistema di reti..... 1137
21.9.1 Sincronizzazione manuale nel sistema di reti..... 1138
21.9.2 Come avviare manualmente la sincronizzazione..... 1138
21.10 Sopravvivenza..... 1138
21.10.1 Come configurare la funzione survivability..... 1141
21.11 Eliminazione di un nodo dal sistema di reti..... 1141

22 Interfacciamenti..... 1143
22.1 Risponditore analogico..... 1143
22.1.1 Come aggiungere risponditori analogici..... 1144
22.1.2 Come modificare il ritardo annuncio..... 1144
22.2 Apparecchio porta e apriporta..... 1145
22.2.1 DoorLine a/b T01-T04..... 1145
22.2.1.1 Come configurare la porta utente del Doorline a/b T01-T04..... 1146
22.2.1.2 Come configurare l'interno per Doorline a/b T01-T04..... 1147
22.2.2 DoorCom Analog..... 1147
22.2.2.1 Come configurare la porta utente di DoorCom Analog..... 1148
22.2.2.2 Come configurare l'interno per DoorCom Analog..... 1148

22.2.3 Citofono con amplificatore (TFE-S)....1148
22.2.3.1 Come configurare l'apparecchio porta....1150
22.2.4 Altoparlante....1150
22.2.4.1 Come configurare l'interfaccia utente analogica per un altoparlante....1151
22.2.4.2 Come configurare l'interfaccia utente analogica per collegare un amplificatore al modulo TFE S....1152
22.3 Relè....1152
22.3.1 Come configurare un relè....1154
22.4 Sensori....1154

23 Application Connectivity....1157
23.1 CSTA....1157
23.1.1 Come modificare il numero di porta per CSTA....1159
23.1.2 Come attivare o disattivare il CMD per l'uso di TAPI 120....1160
23.1.3 Come attivare o disattivare il server DSS per l'uso di tasti DSS a livello di rete....1161
23.1.4 Come attivare o disattivare il CSP....1161
23.1.5 Come attivare o disattivare Media Extension Bridge....1162
23.2 OpenScape Business TAPI 120/170....1162
23.2.1 OpenScape Business TAPI 120....1163
23.2.2 OpenScape Business TAPI 170....1167
23.3 Interfaccia Web Services....1172
23.4 Open Directory Service....1173
23.4.1 Come attivare o disattivare Open Directory Service....1177
23.4.2 Come riavviare Open Directory Service....1178
23.4.3 Come configurare la password per l'accesso a Open Directory Service....1178
23.4.4 Come configurare ODBC-ODBC Bridge Server....1179
23.4.5 Come aggiungere un'origine dati esterna per Open Directory Service....1181
23.4.6 Come visualizzare un'anteprima dei risultati della ricerca LDAP per Open Directory Service....1184
23.4.7 Come eliminare un'origine dati esterna da Open Directory Service....1184
23.5 Servizio di integrazione Active Directory....1185
23.5.1 Come configurare il servizio Active Directory....1186
23.6 Application Launcher....1187
23.6.1 Requisiti per l'uso di Application Launcher....1188
23.6.2 Profilo con i dati di configurazione dell'Application Launcher....1188
23.6.2.1 Come predisporre il profilo con i dati di configurazione dell'Application Launcher....1189
23.7 Panoramica di myPortal for Teams....1189
23.7.1 How to configure myPortal for Teams....1190
23.7.2 Come caricare myPortal for Teams nell'archivio di Teams....1190
23.8 Unify Phone....1191
23.8.1 Come configurare la connettività Unify Phone....1192
23.8.2 Come configurare l'istanza di un utente Unify Phone....1193
23.8.3 Come gestire gli utenti Unify Phone....1193
23.8.3.1 Come creare nuovi utenti Unify Phone....1193
23.8.3.2 Come aggiungere utenti Unify Phone esistenti....1194
23.8.3.3 Come modificare i dettagli dell'utente Unify Phone....1195
23.8.3.4 Come rimuovere o eliminare nuovi utenti Unify Phone....1196
23.8.3.5 Come preparare Numero alternativo e Routing delle chiamate per l'interoperabilità Unify Phone....1197
23.9 Servizio Let's Encrypt....1197
23.9.1 Come configurare il servizio Let's Encrypt....1197
23.10 CloudLink Service....1198
23.10.1 Come configurare il servizio CloudLink....1199
23.10.2 Come aprire l'interfaccia web CloudLink Daemon....1199
23.10.3 Come configurare l'interfaccia web CloudLink Daemon....1200
23.10.4 Come abilitare/configurare il connettore SIP per connettersi a Workflow Studio....1200
23.11 Numeri pilota CloudLink....1201

23.11.1 Come configurare i numeri pilota CloudLink....1201

24 Accounting....1203
24.1 Dati di connessione....1203
24.1.1 Registrazione dei dati di connessione....1203
24.1.1.1 Come attivare o disattivare la registrazione dei dati di connessione....1204
24.1.1.2 Come attivare o disattivare la registrazione della durata connessione....1204
24.1.1.3 Come configurare la registrazione degli importi in denaro o delle unità tariffarie (scatti)....1205
24.1.1.4 Come configurare il fattore tariffario, la valuta e la precisione del computer....1205
24.1.1.5 Come attivare o disattivare la registrazione delle ultime quattro cifre....1206
24.1.1.6 Come attivare o disattivare la funzione di messa a protocollo delle chiamate in uscita senza collegamento....1206
24.1.1.7 Come attivare o disattivare la registrazione delle connessioni in entrata....1207
24.1.1.8 Come attivare o disattivare il protocollo di connessione....1207
24.1.1.9 Come attivare o disattivare la registrazione del MSN....1208
24.1.1.10 Come attivare o disattivare la funzione Formato decimale....1208
24.1.2 Codici di addebito....1208
24.1.2.1 Come configurare un codice addebito....1210
24.1.2.2 Come configurare la procedura di controllo del codice di addebito....1210
24.1.2.3 Come attivare o disattivare la funzione Ripetizione ultimo numero con PKZ....1210
24.2 Visualizzazione e trasmissione dei dati di connessione....1211
24.2.1 Trasmissione degli addebiti (non per USA)....1211
24.2.1.1 Come configurare la trasmissione degli importi in denaro....1212
24.2.2 Visualizzazione dei costi di connessione sul telefono....1212
24.2.3 Visualizzazione della durata della connessione sul telefono....1212
24.2.3.1 Come attivare o disattivare la visualizzazione della durata connessione....1213
24.2.4 Trasmissione dei dati di connessione....1213
24.2.4.1 Come selezionare il formato....1221
24.2.4.2 Come attivare o disattivare la trasmissione dei dati delle connessioni tramite HTTPS....1221
24.3 Controllo dei costi....1221
24.3.1 Notifica dell'utilizzo delle rotte a tariffe più elevate....1222
24.3.1.1 Come configurare un avviso rotta a tariffa elevata....1222
24.3.2 Protezione da frodi tariffarie....1222
24.3.2.1 Come attivare o disattivare la protezione dall'abuso dell'utilizzo delle linee urbane....1223
24.4 Accounting Tools....1223
24.4.1 Accounting Manager....1223
24.4.2 TeleData Office....1224

25 Manutenzione....1225
25.1 Configurazione telefonia....1225
25.1.1 Data e Ora....1225
25.1.1.1 Come configurare manualmente data e ora....1226
25.1.1.2 Come impostare il fuso orario....1226
25.1.1.3 Come configurare il formato data....1227
25.1.2 SNTP....1227
25.1.2.1 Fare riferimento alla data e all'ora di un server SNTP....1227
25.1.3 Loghi del telefono....1228
25.1.3.1 Come caricare un logo del telefono nel sistema....1228
25.1.3.2 Come distribuire un logo per telefono ai telefoni di sistema....1229
25.1.3.3 Come eliminare il logo dei telefoni....1229
25.1.4 Display personalizzato....1229
25.1.4.1 Come modificare il display personalizzato (nome del sistema)....1230
25.1.5 Testo in più lingue....1230
25.1.6 Menu Flexible....1230
25.1.6.1 Come modificare Menu Flexible....1230
25.1.7 Musica su attesa....1231

25.1.7.1 Come importare musica su attesa....1232
25.1.7.2 Come configurare la funzione della musica su attesa interna....1233
25.1.7.3 Come modificare la musica su attesa interna per ogni gruppo con restrizioni di traffico....1233
25.1.8 Annunci....1234
25.1.8.1 Come configurare gli annunci (UC Suite & UC Booster)....1235
25.1.8.2 Come configurare gli annunci (UC Smart)....1236
25.1.9 Segnalazione da utente a utente....1237
25.1.10 Protezione da segnalazione su canale fonia....1237
25.1.11 Temporizzazioni....1237
25.1.12 Controllo dei servizi Centrex....1237
25.1.12.1 Come attivare o disattivare il comando dei servizi Centrex....1237
25.2 Capitolo 24.2 Backup e ripristino....1238
25.2.1 Set di backup....1239
25.2.1.1 Come visuallizare i set di backup....1239
25.2.1.2 Come cancellare un backup....1240
25.2.2 Supporti di backup....1240
25.2.2.1 Come aggiungere i supporti di backup....1241
25.2.2.2 Come modificare i supporti di backup....1242
25.2.2.3 Come cancellare i supporti di backup....1243
25.2.3 Salvataggio immediato....1243
25.2.3.1 Come eseguire il salvataggio immediato dei set di backup....1243
25.2.4 Salvataggio pianificato....1245
25.2.4.1 Come eseguire il salvataggio temporizzato di set di backup....1245
25.2.5 Ripristino....1245
25.2.5.1 Come ripristinare i set di backup....1246
25.3 Aggiornamenti....1246
25.3.1 Uso di un server Web locale....1248
25.3.1.1 Come configurare l'accesso al server Web locale....1248
25.3.2 Aggiornamento del sistema di comunicazione....1249
25.3.2.1 Come aggiornare il sistema tramite un server Web....1251
25.3.2.2 Come aggiornare il sistema tramite un supporto USB....1252
25.3.2.3 Come aggiornare il sistema tramite il caricamento di un file....1253
25.3.2.4 Come aggiornare il sistema tramite un supporto USB senza accesso al WBM....1255
25.3.3 Aggiornamento dei telefoni del sistema....1255
25.3.3.1 Come caricare il software dei telefoni nel sistema....1256
25.3.3.2 Come distribuire il software per telefoni ai telefoni di sistema....1257
25.3.3.3 Come eliminare il software per telefoni....1257
25.3.3.4 Come attivare o disattivare la distribuzione automatica del software dei telefoni....1258
25.3.3.5 Come configurare il reflashing automatico....1258
25.3.4 Stato del software....1259
25.3.4.1 Come interrogare lo stato del software....1260
25.4 Riavvia, Ricarica, Arresta....1260
25.4.1 Riavvio di OpenScape Business....1261
25.4.1.1 Come eseguire il riavvio di OpenScape Business....1261
25.4.2 Ricarica di OpenScape Business....1262
25.4.2.1 Come attivare la ricarica di OpenScape Business....1262
25.4.3 Arresto di OpenScape Business X....1263
25.4.3.1 Come arrestare OpenScape Business X....1263
25.4.4 PIN per l'arresto controllato di OpenScape Business X....1264
25.4.4.1 Come configurare un PIN per l'arresto controllato di OpenScape Business X....1264
25.4.5 Riavvio della UC Booster Card (scheda applicazioni OCAB)....1264
25.4.5.1 Come attivare il riavvio della UC Booster Card (scheda applicazioni OCAB)....1265
25.4.6 Ricarica della UC Booster Card (scheda applicazioni OCAB)....1265
25.4.6.1 Come attivare la ricarica della UC Booster Card (scheda applicazioni OCAB)....1266
25.4.7 Riavvio dell'applicazione UC....1266
25.4.7.1 Come eseguire il riavvio dell'applicazione UC....1266

25.5 Gestione inventario....1267
25.5.1 Stato del sistema 1267
25.5.1.1 Come richiedere lo stato utente....1268
25.5.1.2 Come richiedere lo stato della connessione....1268
25.5.1.3 Come richiedere lo stato ITSP....1269
25.5.1.4 Come visualizzare gli indirizzi IP....1269
25.5.2 Inventario....1270
25.5.2.1 Come controllare l'inventario di OpenScape Business X....1271
25.5.2.2 Come controllare l'inventario di OpenScape Business S....1273
25.6 Azioni automatiche....1273
25.6.1 Azione automatica Garbage Collection....1273
25.6.1.1 Come modificare l'azione automatica Garbage Collection....1274
25.6.1.2 Come avviare (attivare) l'azione automatica Garbage Collection....1275
25.6.1.3 Come arrestare (disattivare) l'azione automatica Garbage Collection....1275
25.6.2 Azione automatica Notifica DLS....1275
25.6.2.1 Come modificare l'azione automatica notifica DLS....1276
25.6.2.2 Come avviare (attivare) la notifica DLS automatica delle azioni....1276
25.6.2.3 Come arrestare (disattivare) la notifica DLS automatica delle azioni....1277
25.6.3 Meccanismo di avviso per la scadenza delle schede SDHC....1277
25.6.3.1 Come impostare una notifica in caso di errori nella scheda SDHC....1279
25.6.3.2 Come avviare l'azione automatica Meccanismo di avviso per la scadenza SDHC....1279
25.6.3.3 Come clonare e cambiare una scheda SDHC....1280
25.6.3.4 Come creare un file di backup dei dati SDHC....1281
25.6.3.5 Come sostituire una scheda SDHC....1283
25.7 Risparmio energia....1285
25.7.1 Come attivare o disattivare la funzione Risparmio energia....1285
25.7.2 Modifica della modalità di collegamento Ethernet dell'interfaccia LAN....1286
25.8 Monitoraggio e manutenzione di OpenScape Business....1287
25.8.1 Test della connessione di rete per OpenScape Business X....1287
25.8.1.1 Come inviare ping....1287
25.8.1.2 Come un test del traceroute....1288
25.8.2 SNMP (Simple Network Management Protocol)....1288
25.8.2.1 Come visualizzare tutte le comunità....1299
25.8.2.2 Come aggiungere una comunità....1300
25.8.2.3 Come modificare una comunità....1300
25.8.2.4 Come cancellare una comunità....1301
25.8.2.5 Come visualizzare i Trap....1301
25.8.2.6 Come visualizzare i dettagli di un Trap....1302
25.8.3 Azioni manuali....1302
25.8.3.1 Come effettuare il download dei dati diagnostica/Registri diagnostica....1304
25.8.4 Tracce....1305
25.8.4.1 Come caricare il file di registro eventi traccia sistema....1311
25.8.4.2 Come cancellare il file di registro traccia sistema....1312
25.8.4.3 Come configurare impostazioni di traccia ai valori predefiniti....1312
25.8.4.4 Come visualizzare tutti i profili di traccia....1313
25.8.4.5 Come avviare o arrestare il profilo di traccia....1314
25.8.4.6 Come visualizzare o modificare la configurazione del formato della traccia....1314
25.8.4.7 Come visualizzare o modificare le interfacce di output traccia....1315
25.8.4.8 Come visualizzare o modificare il registro visualizzatore eventi / registro traccia cliente....1315
25.8.4.9 Come eseguire il download o aprire il registro visualizzatore eventi / registro traccia cliente....1316
25.8.4.10 Come eliminare il registro visualizzatore eventi / registro traccia cliente....1316
25.8.4.11 Come mostrare componenti di traccia M5T....1316
25.8.4.12 Come avviare o arrestare un componente di traccia M5T....1317
25.8.4.13 Come modificare componenti di traccia M5T....1317
25.8.4.14 Come avviare o arrestare Secure Trace....1318
25.8.4.15 Come controllare lo stato di Secure Trace....1318

25.8.4.16 Come modificare la password per Secure Trace..... 1318
25.8.4.17 Come importare il certificato per Secure Trace da un file X.509.....1319
25.8.4.18 Come modificare o visualizzare la configurazione di traccia dello stack H.323.....1319
25.8.4.19 Come modificare i moduli H.323..... 1320
25.8.4.20 Come caricare/aprire il registro di traccia dello stack H.323..... 1320
25.8.4.21 Come cancellare il registro di traccia dello stack H.323.....1320
25.8.4.22 Come modificare la traccia componenti licenza..... 1321
25.8.4.23 Come visualizzare i dettagli di un profilo di traccia..... 1321
25.8.4.24 Come arrestare tutti i profili di traccia..... 1322
25.8.4.25 Come aggiungere un Profilo di traccia..... 1322
25.8.4.26 Come mostrare la componente di traccia..... 1322
25.8.4.27 Come visualizzare i dettagli dei componenti di traccia.....1323
25.8.4.28 Come avviare o arrestare un componente di traccia..... 1323
25.8.4.29 Come arrestare tutti i componenti di traccia.....1324
25.8.4.30 Come configurare impostazioni di traccia ai valori predefiniti..... 1324
25.8.4.31 Come modificare componenti di traccia..... 1324
25.8.4.32 Come inoltrare automaticamente i file del registro di sistema.....1325
25.8.4.33 How to Start the Kernel Crash Data Service.....1325
25.8.4.34 How to Stop the Kernel Crash Data Service.....1326
25.8.4.35 Come avviare Traccia server multimediale..... 1326
25.8.4.36 Come arrestare Traccia server multimediale.....1327
25.9 Trasferimento TCP..... 1327
25.9.1 Come avviare il trasferimento TCP.....1327
25.9.2 Come arrestare il trasferimento TCP.....1328
25.9.3 Come cancellare il trasferimento TCP.....1328
25.10 Daemon RPCAP.....1328
25.10.1 Come attivare il daemon RPCAP..... 1329
25.10.2 Come disattivare il daemon RPCAP.....1329
25.11 Eventi..... 1329
25.11.1 Come modificare la registrazione eventi tramite LAN.....1331
25.11.2 Come caricare il file di registro eventi..... 1332
25.11.3 Come cancellare il file di registro eventi.....1332
25.11.4 Come modificare le impostazioni e-mail per gli eventi..... 1332
25.11.5 Come visualizzare la tabella delle reazioni agli eventi..... 1333
25.11.6 Come modificare le impostazioni di reazione agli eventi.....1333
25.11.7 Come modificare le impostazioni di reazione a più eventi.....1334
25.11.8 Come caricare/aprire registri di diagnostica.....1335
25.11.9 Come cancellare i registri diagnosi.....1335
25.11.10 Come definire le destinazioni per la segnalazione degli allarmi..... 1336
25.12 Dati di configurazione per funzioni diagnostiche.....1336
25.12.1 Come creare i dati di configurazione per le funzioni diagnostiche..... 1337
25.13 Card Manager.....1338
25.13.1 Come utilizzare Card Manager per scrivere il software di comunicazione sull'M.2 SATA SSD.....1339
25.13.2 Come utilizzare Card Manager per scrivere il software di comunicazione sulla scheda SDHC.....1341
25.13.3 Come utilizzare Card Manager per scrivere il software di comunicazione sull'hard disk OCAB..... 1343
25.14 Monitoraggio e manutenzione della UC Suite..... 1345
25.14.1 Logging.....1345
25.14.1.1 Come attivare o disattivare la registrazione del registro di sistema..... 1347
25.14.1.2 Come attivare o disattivare la registrazione di registri client a livello di sistema..... 1347
25.14.1.3 Come attivare o disattivare la registrazione di registri client per i singoli utenti.....1347
25.14.1.4 Come configurare il percorso dell'archivio per i file di registro del client.....1348
25.14.1.5 Come attivare o disattivare il salvataggio centralizzato dei registri client su disco rigido.....1349
25.14.1.6 Come scaricare i registri client di tutti gli utenti interni.....1349
25.14.2 Avviso..... 1350
25.14.2.1 Come configurare le notifiche e-mail degli errori di sistema..... 1352
25.14.3 Manutenzione..... 1353

25.14.3.1 Come configurare l'ora del giorno per la manutenzione....1354
25.14.3.2 Come configurare i tempi di conservazione dei file di registro....1354
25.14.3.3 Come eseguire la manutenzione immediata del sistema....1355
25.14.3.4 Come configurare i tempi di conservazione dei dati Contact Center....1355
25.15 Monitoraggio di UC Smart....1355
25.15.1 Come controllare lo stato corrente di UC Smart....1355
25.16 Servizi di assistenza remoti....1356
25.16.1 RSP.servicelink....1356
25.16.1.1 Come installare, configurare e registrare il plugin RSP.servicelink....1359
25.16.1.2 Come attivare il plugin RSP.servicelink....1361
25.16.1.3 Come disattivare i plugin RSP.servicelink....1361
25.16.1.4 Come reimpostare il plugin servizio RSP....1361
25.16.1.5 Come configurare un PIN per l'attivazione e la disattivazione del plugin RSP.servicelink....1362
25.16.2 Accesso remoto....1362
25.16.2.1 Come attivare l'accesso remoto tramite ISDN....1363
25.16.2.2 Come configurare un PC con Microsoft Windows Vista per l'accesso remoto tramite ISDN....1364
25.16.2.3 Come configurare un PC con Microsoft Windows 7 per l'accesso remoto tramite ISDN....1365
25.16.2.4 Come accedere in remoto tramite Internet con indirizzo IP fisso....1366
25.16.2.5 Come accedere in remoto tramite Internet senza indirizzo IP fisso....1367
25.16.2.6 Come disattivare l'accesso remoto....1368
25.16.3 Utente online....1368
25.16.3.1 Come avviare Utente online....1369

26 Migrazione....1370
26.1 Upgrade software dei sistemi OpenScape Business X....1371
26.1.1 Upgrade del software da OpenScape Business X V2 a OpenScape Business X V3....1372
26.1.1.1 Upgrade software di sistemi con licenza permanente con CLS Connect....1373
26.1.1.2 Upgrade software di sistemi con licenza permanente senza CLS Connect....1373
26.1.1.3 Upgrade software dei sistemi con licenza PayGo....1373
26.2 Upgrade software da un UC Booster Server a OpenScape Business X V3....1374
26.2.1 Come eseguire l'aggiornamento di UC Business Booster Server da V2 a V3....1374
26.3 Migrazione hardware/software dei sistemi OpenScape Business X a V3....1376
26.3.1 Migrazione da OpenScape Business X V2 a OpenScape Business X V3....1377
26.3.1.1 Migrazione ai sistemi su licenza permanente V3 con CLS Connect....1378
26.3.1.2 Migrazione ai sistemi su licenza permanente V3 senza CLS Connect....1379
26.3.1.3 Migrazione ai sistemi su licenza PayGo V3....1380
26.4 Migrazione di un sistema OpenScape Business X V3 da una scheda madre V2 a una scheda madre V3....1381
26.4.1 Migrazione ai sistemi su licenza permanente con scheda madre V3 con CLS Connect....1382
26.4.2 Migrazione ai sistemi su licenza permanente con scheda madre V3 senza CLS Connect....1383
26.4.3 Migrazione ai sistemi su licenza PayGo con scheda madre V3....1384
26.5 Upgrade del software di OpenScape Business S....1385
26.5.1 Upgrade del software da OpenScape Business S V2 a OpenScape Business S V3....1386
26.5.1.1 Upgrade a V3 ai sistemi su licenza permanente con CLS Connect....1387
26.5.1.2 Upgrade a V3 ai sistemi su licenza PayGo....1387
26.5.2 Upgrade del software da OpenScape Business S V2 a OpenScape Business S V3....1388
26.6 Migrazione/upgrade della rete OpenScape Business V2 a V3....1389
26.6.1 Scenario 1: Migrazione hardware di un nodo master, upgrade software dei nodi slave....1390
26.6.1.1 Migrazione/Upgrade con CLS Connect nel nodo master....1390
26.6.1.2 Migrazione/Upgrade senza CLS Connect nel nodo master....1391
26.6.2 Scenario 2: Upgrade software di tutti i sistemi nella rete a V3....1392
26.6.2.1 Upgrade software con CLS Connect nel nodo master....1392
26.6.2.2 Upgrade software senza CLS Connect nel nodo master....1393
26.6.3 Scenario 3a: Upgrade software di tutti i nodi....1394
26.6.4 Scenario 3b: Upgrade software nel nodo master, migrazione hardware dei nodi slave....1394
26.6.4.1 Migrazione/Upgrade con CLS Connect nel nodo master....1394

26.6.4.2 Migrazione/Upgrade senza CLS Connect nel nodo master..... 1395
26.7 Migrazione da HiPath 3000 a OpenScape Business V3..... 1396
26.7.1 Migrazione da HiPath 33xx, 35xx, 3800 a OpenScape Business X3/X5/X8 V3..... 1397
26.7.1.1 Come caricare il CDB da HiPath 3000..... 1402
26.7.1.2 Come visualizzare le impostazioni dell'HG1500..... 1402
26.7.1.3 Come convertire il CDB di HiPath 3000..... 1403
26.7.1.4 Come sostituire l'hardware con il sistema HiPath 3300/3500..... 1403
26.7.1.5 Come sostituire l'hardware con il sistema HiPath 3350/3550..... 1404
26.7.1.6 Come sostituire l'hardware con il sistema HiPath 3800..... 1406
26.7.1.7 Come eseguire l'installazione iniziale..... 1407
26.7.1.8 Come caricare il CDB convertito nel nuovo sistema..... 1407
26.7.1.9 Come generare un nuovo file di licenza..... 1408
26.7.1.10 Come attivare il file di licenza offline..... 1409
26.7.1.11 Come assegnare le licenze..... 1410
26.7.1.12 Come resettare le voci LCR..... 1410
26.7.2 Migrazione di un sistema HiPath 3000 con OpenScape Office V3 HX a OpenScape Business V3 con scheda madre V3..... 1410
26.7.3 Migrazione di un sistema HiPath 3000 con OpenScape Office V3 HX a OpenScape Business V3 con UC Booster Server..... 1412
26.7.3.1 Come convertire un set di backup OpenScape Office V3 HX..... 1414
26.7.4 Migrazione di una rete HiPath 3000 verso una rete OpenScape Business..... 1414
26.7.5 Migrazione di un sistema di reti HiPath 3000 V9 con HiPath 5000 RSM..... 1417
26.7.6 Caratteristiche modificate/abbandonate di HiPath 3000 e Interfacce..... 1420
26.8 Migrazione tra sistemi OpenScape Business V3..... 1426
26.9 Migrazione dei moduli HW..... 1428
26.9.1 Sostituzione di SLMO24N con SLMU..... 1428
26.9.2 Sostituzione di SLM8N con SLMU..... 1428
26.9.3 Sostituzione di SLCN con SLMUC (SLMU + CMAe)..... 1429
26.10 Migrazione da OpenScape Business X1 V2 a OpenScape Business X1W V3..... 1429
26.10.1 Migrazione ai sistemi su licenza permanente X1W V3 con CLS Connect..... 1431
26.10.2 Migrazione ai sistemi su licenza permanente X1W V3 senza CLS Connect..... 1431

27 Limiti di configurazione e capacità..... 1433
27.1 Valori massimi per utente..... 1433
27.2 Valori massimi per le linee..... 1436
27.3 Valori massimi delle risorse..... 1438
27.3.1 Dettagli sull'uso dei canali DSP..... 1439
27.3.2 Dettagli sull'uso dei canali proxy RTP..... 1441
27.4 Valori massimi per funzione..... 1441
27.4.1 Connessione al provider di servizi..... 1441
27.4.2 Utenti..... 1442
27.4.3 Livelli di espansione di UC Smart..... 1442
27.4.4 Livelli di espansione di Smart Voicemail..... 1445
27.4.5 Livelli di espansione di UC Suite..... 1447
27.4.6 Funzioni del telefono..... 1456
27.4.7 Lavoro in team (Gruppi)..... 1458
27.4.8 Routing delle chiamate..... 1463
27.4.9 Contact Center multimediale..... 1464
27.4.10 Limiti di espansioni Mobility..... 1465
27.4.11 Sicurezza..... 1466
27.4.12 Connessione in rete di OpenScape Business..... 1467
27.4.13 Application Connectivity..... 1468
27.4.14 Accounting..... 1470

28 Modalità esperti..... 1471
28.1 Convenzioni di visualizzazione per le descrizioni dei parametri..... 1471

28.2 **Manutenzione** ... 1472
28.2.1 **Configurazione** ... 1472
28.2.1.1 **Configurazione > Musica su attesa > Carica nel gateway** ... 1472
28.2.1.2 **Configurazione > Annunci > Caricamento sul gateway** ... 1473
28.2.1.3 **Configurazione > Configurazione porta** ... 1473
28.2.1.4 **Configurazione > SmartVM** ... 1474
28.2.1.5 **Configurazione > SmartVM > Operazioni con casella postale** ... 1474
28.2.1.6 **Configurazione > SmartVM > Operazioni su file** ... 1475
28.2.1.7 **Configurazione > Branding** ... 1477
28.2.1.8 **Configurazione > Indirizzo IP del gateway** ... 1477
28.2.2 **Immagine del software** ... 1477
28.2.2.1 **Immagine del software > Software di sistema > Aggiornamento via Internet** ... 1478
28.2.2.2 **Immagine del software > Software di sistema > Aggiornamento tramite Carica file** ... 1479
28.2.2.3 **Immagine del software > Software di sistema > Aggiornamento via supporto USB** ... 1479
28.2.2.4 **Immagine del software > Immagini telefono > Carica** ... 1480
28.2.2.5 **Immagine del software > Immagini telefono > Distribuire** ... 1480
28.2.2.6 **Immagine del software > Immagini telefono > Distribuzione per terminale** ... 1481
28.2.2.7 **Immagine del software > Loghi immagine telefono > Carica** ... 1481
28.2.2.8 **Immagine del software > Loghi immagine telefono > Distribuire** ... 1482
28.2.3 **Cordless** ... 1482
28.2.3.1 **Cordless > Base Stations** ... 1482
28.2.4 **Stato porta/modulo** ... 1484
28.2.4.1 **Stato porta/modulo > Stato modulo** ... 1485
28.2.4.2 **Stato porta/modulo > Fuori servizio** ... 1485
28.2.5 **Tracce** ... 1486
28.2.5.1 **Tracce > Configurazione formato traccia** ... 1486
28.2.5.2 **Tracce > Interfacce di output traccia** ... 1487
28.2.5.3 **TracceRegistro traccia** ... 1488
28.2.5.4 **Tracce > Loopback digitale** ... 1488
28.2.5.5 **Tracce > Registro traccia cliente** ... 1489
28.2.5.6 **Tracce > Componenti di traccia M5T** ... 1489
28.2.5.7 **TracceSecure Trace** ... 1490
28.2.5.8 **Tracce > Secure Trace > Certificato Secure Trace** ... 1490
28.2.5.9 **Tracce > Secure Trace > Impostazioni di Secure Trace** ... 1490
28.2.5.10 **TracceTraccia dello stack H.323** ... 1491
28.2.5.11 **Tracce > Ascolto chiamate** ... 1492
28.2.5.12 **Tracce > Componente licenza** ... 1494
28.2.5.13 **Tracce > Profili di traccia** ... 1495
28.2.5.14 **Tracce > Componenti di traccia** ... 1495
28.2.5.15 **Tracce > Trasferimento TCP** ... 1496
28.2.5.16 **Tracce > rpcap Daemon** ... 1497
28.2.5.17 **Traces > Kernel Crash Data** ... 1497
28.2.5.18 **Tracce > Traccia server multimediale** ... 1498
28.2.6 **Eventi** ... 1498
28.2.6.1 **Eventi > Configurazione eventi** ... 1499
28.2.6.2 **Eventi > Registro eventi** ... 1499
28.2.6.3 **Eventi > E-mail** ... 1499
28.2.6.4 **Eventi > Tabella delle reazioni** ... 1500
28.2.6.5 **Eventi > Registri di diagnostica** ... 1501
28.2.6.6 **EventiSegnalazione allarmi** ... 1501
28.2.7 **Riavvia / Ricarica** ... 1501
28.2.7.1 **Riavvia / RicaricaRiavvia / Ricarica** ... 1502
28.2.8 **SNMP** ... 1503
28.2.8.1 **SNMP > Comunità** ... 1503
28.2.8.2 **SNMP > Comunità > Comunità di lettura** ... 1504
28.2.8.3 **SNMP > Comunità > Comunità di scrittura** ... 1504

28.2.8.4 **SNMP** > **Comunità** > **Comunità trap** 1504
28.2.8.5 **SNMP** > **Trap** 1504
28.2.9 **Registro Admin**....1505
28.2.9.1 **Protocollo Admin** > **Configurazione** 1505
28.2.9.2 **Protocollo Admin** > **Dati del registro Admin** 1505
28.2.10 **Azioni**....1506
28.2.10.1 **Azioni** > **Azioni manuali** > **Registri di diagnostica** 1506
28.2.10.2 **Azioni** > **Azioni manuali** > **Manutenzione DLI**.... 1507
28.2.10.3 **Azioni** > **Azioni automatiche** > **Garbage Collection** 1508
28.2.10.4 **Azioni** > **Azioni automatiche** > **Notifica DLS** 1508
28.2.10.5 **Azioni > Azioni automatiche > Controllo di salute SDHC**....1509
28.2.11 **Diagnostica piattaforma**....1509
28.2.12 **Diagnostica applicazione**.... 1509
28.2.12.1 **Diagnostica applicazione** > **Impostazioni sviluppatore** > **Output console traccia** 1509
28.2.12.2 **Diagnostica applicazione** > **Impostazioni sviluppatore** > **Accetta accesso in scrittura** 1510
28.2.12.3 **Diagnostica applicazione** > **Scheda madre** 1510
28.2.12.4 Diagnostica applicazione > Impostazioni sviluppatore > Profili Provider SIP.... 1510
28.2.13 **Diagnosi IP**....1510
28.2.13.1 **Diagnosi IP** > **Scheda madre** > **Protocollo ARP** 1510
28.2.13.2 **Diagnosi IP** > **Scheda madre** > **Richiesta ICMP** > **Ping** 1511
28.2.13.3 **Diagnosi IP** > **Scheda madre** > **Richiesta ICMP** > **Traceroute** 1511
28.2.14 **Utente online**....1511
28.2.14.1 **Utente online** 1511
28.3 **Telefonia**....1512
28.3.1 **Impostazioni di base**....1512
28.3.1.1 **Impostazioni di base** > **Sistema** > **Flag di sistema**....1512
28.3.1.2 **Impostazioni di base** > **Sistema** > **Temporizzazioni** 1520
28.3.1.3 **Impostazioni di base** > **Sistema** > **Display**....1526
28.3.1.4 **Impostazioni di base** > **Sistema** > **DISA** 1529
28.3.1.5 **Impostazioni di base** > **Sistema** > **Rinvio/PO/Hotline**....1530
28.3.1.6 **Impostazioni di base** > **Sistema** > **LDAP**....1533
28.3.1.7 **Impostazione di base** > **Sistema** > **Testi** 1535
28.3.1.8 **Impostazioni di base** > **Sistema** > **Menu Flexible** 1535
28.3.1.9 **Impostazioni di base** > **Sistema** > **Destinazioni di selezione breve**....1535
28.3.1.10 **Impostazioni di base** > **Sistema** > **Codici di servizio**.... 1537
28.3.1.11 **Impostazioni di base** > **Sistema > Password di registrazione HFA**....1537
28.3.1.12 **Impostazioni di base** > **Gateway** 1538
28.3.1.13 **Impostazioni di base** > **DynDNS** > **Servizio DynDNS** 1540
28.3.1.14 **Impostazioni di base** > **DynDNS** > **Ora di aggiornamento del nome di DNS** 1541
28.3.1.15 **Basic Settings** > **Quality of Service** 1541
28.3.1.16 **Impostazioni di base** > **Data e Ora** > **Data e Ora** 1542
28.3.1.17 **Impostazioni di base** > **Data e Ora** > **Impostazioni delle zone orarie** 1543
28.3.1.18 **Impostazioni di base** > **Data e Ora** > **Impostazioni di SNTP** 1543
28.3.1.19 **Impostazioni di base** > **Gestione della porta** 1543
28.3.1.20 **Impostazioni di base** > **Addebiti** > **Addebiti chiamata - Formato di output** 1545
28.3.1.21 **Impostazioni di base** > **Addebiti** > **Addebiti - Coefficienti** 1546
28.3.1.22 **Impostazioni di base** > **Addebiti chiamata** > **Addebiti chiamata - Codici di addebito** 1547
28.3.1.23 **Impostazioni di base** > **Annuncio Player per messaggi vocali/Annunci** 1548
28.3.1.24 **Impostazioni di base** > **Implementazione parametri telefoni**....1548
28.3.1.25 **Impostazioni di base** > **Risparmio energia** 1551
28.3.1.26 Installazione di base> Dati di massa....1552
28.3.2 **Sicurezza**.... 1553
28.3.2.1 **Sicurezza** > **Firewall delle applicazioni**....1553
28.3.2.2 **Sicurezza** > **Client di distribuzione e licenze (DLSC)** 1555
28.3.2.3 **Sicurezza** > **Client di distribuzione e licenze (DLSC)** > **Certificato del client DLSC** 1555

28.3.2.4 **Sicurezza** > **Client di distribuzione e licenze (DLSC)** > **Certificato CA del client DLSC** 1557
28.3.2.5 **Sicurezza** > **Crittografia segnalazione e payload (SPE)** 1558
28.3.2.6 **Sicurezza** > **Crittografia payload segnalazione e payload** > **Certificato SPE** 1559
28.3.2.7 **Sicurezza** > **Crittografia segnalazione/Crittografia Payload** > **Certificati SPE CA** 1559
28.3.2.8 **Sicurezza** > **VPN** 1559
28.3.2.9 **Sicurezza** > **VPN** > **CA Lightweight** 1560
28.3.2.10 **Sicurezza** > **VPN** > **Gestione certificati** 1561
28.3.2.11 **Sicurezza** > **VPN** > **Gestione certificati** > **Certificati CA attendibili** > **Certificati attivi** 1561
28.3.2.12 **Sicurezza** > **VPN** > **Gestione certificati** > **Certificati CA attendibili** > **Certificati configurati** 1563
28.3.2.13 **Sicurezza** > **VPN** > **Certificati Peer** 1563
28.3.2.14 **Sicurezza** > **VPN** > **Servizi** > **Servizi attivi** 1564
28.3.2.15 **Sicurezza** > **VPN** > **Servizi** > **Servizi configurati** 1565
28.3.2.16 **Sicurezza** > **VPN** > **Tunnel** > **Tunnel attivi** 1566
28.3.2.17 **Sicurezza** > **VPN** > **Tunnel** > **Tunnel configurati** 1568
28.3.2.18 **Sicurezza** > **VPN** > **Regole** > **Regole attive** 1572
28.3.2.19 **Sicurezza** > **VPN** > **Regole** > **Regole configurate** 1574
28.3.2.20 **Sicurezza** > **VPN** > **Public Key Infrastructure (PKI)** 1575
28.3.2.21 **Sicurezza** > **SSL** > **Creazione certificati** 1576
28.3.2.22 **Sicurezza** > **SSL** > **Gestione certificati** 1577
28.3.2.23 **Sicurezza** > **SSL** > **Gestione certificati** > **Certificati server** 1577
28.3.2.24 **Sicurezza** > **Sicurezza Web** 1578
28.3.2.25 **Sicurezza** > **Sicurezza SQL** 1579
28.3.3 **Interfacce di rete** 1579
28.3.3.1 **Interfacce di rete** > **Scheda madre** > **Nome host** 1579
28.3.3.2 **Interfacce di rete** > **Scheda madre** > **LAN 1 (WAN)** 1580
28.3.3.3 **Interfacce di rete** > **Scheda madre** > **LAN 2** 1584
28.3.3.4 **Interfacce di rete** > **Scheda madre** > **LAN 3 (Admin)** 1586
28.3.3.5 **Interfacce di rete** > **Scheda madre** > **Server FTP** 1586
28.3.3.6 **Interfacce di rete** > **Scheda madre** > **Modo DHCP** 1587
28.3.3.7 **Interfacce di rete** > **Scheda madre** > **Modalità DHCP** > **Server DHCP** > **Parametri globali** 1587
28.3.3.8 **Interfacce di rete** > **Scheda madre** > **Modalità DHCP** > **Server DHCP** > **Pool di indirizzi IP** 1589
28.3.3.9 **Interfacce di rete** > **Scheda madre** > **Modalità DHCP** > **Server DHCP** > **Indirizzi IP statici** 1590
28.3.3.10 **Interfacce di rete** > **Scheda madre** > **Modalità DHCP** > **Server DHCP** > **Ultimi lease attivi** 1592
28.3.3.11 **Interfacce di rete** > **Scheda madre** > **Modo DHCP** > **Server DHCP** > **Tutti i lease** 1592
28.3.3.12 **Interfacce di rete** > **Scheda applicazioni** > **Nome host** 1593
28.3.3.13 **Interfaccia di rete** > **Scheda applicazioni** > **LAN 1** 1593
28.3.3.14 **Interfaccia di rete** > **Scheda applicazioni** > **LAN 2** 1594
28.3.4 **Routing** 1595
28.3.4.1 **Routing** > **Routing IP** > **Scheda madre** > **Route statiche** 1595
28.3.4.2 **Routing** > **Routing IP** > **Scheda madre** > **Router predefinito** 1596
28.3.4.3 **Routing** > **Routing IP** > **Scheda madre** > **Server DNS** 1596
28.3.4.4 **Routing** > **Routing IP** > **Scheda applicazioni** > **Rotte statiche** 1596
28.3.4.5 **Routing** > **Routing IP** > **Scheda applicazioni** > **Router predefinito** 1597
28.3.4.6 **Routing** > **NAT** 1597
28.3.4.7 **Routing** > **PSTN** 1598
28.3.4.8 **Routing** > **PSTN** > **Protocollo PPP** 1599
28.3.4.9 **Routing** > **PSTN** > **Partner PSTN** 1599
28.3.5 **LCR** 1603
28.3.5.1 **LCR** > **Flag LCR** 1603
28.3.5.2 **LCR** > **Classi di servizio** 1604
28.3.5.3 **LCR** > **Piano di composizione** 1604

28.3.5.4 **LCR** > **Tabella delle rotte** ... 1605
28.3.5.5 **LCR** > **Regola di composizione** ... 1606
28.3.5.6 **LCR** > **Multisito** ... 1608
28.3.6 **Gateway voce** ... 1609
28.3.6.1 **Gateway voceParametri SIP** ... 1609
28.3.6.2 Gateway voce > Impostazioni ID Loc ITSP ... 1610
28.3.6.3 **Gateway voce** > **Parametri Codec** ... 1612
28.3.6.4 **Gateway voce** > **Parametri codec di destinazione** ... 1614
28.3.6.5 **Gateway voce** > **Provider di servizi di telefonia Internet** ... 1615
28.3.6.6 **Gateway voce** > **Servizi di rete** > **Nodi** ... 1626
28.3.6.7 **Gateway voce** > **Servizi di rete** > **Routing** ... 1627
28.3.6.8 **Gateway voce** > **Interconnessione SIPQ** ... 1627
28.3.6.9 **Gateway Voce** > **Linea server SIP nativo** ... 1629
28.3.7 **Utenti** ... 1634
28.3.7.1 **Utente** > **Utente** > **Utenti UP0** ... 1634
28.3.7.2 **Stazione** > **Stazione** > **Client IP** ... 1637
28.3.7.3 **Utente** > **Utente** > **Utenti analogici** ... 1640
28.3.7.4 **Utente** > **Utente** > **Utenti ISDN** ... 1641
28.3.7.5 **Utente** > **Utente** > **Utenti DECT** > **SLC Num. telefono** ... 1642
28.3.7.6 **Utente** > **Utente** > **Utenti DECT** > **Utenti DECT** ... 1643
28.3.7.7 **Utente** > **Utente** > **Porte IVM/EVM** > **EVM** ... 1645
28.3.7.8 **Utente** > **Utente** > **Utenti virtuali** ... 1646
28.3.7.9 **Utente** > **Utente** > **Parametri utente** ... 1647
28.3.7.10 **Utente** > **Utente** > **Applicazioni UC** ... 1657
28.3.7.11 **Utente** > **Utente** > **Profili/Modelli** ... 1659
28.3.7.12 **Utente** > **Utente** > **Estensioni selezione passante** ... 1660
28.3.7.13 **Utente** > **Utente** > **Mobility Entry** ... 1661
28.3.7.14 **Utente** > **Utente** > **Utente SfB** ... 1662
28.3.7.15 **Utenti** > **Utenti** > **Panoramica utenti** ... 1663
28.3.7.16 **Utenti** > **Programmazione dei tasti** ... 1664
28.3.8 **Cordless** ... 1665
28.3.8.1 **Cordless** > **Per tutto il sistema** ... 1665
28.3.8.2 **Cordless** > **SLC** ... 1667
28.3.8.3 **Cordless** > **Multi-SLC** ... 1668
28.3.8.4 **Cordless** > **Utenti base** ... 1668
28.3.9 **Chiamate in entrata** ... 1669
28.3.9.1 **Chiamata in entrata** > **Gruppi/Gruppi di ricerca** ... 1669
28.3.9.2 **Chiamate in entrata** > **Membri del gruppo** ... 1673
28.3.9.3 **Chiamate in entrata** > **Team/top** ... 1675
28.3.9.4 **Chiamate in entrata** > **Risposta per assente** ... 1678
28.3.9.5 **Chiamate in entrata** > **UCD** ... 1678
28.3.9.6 **Chiamate in entrata** > **Inoltri** ... 1681
28.3.10 **Linee/Rete** ... 1683
28.3.10.1 **Linee/Rete** > **Linee** ... 1684
28.3.10.2 **Trunk/Instradamento** > **Gruppo di trunk** ... 1687
28.3.10.3 **Linee/Rete** > **Servizi QSIG** ... 1695
28.3.10.4 **Linee/Rete** > **Assegna MSN** ... 1696
28.3.10.5 **Linee/collegamenti in rete** > **Parametri ISDN** ... 1696
28.3.11 **Autorizzazioni** ... 1697
28.3.11.1 **Classi di autorizzazione** > **Utenti** ... 1697
28.3.11.2 **Classi di autorizzazione** > **Giorno: Gruppi di abilitazione** ... 1698
28.3.11.3 **Classi di autorizzazione** > **Notte: Gruppi di abilitazione** ... 1698
28.3.11.4 **Classi di autorizzazione** > **Liste nr. permessi** ... 1699
28.3.11.5 **Autorizzazioni** > **Liste nr. vietati** ... 1700
28.3.11.6 **Classi di servizio** > **Lista nera** ... 1700
28.3.11.7 **Classi di autorizzazione** > **Servizio notturno** ... 1701

28.3.11.8 **Classi di autorizzazione > Assegnazione gruppi VBZ** 1701
28.3.11.9 **Classi di autorizzazione > Matrice VBZ** 1702
28.3.11.10 **Classi di autorizzazione > Servizio notte auto**....1703
28.3.11.11 **Classi di autorizzazione > Giorni speciali**....1704
28.3.12 **Interfacciamenti**....1704
28.3.12.1 **Apparecchiature ausiliarie > Musica su attesa**....1704
28.3.12.2 **Apparecchiature ausiliarie > Segreteria telefonica**....1705
28.3.12.3 **Apparecchiature ausiliarie > Annunci**....1705
28.3.12.4 **Apparecchiature ausiliarie > Apriporta**....1707
28.3.12.5 **Interfacciamenti > SmartVM**....1708
28.3.13 **Payload**....1712
28.3.13.1 **Payload > Periferiche** 1712
28.3.13.2 **Payload > Media Stream Control (MSC)** 1712
28.3.13.3 **Payload > Moduli HW** 1713
28.3.14 **Statistiche**....1716
28.3.14.1 **Statistiche > Statistiche gateway > Scheda madre > Statistiche periferiche** 1716
28.3.14.2 **Statistiche > Statistiche gateway > Scheda madre > Statistiche MSC** 1716
28.3.14.3 **Statistiche > Statistiche SNMP** 1717
28.3.14.4 **Statistiche > Statistiche di telefonia > Testi di sistema** 1717
28.3.14.5 **Statistiche > Statistiche di telefonia > Agenti UCD** 1717
28.3.14.6 **Statistiche > Statistiche di telefonia > Stato linea**....1718
28.3.14.7 **Statistiche > Statistiche di telefonia > Inoltro** 1718
28.3.14.8 **Statistiche > Statistiche di telefonia > Utenti** 1719
28.4 **Applicazioni**....1721
28.4.1 **Selezione applicazione**....1721
28.4.1.1 **Selezione applicazione** 1721
28.4.2 **Servizio di integrazione Active Directory**....1721
28.4.2.1 **Servizio di integrazione Active Directory**....1721
28.4.3 **UC Smart**....1722
28.4.3.1 **UC Smart > Impostazioni di base** 1722
28.4.3.2 **UC Smart > Gestione utenti**....1723
28.4.3.3 **UC Smart > Stato**....1724
28.4.4 **OpenScape Business, UC Suite**....1725
28.4.4.1 **OpenScape Business, UC Suite** 1725
28.4.4.2 **OpenScape Business UC Suite > Rubrica utente**....1725
28.4.4.3 **OpenScape Business UC Suite > Reparti**....1728
28.4.4.4 **OpenScape Business UC Suite > Gruppi**....1728
28.4.4.5 **OpenScape Business UC Suite > Modelli**....1730
28.4.4.6 **OpenScape Business UC Suite > External Directory**....1730
28.4.4.7 **OpenScape Business UC Suite > Config provider esterni**....1731
28.4.4.8 **OpenScape Business UC Suite > Contact Center**....1733
28.4.4.9 **OpenScape Business UC Suite > Pianificazione**....1741
28.4.4.10 **OpenScape Business UC Suite > Carica file**....1743
28.4.4.11 **OpenScape Business UC Suite > Conferenza in corso**....1744
28.4.4.12 **OpenScape Business UC Suite > Elenco sedi** 1744
28.4.4.13 **OpenScape Business UC Suite > Server**....1745
28.4.4.14 **OpenScape Business, UC Suite > Profili**....1751
28.4.4.15 **OpenScape Business UC Suite > Intestazione fax**....1753
28.4.5 **Web Services**....1754
28.4.5.1 **Servizi Web > Web Collaboration** 1754
28.4.6 **Open Directory Service**....1755
28.4.6.1 **Open Directory Service > Impostazioni di base** 1755
28.4.6.2 **Open Directory Service > Origini dati > Utenti OpenScape Business**....1755
28.4.6.3 **Servizio Open Directory > Origini dati > LXV3** 1756
28.4.6.4 **Servizio Open Directory > Origini dati > LXV3** 1756
28.4.6.5 **Open Directory Service > Manutenzione**....1756

28.4.7 **Application Launcher**....1756
28.4.7.1 **Application Launcher** 1757
28.5 **Middleware**.... 1757
28.5.1 Lettore di annunci.... 1757
28.5.2 Csta Message Dispatcher (CMD) 1757
28.5.3 Provider di servizi CSTA (CSP) 1758
28.5.4 Server DSS 1759
28.5.5 Media Extension Bridge (MEB) 1759

29 Appendice....1760
29.1 Standard supportati.... 1760
29.2 Servizi Euro ISDN.... 1762
29.3 Porte usate.... 1764
29.4 Progettazione dei canali DSP per i sistemi di comunicazione OpenScape Business X3/X5/X8.... 1766

30 Glossario.... 1777
30.1 Glossario.... 1777

Indice analitico....1792

1 Cronologia delle modifiche

Le modifiche menzionate in questo capitolo sono cumulative.

Modifiche in V3R4 FR3

Capitoli modificati	Descrizione delle modifiche	N. problema	Data
Trunk/InstradamentoGruppo di trunk alla pagina 1687	Correzione per COLP (argomenti ITSP)	62	Ott 2025
Procedure guidate - Servizi cloud alla pagina 127 CloudLink Service alla pagina 1198 Come configurare il servizio CloudLink alla pagina 1199 Come configurare l'interfaccia web CloudLink Daemon alla pagina 1200 Come abilitare/configurare il connettore SIP per connettersi a Workflow Studio alla pagina 1200 (nuovo) Numeri pilota CloudLink alla pagina 1201 (nuovo) Come configurare i numeri pilota CloudLink alla pagina 1201 (nuovo)	Supporto contenitore, abilitazione connettore SIP e numeri pilota CL	62	Set 2025
Inventario alla pagina 1270	Riprogettazione hardware OCCe	62	Set 2025

Modifiche in V3R4 FR2

Capitoli modificati	Descrizione delle modifiche	N. problema	Data
Migrazione da OpenScape Business X V2 a OpenScape Business X V3 alla pagina 1377	Aggiunta nota relativa all'indirizzo IP DSP non predefinito durante la migrazione.	61	10 set 2025
Apparecchiature ausiliarie Annunci alla pagina 1705	Aggiunto collegamento a Configurazione > Annunci > Caricamento sul gateway nel parametro file WAVE.	60	Set 2025
Mobilità a casa alla pagina 976	Aggiunta nota relativa alle limitazioni con più dispositivi SIP/HFA e NAT.	56	Luglio 2025
Open Directory Service alla pagina 1173	Aggiunta nota relativa all'integrazione del database ODS in Microsoft Excel.	56	Luglio 2025
Chiamata in entrataGruppi/Gruppi di ricerca alla pagina 1669	Aggiunta nota relativa alla dipendenza con l'inoltro delle chiamate (*1) a un altro gruppo di ricerca, gruppo di attesa di chiamata e gruppo RNA.	56	Luglio 2025

Capitoli modificati	Descrizione delle modifiche	N. problema	Data
Requisiti richiesti per client PC della UC Suite alla pagina 534	Aggiornamenti per sistemi operativi, applicazioni Office/Outlook, software aggiuntivo (ad es. Java / OpenJDK).	56	Luglio 2025
Procedure guidate - Telefoni/ Abbonati alla pagina 123 Struttura della documentazione per l'amministratore alla pagina 70 Utenti alla pagina 419 Stazioni Mitel SIP DECT alla pagina 435 nuovo Come configurare le stazioni Mitel SIP DECT tramite provisioning alla pagina 459 nuovo UtenteUtenteParametri utente alla pagina 1647 Come configurare le stazioni SIP in modalità Esperto alla pagina 461 nuovo	Aggiornamenti per il provisioning di MITEL SIP-DECT	55	Maggio-giugno 2025
Interfacciamenti alla pagina 1704 Apparecchiature ausiliarie Annunci alla pagina 1705 Apparecchiature ausiliarie Segreteria telefonica alla pagina 1705 Come configurare gli annunci (UC Suite & UC Booster) alla pagina 1235 Come configurare gli annunci (UC Smart) alla pagina 1236	Aggiornamenti per la configurazione degli annunci	55	Maggio-giugno 2025
Gateway voceProvider di servizi di telefonia Internet alla pagina 1615	Aggiornamenti per i profili ITSP	55	Maggio-giugno 2025

Modifiche in V3R4 FR1

Capitoli modificati	Descrizione delle modifiche
Configurazione team / gruppo Team alla pagina 701 MULAP di base alla pagina 720	Rielaborazione del paragrafo "Ordinamento dei dispositivi membri Mulap" per LAN/WAN con UP.
Installazione del software di comunicazione alla pagina 223	Aggiunta una nota riguardante la configurazione di DHCP da yast o WBM.
Gestione utenti WBM alla pagina 117	Aggiunta una nota per la registrazione del ruolo di amministratore.

Capitoli modificati	Descrizione delle modifiche
Stazioni SIP alla pagina 432 Chiamata di gruppo alla pagina 680 Gruppo di ricerca alla pagina 684	Aggiornamenti sull'elenco dei codici di servizio compatibili con i dispositivi SIP.
Accesso a Internet alla pagina 166 Come configurare l'accesso a Internet tramite un router Internet esterno sulla LAN con porta WAN dedicata all'ITSP alla pagina 177 Come configurare l'accesso a Internet tramite un router Internet esterno sulla LAN con porta WAN dedicata all'ITSP alla pagina 240 Gateway voceProvider di servizi di telefonia Internet alla pagina 1615	Aggiornamenti relativi a LAN/WAN e ITSP su WAN.
Come abilitare e configurare il server DHCP interno alla pagina 147 Come abilitare il DHCP solo per i dispositivi Mitel/Unify alla pagina 148 Come abilitare e configurare il server DHCP della piattaforma hardware alla pagina 350 Interfacce di reteScheda madre Modalità DHCPServer DHCP Parametri globali alla pagina 1587 Interfacce di reteScheda madre Modalità DHCPServer DHCP Pool di indirizzi IP alla pagina 1589 Interfacce di reteScheda madre Modalità DHCPServer DHCP Indirizzi IP statici alla pagina 1590	Aggiornamenti per la gestione della sottorete DHCP per i dispositivi Mitel/Unify e per l'opzione relè.

Modifiche in V3R4

Capitoli modificati	Descrizione delle modifiche
MULAP di base alla pagina 720	I telefoni SIP sono stati rimossi da uno dei membri MULAP di base.
Dettagli sull'uso dei canali DSP alla pagina 1439	Aggiornamenti in materia di sicurezza e ITSP.
Open Directory Service Origini dati Utenti OpenScape Business alla pagina 1755	Aggiornamenti relativi a ODS Light.
Gateway VoceLinea server SIP nativo alla pagina 1629	Crittografia diretta dei media e del carico utile per Unify Phone.
Unify Phone alla pagina 1191	Aggiunto myAgent ai client UC per il controllo delle chiamate di terze parti.

Capitoli modificati	Descrizione delle modifiche
Modelli software UC (soft switch) alla pagina 107 Hardware UC Booster alla pagina 107 Come installare il software di comunicazione alla pagina 225 Requisiti richiesti per la configurazione iniziale alla pagina 218 Configurazione iniziale di OpenScape Business S alla pagina 218 Requisiti richiesti per la configurazione iniziale alla pagina 273 Configurazione iniziale di OpenScape Business UC Booster alla pagina 271 Configurazione iniziale di OpenScape Business UC Booster alla pagina 271 Come eseguire l'aggiornamento di UC Business Booster Server da V2 a V3 alla pagina 1374	Supporto di SLES 15 per OpenScape Business S e UC Booster Server.

Modifiche all'aggiornamento di V3R3 FR2 GA

Capitoli modificati	Descrizione delle modifiche
Condivisione desk alla pagina 960	Correzione della nota relativa alla funzione di condivisione della scrivania.
Porte usate alla pagina 265	Consolidamento e correzione delle porte utilizzate per i controlli CAR Alive.
Open Directory Service Origini dati Utenti OpenScape Business alla pagina 1755	Correzione dei valori minimi e massimi per le lunghezze massime interne e minime esterne e per il pulsante Nascondi chiamate aperte nel diario.
Immagine del softwareSoftware di sistemaAggiornamento via Internet alla pagina 1478	Aggiunto il pulsante mancante Pulisci memoria prima del trasferimento.
Unify Phone alla pagina 1191 Come aggiungere utenti Unify Phone esistenti alla pagina 1194	Aggiunte informazioni su Unify Phone e le applicazioni di terze parti.
OpenScape Business UC SuiteRubrica utente alla pagina 1725 OpenScape Business UC SuiteServer alla pagina 1745	Aggiunte due note relative alle diverse lunghezze delle password utente e alla reimpostazione di tutte le password utente.

Capitoli modificati	Descrizione delle modifiche
CloudLink Service alla pagina 1198 Come configurare il servizio CloudLink alla pagina 1199 Come aprire l'interfaccia web CloudLink Daemon alla pagina 1199 Come configurare l'interfaccia web CloudLink Daemon alla pagina 1200	Aggiunti nuovi capitoli per il servizio CloudLink.

Modifiche in V3R3 FR2

Capitoli modificati	Descrizione delle modifiche
Capitolo 24.2 Backup e ripristino alla pagina 1238	Aggiunta una nota relativa alla limitazione della sincronizzazione con Unify Phone Cloud.
-	Modificate le schermate dell'interfaccia utente in tutto il documento.
Servizio Let's Encrypt alla pagina 1197	Rimossa la versione BETA e aggiunta una nuova funzionalità per il servizio Let's Encrypt.
Telefoni supportati alla pagina 108 Caratteristiche alla pagina 508 Come caricare un logo del telefono nel sistema alla pagina 1228	Aggiornamenti per i nuovi dispositivi CP205T/CP405T (TDM) supportati.

Modifiche in V3R3 FR1

Capitoli modificati	Descrizione delle modifiche
Unify Phone alla pagina 1191 Come configurare la connettività Unify Phone alla pagina 1192 Come creare nuovi utenti Unify Phone alla pagina 1193 Come aggiungere utenti Unify Phone esistenti alla pagina 1194 Come modificare i dettagli dell'utente Unify Phone alla pagina 1195	Aggiornamenti per l'accesso alla directory e al diario, per la schermata dello schema di numerazione e per il campo del codice di accesso al trunk.
Procedure guidate - Servizi cloud alla pagina 127 Servizio Let's Encrypt alla pagina 1197	Aggiunti la procedura guidata "Servizi cloud" e il servizio "Lets encrypt".
Open Directory Service alla pagina 1173	Aggiunta la sezione "Open Directory Service e schede madri di OpenScape Business".

Capitoli modificati	Descrizione delle modifiche
Come gestire gli utenti Unify Phone alla pagina 1193 Come creare nuovi utenti Unify Phone alla pagina 1193 Come aggiungere utenti Unify Phone esistenti alla pagina 1194 Come modificare i dettagli dell'utente Unify Phone alla pagina 1195	Aggiunta la sezione "Come creare nuovi utenti di Unify Phone" e aggiornati gli altri capitoli di conseguenza.
Come personalizzare un'interfaccia utente moderna alternativa per myPortal for Desktop Impostazioni skin di OpenScape Business UC Suite Procedure guidate – UC Suite (solo con UC Suite) alla pagina 126	Rimossi i file e le menzioni per "Impostazioni skin".
Come importare un file CSV dal file system locale nella rubrica esterna alla pagina 562 Come aggiungere un'origine dati esterna per Open Directory Service alla pagina 1181	Aggiornamenti relativi al campo "customer_id" per l'importazione e l'esportazione dei dati.
UC SmartImpostazioni di baseUC SmartImpostazioni di base alla pagina 1722	Aggiunte informazioni su CloudService e altri campi mancanti.
Come configurare il servizio notte pianificato alla pagina 764	Aggiunte informazioni sul messaggio relativo alla modalità notturna nella pagina di destinazione del portale di amministrazione.
Requisiti richiesti permyPortal to go alla pagina 947	Aggiunto il supporto per le connessioni dati 4G/5G e la raccomandazione di un piano dati a tariffa fissa.
Chiamata in entrataGruppi/Gruppi di ricerca alla pagina 1669	Aggiunte informazioni sulle conversioni dei tipi di gruppo.
Come rimuovere o eliminare nuovi utenti Unify Phone alla pagina 1196	Modificata la funzione di eliminazione o rimozione per gli utenti di Unify Phone.
Come aggiungere pianificazioni alla pagina 916 Come modificare la pianificazione alla pagina 919	Aggiunta una nota per spiegare il collegamento uno-a-molti delle code alle pianificazioni.
Lavoro in team (Gruppi) alla pagina 678	Rimosso il capitolo "17.1.3 Xpressions Compact" e le relative voci dal documento. Aggiornati i gruppi di ricerca riservati.
Limitazione del numero di chiamate simultanee tramite ITSP alla pagina 820	Aggiunte voci per le chiamate Unify Phone e my Portal for Teams.
Classi di autorizzazioneUtenti alla pagina 1697 Come modificare il gruppo di abilitazione per la porta della casella vocale alla pagina 525	Aggiunte note sull'impostazione della lingua dei gruppi di abilitazione e dei testi delle porte EVM.

Capitoli modificati	Descrizione delle modifiche
Come aggiungere una pianificazione XYZ per il Contact Center di esempio alla pagina 903 Come aggiungere una pianificazione Hotline per il Contact Center di esempio alla pagina 908 Modelli alla pagina 839 Pianificazioni alla pagina 830	Rebranding e sostituzione dell'immagine per il Contact Center. Reintrodotta l'immagine commentata per il capitolo Pianificazioni.
Pianificazioni alla pagina 881	Rimosso UCD (incluso Contact Center) e aggiunta una riga relativa all'oggetto CVV Trasferisci in coda.

Modifiche in V3R3 X1R

Capitoli modificati	Descrizione delle modifiche
Accounting alla pagina 1470 Application Connectivity alla pagina 1468 Routing delle chiamate alla pagina 1463 Connessione al provider di servizi alla pagina 1441 Valori massimi per utente alla pagina 1433 Struttura e condizioni ambientali alla pagina 107 Modelli hardware UC alla pagina 106 Utenti DECT alla pagina 435 Funzioni del telefono alla pagina 1456 Valori massimi per le linee alla pagina 1436 Valori massimi delle risorse alla pagina 1438 Limiti di espansioni Mobility alla pagina 1465 Contact Center multimediale alla pagina 1464 Connessione in rete di OpenScape Business alla pagina 1467 Sicurezza alla pagina 1466 Livelli di espansione di Smart Voicemail alla pagina 1445 Utenti alla pagina 1442 Livelli di espansione di UC Smart alla pagina 1442 Lavoro in team (Gruppi) alla pagina 1458	Aggiornamenti per X1R

Modifiche in V3R3

Capitoli modificati	Descrizione delle modifiche
Migrazione alla pagina 1370	Aggiunta nota relativa all'eliminazione degli utenti Unify Phone.

Capitoli modificati	Descrizione delle modifiche
Aggiornamenti alla pagina 1246 Concessione della licenza alla pagina 291 Connessione in rete di OpenScape Business alla pagina 1045	Aggiunte informazioni su rete/licenze durante l'aggiornamento dei sistemi.
Reflashing alla pagina 216 Reflashing alla pagina 269	Aggiunti due nuovi capitoli sulla funzione di reflashing.
Procedura per la concessione della licenza alla pagina 292 Porte usate alla pagina 265 Come attivare CLS Connect alla pagina 307	Rimosso il riferimento alla porta obsoleta 7780
Tracce alla pagina 1305 Tracce alla pagina 1486	Eliminata la sezione relativa a RtpProxy Trace, poiché questa traccia non è più disponibile in WBM
Tracce Traccia server multimediale alla pagina 1498 Come avviare Traccia server multimediale alla pagina 1326 Come arrestare Traccia server multimediale alla pagina 1327	Nuovi capitoli per Media Server
OpenScape Business UC SuiteRubrica utente alla pagina 1725 OpenScape Business UC SuiteServer alla pagina 1745	Aggiornamenti sul formato di data e ora
Come rimuovere o eliminare nuovi utenti Unify Phone alla pagina 1196	Aggiornamenti sulla sostituzione della scheda SDHC
Panoramica di myPortal for Teams alla pagina 1189	myPortal for Teams: supporto per il controllo delle chiamate
Impostazioni di baseImplementazione parametri telefoni alla pagina 1548	Aggiornamenti per le impostazioni di composizione canoniche
Migrazione alla pagina 1370	Aggiunte due note sulle buone pratiche di migrazione e sui punti di errore.
Come concedere licenze agli utenti (indipendente) alla pagina 312 Licenze orientate all'utente alla pagina 297	Aggiunte due note relative all'assegnazione delle licenze della casella vocale.
Immagine del softwareSoftware di sistemaAggiornamento tramite Carica file alla pagina 1479 Come aggiornare il sistema tramite il caricamento di un file alla pagina 1253	Aggiunte informazioni sul nuovo flag per l'aggiornamento tramite caricamento di file.

Capitoli modificati	Descrizione delle modifiche
Elaborazione alla pagina 891 Come aggiungere il motivo per l'elaborazione per "Elaborazione multipla" alla pagina 934	Aggiunte informazioni relative ai gruppi e alle elaborazioni multiple.
Come attivare una porta LAN aggiunta come interfaccia WAN alla pagina 229 Come selezionare il prefisso nazionale e la lingua per i registri di traccia alla pagina 229 Come impostare il logo sul display e il nome del prodotto alla pagina 228	Sostituita la schermata dell'interfaccia utente in modo che venga visualizzato il brand, con l'impatto nei capitoli collegati.
Come configurare la connettività Unify Phone alla pagina 1192 Procedure guidate - Servizi cloud alla pagina 127 Come configurare l'accesso a Internet tramite un ISP standard PPPoE alla pagina 373 Limitazione del numero di chiamate simultanee tramite ITSP alla pagina 820 Licenze di sistema alla pagina 299 Valori massimi per utente alla pagina 1433 Come configurare un ITSP predefinito alla pagina 180 Come configurare l'accesso a Internet tramite ISP preimpostato alla pagina 171 UtenteUtenteParametri utente alla pagina 1647	Rimossi i capitoli e i riferimenti al prodotto Circuit.

Modifiche in V3R2 FR1

Capitoli modificati	Descrizione delle modifiche
Come configurare la registrazione di conferenze alla pagina 589 Come attivare e disattivare la registrazione di chiamate alla pagina 581	Nuova casella di controllo per abilitare o disabilitare la registrazione delle conferenze
Traces Kernel Crash Data alla pagina 1497 How to Start the Kernel Crash Data Service alla pagina 1325 How to Stop the Kernel Crash Data Service alla pagina 1326	Nuovo servizio dati Kernel Crash
Suggerimenti per combinazioni di licenze alla pagina 303	Aggiunte informazioni sulle licenze attive necessarie per utilizzare le funzioni Contact Center e Company AutoAttendant
UtenteUtenteParametri utente alla pagina 1647	Il campo **Numero di telefono stazione esterna attendibile** è obbligatorio

Capitoli modificati	Descrizione delle modifiche
OpenScape Business UC SuiteServer alla pagina 1745	Nuova opzione per eliminare dopo un determinato periodo di tempo i messaggi di richiamata, le chiamate registrate dal vivo, le chiamate fax e le e-mail associate alle chiamate
How to Download a Rule (CCV) as a Backup File alla pagina 921 How to Upload a Downloaded Rule (CCV) in a Backup File Format alla pagina 922	Nuovi capitoli per il download e il caricamento di una regola (CCV)
UC Suite alla pagina 530 Contact Center multimediale alla pagina 865 Manutenzione alla pagina 1225 Modalità esperti alla pagina 1471	Aggiornamento dell'interfaccia utente in tutti i capitoli interessati
Come configurare l'invio di e-mail alla pagina 202 OpenScape Business UC SuiteConfig provider esterni alla pagina 1731 OpenScape Business UC Suite Contact Center alla pagina 1733 Come aggiungere code d'attesa per il Contact Center di esempio alla pagina 909 Come aggiungere una coda d'attesa alla pagina 922 Come modificare la coda d'attesa alla pagina 926 Come connettere il sistema OpenScape Business a Microsoft Office 365 tramite l'autenticazione base alla pagina 617 How to connect OpenScape Business system to Microsoft Office 365 using Modern Authentication alla pagina 623	Supporto per l'autenticazione OAuth 2.0
myReports alla pagina 869	Gli amministratori di myReports non possono più configurare l'account e-mail da utilizzare per l'invio dei report via e-mail
Panoramica di myPortal for Teams alla pagina 1189	myPortal for Teams: supporto per tastierino e preferiti
Requisiti richiesti permyPortal to go alla pagina 947	Aggiornati i prerequisiti per il client iOS di myPortal to go
Gestione utenti alla pagina 857	In myAttendant, il numero predefinito di pulsanti utente è stato aumentato e può essere cambiato
Utenti della alla pagina 541 OpenScape Business UC SuiteRubrica utente alla pagina 1725	Elenco aggiornato dei formati di file supportati per il caricamento di un'immagine

Capitoli modificati	Descrizione delle modifiche
Accesso dell'utente alle funzioni UC (client UC) alla pagina 98 Telefoni supportati alla pagina 108 Servizio di distribuzione (DLI e DLS) alla pagina 359 Client UC Smart alla pagina 485 Requisiti richiesti per myPortal @work alla pagina 487 Come configurare le rubriche dei telefoni del sistema alla pagina 505 Caratteristiche alla pagina 508 Requisiti richiesti per client PC della UC Suite alla pagina 534 Configurazione team / gruppo Team alla pagina 701 OpenScape Business Attendant alla pagina 841 myAttendant alla pagina 855 Requisiti richiesti per l'uso di myAgent alla pagina 867 Come caricare un logo del telefono nel sistema alla pagina 1228 Come configurare il reflashing automatico alla pagina 1258 Upgrade software dei sistemi OpenScape Business X alla pagina 1371 Come eseguire l'aggiornamento di UC Business Booster Server da V2 a V3 alla pagina 1374 Migrazione hardware/software dei sistemi OpenScape Business X a V3 alla pagina 1376 Upgrade del software di OpenScape Business S alla pagina 1385 Livelli di espansione di UC Smart alla pagina 1442 Livelli di espansione di UC Suite alla pagina 1447 Application Connectivity alla pagina 1468	Nuovi telefoni supportati: • OpenScape Desk Phone CP 210 • OpenScape Desk Phone CP 710
Telefoni supportati alla pagina 108	Nuovi moduli chiave supportati: • OpenScape Key Module 410 • OpenScape Key Module 710
Impostazioni di baseSistema LDAP alla pagina 1533	Aggiunta nota sulla visualizzazione delle origini LDAP.
DISA alla pagina 667	Aggiunta nota sulla composizione di numeri DISA in OSBiz S e OSBiz X.
OpenScape Business UC SuiteServer alla pagina 1745	Rimossa la voce della tabella DB.

Capitoli modificati	Descrizione delle modifiche
Open Directory Service alla pagina 1173	Modificate le origini dati esterne e aggiunte informazioni sul campo "Descrizione".
Come migrare dalla scheda madre V2 alla scheda madre V3 (sistema indipendente) alla pagina 339	Aggiunto testo relativo a problemi con la funzionalità UC Fax.
Migrazione da OpenScape Business X1 V2 a OpenScape Business X1W V3 alla pagina 1429	Aggiunti i capitoli relativi alla migrazione da X1 V2 a X1W V3.
Passaggio da CLS connect alla pagina 308	Introdotto il capitolo Passaggio da CLS Connect.
Come migrare dalla scheda madre V2 alla scheda madre V3 (sistema indipendente) alla pagina 339	Migrazione di OCCLA standalone
Accesso remoto alla pagina 1362 Panoramica di funzioni e codici alla pagina 673 Schema indirizzi IP alla pagina 137 Come attivare l'accesso remoto tramite ISDN alla pagina 1363 Come configurare un PC con Microsoft Windows Vista per l'accesso remoto tramite ISDN alla pagina 1364 Come configurare un PC con Microsoft Windows 7 per l'accesso remoto tramite ISDN alla pagina 1365	Modificati i metodi di accesso remoto obsoleti e rimossi gli ultimi tre capitoli.
Migrazione da OpenScape Business X1 V2 a OpenScape Business X1W V3 alla pagina 1429	Aggiunti i capitoli relativi alla migrazione da X1 V2 a X1W V3.
Gateway VoceLinea server SIP nativo alla pagina 1629	Aggiunte voci di tabella per la sicurezza del trasporto e dei media.
OpenScape Business UC SuiteServer alla pagina 1745	Aggiunto il testo relativo al riavvio dell'applicazione UC.
Passaggio da CLS connect alla pagina 308	Aggiunto il capitolo relativo al passaggio da CLS Connect.
OpenScape Business UC SuiteServer alla pagina 1745	Aggiunto il testo relativo al riavvio dell'applicazione UC.
Gateway VoceLinea server SIP nativo alla pagina 1629	Aggiunte voci di tabella per la sicurezza del trasporto e dei media.
Accesso remoto alla pagina 1362	Eliminati i metodi di accesso remoto obsoleti.
Passaggio da CLS connect alla pagina 308	Aggiunto il capitolo relativo al passaggio da CLS Connect.

Modifiche in V3R2

Capitoli modificati	Descrizione delle modifiche
Telefoni supportati alla pagina 108 Requisiti richiesti per myPortal @work alla pagina 487 Caratteristiche alla pagina 508 Requisiti richiesti per client PC della UC Suite alla pagina 534 OpenScape Business Attendant alla pagina 841 myAttendant alla pagina 855 Requisiti richiesti per l'uso di myAgent alla pagina 867 Come configurare il reflashing automatico alla pagina 1258 Importanza dei risultati ottenuti dai test della gamma delle frequenze radio alla pagina 966	Nuovi telefoni supportati: • OpenScape Desk Phone CP 110 • OpenScape DECT Phone S6/SL6/R6
Panoramica di myPortal for Teams alla pagina 1189	myPortal for Teams: supporto per il diario
Livelli di espansione disponibili presso il reparto commerciale alla pagina 102 Valori massimi per utente alla pagina 1433 Livelli di espansione di UC Smart alla pagina 1442 Livelli di espansione di UC Suite alla pagina 1447 Limiti di espansioni Mobility alla pagina 1465 Application Connectivity alla pagina 1468	myPortal for Teams: Limiti di configurazione e capacità
myPortal @work alla pagina 485	Gli scenari di avviso di chiamata in attesa sono supportati con myPortal @work
Unify Phone alla pagina 1191 Come configurare la connettività Unify Phone alla pagina 1192 Come gestire gli utenti Unify Phone alla pagina 1193 Come aggiungere utenti Unify Phone esistenti alla pagina 1194 Come modificare i dettagli dell'utente Unify Phone alla pagina 1195 Come preparare Numero alternativo e Routing delle chiamate per l'interoperabilità Unify Phone alla pagina 1197 Impostazioni di baseSistema Flag di sistema alla pagina 1512	Capitoli nuovi/aggiornati per la connettività Unify Phone

Capitoli modificati	Descrizione delle modifiche
Licenze alla pagina 294 Suggerimenti per combinazioni di licenze alla pagina 303 Licenze utente alla pagina 296 Licenze orientate all'utente alla pagina 297 Licenze di sistema alla pagina 299 Assegnazione della licenza (indipendente) alla pagina 310 Come concedere licenze agli utenti (indipendente) alla pagina 312 Assegnazione della licenza (sistema di reti) alla pagina 321 Come concedere licenze agli utenti (sistema di reti) alla pagina 323	Nuova licenza Unify Phone
Dettagli sull'uso dei canali proxy RTP alla pagina 1441	Aggiunte informazioni sui canali proxy RTP richiesti per ogni chiamata Unify Phone
Stato presenza (presenza) alla pagina 551	Aggiunta nota sulla visibilità dello stato di presenza.
Utenti della alla pagina 541	Aggiunta nota sulla restrizione alla modifica del nome utente.
Concessione della licenza alla pagina 291	Rinominati OCCLA e OCCL rispettivamente in Scheda madre V3 e Scheda madre V2, nei capitoli da 8.11 a 8.14

Modifiche in V3R1 FR2

Capitoli modificati	Descrizione delle modifiche
Requisiti richiesti permyPortal to go alla pagina 947	myPortal to go: supporto callkit iOS
RSP.servicelink alla pagina 1356	Memorizzazione delle credenziali RSP nel set di backup
OpenScape Business UC SuiteGruppi alla pagina 1728 OpenScape Business, UC SuiteProfili alla pagina 1751	UC Suite: Gruppi Preferiti
Trunk/InstradamentoGruppo di trunk alla pagina 1687 UtenteUtenteParametri utente alla pagina 1647	SBC affidabile
myPortal @work alla pagina 485	myPortal @work: supporto risposta per assente
Panoramica di myPortal for Teams alla pagina 1189 How to configure myPortal for Teams alla pagina 1190 Come caricare myPortal for Teams nell'archivio di Teams alla pagina 1190	myPortal for Teams

Modifiche in V3R1 FR1

Capitoli modificati	Descrizione delle modifiche
Come aggiungere un'Eccezione in CCV alla pagina 838	Aggiunto nuovo tipo di eccezione CCV
OpenScape Business UC SuiteServer alla pagina 1745	Aggiunto parametro **Disattiva monitoraggio conversazioni**
OpenScape Business UC SuiteServer alla pagina 1745	Aggiunto parametro **La cache di ricerca nella rubrica scade tra**

Modifiche in V3R1

Capitoli modificati	Descrizione delle modifiche
• Telefoni supportati alla pagina 108 • Requisiti richiesti per myPortal @work alla pagina 487 • Servizio di distribuzione (DLI e DLS) alla pagina 359 • Caratteristiche alla pagina 508 • myAttendant alla pagina 855 • Requisiti richiesti per l'uso di myAgent alla pagina 867 • OpenScape Business Attendant alla pagina 841 • Come configurare il reflashing automatico alla pagina 1258 • Upgrade software dei sistemi OpenScape Business X alla pagina 1371 • Migrazione hardware/software dei sistemi OpenScape Business X a V3 alla pagina 1376 • Upgrade del software di OpenScape Business S alla pagina 1385 • Livelli di espansione di UC Smart alla pagina 1442 • Livelli di espansione di UC Suite alla pagina 1447 • Application Connectivity alla pagina 1468	Nuovo telefono supportato OpenScape Deskphone CP 700 e CP 700X
Telefoni supportati alla pagina 108	Nuovo telefono supportato OpenScape WLAN Phone WL4/WL4 Plus
• Gateway voceProvider di servizi di telefonia Internet alla pagina 1615 • Gateway VoceLinea server SIP nativo alla pagina 1629 • StatisticheStatistiche di telefonia Stato linea alla pagina 1718	Miglioramenti ITSP
OpenScape Business UC Suite External Directory alla pagina 1730	Nuovo pulsante **Rimuovi tutto**
OpenScape Business UC SuiteServer alla pagina 1745	Nuovo flag **Visualizza nomi agente in associazione coda myAgent** per la visualizzazione di nomi utente insieme ai relativi numeri di estensione.
Come visualizzare i dati di massa alla pagina 162	I dati di massa sono disponibili anche nel menu di livello superiore delle configurazioni guidate.

Capitoli modificati	Descrizione delle modifiche
Installazione di base> Dati di massa alla pagina 1552	Aggiunte due nuove colonne **Numero di cellulare** e **Indirizzo e-mail**
Classi di autorizzazione Servizio notte auto alla pagina 1703	Aggiunta la funzionalità **Copia servizio**.
• Valori massimi per utente alla pagina 1433 • Valori massimi per le linee alla pagina 1436 • Connessione al provider di servizi alla pagina 1441 • Livelli di espansione di UC Smart alla pagina 1442 • Livelli di espansione di Smart Voicemail alla pagina 1445 • Livelli di espansione di UC Suite alla pagina 1447 • Lavoro in team (Gruppi) alla pagina 1458 • Limiti di espansioni Mobility alla pagina 1465 • Application Connectivity alla pagina 1468	Valori massimi per nuove schede aggiornati
• Come configurare l'invio di e-mail alla pagina 202 • Come modificare le impostazioni e-mail per gli eventi alla pagina 1332 • EventiE-mail alla pagina 1499	Notifica sicurezza in loco per chiamate di emergenza
• Come eseguire l'aggiornamento di UC Business Booster Server da V2 a V3 alla pagina 1374 • Upgrade del software di OpenScape Business S alla pagina 1385	Sicurezza - OpenSSL V1.1.1
Come inoltrare automaticamente i file del registro di sistema alla pagina 1325	Inoltro di file Linux Syslog esternamente
Installazione di base> Dati di massa alla pagina 1552	Numero cellulare UC aggiunto nella configurazione guidata dati di massa
Come raccogliere tracce diagnostiche per un evento di errore alla pagina 215	Raccolta e trasferimento automatici dati di diagnostica

Modifiche in V3

Capitoli modificati	Descrizione delle modifiche
Modelli software UC (soft switch) alla pagina 107 Hardware UC Booster alla pagina 107 Come installare il software di comunicazione alla pagina 225 Requisiti richiesti per la configurazione iniziale alla pagina 218 Configurazione iniziale di OpenScape Business S alla pagina 218 Requisiti richiesti per la configurazione iniziale alla pagina 273 Configurazione iniziale di OpenScape Business UC Booster alla pagina 271	Aggiornamento a SLES 12 SP5.
Circuit Come configurare il numero della casella vocale Circuit Come configurare Numero alternativo e Routing delle chiamate per l'interoperabilità Circuit	Miglioramenti sistema di rete Circuit.
UC SmartGestione utenti alla pagina 1723 Migrazione tra sistemi OpenScape Business V3 alla pagina 1426 Suggerimenti per combinazioni di licenze alla pagina 303 Licenze orientate all'utente alla pagina 297 Licenze di sistema alla pagina 299 Scenario 5: OpenScape Business BLF collegato a un singolo sistema OpenScape Business alla pagina 853 Scenario 6: OpenScape Business BLF collegato a un sistema di reti OpenScape Business (stato BLF e Presenza tramite WSI) alla pagina 855 OpenScape Business BLF alla pagina 844 OpenScape Business TAPI 120 alla pagina 1163 Impostazioni di base per UC Smart alla pagina 481 myPortal @work alla pagina 485	Licenze UC Suite per client UC Smart.
Come migrare dalla scheda madre V2 alla scheda madre V3 (sistema indipendente) alla pagina 339	Dispositivi Block OptiPoint su OCC Evolution V3.
Come accedere al WBM alla pagina 117	Accesso WBM esterno rafforzato.

Capitoli modificati	Descrizione delle modifiche
Come migrare dalla scheda madre V2 alla scheda madre V3 (sistema indipendente) alla pagina 339 Come migrare il nodo master di un sistema connesso in rete dalla scheda madre V2 alla scheda madre V3 alla pagina 341 Come migrare il nodo slave di un sistema connesso in rete dalla scheda madre V2 alla scheda madre V3 alla pagina 342 Migrazione dei sistemi HiPath 3000 al software OSBiz V3 con scheda madre V3 alla pagina 342 Aggiornamento da V2 a V3 con CLS Connect alla pagina 342 Aggiornamento da V2 a V3 senza CLS Connect alla pagina 343	OCC Evolution.
Come caricare un logo del telefono nel sistema alla pagina 1228	Supporto carico logo telefono CP con WBM
Aggiornamenti automatici alla pagina 541 myPortal @work alla pagina 485 myPortal @work alla pagina 533	Aggiornamenti su myPortal @work

Modifiche in V2R7

Capitoli modificati	Descrizione delle modifiche
Procedure guidate – Telefonia centrale Servizio di integrazione Active Directory Come configurare il servizio Active Directory Servizio di integrazione Active Directory	Aggiunte informazioni sul servizio di integrazione Active Directory
Stazione > Stazione > Parametri stazione	Eliminata opzione disattivazione controllo PW
Circuit	Aggiunte funzionalità deviazione chiamate, conferenza e informazione occupato in conversazione
OpenScape Business UC Suite > Server	Aggiunto flag Disattiva modifica nome
OpenScape Business, UC Suite > Profili	Aggiunto gruppo tasti di scelta rapida nelle impostazioni dei profili di UC Suite
myPortal @work	Aggiunta disponibilità su MacOS

Capitoli modificati	Descrizione delle modifiche
Modelli software UC (soft switch) Hardware UC Booster Migrazione di un sistema indipendente HiPath 3000 con OpenScape Office V3 HX Come installare il software di comunicazione Requisiti richiesti per la configurazione iniziale Configurazione iniziale di OpenScape Business S Requisiti richiesti per la configurazione iniziale Configurazione iniziale di OpenScape Business UC Booster	Aggiunto supporto di SLES 12 SP3
Gateway voce > Provider di servizi di telefonia Internet Gateway voce > Trunk server SIP nativo	Aggiunte informazioni su wiki (ITSP)

Modifiche in V2R6FR2

Nota: Questo documento può contenere descrizioni di caratteristiche che si trovano ancora in fase beta. Per i dettagli, vedere le informazioni sulle vendite e le note sulla versione.

- Suggerimenti per combinazioni di licenze
  - Aggiunte licenze per la telefonia VoIP di myPortal @work
- myPortal @work
  - Aggiunte informazioni VoIP
- Requisiti richiesti per myPortal @work
  - Aggiunte informazioni VoIP
- Musica su attesa
  - Utilizzo del MoH in UC Suite
- Come importare la musica su attesa
  - Utilizzo del MoH in UC Suite
- OpenScape Business UC Suite > Server
  - Chiudi conversazione dopo aggiunta del flag

1.1 Cronologia dei miglioramenti/risoluzioni

Le modifiche menzionate in questo capitolo sono cumulative.

Modifiche in V3R4 FR2

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati	N. problema
PRB000086522	23 ott 2025	Aggiunta sezione con linee guida per l'aumento dell'intervallo di sottorete.	Configurazione iniziale di OpenScape Business X alla pagina 133	63
PRB000086522	26 ago 2025	Aggiunta una dichiarazione relativa alla connessione simultanea di due ITSP su LAN e WAN.	Come configurare l'accesso a Internet tramite un router Internet esterno sulla LAN con porta WAN dedicata all'ITSP alla pagina 177	59
PRB000081445	18 ago 2025	Aggiunte note relative alla generazione automatica dei canali multimediali.	Come configurare la UC Suite alla pagina 199 Come configurare la UC Suite alla pagina 250	58
PRB000082631	15 lug 2025	Aggiunte informazioni relative a Client IP > Informazioni dispositivo, scheda WBM, meccanismo di ordinamento	StazioneStazioneClient IP alla pagina 1637	57

Modifiche in V3R4 FR1

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000082944	22 apr 2025	Aggiunta una nota relativa al fatto che i dati utente di Unify Phone non fanno parte del file di esportazione.	ConfigurazioneConfigurazione porta alla pagina 1473

Modifiche in V3R4

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000080604	19 feb 2025	Modificata la frase relativa al numero di telefono da utilizzare per le chiamate in uscita quando non è disponibile un numero DID del chiamante.	Come configurare un ITSP predefinito alla pagina 180 Come configurare un ITSP predefinito alla pagina 385
PRB000080170	15 gen 2025	Correzione della descrizione del nome visualizzato/voce della tabella degli algoritmi.	Impostazioni di baseSistema Display alla pagina 1526
PRB000077322	09 dicembre 2024	Correzione di entrambi i valori massimi per le stazioni e le stazioni TDM per X1R/W.	Valori massimi per utente alla pagina 1433

Modifiche all'aggiornamento di V3R3 FR2 GA

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000079549	15 set 2024	Correzione nel passaggio 5 delle notifiche via e-mail.	Come configurare le notifiche e-mail degli errori di sistema alla pagina 1352
PRB000076788	13 set 2024	Aggiunta una nota di aggiornamento sul firewall delle applicazioni.	Sicurezza Firewall delle applicazioni alla pagina 1553 Firewall applicaz. alla pagina 990 Sopravvivenza alla pagina 1138
PRB000075233	18 luglio 2024	Correzioni riguardo alla priorità degli orari e le loro eccezioni.	Come aggiungere un'Eccezione in CCV alla pagina 838
PRB000077767	28 ago 2024	Aggiunta una nota relativa all'inoltro delle chiamate alla casella vocale.	Stato presenza (presenza) alla pagina 551
PRB000072194	18 luglio 2024	Correzione dei valori per le porte usate dei controlli CAR alive	Porte usate alla pagina 265

Modifiche in V3R3 FR2

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000072191	13 giugno 2024	Correzione dei valori degli annunci X1 a/b e dei canali MEB per X1W/R	Valori massimi per le linee alla pagina 1436 Valori massimi delle risorse alla pagina 1438
PRB000076108	13 giugno 2024	Correzione sulle porte CLS e nuova sezione alla fine del capitolo	Porte usate alla pagina 265

Modifiche in V3R3 FR1

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000072445	1 aprile 2024	Aggiunto il campo "Lunghezza massima numero interno" in Impostazioni di composizione canoniche	Impostazioni di baseImplementazione parametri telefoni alla pagina 1548
PRB000074047	15 marzo 2024	Aggiunta una nota per spiegare il funzionamento del flag "Rimuovi dati prima dell'importazione".	Come importare un file CSV dal file system locale nella rubrica esterna alla pagina 562
PRB000072007	1 aprile 2024	Aggiunto il nuovo capitolo "Come modificare il piano di composizione con numeri a 4 cifre" e le relative informazioni.	Come modificare il piano di composizione con numeri a 4 cifre alla pagina 230, Impostazioni di sistema alla pagina 227
PRB000074908	08 aprile 2024	Aggiunta la capacità degli utenti per quanto riguarda i promemoria temporizzati.	Promemoria e appuntamenti alla pagina 672

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000073511	14 aprile 2024	Correzioni del problema relativo alle eccezioni annuali ricorrenti.	Come aggiungere pianificazioni alla pagina 916 Come aggiungere un'Eccezione in CCV alla pagina 838

Modifiche in V3R3

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000068453	27 giugno 2023	Aggiunte informazioni su SMTP autenticato e OAuth 2.0.	Come configurare l'invio di e-mail alla pagina 202
PRB000066465	17 lug 2023	Aggiunte informazioni sulla nuova porta del firewall per CLS Connect.	Attivazione licenza (sistema indipendente) alla pagina 308, Procedura per la concessione della licenza alla pagina 292, Porte usate alla pagina 265, Come attivare CLS Connect alla pagina 307
PRB000068453	17 lug 2023	Aggiornati i formati immagine supportati.	OpenScape Business UC SuiteRubrica utente alla pagina 1725, Utenti della alla pagina 541
PRB000071258	18 ott 2023	Aggiunti limiti di lunghezza per i dati CSV.	Come importare un file CSV dal file system locale nella rubrica esterna alla pagina 562
PRB000061414	20 ott 2023	Aggiunto nuovo flag - Usa route statica dedicata.	Immagine del softwareSoftware di sistemaAggiornamento via Internet alla pagina 1478
PRB000064083	26 ott 2023	Aggiunti valori mancanti per il campo Applica autenticazione per i dispositivi HFA.	Impostazioni di baseSistema > Password di registrazione HFA alla pagina 1537

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000071163	24 nov 2023	Aggiunti nuovi capitoli e informazioni sulla gestione dei certificati.	Introduzione alla pagina 1031 (nuovo) Come importare i certificati server (PEM) alla pagina 1035 (nuovo) Gestione dei certificati per Booster Server alla pagina 1038 (nuovo) Come generare una richiesta di firma di un certificato (CSR) alla pagina 1033 Come generare un certificato CA alla pagina 1032 Come importare un certificato server (PKCS#12) alla pagina 1035 Gestione dei certificati alla pagina 1030
PRB000072442	04 gen 2023	Aggiunta nota sul comportamento di DND nei team.	Configurazione team / gruppo Team alla pagina 701
PRB000069431	05 gen 2024	Aggiunte informazioni su UC Suite, routing CLI e MS Teams.	Pianificazioni alla pagina 830 Pianificazioni alla pagina 881
PRB000054882	02 feb 2024	Aggiunte informazioni per la sezione mancante "Autorizzazione del trunk commutato".	Impostazioni di baseSistema Rinvio/PO/Hotline alla pagina 1530
PRB000073109	22 feb 2024	Aggiunta riga ITSP ai canali dei trunk SIP nelle tabelle.	Valori massimi per le linee alla pagina 1436
PRB000073818	1 mar 2024	Correzione dei valori predefiniti per i parametri Conteggio allarme coda, Ora allarme coda, Timeout chiamata persa e Soglia chiamate abbandonate.	OpenScape Business UC Suite Contact Center alla pagina 1733

Modifiche in V3R2 FR1

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000066080	11 maggio 2023	Aggiunta nota per il comportamento dell'avviso di chiamata in attesa.	Come attivare o disattivare l'avviso di chiamata in attesa immediato tramite la console posto operatore alla pagina 662
PRB000067262	12 maggio 2023	Corretti i valori del timer di ritardo MOH.	Impostazioni di baseSistema TemporizzazioniTemporizzazioni, Modalità espertiImpostazioni di baseSistema, Modalità esperti alla pagina 1520

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000065660	29 giu 2023	Aggiunta nota relativa all'aggiunta e alla rimozione dei contatti UC.	Rubriche alla pagina 505, Rubriche alla pagina 556
PRB000067012	01 ago 2023	Aggiunta nota sulla selezione rapida del sistema e sulle regole di restrizione della selezione.	Selezione breve del sistema alla pagina 628
PRB000056655	05 set 2023	Aggiunta nota sull'aggiornamento delle informazioni sul display dopo il trasferimento di una chiamata.	Trasferisci alla pagina 643

Modifiche in V3R2

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000052166	20 giu 2022	Eliminata la sezione relativa a Auto DSP Trace, poiché questa traccia non è più disponibile in WBM	Tracce alla pagina 1486
PRB000058845	01 lug 2022	Aggiornate le informazioni sul supporto SPE nelle reti	Servizio di distribuzione (DLI e DLS) alla pagina 359
PRB000058415	22 ago 2022	Eliminata la sezione relativa alle schede e ai dispositivi non supportati, poiché questa sezione è stata spostata nella Documentazione di manutenzione.	Appendice alla pagina 1760
PRB000058021	22 ago 2022	Aggiornate le informazioni sui componenti da sostituire	Migrazione hardware/software dei sistemi OpenScape Business X a V3 alla pagina 1376
PRB000061111	27 ott 2022	Aggiunta nota relativa al comportamento VoIP di myPortal@work	Client UC Smart alla pagina 485
PRB000062363	25 nov 2022	Aggiunti capitolo e sottocapitoli relativi alla migrazione delle schede HW	Migrazione dei moduli HW alla pagina 1428
PRB000063445	30 nov 2022	Aggiunta nota relativa al gruppo UCD di backup nella soluzione di fallback di base	Soluzione secondaria (soluzione fallback) alla pagina 893
RB000055773, PRB000055775	12 gen 2023	Aggiunta nota relativa all'aggiunta di una nuova origine dati in ODS.	Come aggiungere un'origine dati esterna per Open Directory Service alla pagina 1181
PRB000061481	12 gen 2023	Aggiunti una nota e un sottocapitolo relativi all'eliminazione degli utenti Unify Phone	Unify Phone alla pagina 1191
PRB000063445	12 gen 2023	Aggiunta nota nella soluzione di fallback di base	Soluzione secondaria (soluzione fallback) alla pagina 893
PRB000062971	25 gen 2023	Rimossi gli eventi non presenti in WBM. Aggiunta nota e modificata la tabella per adattarla ai contenuti.	SNMP (Simple Network Management Protocol) alla pagina 1288

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000065939	5 apr 2023	Modifiche al flag "Disabilita e-mail di invito a myPortal".	OpenScape Business UC SuiteServer alla pagina 1745
PRB000065939	5 apr 2023	Modifiche al flag "Disabilita e-mail di invito a myPortal".	OpenScape Business UC SuiteServer alla pagina 1745
PRB000067211	26 apr 2023	Aggiunta sezione sui limiti della migrazione e sulle soluzioni.	Migrazione di un sistema OpenScape Business X V3 da una scheda madre V2 a una scheda madre V3 alla pagina 1381

Modifiche in V3R1

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000052438	20 apr. 2021	Aggiunta sezione per modalità OCCLA e UC Suite/Smart	Come migrare dalla scheda madre V2 alla scheda madre V3 (sistema indipendente) alla pagina 339
PRB000051654	14 maggio 2021	Aggiunti nuovi capitoli Integrazione con MS Office 365	Panoramica sull'integrazione di Microsoft Office 365 alla pagina 616
PRB000051803	19 maggio 2021	Aggiunta nota per gli scenari di avviso di chiamata in attesa	myPortal @work alla pagina 485
PRB000052202	02 set 2021	Aggiunte informazioni sulle chiamate Internet	Limitazione del numero di chiamate simultanee tramite ITSP alla pagina 820

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000054381	03 set 2021	Rimuovere le voci di myPortal Smart	• Funzioni UC alla pagina 92 • Livelli di espansione disponibili presso il reparto commerciale alla pagina 102 • Lingue supportate alla pagina 109 • Programmazione dei tasti alla pagina 441 • UC Smart alla pagina 480 • Client UC Smart alla pagina 485 • Stato presenza (presenza) alla pagina 504 • Connessione in rete di OpenScape Business X e OpenScape 4000 alla pagina 1117 • Caratteristiche modificate/ abbandonate di HiPath 3000 e Interfacce alla pagina 1420 • Accesso dell'utente alle funzioni UC (client UC) alla pagina 98 • Come concedere licenze agli utenti (indipendente) alla pagina 312 • myPortal @work alla pagina 485 • myPortal to go alla pagina 945 • Upgrade software dei sistemi OpenScape Business X alla pagina 1371
PRB000054046	06 set 2021	Aggiunta nota sui dispositivi	Configurazione team / gruppo Team alla pagina 701Direttore/ Segretaria / Gruppo Top alla pagina 705
PRB000053988	06 set 2021	Aggiunta nota sulla ricerca del nome del gruppo in myPortal @work	Caratteristiche alla pagina 508

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000054258	10 set 2021	Capitoli aggiornati per configurare i telefoni DECT	Come inserire l'identificativo del sistema DECT e configurare eventuali parametri cordless aggiuntivi (dati a livello di sistema) alla pagina 968 Come configurare le stazioni base cordless alla pagina 969 Come effettuare la prima configurazione dei telefoni DECT alla pagina 969 Come accedere al cordless di un telefono DECT (portatile OpenStage/Gigaset) alla pagina 970 Come aggiungere altri telefoni DECT alla pagina 972 Come eliminare i telefoni DECT alla pagina 972 Come configurare i parametri Multi-SLC alla pagina 973 Come richiedere i dati sulle stazioni base alla pagina 973 Come attivare il tono di avviso dell'indicazione messaggio in attesa (MWI) per i telefoni DECT alla pagina 974 Come controllare lo stato di connessione dei telefoni DECT alla pagina 974
PRB000051960, PRB000052019	11 ott 2021	Aggiunta nota sull'account utente myPortal @work bloccato in modalità UC Suite	Configurazione utente myPortal @work alla pagina 489
PRB000053691	18 ott 2021	Aggiornata tabella su come viene eseguita la ricerca LDAP	Impostazioni di baseSistema LDAP alla pagina 1533
PRB000054934	12 nov 2021	Aggiunte informazioni sul numero di conversazioni visualizzate nel client	myPortal @work alla pagina 485
PRB000054816	03 feb 2022	Aggiunta nota sul servizio CallMe	Servizio CallMe alla pagina 553
PRB000054995/ PRB000055780	18 feb 2022	Aggiunta nota per Bridge Server da ODBC a ODBC	Come configurare ODBC-ODBC Bridge Server alla pagina 1179
PRB000055651	28 feb 2022	Aggiunte informazioni sul completamento del processo di registrazione dei telefoni DECT	Come accedere al cordless di un telefono DECT (portatile OpenStage/Gigaset) alla pagina 970
PRB000056047	15 mar 2022	Aggiunta nota per RSP	RSP.servicelink alla pagina 1356

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000055842	30 mar 2022	Aggiunte le informazioni sui formati di file supportati e sul limite di dimensioni per il caricamento di un'immagine	Utenti della alla pagina 541 OpenScape Business UC SuiteRubrica utente alla pagina 1725

Modifiche in V3

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
NA16738104	19 ago 2020	Aggiunta nota sull'a compilazione dei campi Nome e Cognome nella directory esterna	Rubrica esterna alla pagina 560
NA16759874	13 nov 2020	Aggiunta info per il supporto della modalità full-duplex con OCCLA	Come migrare dalla scheda madre V2 alla scheda madre V3 (sistema indipendente) alla pagina 339 Risparmio energia alla pagina 1285Interfacce di reteScheda madre LAN 2LAN 2, Modalità espertiInterfacce di rete Scheda madre, Modalità esperti alla pagina 1584Interfacce di reteScheda madreLAN 3 (Admin)LAN 3 (Admin), Modalità espertiInterfacce di rete Scheda madre, Modalità esperti alla pagina 1586Interfaccia di reteScheda applicazioniLAN 1LAN 1, Modalità espertiInterfacce di rete Scheda applicazioni, Modalità esperti alla pagina 1593Interfaccia di reteScheda applicazioniLAN 2LAN 2, Modalità espertiInterfacce di rete Scheda applicazioni, Modalità esperti alla pagina 1594Interfacce di reteScheda madre LAN 1 (WAN) alla pagina 1580
PRB000050351	12 nov 2020	Corretta una nota sui telefoni CP0	Come configurare un PIN per l'arresto controllato di OpenScape Business X alla pagina 1264
PRB000050248	12 nov 2020	Aggiunte voci per CAR nella tabella	Porte usate alla pagina 265
NA16756853/ PRB000049732	10 dic 2020	Aggiunta nota per il riavvio di Booster Server in caso di modifiche della configurazione nell'inoltro e-mail.	Come configurare l'invio di e-mail alla pagina 612
PRB000050722	15 dic 2020	Aggiunta ingo per abilitare la conversione del numero per i numeri di selezione breve tramite LDAP.	Regole e convenzioni alla pagina 512

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
PRB000051401	09 feb 2021	Aggiunta nota per le impostazioni del firewall in Device@Home.	Configurazione del DispositivoSistema@Home alla pagina 979
PRB000050983	11 feb 2021	Aggiunta nota per il numero di utenti Circuit per sistema.	Valori massimi per utente alla pagina 1433
PRB000051647	11 feb 2021	Aggiunta info per inoltro di chiamata verso trasferimento Deflect call / Single step e gestione chiamate in caso di flag trasferimento Deflect call / Single step.	Impostazioni di baseSistema Flag di sistema alla pagina 1512
PRB000051165	19 feb 2021	Corretta nota con tipo di dispositivo.	Direttore MULAP alla pagina 723
PRB000050983	15 feb 2021	Aggiunta nota per funzionalità non supportata	Stazioni SIP alla pagina 432

Modifiche in V2R7

ID caso di servizio	Data della modifica	Descrizione della modifica	Capitoli modificati
NA16740815	11 ago 2020	Aggiunta nota sul numero max di chiamate simultanee in MOH	Valori massimi delle risorse alla pagina 1438
NA16653104	2 giugno 2020	Aggiornamento della documentazione relativo alle porte utilizzate	Porte usate alla pagina 265
NA16692823	30 apr. 2020	Aggiunta di un'opzione per utilizzare l'indirizzo FQDN anche nel campo WAN di myPortal @work	Requisiti richiesti per myPortal @work alla pagina 487
NA16652178	8 apr. 2020	Aggiunta nota di apertura porta 8101 in un proxy per il funzionamento corretto di `CommunicationsServer.exe`.	Come eseguire la disinstallazione Silent alla pagina 540 Come eseguire l'installazione Silent alla pagina 539
NA16582432	6 apr. 2020	Aggiunta di un'informazione sull'attivazione della funzione **Ascolto chiamate**.	Ascolto di una chiamata alla pagina 645

2 Introduzione e informazioni importanti

Nell'introduzione viene fornita una panoramica della struttura del documento. L'introduzione aiuta il lettore a reperire rapidamente le informazioni sugli argomenti desiderati. Prima di procedere all'installazione e alla messa in funzione del sistema di comunicazione, occorre leggere e assicurarsi di avere compreso le istruzioni di sicurezza, gli avvisi e le note importanti.

Suggerimento: Le istruzioni di sicurezza e gli avvisi forniscono informazioni sulle prescrizioni di sicurezza e sugli avvertimenti da rispettare. Le note importanti forniscono informazioni sul comportamento in caso di emergenza, sulle norme e sulle linee guida per l'installazione, sulle specifiche per le interferenze radio del sistema di comunicazione. Oltre a ciò vengono fornite informazioni sullo smaltimento e sul riciclaggio.

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

2.1 Con questa documentazione

Questa documentazione descrive le procedure di amministrazione di OpenScape Business™.

Si riferisce ai modelli hardware OpenScape Business X1, OpenScape Business X3, OpenScape Business X5 e OpenScape Business X8 oltre al modello soft switch OpenScape Business S (Soft switch). La soluzione di comunicazione unificata UC Smart è integrata in tutti i modelli di OpenScape Business. Le funzionalità della soluzione di comunicazione unificata UC Suite sono offerte in combinazione con le opzioni UC Booster Card o UC Booster Server; per il soft switch è possibile scegliere tra UC Smart o UC Suite.

Nota: Nella presente documentazione, i modelli hardware OpenScape Business X1/X3/X5/X8 (per brevità chiamate OpenScape Business X) e il soft switch OpenScape Business S sono definiti anche "sistemi di comunicazione".

La UC Suite comprende funzioni di comunicazione unificata tra cui il Contact Center multimediale.

Le informazioni riportate in questa documentazione contengono descrizioni generali di caratteristiche tecniche che non sono sempre disponibili in tutti i casi. Le caratteristiche desiderate devono essere definite nei singoli casi in sede di stipula del contratto.

Se una funzione non è disponibile come descritto, ciò può essere dovuto a quanto segue:

- Il sistema di comunicazione non dispone di tale funzione:
- La licenza richiesta non è disponibile o non è attivata.

2.1.1 Documentazione e destinatari

La documentazione su OpenScape Business è rivolta a più categorie di utenti.

Aspetti commerciali e pianificazione del progetto

La seguente documentazione è destinata agli aspetti commerciali e alla pianificazione del progetto.

- Descrizione dei servizi

  Questa documentazione descrive tutti i servizi. Questo documento è un estratto della documentazione per l'amministratore.

installazione e assistenza

La seguente documentazione è destinata ai tecnici dell'assistenza.

- OpenScape Business X1/X1W, Guida all'installazione

  Questa documentazione descrive l'installazione dell'hardware e la prima configurazione di OpenScape Business X1.
- OpenScape Business X3/X5/X8, Istruzioni di installazione

  Questa documentazione descrive l'installazione dell'hardware e la prima configurazione di OpenScape Business X3/X5/X8.
- OpenScape Business S, Istruzioni di installazione

  Questa documentazione descrive l'installazione iniziale del softswitch OpenScape Business S.
- OpenScape Business X1/X1W, Documentazione per la manutenzione

  Questa documentazione descrive l'hardware di OpenScape Business X1.
- OpenScape Business X3/X5/X8, Documentazione di manutenzione

  Questa documentazione descrive l'hardware di OpenScape Business X3/X5/X8.
- OpenScape Business X1R, Guida all'assistenza e all'installazione, Documentazione per la manutenzione

  Questa documentazione descrive l'installazione dell'hardware la prima installazione e la manutenzione di OpenScape Business X1R.

Amministrazione

La seguente documentazione è destinata agli amministratori.

- Documentazione per l'amministratore

  Questa documentazione descrive la configurazione dei servizi che possono essere impostati tramite OpenScape Business Assistant (WBM). La documentazione per l'amministratore è disponibile nel sistema sotto forma di guida in linea.
- Configurazione per l'amministratore del cliente, documentazione per l'amministratore

  Questa documentazione descrive la configurazione dei servizi che possono essere impostati tramite OpenScape Business Assistant (WBM) con il profilo amministratore **Basic**.

- Manager E, Documentazione per l'amministratore

  Questa documentazione descrive la configurazione dei servizi che possono essere impostati tramite Manager E.

Client UC / Telefon User Interface (TUI)

La seguente documentazione è destinata all'utente UC.

- myPortal for Desktop, Istruzioni per l'uso

  Questa documentazione descrive l'installazione, la configurazione e il funzionamento del client UC myPortal per desktop.
- myPortal for Outlook, Istruzioni per l'uso

  Questa documentazione descrive l'installazione, la configurazione e il funzionamento del client UC myPortal per Outlook.
- myPortal @work, Manuale dell'utente

  Questa documentazione descrive l'installazione, la configurazione e il funzionamento del client UC myPortal @work.
- Fax Printer, Istruzioni per l'uso

  Questa documentazione descrive l'installazione, la configurazione e il funzionamento della stampante fax.
- myPortal to go, Istruzioni per l'uso

  Questa documentazione descrive la configurazione e il funzionamento dei client mobili UC myPortal to go per smartphone e tablet-PC.
- myAgent, Istruzioni per l'uso

  Questa documentazione descrive l'installazione, la configurazione e il funzionamento del client myAgent del Contact Center.
- myReports, Istruzioni per l'uso

  Questa documentazione descrive l'installazione, la configurazione e il funzionamento del client myReports del Contact Center.
- myAttendant, Istruzioni per l'uso

  Questa documentazione descrive l'installazione, la configurazione e il funzionamento della Console posto operatore myAttendant.
- OpenScape Business Attendant, Manuale d’uso

  Questa documentazione descrive l'installazione, la configurazione e il funzionamento della console operatore di OpenScape Business Attendant.
- UC Smart Telefon User Interface (TUI), Guida rapida

  Questa documentazione descrive il menu della casella vocale del telefono della soluzione UC Smart.
- UC Suite - Telefon User Interface (TUI), Guida rapida

  Questa documentazione descrive il menu della casella vocale del telefono della soluzione UC Suite.

2.1.2 Struttura della documentazione per l'amministratore

Questa sezione mostra come è strutturato il contenuto della Documentazione per l'amministratore. L'hardware è descritto nella Documentazione di servizio.

Sezione	Contenuto
Introduzione e note importanti	Panoramica della struttura della presente documentazione e delle informazioni importanti/di sicurezza da osservare durante l'installazione e il funzionamento
Panoramica sul sistema	Panoramica sul sistema di comunicazione per un avvio rapido
Concetto di amministrazione	Panoramica sui programmi di amministrazione e sui ruoli degli utenti nel WBM
Installazione iniziale di OpenScape Business X	Integrazione di OpenScape Business X3/X5/X8 nella LAN del cliente e configurazione di base tramite procedure guidate
Installazione iniziale di OpenScape Business S	Integrazione di OpenScape Business S nella LAN del cliente e configurazione di base tramite procedure guidate
Installazione iniziale di OpenScape Business UC Booster	Integrazione di OpenScape UC Business Booster nella LAN del cliente e configurazione di base tramite procedure guidate
Licenza	Procedure di concessione di licenze e licenze
Integrazione nella rete dati interna (LAN)	Interfaccia LAN/WAN, risoluzione dei nomi, instradamento dei dati, DLI e DLS
Connessione al provider di servizi	Accesso a Internet, telefonia IP, accesso ai trunk
Utente	Piano di composizione, stazioni IP, stazioni UP0; stazioni DECT, stazioni Mitel SIP-DECT, stazioni ISDN e analogiche, stazioni virtuali, utenti dei client UC, profili utente
UC Smart	Client e funzioni della soluzione di comunicazione unificata UC Smart, compresa Smart Voicemail. Stato della presenza, directory e diario, conferenze, funzioni di gruppo, caselle vocali
UC Suite	Client e funzioni della soluzione di comunicazione unificata UC Suite: Stato della presenza e CallMe, directory e diario, conferenze e collaborazione web, messaggi vocali e fax, messaggistica istantanea
Funzioni sul telefono	Esecuzione di chiamate, segnalazione di chiamata, ID della linea chiamante, funzioni durante la chiamata, ottimizzazione della comunicazione
Lavoro in team (gruppi)	Gruppo di raccolta delle chiamate, gruppo di chiamata, gruppo di ricerca, team/top, MULAP, UCD

Sezione	Contenuto
Routing delle chiamate	Classi di servizio, restrizione della selezione, sistema tenant, LCR, chiamate di emergenza
Assistenti	AutoAttendant, OpenStage Attendant, assistenti basati su PC, posizione di intercettazione
Multimedia Contact Center	Client e funzioni del Contact Center: agenti, code e orari, servizio VIP, fallback, report
Mobility	myPortal to go, Mobility Entry, One Number Service, telefonia dual-mode, mobilità IP, Cordless/DECT
Sicurezza	Firewall, SPE, VPN, certificati
Collegamento in rete di OpenScape Business	Piano di rete, scenari di rete, posizione centrale di intercettazione, sopravvivenza
Interfacciamenti	Dispositivi di annuncio, telefono d'ingresso e apriporta, attuatori e sensori
Connettività delle applicazioni	CSTA, TAPI, avvio applicazioni
Registrazione account	Registrazione dei dettagli delle chiamate, addebiti e durata delle chiamate, controllo dei costi
Manutenzione	Backup e ripristino, aggiornamento, riavvio, ricarica, spegnimento, reimpostazione di fabbrica, inventario, azioni, servizi remoti
Migrazione	Aggiornamento da HiPath 3000 a OpenScape Business
Limiti di configurazione e capacità	Valori massimi per i limiti di configurazione e le capacità dei diversi sistemi di comunicazione
Modalità Esperto	Descrizione di riferimento delle finestre/ maschere in modalità Esperto
Appendice	Elenco degli standard supportati, delle funzionalità Euro-ISDN e dei protocolli IP e dei numeri di porta utilizzati
Glossario	Brevi descrizioni dei termini comunemente utilizzati

2.1.3 Tipi di argomenti

Gli argomenti trattati possono essere concetti di base o task:

Tipo di argomento	Descrizione
Concetti	Spiega di cosa si tratta e fornisce una panoramica del contesto con informazioni di base ad esempio sui servizi.
Task (istruzione operativa)	Descrive passo per passo le procedure per le applicazioni pratiche e presuppone la conoscenza dei relativi concetti. I titoli delle procedure sono facilmente riconoscibili in quanto iniziano con **Come...**.

2.1.4 Convenzioni di visualizzazione/rappresentazione

La presente documentazione utilizza diverse convenzioni per rappresentare i vari tipi di informazioni.

Tipo di informazioni	Aspetto	Esempio
Elementi dell'interfaccia utente	grassetto	Fare clic su **OK**.
Percorsi di menu	>	**File** > **Fine**
Aspetti particolarmente importanti	grassetto	Il Nome **non può essere eliminato**.
Testo dei riferimenti incrociati	corsivo	Ulteriori informazioni sono disponibili nell'argomento *Rete*.
Versione	Tipo di carattere con spaziatura fissa, ad es. Courier	`Comando non trovato.`
Input	Tipo di carattere con spaziatura fissa, ad es. Courier	`Immettere` LOCAL come nome file.
Combinazioni di tasti	Tipo di carattere con spaziatura fissa, ad es. Courier	`<Ctrl>+<Alt>+<Esc>`

2.2 Avvertimenti di sicurezza e attenzione

Gli avvertimenti di sicurezza e attenzione si riferiscono a situazioni che possono comportare morte, lesioni gravi, danni materiali e/o perdita di dati.

Gli interventi al sistema di comunicazione e ai dispositivi devono essere eseguiti **esclusivamente** da personale qualificato.

Nel contesto degli avvertimenti di sicurezza e attenzione, per personale qualificato si intendono persone autorizzate a mettere in funzione, mettere a

terra e a registrare i sistemi, i dispositivi e le linee in conformità alle normative e agli standard di sicurezza in vigore.

Leggere attentamente e rispettare i seguenti avvertimenti di sicurezza e attenzione prima di procedere al montaggio e alla messa in servizio del sistema di comunicazione.

Leggere attentamente e rispettare tutti gli avvertimenti di sicurezza e attenzione relativi al sistema di comunicazione e ai dispositivi.

È inoltre importante essere a conoscenza dei numeri di telefono d'emergenza.

Tipi di avvertimenti di sicurezza e attenzione

Nella presente documentazione sono utilizzati i seguenti tipi di avvertimenti di sicurezza e attenzione:

Pericolo: Indica una situazione di pericolo immediato che comporta morte o lesioni gravi.

Attenzione: Indica una situazione di pericolo generico che può comportare morte o lesioni gravi.

Avvertenza: Indica una situazione di pericolo che può comportare lesioni personali.

Nota: Indica situazioni che possono comportare danni materiali e/o perdita di dati.

Altri simboli per la descrizione più dettagliata delle fonti di pericolo

Il simbolo seguente non viene normalmente utilizzato nella presente documentazione, ma può essere riportato sui dispositivi o sugli imballi.



ESD Componenti sensibili a carica elettrostatica

Concetti correlati

Informazioni importanti. alla pagina 81

2.2.1 Tipo di avvertimento: Pericolo

Gli avvertimenti di tipo "Pericolo" indicano una situazione di pericolo immediato che può comportare morte o lesioni gravi.

Pericolo: Scossa elettrica per contatto con linee sotto tensione

- Pericolo: le tensioni superiori a 30 VCA (corrente alternata) o 60 VCC (corrente continua) sono pericolose!
- I lavori sulla rete a bassa tensione (<1000 VCA) possono essere eseguiti solo con un'adeguata qualifica o da elettrotecnici debitamente qualificati e devono essere conformi alle normative nazionali e locali in materia di allacciamenti elettrici.

2.2.2 Tipo di avvertimento: Avvertenza

Gli avvertimenti di tipo "Avvertenza" indicano una situazione di pericolo generico che può comportare morte o lesioni gravi.



Attenzione: Scossa elettrica per contatto con linee sotto tensione

- Collegare i sistemi di comunicazione OpenScape Business X3R, X3W, X5R e X5W alla terra di protezione tramite un conduttore di protezione separato. Collegare il sistema di comunicazione prima della messa in servizio e collegare come d'abitudine telefoni e linee al conduttore di protezione.
- Collegare ogni box del sistema di comunicazione OpenScape Business X8 alla terra di protezione mediante un conduttore di protezione separato. Collegare il sistema di comunicazione prima della messa in servizio e collegare come d'abitudine telefoni e linee al conduttore di protezione.
- Utilizzare soltanto sistemi, strumenti ed apparecchiature in condizioni perfette. Non è consentito l'uso di dispositivi che presentano danni esterni.
- Sostituire immediatamente anche i dispositivi di protezione danneggiati (coperture, targhette adesive e cavi di messa a terra).
- Se il cavo di rete è danneggiato, sostituirlo immediatamente.
- Utilizzare il sistema di comunicazione e il server solo se collegati a prese con contatto di terra.
- Durante un temporale le linee di comunicazione non devono essere collegate o rimosse, lo stesso vale per i moduli.
- In caso di lavori specifici per cui l'alimentazione del sistema di comunicazione non è richiesta, scollegare tutte le linee di alimentazione (ad esempio per la modifica del cablaggio). Scollegare completamente la presa di alimentazione del sistema di comunicazione e assicurarsi che il sistema non sia collegato ad altre fonti di alimentazione (ad esempio, un gruppo di continuità).

  Prima di iniziare, verificare che il sistema di comunicazione non sia sotto tensione. Se un fusibile o un interruttore sono aperti, non dare per scontato che tutti i circuiti siano disconnessi dall'alimentazione.
- Tenere conto della corrente derivata dalla rete telefonica. Scollegare tutte le linee di comunicazione del sistema di comunicazione prima di scollegare dal sistema il conduttore di terra previsto.

- Se si lavora su dispositivi sotto tensione, prestare la massima attenzione quando si effettuano misurazioni su parti in tensione o interventi di manutenzione a moduli o sportelli.

  Le superfici con rivestimento in metallo (ad esempio uno specchio) conducono elettricità; in caso di contatto sussiste il pericolo di folgorazione o cortocircuito.

2.2.3 Avvertenze: Attenzione

Gli avvertimenti di tipo "Attenzione" indicano situazioni pericolose che possono comportare lesioni.

Avvertenza: Pericolo di esplosione in caso di sostituzione non appropriata di accumulatori e batterie

- Utilizzate esclusivamente le batterie approvate.
- Sostituire le batterie al litio solo con batterie identiche o di produttori dei tipi consigliati.

Avvertenza: Pericolo di incendio

- Utilizzare solo linee di comunicazione con conduttori di sezione minima pari a 0,4 mm (AWG 26).
- Non lasciare alcuna documentazione o simili oggetti infiammabili sul sistema di comunicazione.

Avvertenza: Pericolo di lesioni e incidenti generici sul luogo di lavoro

- Dopo il collaudo e gli interventi di manutenzione, rimontare in posizione tutti i dispositivi di sicurezza e chiudere gli sportelli e gli alloggiamenti.
- Posare le linee in modo che non costituiscano una fonte di pericolo (pericolo di inciampare) e che non vengano danneggiate.
- Assicurarsi che quando si eseguono lavori su un sistema di comunicazione o sul server aperti, questi non rimangano incustoditi.
- Utilizzare uno strumento adatto a sollevare oggetti o carichi pesanti.
- Controllare regolarmente lo stato degli utensili ed utilizzare soltanto quelli in condizioni perfette.
- Quando vengono eseguiti lavori sui sistemi, indossare abiti appropriati e raccogliere, ovvero legare, i capelli - se lunghi.
- Non indossare gioielli, cinturini d'orologio in metallo o capi d'abbigliamento con ornamenti in metallo o borchie.
- Indossare sempre la protezione per gli occhi in tutte le situazioni che lo richiedono.
- Indossare sempre un casco di protezione se sussiste il pericolo di caduta di oggetti.
- Fare in modo che il luogo d'installazione sia adeguatamente illuminato e ordinato.

2.2.4 Avvertimento: Avviso

I tipi di avvertimento "Avviso" indicano situazioni che possono comportare danni materiali e/o perdita di dati.

Osservare quanto riportato in questo tipo di avvertimenti per evitare danni ai beni materiali e/o perdite di dati:

- Prima della messa in servizio, assicurarsi che la tensione nominale della rete corrisponda a quella prevista per il sistema di comunicazione o il server (tensione di targa).
- Attenersi alle seguenti misure per la protezione dei dispositivi sensibili alle scariche elettrostatiche:
  - Indossare sempre il bracciale antistatico secondo le modalità previste prima di eseguire qualsiasi intervento su moduli e unità.
  - Posizionare i moduli e le unità sempre su una superficie conduttiva dotata di messa a terra.
  - Trasportare e spedire i componenti del sistema di comunicazione (ad esempio i moduli) solo in imballaggi di tipo adatto.
- Utilizzate esclusivamente accessori originali. Il mancato rispetto di quanto indicato potrebbe causare danni al sistema o comportare la violazione delle norme sulla sicurezza e sulla compatibilità elettromagnetica.
- Una modifica improvvisa della temperatura può determinare la condensazione dell'umidità dell'aria. Se il sistema di comunicazione o il server viene portato da un ambiente freddo a uno più caldo, l'umidità può condensare. Prima della messa in funzione, accertarsi che il sistema di comunicazione o il server abbiano raggiunto la temperatura ambiente e siano perfettamente asciutti.
- Collegare i cavi soltanto nei punti di connessione previsti.
- Se non è disponibile alcuna alimentazione di emergenza oppure se, in caso di caduta di tensione, non è possibile passare a un telefono d'emergenza analogico, nell'eventualità di un guasto al sistema di alimentazione risulterà impossibile effettuare chiamate di emergenza tramite il sistema di comunicazione.
- Prima di procedere al montaggio a parete, occorre verificare che la parete presenti una capacità portante sufficiente. Utilizzare sempre materiali di installazione e fissaggio adatti per montare il sistema di comunicazione e i relativi dispositivi in modo sicuro.
- Non è consentito depositare materiali facilmente infiammabili nelle vicinanze del sistema di comunicazione.

2.2.5 Istruzioni di sicurezza specifiche del paese

Qui sono riportate informazioni sulla sicurezza da rispettare per l'installazione, la messa in servizio e l'uso del sistema di comunicazione, applicabili in paesi specifici.

2.2.5.1 Istruzioni di sicurezza per l'Australia

Per quanto riguarda il montaggio, la messa in servizio e l'uso in Australia dei sistemi di comunicazione OpenScape Business X e OpenScape Business S e

dell'OpenScape Business UC Booster Server (server applicazioni) in Australia occorre rispettare le seguenti norme di sicurezza:

- L'installazione e la manutenzione dei sistemi di comunicazione OpenScape Business X e OpenScape Business S e di OpenScape Business UC Booster Server (server applicazioni) possono essere eseguite solo da personale qualificato e debitamente autorizzato.
- I sistemi a parete OpenScape Business devono essere installati vicino alla presa a muro tramite la quale verrà alimentato il rispettivo sistema di comunicazione. La presa a muro deve essere facilmente accessibile. Assicurarsi che il contatto di terra della presa di corrente installata a parete sia intatto.
- I sistemi di comunicazione OpenScape Business X e OpenScape Business S e l'OpenScape Business UC Booster Server (server applicazioni) devono essere configurati in modo che sia sempre possibile chiamare i numeri di emergenza (ad esempio 000).
- In caso di interruzione di corrente non è possibile eseguire chiamate di emergenza tramite il sistema di comunicazione se non è disponibile alcuna alimentazione di riserva o in caso di mancanza di tensione non è possibile effettuare la commutazione ai telefoni analogici di emergenza (commutazione linea esterna).
- La musica in attesa e i dispositivi di paging devono essere collegati al sistema di comunicazione tramite tramite un'unità di isolamento della linea approvata dall'Australian Communications Authority (ACA).

2.2.5.2 Istruzioni di sicurezza per Brasile

Per quanto riguarda il montaggio, la messa in servizio e l'uso in Brasile dei sistemi di comunicazione OpenScape Business X e OpenScape Business S e dell'OpenScape Business UC Booster Server (server applicazioni), occorre rispettare le seguenti norme di sicurezza:

- Si osservi che è obbligatorio l’uso di una striscia di prese dotata di protezione da sovratensione con il codice C39334-Z7052-C33. Per il collegamento a tensione di rete dei sistemi di comunicazione OpenScape Business X e OpenScape Business S e di OpenScape Business UC Booster Server (server applicazioni) è richiesto l'uso di una striscia di prese con protezione da sovratensioni.
- È obbligatorio l'uso di cavi Ethernet schermati per le porte/interfacce LAN/WAN della scheda madre OCCL, OCCM e OCCMR e della UC Booster Card OCAB (scheda applicazioni).

2.2.5.3 Istruzioni di sicurezza per USA

Per quanto riguarda il montaggio, la messa in servizio e l'uso negli USA dei sistemi di comunicazione OpenScape Business X e OpenScape Business S e dell'OpenScape Business UC Booster Server (server applicazioni) occorre rispettare le seguenti norme di sicurezza:

- Interruzioni di alimentazione e guasto del T1

  In caso di collegamento in rete di sistemi di comunicazione tramite T1 (1,544 Mbit/s), l'azienda di telecomunicazioni (Federal Communications

Commission (FCC) deve essere informata quando un sistema di comunicazione viene rimosso dalla rete.

Se uno dei sistemi di comunicazione descritti in questa documentazione di Unify Software and Solutions GmbH & Co. KG interferisce con il funzionamento della rete pubblica di telecomunicazioni, la società di telecomunicazioni ha il diritto di sospendere temporaneamente l'accesso alla linea esterna. In normali circostanze, la compagnia di telecomunicazioni informa l'utente anticipatamente di questa eventualità. Se questo non è possibile, viene inviato un messaggio non appena possibile. In questa circostanza, si verrà informati che è possibile presentare un reclamo alla società di telecomunicazioni.

- Modifica delle apparecchiature di telecomunicazione

  La compagnia telefonica ha il diritto di apportare all'occorrenza modifiche alle proprie apparecchiature, dispositivi, procedure operative e processi. Tali modifiche possono eventualmente compromettere il funzionamento dei sistemi di comunicazione. In normali circostanze si riceve anticipatamente una notifica per evitare interruzioni nel servizio di telecomunicazioni.
- Apparecchiature di riproduzione della voce

  Le apparecchiature di riproduzione della voce quali ad esempio apparecchi per musica su attesa o risponditori devono essere approvati e rilasciati da Unify Software and Solutions GmbH & Co. KG nonché assicurare la conformità alle linee guida e alle disposizioni delle norme FCC Parte 68, Paragrafo C.

  Le apparecchiature di riproduzione della voce non rilasciate possono essere collegati solo mediante circuito di protezione di tipo approvato e rilasciato da Unify Software and Solutions GmbH & Co. KG, assicurando inoltre la conformità alle linee guida e alle disposizioni delle norme FCC Parte 68, Paragrafo C.
- REN (Ringer Equivalence Number)

  Il Ringer Equivalence Number (REN) determina il numero di dispositivi che può essere collegato contemporaneamente a una linea telefonica e ai quali può essere segnalata la chiamata quando viene composto il numero in questione. Nella maggior parte delle aree, ma limitatamente a queste, il numero REN totale dei dispositivi connessi ad una linea non deve superare le cinque (5) unità. Per determinare il numero totale ammesso nella propria area, contattare la compagnia telefonica locale.
- Nuovi indicativi interurbani e codici di accesso alla linea urbana

  Il Least Cost Routing (LCR) è configurato in modo che i cambiamenti nei codici per rete locale e le linee esterne vengano automaticamente riconosciuti e applicati. In caso contrario, questi codici non possono essere utilizzati per le chiamate dopo la modifica.
- Compatibilità con apparecchi acustici

  Telefoni di emergenza e telefoni pubblici (ad esempio telefoni in atri, sale ospedaliere, ascensori e camere d'albergo) devono essere dotati di telefoni che assicurano l'uso di apparecchi acustici accoppiati magneticamente. Se necessario, le persone con problemi di udito che non si trovano in aree pubbliche devono essere dotate di apparecchi acustici adeguati.

  Tutti i telefoni digitali prodotti dopo il 16 agosto 1989 da Unify Software and Solutions GmbH & Co. KG sono compatibili con gli apparecchi acustici e soddisfano i requisiti delle norme FCC, Parte 68, Sezione 68.316 e 68.317.

- Funzioni di selezione preprogrammate

  Se si programmano i numeri di emergenza o se si eseguono test di numeri di emergenza con un prodotto di Unify Software and Solutions GmbH & Co. KG dotato di funzioni di composizione programmate, restare in linea e spiegare brevemente al direttore operativo il motivo della chiamata, prima di riagganciare. Queste attività devono essere eseguite fuori dagli orari di punta, ad esempio la mattina presto o la sera tardi.
- Interfacciamento di terminali fuori dai locali

  I clienti che desiderano collegamenti di postazioni esterne (Off-Premises Station, OPS) devono contattare la compagnia di telecomunicazione comunicando in quale classe OPS sono registrati i dispositivi e che tipo di connessione richiedono.
- Supervisione dell'accettazione chiamate con selezione passante

  I clienti che utilizzano uno dei sistemi di comunicazione Unify Software and Solutions GmbH & Co. KG descritti nella presente documentazione senza prevedere una supervisione adeguata della risposta alle chiamate sono inadempienti rispetto alle norme FCC Parte 68.

  I sistemi di comunicazione di Unify Software and Solutions GmbH & Co. KG, descritti nella presente documentazione, supportano le conferme inoltrate tramite PSTN per le chiamate DID:

  – risposte dall'utente chiamato.
  – risposte da una console posto operatore.
  – inoltrate a un annuncio gestito dal cliente.

  Inoltre, i sistemi di comunicazione di Unify Software and Solutions GmbH & Co. KG, descritti in questa documentazione, restituiscono la conferma di supervisione corretta a tutte le chiamate DID inoltrate tramite PSTN. Eccezioni ammesse:

  – Una chiamata non viene accettata.
  – Viene segnalato come occupato.
  – Viene segnalato con un tono di congestione (Reorder Tone).
- Premesse per l'accesso con la stessa abilitazione

  Per entità con elevati volumi di traffico (ad esempio, alberghi, ospedali, aeroporti, scuole) gli utenti devono disporre di codici di accesso con pari diritti per il provider desiderato. I codici correnti per l'accesso con lo stesso livello di abilitazione (Carrier Access Codes CAC) sono 10xxx e 101xxxx, oltre a 800/888 e 950, dove xxx o xxxx sostituiscono il codice del rispettivo provider.

  Per realizzare la connessione con un provider specifico, l'utente deve inserire un codice di accesso specifico del provider prima del numero di telefono del partner desiderato. È possibile accedere con lo stesso livello di abilitazione anche utilizzando i codici 800/888 o 950 del provider desiderato.

  I sistemi di comunicazione di Unify Software and Solutions GmbH & Co. KG, descritti in questa documentazione consentono l'accesso a provider interstate mediante l'uso di codici di accesso con gli stessi diritti.

  Modifiche di queste funzionalità costituiscono una violazione del Telephone Operator Consumer Services Improvement Act del 1990 e della Parte 68 delle normative FCC.

2.2.5.4 Istruzioni di sicurezza per Canada



Pericolo: Scossa elettrica per contatto con linee sotto tensione

I lavori sulla rete a bassa tensione (<1000 VCA) possono essere eseguiti solo con un'adeguata qualifica o da elettrotecnici debitamente qualificati e devono essere conformi alle normative nazionali e locali in materia di allacciamenti elettrici.

Per quanto riguarda il montaggio, la messa in servizio e l'uso in Canada dei sistemi di comunicazione OpenScape Business X e OpenScape Business S e dell'OpenScape Business UC Booster Server (server applicazioni), occorre rispettare le seguenti norme di sicurezza:

- REN (Ringer Equivalence Number)

  Il Ringer Equivalence Number (REN) determina il numero di dispositivi che può essere collegato contemporaneamente a una linea telefonica. La terminazione dell'interfaccia può essere costituita da qualsiasi combinazione di dispositivi, a condizione che la somma dei REN di tutti i dispositivi sia inferiore o uguale a cinque.
- Limitazioni per il collegamento di dispositivi

  L'etichetta ISED (Innovation, Science and Economic Development) Canada identifica i dispositivi certificati. La certificazione indica che il dispositivo soddisfa determinati requisiti in termini di protezione, gestione e sicurezza delle reti di telecomunicazione. I requisiti sono documentati nel Terminal Equipment Technical Requirements. L'ISED (Innovation, Science and Economic Development) Canada non fornisce alcuna garanzia che i dispositivi certificati funzioneranno sempre con piena soddisfazione del cliente.

  Prima dell'installazione dei dispositivi e componenti descritti nella presente documentazione, l'utente è tenuto ad assicurarsi che sia consentito il collegamento alle strutture della compagnia di telecomunicazioni locale. Inoltre, durante l'installazione del sistemi di comunicazione e del server assicurarsi che venga utilizzato un metodo di collegamento adeguato. Informare il cliente che in determinate situazioni, la mancata osservanza delle prescrizioni menzionate, possono pregiudicare la prestazione delle apparecchiature.

  Le riparazioni di apparecchi omologati devono essere coordinate da un tecnico dell'assistenza del produttore o del fornitore. Eventuali riparazioni o modifiche eseguite dall'utente ai dispositivi e ai componenti o eventuali malfunzionamenti dei dispositivi possono autorizzare il provider di telecomunicazioni a richiedere all'utente la disinstallazione di tali dispositivi.

  Per la propria protezione, gli utenti sono tenuti ad assicurarsi che i collegamenti di terra dell'alimentazione, delle linee telefoniche e dell'impianto idraulico in metallo (ove presente) siano intercollegati. Questa precauzione può essere di particolare importanza in aree rurali.

2.3 Informazioni importanti.

Le informazioni importanti indicano il comportamento in caso di emergenza, il corretto smaltimento e riciclo, la destinazione d'uso e le condizioni di

funzionamento dei sistemi di comunicazione e del server. Sono inoltre riportate informazioni sugli standard e le linee guida sull'installazione, le caratteristiche della trasmissione radio del sistema di comunicazione e la protezione e la sicurezza dei dati.

Concetti correlati

Avvertimenti di sicurezza e attenzione alla pagina 73

2.3.1 Comportamento in caso di emergenza

In questa sezione vengono fornite informazioni sulle misure da adottare in caso di emergenza.

Comportamento in caso di incidenti

Interventi di pronto soccorso

Chiamata di emergenza

Segnalazione di incidenti

- In caso di incidente, mantenere la calma ed agire con prudenza.
- Prima di toccare la persona infortunata, disattivare sempre l'alimentazione di corrente.
- Se non dovesse essere possibile disattivare immediatamente l’alimentazione, toccare la persona infortunata soltanto con oggetti in materiale non conduttore (ad es. manico di legno di una scopa) cercando di isolarla immediatamente dalla fonte di corrente.
- È importante essere a conoscenza della basi di pronto soccorso. In situazioni di emergenza è fondamentale essere in grado di eseguire i diversi interventi di rianimazione in caso di arresto respiratorio o cardiaco, nonché di prestare le prime cure in caso di ustione.
- In caso di arresto respiratorio, eseguire immediatamente la respirazione bocca a bocca o bocca a naso.
- Se si dispone delle conoscenze adeguate, eseguire il relativo massaggio di rianimazione in caso di arresto cardiaco.

Chiamare senza esitazione un'ambulanza o un medico di guardia e comunicare quanto segue nell’ordine riportato:

- Luogo dell'accaduto
- Cosa è accaduto
- Numero di feriti
- Tipo di lesioni
- Attendere che vi vengano poste domande.
- Segnalare ai propri superiori tutti gli incidenti accaduti, circostanze e potenziali fonti di pericolo.
- Segnalare ogni scarica elettrica - anche se minima.

2.3.2 Uso previsto

Il sistema di comunicazione e il server possono essere utilizzati solo per le applicazioni descritte nella presente documentazione ed esclusivamente in combinazione con dispositivi accessori e componenti consentiti e consigliati da Unify Software and Solutions GmbH & Co. KG.

L'uso previsto del sistema di comunicazione e del server sottintende la predisposizione di tipologie di trasporto, stoccaggio, montaggio, messa in funzione appropriate nonché l'adozione di pratiche di uso e manutenzione accurate.

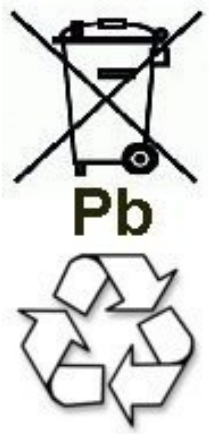
Nota: Pulire l'alloggiamento del sistema di comunicazione e del server solo con un panno morbido e leggermente umido. Non utilizzare detergenti aggressivi o pagliette.

2.3.3 Smaltimento e riciclaggio appropriati

Rispettare le indicazioni relative alle pratiche appropriate di smaltimento e riciclaggio per i dispositivi elettrici ed elettronici e le batterie e gli accumulatori usati.



Tutti i dispositivi elettrici ed elettronici non possono essere smaltiti con i rifiuti domestici, pertanto occorre attenersi alle prescrizioni nazionali in tal senso. Lo smaltimento adeguato e la raccolta differenziata dei dispositivi obsoleti contribuiscono a ridurre i potenziali danni all'ambiente e alla salute. Rappresentano le premesse per il riutilizzo e il riciclo dei dispositivi elettrici ed elettronici usati. Per ulteriori informazioni sullo smaltimento dei dispositivi obsoleti, rivolgersi al proprio comune, all'azienda che si occupa della raccolta e dello smaltimento dei rifiuti, al rivenditore presso il quale è stato acquistato il prodotto o al proprio partner commerciale. Queste indicazioni sono valide solo per dispositivi che vengono installati e venduti nei paesi dell'Unione Europea e che sono soggetti alla Direttiva 2012/19/UE. Nei paesi che non fanno parte dell'Unione Europea sono valide le disposizioni locali per lo smaltimento dei dispositivi elettrici ed elettronici.



Le batterie o gli accumulatori usati con queste cifre sono beni economici riutilizzabili e devono essere sottoposti a processo di riciclaggio. Ai fini di legge, le batterie o gli accumulatori usati che non vengono riciclati devono essere considerati come rifiuti tossici.

2.3.4 Norme e linee guida per l'installazione

Rispettare le indicazioni relative ai requisiti richiesti per il collegamento del sistema di comunicazione e del server alla linea di alimentazione nonché alla schermatura del cablaggio per le connessioni LAN e WAN.

2.3.4.1 Collegamento di OpenScape Business X al circuito di alimentazione

I sistemi di comunicazione OpenScape Business X sono abilitati alla connessione a sistemi di alimentazione TN-S. È inoltre consentita la connessione a sistemi di alimentazione TN-C-S nei quali il conduttore PEN è rispettivamente suddiviso in conduttore di protezione e conduttore neutro. TN-S e TN-C-S secondo la definizione delle norme IEC 60364-1 e IEC60364-5-51.

Se occorre procedere a interventi sulla rete a bassa tensione, rivolgersi a un elettrotecnico qualificato. Queste attività di installazione per il collegamento del sistema di comunicazione devono essere condotte rispettando quanto previsto dalle norme IEC 60364-1 e IEC 60364-4-41 o dalle corrispondenti normative vigenti o prescrizioni nazionali.

2.3.4.2 Allacciamento di OpenScape Business S e OpenScape Business UC Booster Server al circuito di alimentazione

Per informazioni sul collegamento di OpenScape Business S e OpenScape Business UC Booster Server (server applicazioni) fare riferimento alla documentazione del produttore del PC server e degli altri componenti.

Se occorre procedere a interventi sulla rete a bassa tensione, rivolgersi a un elettrotecnico qualificato. Queste attività di installazione per il collegamento di OpenScape Business S e OpenScape Business UC Booster Server devono essere condotte rispettando quanto previsto dalle norme IEC 60364-1 e IEC 60364-4-41 o dalle corrispondenti normative vigenti o prescrizioni nazionali (ad esempio, negli USA e in Canada).

2.3.4.3 Cablaggio schermato per allacciamenti LAN e WAN di OpenScape Business X

Per la conformità ai requisiti CE in relazione alla compatibilità elettromagnetica dei sistemi di comunicazione OpenScape Business X e delle corrispondenti interfacce LAN e WAN, è necessario quanto segue:

- I sistemi di comunicazione possono essere messi in funzione soltanto se dotati di cablaggio schermato. Ciò significa che tra le prese di connessione LAN e WAN schermate dei sistemi di comunicazione e la connessione alla rete dell'edificio o la connessione ai componenti esterni attivi, deve essere utilizzato un cavo schermato di categoria 5 (Cat. 5) di lunghezza pari ad almeno 3 metri. Sulla terminazione del cavo rivolto verso l'installazione dell'edificio o i componenti esterni attivi, deve essere collegato a terra lo schermo del cavo (connessione all'equipotenziale dell'edificio).
- L'uso di un cavo schermato di categoria 5 (CaT.5), è richiesto anche in caso di connessioni di lunghezza ridotta con un componente esterno attivo (switch LAN o simili). Il componente attivo deve tuttavia presentare un'interfaccia LAN adeguatamente schermata con connessione dello schermo collegata a terra (connessione all'equipotenziale dell'edificio).
- Le proprietà schermanti dei componenti di cablaggio devono essere almeno conformi ai requisiti della Norma Europea EN 50173-1[*)] "Tecnologia dell'informazione. Sistemi di cablaggio generico" (e rimandi).[***)]
- Le installazioni dell'edificio dotate di cablaggio in rame simmetrico interamente schermato secondo i requisiti della classe D[**)] della norma EN 50173-1 soddisfano le condizioni sopra descritte.[***)]

2.3.4.4 Requisiti antincendio

I requisiti di protezione antincendio sono disciplinati dalle norme edilizie specifiche del proprio paese. Attenersi alle prescrizioni di legge in vigore.

Per garantire la conformità alle norme di protezione antincendio e sulla compatibilità elettromagnetica, i sistemi di comunicazione OpenScape Business X possono essere utilizzati solamente se in configurazione chiusa. È consentito aprire i sistemi solo per tempi ridotti a scopo di montaggio e manutenzione.

I cavi di sistema di OpenScape Business sono conformi ai requisiti dello standard internazionale IEC 60332-1 in relazione alla resistenza al fuoco. I seguenti standard contengono requisiti simili in materia di resistenza al fuoco dei cavi:

---

*) La norma europea EN 50173-1 è derivata dalla norma internazionale ISO/IEC 11801.

**) La classe D si ha quando sono installati componenti (cavi, prese, cavi di collegamento, ecc.) di categoria 5 (CAT.5).

***) Nel mercato nordamericano è prevalentemente in uso il cablaggio UTP (norma USA EIA/TIA 568 A/B), per cui per le connessioni LAN e WAN dei sistemi di comunicazione vale quanto segue: I sistemi possono essere messi in funzione soltanto se dotati di cablaggio schermato. Ciò significa che tra le prese di connessione LAN e WAN schermate dei sistemi di comunicazione e la connessione alla rete dell'edificio o la connessione ai componenti esterni attivi, deve essere utilizzato un cavo schermato di categoria 5 (Cat. 5) di lunghezza pari ad almeno 3 metri. Sulla terminazione del cavo rivolto verso l'installazione dell'edificio o i componenti esterni attivi, deve essere collegato a terra lo schermo del cavo (connessione all'equipotenziale dell'edificio).

IEC 60332-1 Nota: IEC 60332-1 equivale al metodo di prova UL VW-1	EN 60332-1-1 e EN 60332-2-1	DIN EN 60332-1-1 (VDE 0482-332-1-1) e DIN EN 60332-2-1 (VDE 0482-332-2-1)

Ai reparti competenti in materia di progettazione e assistenza viene fatta richiesta di verificare se lo standard IEC 60332-1 sia sufficiente per i requisiti richiesti dai rispettivi regolamenti edilizi e dalle eventuali disposizioni correlate.

2.3.4.5 Requisiti di protezione contro i fulmini

La protezione dei sistemi di comunicazione contro le sovratensioni ad alta energia richiede una connessione di terra a bassa impedenza, come specificato nelle *istruzioni di installazione di OpenScape Business*.

Nota: Dopo la messa a terra del sistema di comunicazione, occorre verificare il collegamento a terra a bassa impedenza del sistema tramite il conduttore di protezione del circuito di alimentazione e il collegamento a bassa impedenza del conduttore di protezione aggiuntivo, permanentemente collegato alla barra equipotenziale dell'edificio.

Nota:

Pericolo d'incendio a causa di sovratensioni

Linee di telecomunicazione di lunghezza superiore a 500 m o che devono uscire dall'area dell'edificio devono essere adeguatamente protette tramite una protezione parafulmine esterna.

Questa protezione antifulmine viene denominata Protezione primaria supplementare La protezione primaria aggiuntiva viene assicurata dall'installazione corretta di uno scaricatore di sovratensioni (ÜSAG) nel ripartitore principale, nel pannello di permutazione o nel punto di ingresso delle linee nell'edificio. A tal fine, mettere a terra uno scaricatore di sovratensioni con una tensione nominale di 230 V da ognuno dei fili da proteggere.

Senza tale protezione primaria supplementare, i moduli potrebbero venire distrutti in caso di fulmine. Ciò può comportare il guasto dell'intero sistema di comunicazione e il surriscaldamento dei componenti (pericolo di incendio).

2.3.4.6 Identificativi di OpenScape Business X



Come attestato dal marchio CE, la presente apparecchiatura è conforme alla direttiva UE 1999/5/CE.

2.3.5 Informazioni sull'emissione di interferenze e interferenze radio di OpenScape Business X

I sistemi di comunicazione OpenScape Business X sono dispositivi di classe B conformi alla norma EN 55032.

2.3.6 Protezione e sicurezza dei dati

Rispettare le informazioni sulle procedure da adottare per garantire la protezione e la sicurezza dei dati.

Con i sistemi di comunicazione e server descritti in questo documento vengono utilizzati ed elaborati anche dati strettamente personali come ad esempio quelli sulla documentazione degli addebiti, visualizzazioni a display e dati relativi agli utenti.

Per l'elaborazione e l'utilizzo dei dati personali, in Germania viene applicata la rispettiva normativa in vigore (BDSG). Si richiede di attenersi alle normative nazionali del paese in cui il sistema viene utilizzato.

Le norme sulla sicurezza e la protezione dei dati tutelano la privacy e i diritti delle singole persone.

Le norme sulla sicurezza e la protezione dei dati tutelano dall'utilizzo improprio e non autorizzato delle informazioni personali, preservando il diritto alla riservatezza.

Suggerimento: Il cliente è responsabile dell'installazione, dell'utilizzo e della manutenzione del sistema di comunicazione e del server, in conformità alle normative di sicurezza dei dati, sicurezza sul lavoro e dei lavoratori.

I collaboratori di Unify Software and Solutions GmbH & Co. KG sono obbligati alla riservatezza per quanto riguarda i dati aziendali e del cliente.

Al fine di un rispetto coerente delle disposizioni relative all'assistenza tecnica, sia "in loco" che "in remoto", è fatto obbligo di osservare assolutamente le seguenti regole. In tal modo, oltre a tutelare gli interessi dei vostri e nostri clienti, vengono evitate anche conseguenze sul piano personale.

Garantire la protezione e la sicurezza dei dati lavorando in modo responsabile:

- Fare attenzione che ai dati del cliente possano accedere soltanto persone autorizzate.
- Utilizzare tutte le opzioni offerte dalla procedura password; non comunicare ad altri le password, specie in modalità non protette come ad esempio gli appunti/le note su foglietti adesivi.
- Fare attenzione che persone non autorizzate possano in qualche modo elaborare o utilizzare i dati dei clienti (memorizzare, modificare, trasmettere, bloccare, cancellare).

- Evitare che persone non autorizzate abbiano accesso ai supporti dati, come ad esempio CD/DVD di sicurezza o protocolli su carta. sia durante la prestazione di servizio che durante il deposito e il trasporto.
- Distruggere i supporti dati contenenti dati non più necessari. Assicurarsi che non rimangano residui cartacei accessibili.
- Collaborare con il proprio interlocutore presso il cliente, in questo modo si stabilisce e rafforza un rapporto di fiducia.

2.3.7 Requisiti tecnici e conformità di OpenScape Business X

In questa sezione vengono fornite informazioni sull'adempimento dei requisiti richiesti (conformità) per i sistemi di comunicazione OpenScape Business X.

2.3.7.1 Conformità CE

La certificazione CE si basa su: 2014/35/UE - Direttiva sulla bassa tensione (LVD); (Gazzetta ufficiale dell'UE EU L96, 29/03/2014, p. 357-374) 2014/30/UE - Direttiva sulla compatibilità elettromagnetica (EMC); (Gazzetta ufficiale dell'UE L96, 29/03/2014, p. 79-106) 2011/65/UE - Direttiva sulla restrizione dell'uso di determinate sostanze pericolose (ROHS); (Gazzetta ufficiale dell'UE L174, 01/07/2011, p. 88-110)

	Riferimento normativo
Safety	EN 62368-1
Electromagnetic Compatibility EMC	EN55032 (EMC Emission) EN55024 (EMC Immunity Residential)

2.3.7.2 Conformità alle norme degli Stati Uniti e del Canada

	Riferimento normativo
Sicurezza USA e Canada	CSA/UL 62368-1
Emissione EMC Canada	ICES-003 Edizione 6 Classe B
Emissione EMC USA	FCC 47 CFR Parte 15 Paragrafo B Classe B

Numero di registrazione FCC e potenza assorbita

Sul lato posteriore dell'involucro dei sistemi di comunicazione, è stato applicato un adesivo con il numero di registrazione FCC, il Ringer Equivalence Number (REN) e altre informazioni. Su richiesta, queste informazioni possono essere comunicate alla compagnia telefonica.

2.3.7.3 Conformità alle norme internazionali

	Riferimento normativo
Safety	IEC 60950-1 e IEC 62368-1
Emissione EMC	CISPR 32

2.3.8 Condizioni d'uso

Rispettare le condizioni ambientali e meccaniche per l'uso dei sistemi di comunicazione OpenScape Business X e OpenScape Business S e del OpenScape Business UC Booster Server (server applicazioni).

2.3.8.1 Condizioni d'uso per OpenScape Business X

Di seguito sono riportate le specifiche climatiche e meccaniche per l'uso dei sistemi di comunicazione OpenScape Business X.

Specifiche climatiche

Limiti di servizio:

- Temperatura ambiente: da + 5 a + 40 °C (da 41 a 104 °F)
- Umidità assoluta: da 1 a 25 g H_2O/m^3
- Umidità relativa: da 5 a 80%

La ventilazione del sistema di comunicazione è di tipo a convezione. Con OpenScape Business X5W è necessaria la ventilazione forzata se sono presenti più di 32 interfacce a/b.

Nota: Danni dovuti ad aumenti locali della temperatura

Evitare l'esposizione diretta dei sistemi di comunicazione ai raggi solari o al calore prodotto da elementi scaldanti.

Nota: Danni dovuti a condensa prodotta dall'umidità nell'aria

Evitare sempre la formazione di condensa sul sistema di comunicazione, sia prima dell'accensione che durante il funzionamento.

Il sistema di comunicazione deve essere accuratamente asciugato prima di essere messo in funzione.

Dati meccanici

I sistemi di comunicazione sono progettati principalmente per un ambiente stazionario.

2.3.8.2 Condizioni d'uso - OpenScape Business S e OpenScape Business UC Booster Server

Per le specifiche climatiche e meccaniche relative all'uso di OpenScape Business S e OpenScape Business UC Booster Server (server applicazioni), fare riferimento alla documentazione del produttore del PC server e degli altri componenti.

3 Panoramica

OpenScape Business si rivolge alle piccole e medie imprende fornendo loro una soluzione personalizzata, diversificata, flessibile e scalabile per le proprie esigenze di comunicazione. L'architettura di OpenScape Business ne consente l'uso indipendentemente dall'infrastruttura di telefonia esistente, che può essere costituita sia da telefoni classici, IP o DECT. Dalla telefonia ad alte prestazioni a soluzioni complete di comunicazione unificata (UC), OpenScape Business offre sempre la soluzione più adatta.

Flessibile, scalabile e potente

OpenScape Business riunisce il meglio di HiPath 3000 e di OpenScape Office in una nuova piattaforma completa.

3.1 Punti salienti

OpenScape Business è la soluzione all-in-one che offre a piccole e medie imprese le seguenti funzioni.

Punti salienti

- Servizi vocali integrati, gestione presenza (stato presenza), conferenze drag&drop, casella vocale visuale (segreteria telefonica), AutoAttendant, Contact Center multimediale, messaggistica istantanea (IM), mobilità, accesso a rubriche con collegamento ai database, fax, integrazione nei processi aziendali e molto altro
- Client UC singolarmente personalizzati in base al luogo di lavoro e al modo di lavorare
- Integrazione di superficie di OpenScape Web Collaboration
- Per clienti con una sede o come soluzione UC di rete con più sedi
- OpenScape Business offre un'architettura unificata.
- A seconda dell'infrastruttura esistente sono disponibili diversi modelli di OpenScape Business per rispondere alle esigenze di configurazioni di diverse dimensioni. In alternativa è possibile utilizzare il software OpenScape Business su un server standard (soft switch). Questo naturalmente anche in ambienti completamente virtualizzati.
- La soluzione UC Smart è già integrata sulla scheda madre. La soluzione di comunicazione unificata aggiuntiva UC Suite supporta un maggiore numero di utenti UC e offre funzionalità UC avanzate. A tale fine è necessario utilizzare una UC Booster Card o un UC Booster Server.
- Per esigenze diverse ed eterogenee sono già disponibili tutte le interfacce di comunicazione: IP, digitali, analogiche e DECT, oltre alle interfacce più comuni per le comunicazioni vocali

3.2 Comunicazione unificata

La comunicazione unificata (UC) è una tecnologia che consente di migliorare la comunicazione nelle aziende e integra vari mezzi di comunicazione in un unico ambiente applicativo. La comunicazione unificata semplifica i processi aziendali attraverso una gestione integrata dello stato presenza (ad esempio, le chiamate vengono deviate automaticamente al cellulare quando l'utente è lontano da casa). Servizi quali conferenze dial-in, casella vocale personale (voicemail),

casella fax personale, instant messaging (IM), l'uso del cellulare come interno del sistema di comunicazione, Contact Center, video e Web Collaboration sono tutti inclusi in questa soluzione unificata.

Basato sulla flessibilità di un approccio di comunicazione unificata, OpenScape Business offre diverse soluzioni UC, in funzione dei requisiti del luogo di lavoro e dell'infrastruttura esistente. Con la soluzione UC, è possibile scegliere tra UC Smart e UC Suite (UC Smart e UC Suite non possono essere utilizzati contemporaneamente).

È possibile migrare in qualsiasi momento dalla soluzione UC Smart integrata in OpenScape Business alla soluzione UC Suite, più avanzata, effettuando un upgrade della licenza. A seconda del numero di utenti UC, OpenScape Business può essere ampliato solo con il modulo interno "UC Booster Card" o con un server Linux esterno "UC Booster Server". Quale soft switch puro, è disponibile OpenScape Business S come soluzione server con UC Smart o UC Suite.

3.2.1 Funzioni UC

A seconda della soluzione UC scelta (Smart UC o UC Suite) sono disponibili funzioni UC diverse.

Le seguenti tabelle facilitano la selezione della soluzione UC più adatta alle proprie esigenze. I limiti funzionali vengono descritti nel dettaglio nel relativo capitolo (UC Smart, UC Suite, Attendant) della descrizione delle funzioni o nella documentazione per l'amministratore.

Funzione UC	**UC Smart**	**UC Suite**			**Note**
	myPortal to go	**myPortal for Desktop/ Outlook**	**myPortal @work**	**myPortal to go**	
Stato presenza					
Stato presenza (gestione presenza)	x	x	x	x	
Modifica dello stato presenza tramite client	x	x	x	x	
Modifica dello stato presenza tramite TUI	-	x	-	-	
Deviazione di chiamata basata sullo stato	x	x	x	Tramite destinazioni definite in myPortal	Con UC Smart, è possibile selezionare come destinazione un numero a scelta. Con la UC Suite, è possibile selezionare solo un numero dalla preselezione

Funzione UC	UC Smart	UC Suite			Note
	myPortal to go	myPortal for Desktop/ Outlook	myPortal @work	myPortal to go	
Visualizzazione stato nei Preferiti	x	x	x	x	
Visualizzazione stato nelle rubriche	x	x	x	x	
Visualizzazione stato nel diario	-	x	-	-	
Attivazione del servizio CallMe	-	x	x	x	
Integrazione calendario (Outlook)	-	x	-	-	
Integrazione calendario, iCal (solo myPortal for Desktop)	-	x	-	-	
Preferiti					
Visualizzazione dello stato chiamata	x	x	x	x	
Creazione di gruppi	x	x	-	-	
Visualizzazione compatta dei Preferiti	-	x	-	-	
Rubriche					
Rubrica personale	x	x	x	x	
Rubrica interna	x	x	x	x	
Rubrica esterna	-	x	x	x	
Cerca nelle rubriche	x	x	x	x	
Accesso al sistema di destinazioni di selezione breve definite (KWZ)	x	-	x	x	
Importazione/Gestione dei contatti personali (CSV/XML)	-	x	-	-	
Accesso ai contatti di Outlook	-	x	-	-	
Importazione di contatti personali (Mac OS) (myPortal for Desktop)	-	x	-	-	
Integrazione server directory esterno tramite LDAP	-	x	-	-	
Diario					
Tutte le chiamate	x	x	-	x	
Chiamate perse	-	x	-	-	
Chiamate perse	x	x	-	x	
Chiamate risposte	x	x	-	x	
Chiamate pianificate	-	x	-	-	
Casella vocale	x	x	-	x	

Funzione UC	UC Smart	UC Suite			Note
	myPortal to go	myPortal for Desktop/ Outlook	myPortal @work	myPortal to go	
Diario fax	-	x	-	-	
Conversazioni					
Chat	-	-	-	-	
Diario	-	-	x	-	
Casella vocale	-	-	x	-	
Chiamate					
Composizione manuale	x	x	x	x	
Dialer sul desktop (clic per chiamare)	-	x	-	-	
Inoltro chiamate	x	x	x	x	
In attesa	x	x	x	x	
Registrazione di chiamate (registrazione vocale)	-	x	-	-	
Invia e-mail	x	x	x	x	
Invia SMS	x	-	-	x	
Inizia chat	-	x	-	-	
Popup	-	x	-	-	
Conferenze					
Conferenza AdHoc	x	x	x	x	
Conferenze pianificate	-	x	-	-	
Conferenza permanente e aperta (conferenza Drag&Drop)	-	x	-	-	
Integrazione di Web Collaboration	-	x			
Messaggi vocali e fax					
Casella vocale (Voicemail visivo)	x	x	x	x	Funzionalità casella vocale per utenti (IP, TDM)
Ascolto tramite telefono	x	x	x	x	
Ascolto tramite scheda audio PC	-	x	-	-	
Come inviare messaggi vocali tramite e-mail	x	x	-	-	
Fax	-	x	-	-	
Invio messaggi immediato					
Invio messaggi immediato (chat)	-	x	-	-	

1 myPortal to go consente l'accesso anche ai contatti locali di numeri smartphone.

Contact Center

Funzione UC	UC Smart	UC Suite		Note
		myAgent	myReports	
Agenti, code d'attesa e pianificazioni	-	x	-	
Fax e e-mail	-	x	-	
Rapporti/modelli di rapporti predefiniti	-	x	x	
Creazione pianificata di rapporti	-	-	x	

Il collegamento di OpenScape Contact Center è opzionale.

Attendant (posto operatore)

Funzione UC	UC Smart	UC Suite	Note
	Business Attendant	myAttendant	
Visualizzazione delle chiamate in attesa con tipo, nome e numero di telefono	x	x	
Visualizzazione dello stato connessione	x	x	
Commutazione rapida delle chiamate	x	x	
Selezione breve BLF/pulsanti utente. Configurazione personalizzata dei campo BLF/pulsanti utente con numero di telefono o nome	x	x	
Visualizzazione dello stato presenza di altri utenti	x	x	In OpenStage Business Attendant per lo stato presenza è necessario la UC Booster Card/Server o Business S
Modifica dello stato presenza di altri utenti	x	x	
Rubrica personale	-	x	
Rubrica interna	x	x	
Rubrica esterna	x	x	
Contatti Outlook	x	x	
Accesso LDAP	x	x	
Diario	-	x	
Conferenza AdHoc	x	x	
Conferenza pianificata, permanente e aperta (conferenza Drag&Drop)	-	x	

Funzione UC	UC Smart	UC Suite	Note
	Business Attendant	**myAttendant**	
Centro messaggi	-	x	Nel Centro messaggi è possibile registrare e gestire, messaggi vocali, fax, istantanei, nonché e-mail ed SMS.
Accesso ai messaggi vocali e fax di altri partecipanti	-	x	Deve essere rilasciata dal rispettivo utente
Invio messaggi immediato (chat)	-	x	
Servizio notte	x	x	

Il client Attendant consigliato per la UC Suite è myAttendant. OpenScape Business Attendant può essere utilizzato anche con la UC Suite.

Voicemail e Company AutoAttendant

Funzione UC	UC Smart	UC Suite	Nota
Funzionalità base di UC Smart Voicemail e Company AutoAttendant	x	-	
Funzionalità base di UC Suite Voicemail e Company AutoAttendant	-	x	Richiesto UC Booster Card/ Server o Business S
Funzioni UC			
Utilizzo della grafica della casella vocale per gli utenti (interfaccia Web o interfaccia client)	x	x	
Annunci casella vocale per la funzione presenza	x	x	Annunci diversi in funzione dello stato presenza UC impostato
Regole personali per gli annunci di benvenuto per mailbox	-	x	L'utente definisce regole dettagliate per la definizione degli annunci personali
Da casella vocale a e-mail	x	x	I messaggi nella casella vocale vengono allegati alle e-mail come file Wave
Funzioni AutoAttendant			
Caselle vocali per smistamento (AutoAttendant base)	100	20	
AutoAttendant aziendale	x	x	Posto operatore centrale e la casella postale centrale con annunci alternativi all'interno

Funzione UC	UC Smart	UC Suite	Nota
Annunci prima della risposta/ segnalazione parallela	x	x	Annuncio al chiamante mentre l'utente è chiamato con la Suite UC ciò è possibile solo in combinazione con il Contact Center
Destinazioni di selezione per 4 sezioni della giornata/calendario per AutoAttendant	x	x	Commutazione automatica diversa in base ai momenti della giornata Funzione calendario per UC Smart possibile tramite servizio notturno automatico
Calendario centrale per mailbox	x	x	Annunci e gestione delle chiamate per appuntamenti a livello dell'azienda, ad esempio giorni di ferie, feste aziendali ecc..
Profili individuali per mailbox e AutoAttendant personale	-	x	Gestione delle chiamate in base allo stato presenza dei singoli utenti configurabile
Pianificazioni	Servizio giorno-notte	Pianificazione con regole (CCV, Call Control Vector)	
Modelli	1 AutoAttendant configurato per impostazione predefinita	5 modelli personalizzabili	
Editor regole grafico (Editor CCV)	-	x	
Concatenazione di mailbox/ AutoAttendant multistep	x	-	La chiamata viene inoltrata da una mailbox concatenata alla successiva e ogni volta viene riprodotto l'annuncio
Componi per nome	-	x	
Componi interno (Dial by Extension)	x	x	
Funzioni messaggio vocale			
Annunci individuali per mailbox	4	10	Salvataggio e configurazione di più annunci
Inoltro di messaggi vocali	-	x	Inoltro di messaggi a un altro utente/mailbox
Richiamata dalla casella vocale	x	x	Richiamata del chiamante del messaggio attivabile

Funzione UC	UC Smart	UC Suite	Nota
Chiamata di avviso	-	x	Se è presente un messaggio viene eseguita una chiamata a una destinazione esterna, ad esempio un cellulare
Funzione di sostituto	-	x	Inoltro del chiamante al sostituto con annuncio personale
Casella vocale basata sul chiamante/ Istradamento CLI	-	x	Gestione del numero di telefono in base ad esempio al messaggio di benvenuto nella lingua del chiamante
Mailbox di gruppo centrale	x	x	con annunci per reparti/ gruppi
Registrazione in tempo reale	-	x	Registrazione delle chiamate in tempo reale con funzione di sicurezza In OpenScape Business S in cui viene utilizzata la registrazione in tempo reale da UC, G.729A non viene considerato.
Salvataggio di messaggi	-	x	Gli utenti possono salvare singoli messaggi vocali per sé stessi
Cancellazione automatica dei messaggi	x	x	Dopo un certo tempo, i messaggi vengono eliminati per liberare memoria
Cambio della lingua della mailbox in base all'utente	-	x	Selezione dell'annuncio automatico nella singola lingua

Concetti correlati

UC Smart alla pagina 480

3.2.2 Accesso dell'utente alle funzioni UC (client UC)

Per accedere alle funzionalità UC viene usato il client UC. Per accedere allo stato di presenza (UC Suite) e alla casella vocale (UC Smart e UC Suite) si può utilizzare anche TUI (Telephone User Interface).

I client UC sono disponibili nelle versioni adatte ai principali sistemi operativi. A tal fine, rispettare inoltre i requisiti del client riportati nelle release note dei rispettivi prodotti.

Client di comunicazione (desktop e client Groupware)

Client	consigliato per		Descrizione
	UC Smart	UC Suite	
myPortal @work	x	x	Client desktop UC per Microsoft Windows e Mac OS X
myPortal for Desktop	-	x	Client avanzato desktop UC per Microsoft Windows e Apple Mac
myPortal for Outlook	-	x	Client groupware UC per integrazione Microsoft Outlook
OpenScape Desk Phone CP 400/600/600E/ 700/700X/710 HFA (client integrato nel software del telefono)	x	x	Controllo della presenza e accesso alla rubrica per UC Suite e UC Smart

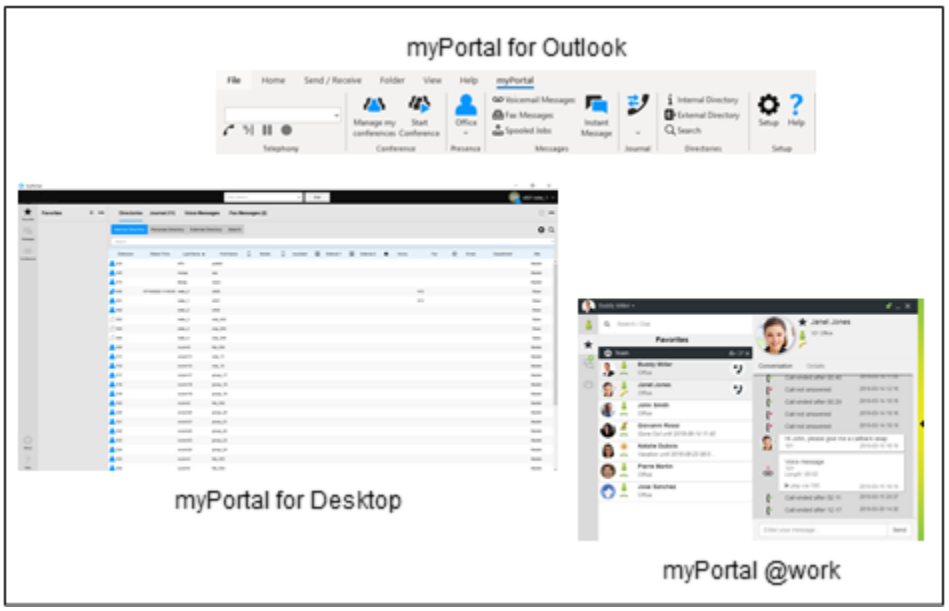


Figura 1: myPortal for Desktop, myPortal for Outlook, myPortal @work

Mobility Clients

Client	consigliato per		Descrizione
	UC Smart	UC Suite	
myPortal to go	x	x	App mobile per smartphone e tablet PC myPortal to go è disponibile con funzionalità leggermente diverse, nelle versioni per UC Smart e UC Suite



Figura 2: myPortal to go

Client del Contact Center

Client	consigliato per		Descrizione
	UC Smart	UC Suite	
myAgent	-	x	Client del Contact Center
myReports	-	x	Interfaccia di analisi/reporting per Contact Center myReports può essere utilizzato indipendentemente dal Contact Center anche per le statistiche di sistema

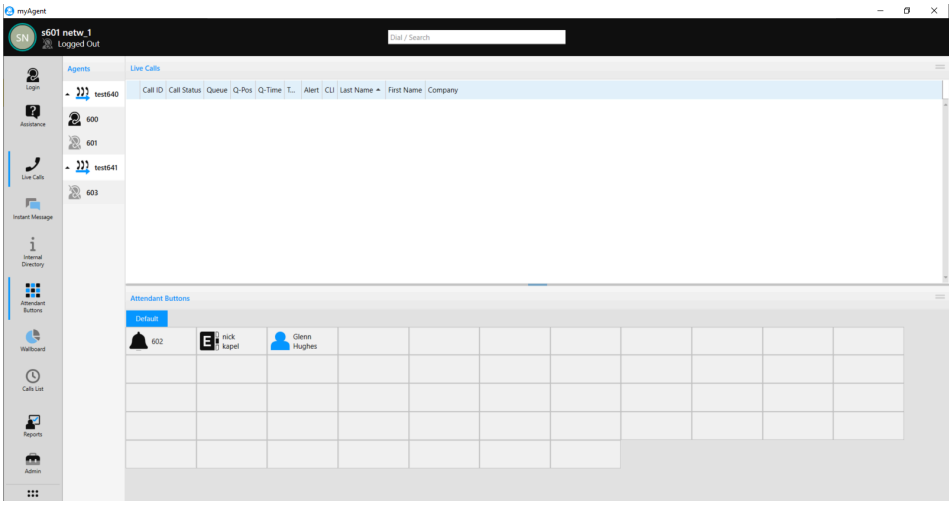


Figura 3: myAgent

Attendant/Posto operatore

Client	consigliato per		Descrizione
	UC Smart	UC Suite	
OpenScape Business Attendant	x	-	Console posto operatore UC con funzioni presenza
myAttendant	-	x	Console posto operatore UC avanzato per Suite UC

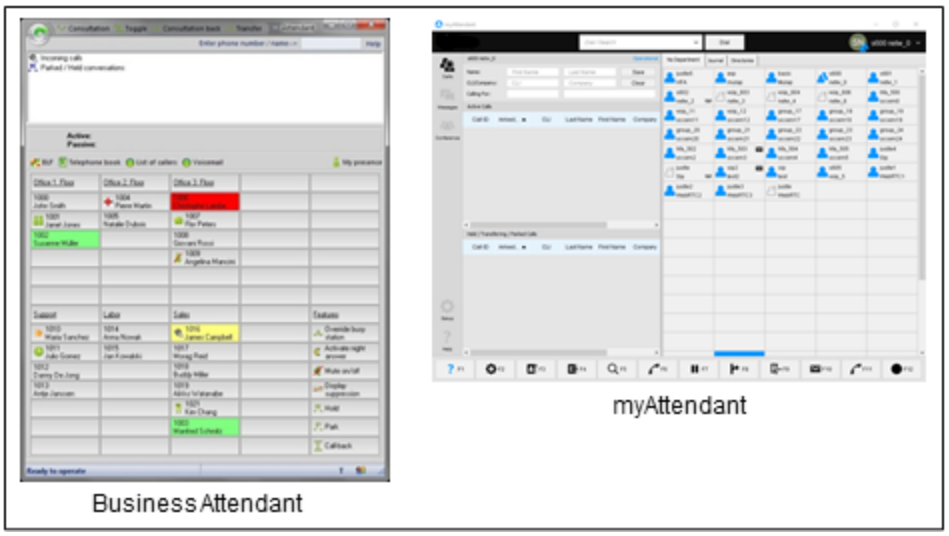


Figura 4: myAttendant

3.2.3 Integrazione in applicazioni commerciali

OpenScape Business può essere integrato in infrastrutture IT e applicazioni esistenti.

Applicazioni

- Application Launcher per un'interazione attiva con applicazioni CRM/ERP
- Software di accounting per il calcolo degli addebiti

Servizi integrati

- Servizi di directory per informazioni su chiamanti e ricerca in rubriche interne ed esterne
- Gestione presenza e messaggistica istantanea (IM) su per social network
- Web Services per le interazioni con applicazioni basate sul Web ad esempio su telefoni cellulari e tablet PC

Middleware CTI

- Provider di servizi TAPI first-party and third-party per il controllo delle chiamate tramite applicazioni CTI o CRM/ERP

Interfacce e protocolli

- CSTA per il monitoraggio e controllo di diverse applicazioni
- SIP per la connessione ad applicazioni basate su trunking SIP
- LDAP per la connessione a directory esterne o da client LDAP esterni
- HTTP e HTTPS per l'accesso alle funzioni UC dei server Web integrati
- TCP/IP come protocollo base per tutte le connessioni Ethernet
- Connettore SQL per il collegamento di database SQL (Microsoft SQL Server, PostgreSQL, Sybase SQL Server)
- Connettore LDAP per server LDAP esterno, ad esempio Active Directory

3.3 OpenScape Business - Modelli

Per l'utilizzo delle funzioni di telefonia e UC sono disponibili diversi modelli. È possibile scegliere tra modelli hardware e modelli puramente software utilizzabili su server standard o in un ambiente virtuale con VMware vSphere.

La funzionalità di comunicazione unificata di UC Smart è già integrata in OpenScape Business. La UC Suite richiede inoltre un modulo rimovibile interno "UC Booster Card" o un server Linux esterno "UC Booster Server". Il soft switch OpenScape Business S supporta sia UC Smart che UC Suite.

3.3.1 Livelli di espansione disponibili presso il reparto commerciale

I modelli di OpenScape Business presentano diversi livelli di configurazione.

	X1	X3R/X3W	X5R/X5W	X8	S
Connessione al provider di servizi					
Canali ITSP (Provider SIP)	30	60	60	60	180
Numero max. di provider SIP attivi	8	8	8	8	8

	X1	X3R/X3W	X5R/X5W	X8	S
ISDN S_0 (BRI)	4	20	52	128	-
	Tramite scheda madre	X3R: 2* STLSX4R X3W: 2* STLSX4	X5R: 6* STLSX4R X5W: 6* STLSX4	Limite SW, ovvero indipendentemente dal numero di moduli STDM3	
ISDN S_{2M} (PRI)	-	30	30	120	-
			1* TS2	3* DIUT3	
Max. numero di canali (ITSP SIP-Q, nativo SIP, linee TDM, MEB)	250	250	250	250	250
Utenti					
ISDN	4	20	52	128	-
	Tramite scheda madre	X3R: 2* STLSX4R X3W: 2* STLSX4	X5R: 6* STLSX4R X5W: 6* STLSX4	8* STMD3	
Analogico	4	20	52/68	384	-
	Tramite scheda madre	X3R: 2* SLAV8R X3W: 1* SLAV16	X5R: 6* SLAV8R X5W: 4* SLAV16	16 * SLMA	
Digitale ($U_{P0/E}$)	8	24	56	384	-
	Tramite scheda madre	2* SLU8(R)	6* SLU8(R)	16* = SLMO2	
Utente IP	20[1]	500	500	500	2000 (max. 500 utenti SIP)
Cordless/DECT(CMI)	16	32	32/64	250	-
	1-7 stazioni base tramite scheda madre	1-7 stazioni base tramite scheda madre + 8-15 tramite SLUN	1-7 stazioni base tramite scheda madre + 8-15 tramite SLUN	4* SLMUC	
Massimo numero di utenti	30[1]	500	500	500	2000
Comunicazione unificata (UC Smart)					
UC Smart VoiceMail (Smart VM)	30	500/320[2]	500/320[2]	500/320[2]	1500
Numero max. di client UC Smart attivi contemporaneamente (Somma di myPortal to go, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF e client WSI di terzi)	30	250/50[2]	250/50[2]	250/50[2]	250
OpenScape Business Attendant	8	8	8	8	8

	X1	X3R/X3W	X5R/X5W	X8	S
OpenScape Business BLF	30	250	250	250	250
	Max. 350 tasti BLF	Max. 350 tasti BLF	Max. 350 tasti BLF	Max. 350 tasti BLF	Max. 350 tasti BLF
Massimo numero di utenti mobili	30	250/50[2]	250/50[2]	250/50[2]	250
Numero di utenti Mobility Entry	30	150	150	150	250
myPortal to go	30	250/50[2]	250/50[2]	250/50[2]	250
myPortal for Teams	-	-	-	-	250
Numero max. canali per conferenze UC	30	30	30	30	60
Comunicazione unificata (UC Suite)					
Casella vocale UC Suite	-	500	500	500	1500
Numero max. di client UC Suite attivi contemporaneamente (Somma di myPortal for Desktop, myPortal for Outlook, myAttendant, myAgent)	-	500/150[3]	500/150[3]	500/150[3]	1500
Max. numero di altri client attivi contemporaneamente (Somma di myPortal to go, myPortal for Teams, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF, client WSI di terzi)	-	-	-	-	500
myPortal for Desktop	-	500/150[3]	500/150[3]	500/150[3]	1500
myPortal for Outlook	-	500/150[3]	500/150[3]	500/150[3]	1500
myAttendant	-	20	20	20	20
OpenScape Business Attendant	8	8	8	8	8
OpenScape Business BLF	30	250	250	250	500
	Max. 350 tasti BLF	Max. 350 tasti BLF	Max. 350 tasti BLF	Max. 350 tasti BLF	Max. 350 tasti BLF
myAgent	-	192 configurabili / 64 attivi in parallelo	192 configurabili / 64 attivi in parallelo	192 configurabili / 64 attivi in parallelo	192 configurabili / 64 attivi in parallelo
Massimo numero di utenti mobili	-	250/150[3]	250/150[3]	250/150[3]	250
Numero di utenti Mobility Entry	-	150	150	150	250
myPortal to go	-	250/100[3]	250/100[3]	250/100[3]	250
myPortal for Teams	-	-	-	-	250
myReports	-	1	1	1	1
Numero max. di canali fax simultanei	-	8	8	8	8

	X1	X3R/X3W	X5R/X5W	X8	S
Numero max utenti fax	-	500/150[3]	500/150[3]	500/150[3]	1500
Numero max. canali per conferenze UC	-	20	20	20	60
Comunicazione unificata (CRM, collegamento database)					
Application Launcher	30 configurabili/30 attivi in parallelo	500 configurabili/50 attivi in parallelo	500 configurabili/50 attivi in parallelo	500 configurabili/50 attivi in parallelo	500
Utente TAPI 120/170 (tramite CSTA, richiesto UC Booster Server/UC Booster Card)	-	500/150[3]	500/150[3]	500/150[3]	1500
Utente TAPI 120 (in modalità UC Smart tramite scheda madre senza CSTA)	30	30	30	30	-
Directory Service Connector (richiesti UC Booster Card/ Server)	-	4	4	4	4

Per una descrizione dettagliata dei livelli di espansione e dei limiti di capacità, vedere anche Limiti di configurazione e capacità.

Connessione in rete con funzionalità UC di OpenScape Business

OpenScape Business offre diverse possibilità di connessione in rete con funzionalità di comunicazione unificata:

- Estese funzionalità voce e UC tra i diversi OpenScape Business X (UC Booster Card/Server richiesti per connessione di rete UC) e OpenScape Business S
- con diversi edifici all'interno dell'area aziendale
- con sedi distribuite
- Amministrazione centralizzata comprensiva delle licenze (HiPath 5000 RSM non è più necessario)
- Connessione di rete per servizi voce in OpenScape Enterprise in preparazione

Per i collegamenti voce sono supportati fino a 32 nodi. Per i collegamenti in rete UC sono supportati un massimo di 8 nodi e fino a 1000 utenti (1500 utenti con OpenScape Business S). Oltre a ciò, è possibile ottenere release specifiche per un progetto.

Per una descrizione dettagliata degli scenari di collegamento, vedere Limiti di configurazione e capacità.

1 Numero totale max. di utenti IP e DeskShare = 20 (limitazione tramite configurazione) - max. somma di utenti IP, DeskShare, analogici e digitali = 30 (limitazione tramite licenza)
2 1° valore: configurazione massima con UC Booster Server o UC Booster Card / 2° valore: configurazione massima con scheda madre
3 1° valore: configurazione massima con UC Booster Server / 2° valore: configurazione massima con UC Booster Card

3.3.2 Modelli hardware UC

I sistemi di comunicazione OpenScape Business X offrono un alto grado di flessibilità in termini di servizi disponibili e struttura. A seconda del modello OpenScape Business X, sono supportati fino a 500 utenti di tipo IP, digitali (ISDN), analogici (a/b) e cordless (DECT), oltre a collegamenti alla rete pubblica tramite ITSP (SIP), ISDN (BRI e PRI), CAS, analogico e IP onboard (disponibili sulla scheda madre).

- OpenScape Business X1W

  Sistema di comunicazione in alloggiamento a parete, per montaggio a parete.
- OpenScape Business X1R

  Il sistema di comunicazione montato in un rack da 19" all'interno di un armadio da 19" può essere liberamente posizionabile (unità a scrivania) o montato a parete.
- OpenScape Business X3W

  Sistema di comunicazione in alloggiamento a parete, per montaggio a parete.
- OpenScape Business X3R

  Il sistema di comunicazione montato in un rack da 19" all'interno di un armadio da 19" può essere liberamente posizionabile (unità a scrivania) o montato a parete.
- OpenScape Business X5 W

  Sistema di comunicazione in alloggiamento a parete, per montaggio a parete.
- OpenScape Business X5R

  Il sistema di comunicazione montato in un rack da 19" all'interno di un armadio da 19" può essere liberamente posizionabile (unità a scrivania) o montato a parete.
- OpenScape Business X8

  Il sistema di comunicazione modulare può essere utilizzato come sistema a un box (cabinet di base) o come sistema a due box (cabinet di base + box di espansione). Il sistema di comunicazione può essere autonomo o installato in un armadio da 19’’.



Figura 5: Piattaforme hardware

3.3.3 Hardware UC Booster

Hardware UC Booster per OpenScape Business X.

- OpenScape Business UC Booster Card

  Board for OpenScape Business X se la UC Suite verrà utilizzata come soluzione UC con un massimo di 150 utenti UC.
- OpenScape Business UC Booster Server

  Server UC Booster esterno (Linux) per OpenScape Business X se la UC Suite verrà utilizzata come soluzione UC con un massimo di 500 utenti UC.

  Su UC Booster Server viene utilizzato SLES 12 SP5 a 64 bit o SLES 15 SP6 a 64 bit. UC Booster Server può essere eseguito anche in un ambiente virtuale con VMware vSphere.

  Quando si utilizza UC Booster Server, la scheda UC Booster non è necessaria.
- Scheda Booster con canali voce OpenScape Business

  Due moduli opzionali per l'estensione di OpenScape Business X con canali DSP aggiuntivi (ad esempio, per connessioni vocali simultanee con transizioni IP/TDM).

  Sulla scheda madre sono presenti otto canali DSP. Scheda Booster con canali voce OCCB/1 fornisce altri 48 canali DSP, mentre la scheda Booster con canali voce OCCB/3 offre fino a 128 canali DSP.

3.3.4 Modelli software UC (soft switch)

Soluzione software UC all-in-one basata su server che supporta fino a 1000 stazioni IP con connessioni alla rete pubblica tramite ITSP (SIP).

Indipendentemente dalla piattaforma utilizzata, OpenScape Business S può essere installato su un server Linux. Come sistemi operativi vengono utilizzati SLES 12 SP5 a 64 bit o SLES 15 SP6 a 64 bit. OpenScape Business S può essere eseguito anche in un ambiente virtuale con VMware vSphere. Se sono necessarie interfacce TDM per la connessione a telefoni o trunk TDM, i sistemi OpenScape Business X possono essere utilizzati come gateway.

3.3.5 Struttura e condizioni ambientali

	X1	X1R	X3W	X3R	X5W	X5R	X8
Struttura	Sistema da parete	Rack	Sistema da parete	Rack	Sistema da parete	Rack	Sistema standa (anche con inserimento in rack)
Dimensioni (AxLxP in mm)	470x370x80	450x460x130	450x460x130	89x440x380 (2U)	450x460x200	155x440x380 (3,5U)	490x440x430
Peso	circa 2,8 kg	circa 6 kg	circa 6 kg	circa 6 kg	circa 8 kg	circa 8 kg	circa 34 kg (completament riempito)

	X1	X1R	X3W	X3R	X5W	X5R	X8
Colori alloggiamento	Bianco	Nero	Bianco	Verde/grigio scuro	Bianco	Verde/grigio scuro	Verde/grigio scuro
Alimentazione	Per impostazione predefinita, i modelli sono dotati di connessione all'alimentazione di rete • Tensione nominale di ingresso (AC): Da 100 a 240 V • Frequenza nominale: 50/60 Hz • Alimentazione della batteria (DC): -48 V						
Assorbimento potenza	Seconda della piattaforma hardware e dell'espansione						
Condizioni ambientali	• Condizioni operative: Da +5 a +40 °C (da 41 a 104 °F) • Umidità: dal 5 all'85%						

3.3.6 Telefoni supportati

OpenScape Business X consente l'esecuzione di telefonate tramite IP/HFA (HiPath Feature Access), SIP, TDM, a/b, cordless/DECT e WLAN. I telefoni IP/HFA, SIP e wireless possono essere collegati direttamente al sistema OpenScape Business S.

Telefoni OpenStage (IP/HFA, SIP e T)	• OpenStage 5/10/15/20/30/40/60/80
OpenScape Desk Phone (IP/HFA, SIP e T)	• OpenScape Desk Phone IP 35G/55G/35G Eco • OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA e SIP 200/400/205/405 TDM • OpenScape Desk Phone CP 110/210/410/710 HFA e SIP
Moduli aggiuntivi	• Modulo OpenStage Key solo per OpenStage 15/40/60 • OpenStage BLF 40 (Busy Lamp Field) solo per OpenStage 40 e OpenStage 30 T • OpenScape Key Module 400/600, solo per CP 400/600/600E/700/700X • Modulo OpenScape Key 410/710, solo per CP 710
OpenScape Business Cordless	• OpenStage M3 • OpenScape DECT Phone S6/SL6/R6
Client PC (HFA), SIP)	• OpenScape Persone Edition (con SIP incl. video)
Telefoni SIP (UC Suite/ adattatore AP	• Telefoni SIP con supporto per RFC 3725 • Mediatrix 4102S (per la connessione di 2 telefoni o dispositivi fax analogici)

Telefoni WLAN	• OpenStage WL3 professional • OpenScape WLAN Phone WL4/WL4 Plus
Telefoni analogici e ISDN	• Telefoni analogici (a/b) • Telefoni digitali ISDN (S_0)

Sono supportati i dispositivi precedenti (ad esempio, optiPoint 410/420/500, Gigaset M2/SL3/S4/SL4/S5 e optiPoint WL2 SIP). I dispositivi Optiset E non possono essere utilizzati.

Funzioni e configurazione dei telefoni SIP

OpenScape Business offre una vasta gamma di funzionalità per la comunicazione vocale per i telefoni OpenStage HFA. Molte funzioni sono disponibili anche per i telefoni SIP standard.

Per una panoramica delle funzioni supportate con i telefoni OpenStage SIP e per ulteriori informazioni, consultare il sito Unify Wiki all'indirizzo

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

Per il controllo delle chiamate vocali per i telefoni SIP via CTI (3PCC) con OpenScape Business X3/X5/X8 è necessaria una UC Booster Card o un UC Booster Server.

Il controllo delle chiamate vocali per i telefoni SIP tramite client UC Smart è supportato per OpenScape Business X3/X5 Rack con UC Booster Card.

Utilizzando le funzioni DLI, è possibile gestire centralmente e implementare il software nei telefoni OpenScape Desk Phone (SIP).

Concetti correlati

CSTA alla pagina 1157

3.4 Altre informazioni

Ulteriori informazioni sono disponibili in Internet e nella extranet. Per le limitazioni e le ultime modifiche, consultare le release note.

3.4.1 Lingue supportate

I diversi componenti software (client e WBM), la documentazione e la Guida in linea sono disponibili in diverse lingue.

Le seguenti lingue sono state predisposte nell'ambito dell'introduzione sul mercato nei diversi paesi.

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
Client UC Smart										
myPortal @work (Client)	X	X	X	X	X	X	X	-	-	-
myPortal @work (Manuale dell'utente)	X	X	X	X	X	X	X	-	-	-
myPortal to go (Client)	X	X	X	X	X	X	X	X	X	–
myPortal to go (Istruzioni per l'uso/Guida in linea)	X	X	X	X	X	X	X	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	–	X	–	X
TUI (Guida rapida all'uso)	X	X	–	–	–	–	–	–	–	–
OpenScape Business Attendant / BLF (Client)	X	X	–	–	–	X	–	–	–	–
OpenScape Business Attendant / BLF (Manuale dell'utente)	X	X	–	–	–	X	–	–	–	–
Client UC Suite										
myPortal @work (Client)	X	X	X	X	X	X	X	-	-	-
myPortal @work (Manuale dell'utente)	X	X	X	X	X	X	X	-	-	-
myPortal for Desktop (Client)	X	X	X	X	X	X	X	X	X	X
myPortal for Desktop (Manuale dell'utente/ Guida in linea)	X	X	X	X	X	X	X	–	–	–
myPortal for Outlook (Client)	X	X	X	X	X	X	X	X	X	X
myPortal for Outlook (Manuale dell'utente/ Guida in linea)	X	X	X	X	X	X	X	–	–	–
myPortal to go (Client)	X	X	X	X	X	X	X	X	X	–
myPortal to go (Istruzioni per l'uso/Guida in linea)	X	X	X	X	X	X	X	–	–	–
myAttendant (Client)	X	X	X	X	X	X	X	X	X	X
myAttendant (Manuale dell'utente/Guida in linea)	X	X	X	X	X	X	X	–	–	–
myAgent (Client)	X	X	X	X	X	X	X	X	X	X
myAgent (Manuale dell'utente/Guida in linea)	X	X	X	X	X	X	X	–	–	–
myReports (Client)	X	X	–	X	X	X	X	–	–	–
myReports (Manuale dell'utente/Guida in linea)	X	X	–	X	X	X	X	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	X	X	X	X

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
TUI (Guida rapida all'uso)	X	X	–	–	–	–	–	–	–	–
Amministrazione										
OpenScape Business Assistant (WBM)	X	X	–	–	–	–	–	–	–	–
OpenScape Business Assistant (Documentazione per l'amministratore/Guida in linea)	X	X (nessuno nl)	–	–	–	–	–	–	–	–
Manager E	X	X	X	X	X	X	X	–	–	–
Manager E (Documentazione per l'amministratore/Online/Guida)	X	X	–	–	X	–	–	–	–	–

Inoltre, la TUI di UC Smart è disponibile anche nelle lingue belga (fiammingo) e slovena.

Suggerimento: Per l'uso dell'interfaccia utente in lingua russa o cinese, è necessario il sistema operativo Windows in versione russa o cinese.

Le abbreviazioni utilizzate nella tabella rappresentano i seguenti codici lingua (ISO 639-1):

- de = Tedesco
- en = Inglese
- cs = Ceco
- da = Danese
- es = Spagnolo
- fi = Finlandese
- fr = Francese
- hr = Croato
- hu = Ungherese
- it = Italiano
- nl = Olandese
- no = Norvegese
- pl = Polacco
- pt = Portoghese
- ru = Russo
- sv = Svedese
- tr = Turco
- zh = Cinese

3.4.2 Collegamenti Internet

Per ulteriori informazioni e aggiornamenti, consultare la pagina iniziale di Unify, nel nostro sito Expert-Wiki e nel portale partner Unify.

Collegamenti Internet

- Pagina iniziale di Unify:

  `http://www.unify.com`
- Wiki-esperti per telefoni, sistemi di comunicazione e comunicazione unificata:

  `http://wiki.unify.com`
- Portale partner (è richiesta la registrazione):

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

  o

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

4 Principi di base per l'amministrazione

L'amministrazione del sistema di comunicazione viene eseguita tramite OpenScape Business Assistant.

4.1 OpenScape Business Assistant (WBM)

OpenScape Business Assistant è basato sul Web e viene pertanto chiamato anche Web Based Management (WBM).

L'entità dei compiti amministrativi disponiblii dipende dal profilo di amministratore utilizzato.

In ogni pagina del WBM è presente una guida online.

4.1.1 Requisiti per il WBM

Per poter utilizzare il WBM il PC di amministrazione necessita di software adeguato.

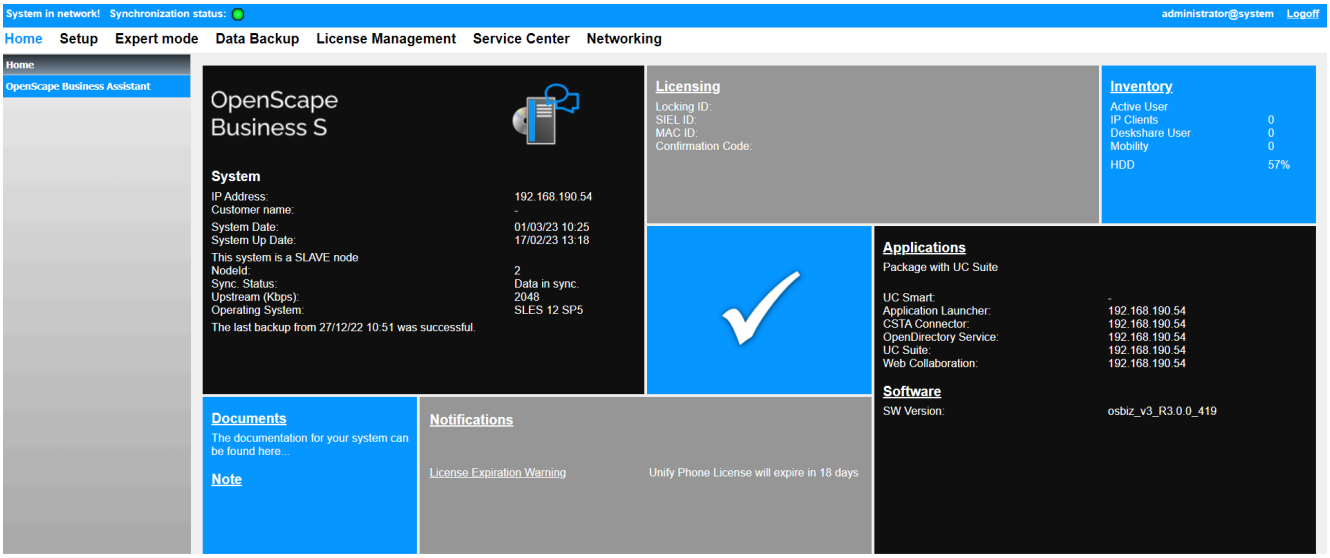
Browser Web supportati:

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

4.1.2 Pagina iniziale di WBM

La pagina iniziale di WBM mostra le informazioni importanti sul sistema suddivise in diverse aree (riquadri). Sono inoltre disponibili informazioni e note su errori di sistema, eventi e operazioni.

Le informazioni di sistema indicate dipendono dal profilo di amministratore utilizzato. Le didascalie sottolineate nelle singole aree sono selezionabili e si riferiscono al relativo tema in WBM.



Vengono visualizzate le seguenti informazioni:

- Area: **Stato** (centrale)
  - Segno di spunta bianco su sfondo blu: il sistema di comunicazione è completamente funzionale - i messaggi sottolineati in rosso in altri campi si riferiscono ad azioni che devono essere eseguite.
  - Punto esclamativo bianco su sfondo rosso: il sistema di comunicazione non è completamente funzionale e richiede l'intervento dell'amministratore - i messaggi sottolineati in rosso in altri campi si riferiscono a errori di sistema o eventi che devono essere risolti.
- Area: **Sistema**
  - Brand
  - Indirizzo IP del sistema di comunicazione
  - Data e ora correnti
  - Data e ora dell'ultimo riavvio del sistema
  - Istruzioni sull'uso in un sistema di reti (il sistema è master o slave, visualizzazione dell'ID del nodo)
  - Stato sincronizzazione
  - Larghezza di banda upstream in kbps
  - Stato di salute SDHC
  - Istruzioni per il salvataggio e il ripristino
  - Stato Booster Card
- Area: **Documenti**
  - Collegamento alla documentazione
- Area: **Avvisi**
  - Varie notifiche sul sistema
- Area: **Nota**
  - Mostra le ultime informazioni inserite da un amministratore. Facendo clic sul titolo sottolineato si apre una finestra di testo in cui sono visualizzate tutte le informazioni ed è possibile inserire altre informazioni.

    I dati del campo Nota non sono inclusi nel set di backup del sistema. Di conseguenza, in occasione del ripristino di un set di backup, tali dati non verranno ripristinati.

- Area: **Concessione della licenza**
  - Locking ID per l'attivazione della licenza
  - ID SIEL per l'attivazione della licenza
  - Nota sullo stato della licenza che indica se il sistema è in modalità di licenza "Permanente" o di "Pagamento al consumo".
- Area: **Inventario**
  - Tipo e numero di utenti attivi
  - Numero di ITSP attivati e un collegamento alla finestra di dialogo di stato ITSP nel Centro assistenza degli utenti attivi
- Area: **Applicazioni** e software

  Applicazioni:
  - Pacchetto applicativo utilizzato (UC Smart o UC Suite) e relativi componenti, compresi gli indirizzi IP del server utilizzato.
  - Indicazione della presenza o meno di una UC Booster Card.

  Software:
  - Versione del software del sistema di comunicazione installata
  - Indicazione della presenza o meno di una UC Booster Card. Inoltre se è raggiungibile tramite un indirizzo IP, viene visualizzata la versione del software UC Booster Card installata.

    La UC Booster Card e il sistema di comunicazione devono essere sempre della stessa versione del software.
  - Data di scadenza del supporto software di 3 anni.

    Trascorsa la data di scadenza, viene visualizzato il messaggio: "La licenza di supporto software è scaduta, aggiornarla".
  - Nota sulla nuova versione software

4.1.3 Introduzione su WBM

Il WBM è l'applicazione basata sul Web per l'amministrazione del sistema.

Lingua dell'interfaccia utente

Accedendo al sistema è possibile selezionare una delle seguenti lingue:

- Tedesco
- Inglese
- Francese
- Italiano
- Olandese (Guida in linea disponibile solo in inglese)
- Portoghese
- Spagnolo

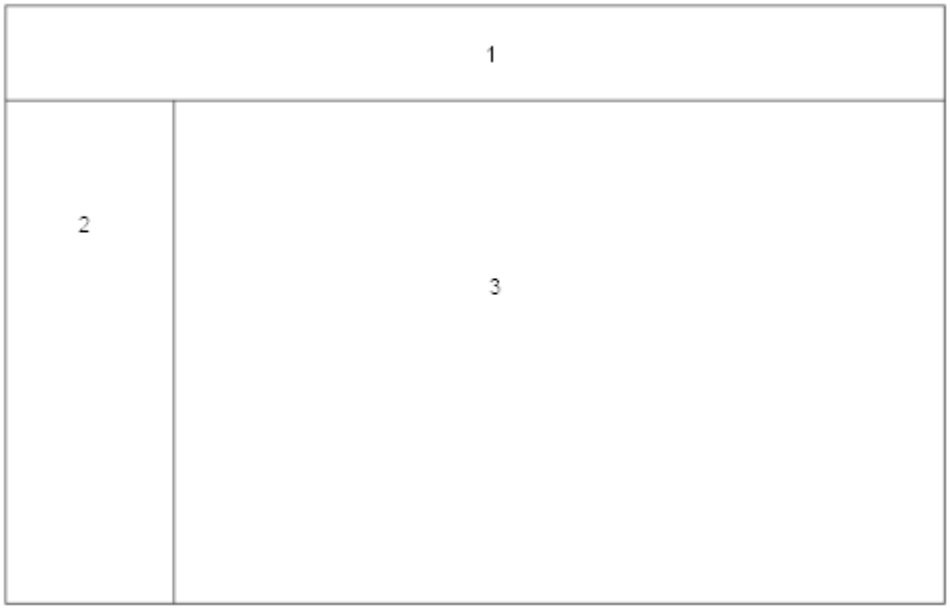
Classificazione delle interfacce utente descritte

Tutte le attività eseguibili con procedura guidata sono descritte solo in relazione alla corrispondente procedura guidata.

Le altre attività che possono essere eseguite in Modalità esperti, sono descritte solo in relazione a tale modalità.

Per Manager E sono descritte solo le attività rimanenti.

Elementi dell'interfaccia utente



- Barra di navigazione (1)

  La barra di navigazione è la barra principale che mostra sempre gli stessi collegamenti ai centri attività principali, vale a dire **Home**, **Amministratori**, **Configurazione**, **Modalità esperti**, **Backup dei dati**, **Gestione delle licenze** e **Centro assistenza**, nonché il nome utente corrente e il link **Disconnetti**. Facendo clic su un centro funzione, nell'area di navigazione si apre la relativa struttura ad albero e nell'area di lavoro la pagina iniziale del centro funzione.
- Area di navigazione (2)

  L'area di navigazione rappresenta un altro importante elemento e contiene la struttura ad albero di navigazione comprendente le funzioni del menu relative al centro funzione selezionato. Il nome del centro attività selezionato viene visualizzato nella parte superiore della struttura di navigazione con i gruppi di menu espandibili e comprimibili e le voci di menu sottostanti. Le opzioni contenute in ogni menu dipendono dalle diverse impostazioni. Facendo clic su un'opzione del menu, viene visualizzata la relativa pagina nell'area di lavoro.
- Area di lavoro (3)

  L'area di lavoro consente di eseguire tutte le operazioni di amministrazione. Normalmente l'area di lavoro si apre in una finestra separata. Il numero e la gamma delle informazioni e delle azioni visualizzate dipende dall'opzione selezionata nella struttura di navigazione. In Modalità esperti, nel collegamento all'area di lavoro viene visualizzata a sinistra della struttura dei menu.

Navigazione nella struttura dei menu

La struttura a menu consente la navigazione nella Modalità esperti del WBM. La struttura a menu contiene le cartelle (ad esempio **Manutenzione**) con altri elementi (quali **Riavvio/Ricarica**).

Per navigare nella struttura dei menu, fare clic su una cartella (per espandere o comprimere alternativamente la relativa struttura).

Disconnessione automatica a tempo

L'utente registrato verrà disconnesso automaticamente dal sistema dopo 30 minuti trascorsi senza eseguire alcuna azione. Per eseguire ulteriori azioni con WBM sarà necessario accedere nuovamente. Per motivi di sicurezza, dopo una pausa è opportuno ricaricare la pagina prima di apportare modifiche, per evitare che queste vadano perse a causa di una disconnessione automatica.

4.1.3.1 Come accedere al WBM

Prerequisiti

È necessario avere accesso alle proprie credenziali utente (nome utente e password). In caso contrario, rivolgersi all'amministratore.

TLS 1.2 è abilitato nelle impostazioni del browser web.

Passo a passo

1) Aprire la pagina di accesso nel proprio browser web inserendo il seguente indirizzo: `https://<indirizzo IP del sistema di comunicazione>`. L'indirizzo IP predefinito è 192.168.1.2.
2) Fare clic sul codice della lingua in alto a destra e selezionare dal menu la lingua in cui visualizzare l'interfaccia utente del WBM. La pagina di accesso verrà visualizzata nella lingua selezionata.
3) Inserire il nome dell'utente in **Accesso** nel primo campo. "@system" viene aggiunto automaticamente all'uscita del campo.
4) Inserire la propria password nel secondo campo di **Accesso**. Osservare l'uso del caso e lo stato del tasto **Num**. La password è indicata con un asterisco (*).
5) Fare clic su **Accedi**.

Se si immettono credenziali non valide, dopo il terzo tentativo di accesso non riuscito viene visualizzato un messaggio che informa che l'account è bloccato per 5 minuti. È possibile riprovare ad accedere dopo questo periodo di tempo.

Per ogni ulteriore tentativo di accesso non riuscito, questo periodo di tempo viene raddoppiato, raggiungendo i 160 minuti all'ottavo tentativo fallito. Per ogni successivo tentativo non riuscito, il tempo di blocco dell'account è di 160 minuti.

4.1.3.2 Come disconnettersi dal WBM

Procedura

- Fare clic in alto a destra su **Disconnetti**.

4.1.4 Gestione utenti WBM

È possibile configurare e gestire fino a 16 amministratori per il WBM (gestione basata sul web). A ogni amministratore viene assegnato un profilo che specifica

l'ambito della sua autorizzazione. È anche possibile modificare la password di un amministratore di Manager E.

Gli utenti di WBM sono anche chiamati amministratori.

L'amministratore predefinito è `administrator@system` con la password predefinita `administrator` e con profilo **Avanzato**. La password deve essere modificata al primo accesso. La password di un amministratore deve essere composta da almeno 8 caratteri e da un massimo di 128 caratteri, di cui almeno un carattere deve essere una cifra. Inoltre, per una password sicura, è necessario includere almeno una lettera maiuscola, una lettera minuscola e un carattere speciale.

Nota: L'accesso amministrativo (compreso il ruolo di utente amministratore) viene registrato nel file di registro dei messaggi/ syslog. È possibile accedervi tramite il menu **Diagnostica** > **Traccia**.

Profili

Il WBM supporta quattro profili con diverse classi di servizio (autorizzazioni) per amministratori con diversi livelli di competenza tecnica e compiti.

Per evitare che un utente malintenzionato possa accedere tramite ISDN e modificare la password predefinita al primo accesso, è obbligatorio che l'utente modifichi la password tramite Manager E come passaggio di installazione.

Nota: Una password composta da 5 caratteri (*****) non sarà accettata dal sistema per motivi di sicurezza.

Tabella 1: Profilo Classi di servizio

Profilo	Abilitazione
Basic Conoscenza di base della configurazione del sistema	Informazioni sul sistema nella pagina iniziale
	Procedura guidata **Programmazione dei tasti**
	Procedura guidata **Rubrica telefonica/Composizione rapida**
	Procedura guidata **Registrazione dei dettagli delle chiamate**
	Procedura guidata **Musica di attesa/Annunci**
	Procedura guidata **Nome e versione della stazione**
	Accesso ad **Amministratori** (solo per modificare le proprie password)
	Accesso a **Gestione licenze** > **Informazioni sulle licenze**
	Accesso a **Centro servizi** > **Documenti**
	Accesso a **Centro servizi** > **Software**

Profilo	Abilitazione
Avanzato Buona conoscenza della configurazione del sistema	Come per il profilo **Base**, con in più: Accesso a tutte le procedure guidate (ad eccezione delle procedure guidate **Installazione di base**, **UC Suite** e **UC Smart**) **Nota:** L'accesso a tutte le procedure guidate non è supportato nei sistemi OpenScape Business S. Accesso ad **Amministratori** (solo per modificare le proprie password) Accesso a **Backup e ripristino** Accesso a **Gestione delle licenze** (escluse la registrazione, l'attivazione della licenza e le impostazioni) Accesso a **Centro servizi** > **Inventario** Accesso a **Centro servizi** > **Riavvio/Ricaricamento** (senza ricaricamento) Accesso a **Centro servizi** > **Diagnostica** > **Stato** Accesso a **Centro servizi** > **Diagnostica** > **Visualizzatore eventi**
Avanzato Utenti formati	Come per il profilo **Avanzato**, con in più: Accesso a tutte le procedure guidate Accesso ad **Amministratori** (solo per modificare le proprie password) Accesso alla **Gestione delle licenze** completa Accesso al **Centro servizi** completo Accesso alla **Connettività di rete**
Esperto Tecnici di assistenza formati	Come per il profilo **Avanzato**, con in più: Accesso ad **Amministratori** (completo) Accesso alla **Modalità Esperto**

Tabella 2: Gestione dei profili

Profilo	Manutenzione
Basic Conoscenza di base della configurazione del sistema	Può cambiare la propria password. Non vede altri amministratori configurati se non se stesso.

Profilo	Manutenzione
Avanzato Buona conoscenza della configurazione del sistema	Può cambiare la propria password. Non vede altri amministratori configurati se non se stesso.
Avanzato Utenti formati	Può cambiare la propria password. Non vede altri amministratori configurati se non se stesso.
Esperto Tecnici di assistenza formati	Può modificare la propria password e i nomi utente e le password degli altri amministratori. Visualizza tutti gli amministratori configurati. Può aggiungere, modificare e rimuovere gli amministratori.

Nota: Finché non esiste un amministratore con il profilo **Esperto**, gli amministratori con il profilo **Avanzato** possono aggiungere, modificare e rimuovere altri amministratori. Non appena esiste un amministratore con il profilo **Esperto**, solo gli amministratori con il profilo **Esperto** possono aggiungere, modificare e rimuovere altri amministratori.

Gestione degli amministratori nella rete Internet

La gestione diretta degli amministratori è possibile solo nel WBM del nodo master. Il menu **Amministratore** non viene visualizzato sui nodi slave. Tutte le configurazioni dell'amministratore vengono trasmesse ai nodi slave. È tuttavia possibile richiamare il WBM del nodo master dall'interno del WBM del nodo slave tramite la Node View. Qui viene visualizzato il menu **Amministratore**, che può essere visualizzato solo dagli amministratori.

Nota: L'aggiunta/modifica/cancellazione degli utenti non è possibile tramite l'accesso WBM in modalità slave (ma solo tramite l'accesso WBM in modalità master).

Amministrazione delle password in Manager E

L'amministratore può modificare (ma non creare un nuovo ruolo utente) la password degli utenti esistenti che possono accedere al sistema incorporato tramite Manager E.

All'utente verrà richiesto di cambiare la password solo per gli utenti esistenti e non sarà in grado di cambiare il gruppo dell'utente e le opzioni come Creato, Ultimo utilizzo non sono visualizzabili. Si tratta di una funzione di sicurezza e quindi non fornisce l'intera schermata di amministrazione del Manager E.

4.1.4.1 Come aggiungere amministratori

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**. (Se non esiste ancora alcun amministratore con il profilo **Expert**).

Si è connessi al WBM con il profilo **Expert**. (Se esiste già un amministratore con il profilo **Expert**).

Passo a passo

1) Nella barra di navigazione fare clic su **Amministratori**.
2) Fare clic su **Aggiungi...**.
3) Inserire i seguenti dati: **Nome utente**, **Nome**, **Cognome**, **Password**, **Ripeti password**.
4) Nell'elenco a discesa **Funzione utente**, selezionare il profilo utente desiderato.
5) Fare clic su **OK & Avanti**.

4.1.4.2 Come modificare amministratori

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Amministratori**.
2) Nell'**Elenco amministratori**, selezionare la casella di controllo dell'amministratore desiderato.
3) Fare clic su **Modifica**.
4) Modificare i dati (nome utente, nome e cognome, password e ruolo utente).
5) Fare clic su **OK & Avanti**.

4.1.4.3 Come modificare la propria password amministratore

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Amministratori**.
2) Nel campo **Password** e **Ripeti password** inserire la nuova password.

   Nota: Per motivi di sicurezza, una password costituita da 5 asterischi (*****), non sarà accettata dal sistema.

3) Fare clic su **OK & Avanti**.

Concetti correlati

Salvataggio immediato alla pagina 1243

4.1.4.4 Come cancellare amministratori

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Amministratori**.
2) Nell'**Elenco amministratori**, selezionare la casella di controllo dell'amministratore desiderato.
3) Fare clic su **Cancella...**.

4.1.4.5 Come modificare una password di amministratore Manager E

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Amministratori**.
2) Fare clic su **Elenco amministratori** Manager E.
3) Modificare i dati (Account utente, Nuova password, Conferma password) come necessario.
4) Fare clic su **Salva**.

Nota: Tale password deve essere composta da almeno 5 cifre. L'uso di lettere o altri caratteri non è consentito. Inoltre, le vecchie password non possono essere riutilizzate.

4.1.5 Procedure guidate

Le procedure guidate facilitano l'installazione e la configurazione del sistema. Per l'amministratore di un cliente (profilo **Basic**) è disponibile una selezione di procedure guidate. Invece per un amministratore con conoscenze tecniche o per un tecnico dell'assistenza qualificato (profilo **Advanced**) sono disponibili tutte le procedure guidate.

Le procedure guidate disponibili dipendono dalla configurazione del sistema (UC Smart o UC Suite). Le procedure guidate possono essere costituite da più pagine consecutive. OK & Avanti consente di salvare le modifiche apportate e porta alla pagina seguente della procedura guidata. Le modifiche salvate con OK & Avanti non possono più essere annullate. Se non sono state salvate modifiche, premendo **Annulla** si interrompe la procedura guidata. Facendo clic sull'icona a forma di **X** nell'angolo in alto a destra della finestra della procedura guidata, si chiude la procedura guidata mantenendo le modifiche precedentemente apportate premendo OK & Avanti.

4.1.5.1 Procedure guidate – Installazione di base

Le procedure guidate in **Installazione di base** consentono di eseguire semplici funzioni di configurazione per l'installazione di base.

Sono disponibili le seguenti procedure guidate in **Installazione di base**:

- **Prima installazione**

  Utilizzo singolo al momento dell'impostazione iniziale. Inizializzazione paese, indirizzo IP del sistema e server DHCP.
- **Installazione di base**

  Impostazione di base del sistema con dati utente, linee, parametri di rete, Internet.
- **Concessione della licenza**

  Attivare licenze on-line tramite il server licenze.
- **Configurazione di rete**

  Impostazione del sistema come parte di una rete.
- **Risparmio energia**

  Impostazione e attivazione del risparmio energetico

4.1.5.2 Procedure guidate – Rete / Internet

Le procedure guidate in **Rete/Internet** consentono di eseguire semplici configurazioni di rete e dell'accesso a Internet.

In **Rete / Internet** sono disponibili le seguenti procedure guidate:

- **Configurazione di rete**

  Impostare DHCP, routing IP e server DNS.
- **Configurazione Internet**

  Accedere ai parametri dei dati del provider Internet, ad es., account utente e password.
- **Configurazione VPN**

  Connessione degli ambienti di lavoro tramite Internet.

4.1.5.3 Procedure guidate - Telefoni/Abbonati

Le procedure guidate in **Telefoni/Abbonati** consentono di configurare in modo semplice telefoni e abbonati.

In **Telefoni/Abbonati** sono disponibili le seguenti procedure guidate:

- **Dispositivi IP**

  Consente di configurare telefoni IP e SIP specifici del sistema, numeri di chiamata FAX e adattatori IP/analogici.
- **Dispositivi UP0**

  Consente di configurare i telefoni UP0, i numeri di chiamata FAX.
- **Telefoni DECT**

  Consente di configurare il telefono DECT, i numeri di chiamata FAX.

- **Mitel SIP DECT**

  Configurazione dei dispositivi Mitel SIP DECT RFP.
- **Dispositivi ISDN**

  Porte ISDN non alimentate per schede/modem ISDN e stazioni S0.
- **Terminali analogici**

  Porte analogiche DTMF e CLIP per fax e telefono.
- **Programmazione dei tasti**

  Programmazione dei nomi e dei tasti funzione per i dispositivi IP specifici del sistema e per i telefoni UP0.

4.1.5.4 Procedure guidate – Telefonia centrale

Le procedure guidate in **Telefonia centrale** consentono di eseguire semplici configurazioni di servizi di telefonia centralizzati.

In **Telefonia centrale** sono disponibili le seguenti procedure guidate:

- **Linea ISDN / analogica / ITSP**

  Allacciamento di più dispositivi (MSN) e numero di sistema per la linea ISDN nonché accesso per le linee urbane analogiche e ITSP.
- **Telefonia Internet**

  Accedere ai parametri del provider di servizi di telefonia Internet (ITSP), ad es. account utente, password, numero di telefono SIP.
- **Rubrica/Selezione breve**

  Impostare le destinazioni centrali di selezione breve per la rubrica interna del sistema.
- **Registrazione dettagli chiamata**

  Impostare parametri di connessione per la registrazione dei dettagli delle chiamate, specifici per applicazioni.
- **Musica su attesa / Annunci**

  Registrare nuove melodie e annunci per la musica su attesa e l’annuncio prima della risposta.
- **Citofono (apriporta)**

  Impostare l’allocazione delle chiamate e l’autorizzazione all’accesso per il telefono di entrata nella connessione analogica dell’utente.
- **SmartVM**

  Configurazione della casella vocale UC Smart (SmartVM).
- **Lista nera per chiamate entranti**

  Definire un elenco di numeri per bloccare i chiamanti indesiderati in modo permanente.
- **Servizio di integrazione Active Directory**

  Impostare Active Directory.

4.1.5.5 Procedure guidate – Telefonia utenti

Le procedure guidate in **Telefonia utenti** supportano semplici funzioni di configurazione di servizi per la telefonia utenti.

Le seguenti procedure guidate sono disponiblii in **Telefonia utenti**:

- **Abilitazione**

  Impostare i gruppi di abilitazione con i numeri esterni che possono essere assegnati all'utente, ad es. numeri di emergenza, numeri consentiti, numeri non consentiti, nonché assegnazione della autorizzazione per il servizio notte.
- **Nome utente e rilascio**

  Modificare i nomi di utenti e gruppi, resettare il codice di blocco per singoli utenti.
- **Chiamata di gruppo / Gruppo di ricerca**

  Impostare le chiamate in entrata per gruppo di utenti (ordine chiamate parallelo, lineare o ciclico).
- **Inoltro di chiamata**

  Impostare le assegnazioni centrali dei numeri utente a livello del sistema e l’inoltro "a tempo" e "su occupato".
- **Risposta per assente**

  Configurare gli utenti in un gruppo di risposta con l’opzione di rispondere alle chiamate reciproche.
- **Configurazione team**

  Impostare gli utenti per cui le chiamate in entrata vengono segnalate in parallelo con l’utente centrale e che possono utilizzare il proprio numero di telefono per rispondere a quelle in uscita.
- **Integrazione con il numero di cellulare**

  Impostare un collegamento tra un numero di cellulare e un utente interno, allo scopo di consentire le chiamate in entrata e in uscita utilizzando un unico numero di telefono (One Number Service).
- **Direttore / Segretaria**

  Impostare un collegamento tra uno o più telefoni di un dirigente e uno o più telefoni del loro assistente, allo scopo di consentire servizi semplificati di trasferta delle chiamate e degli squilli.
- **UCD**

  Impostare una distribuzione delle chiamate automatica e intelligente per un gruppo con utenti selezionati.
- **Posto operatore**

  Impostare gli utenti come numeri di console Posto operatore e il loro comportamento nei casi su occupato, composizione errata e mancata risposta.
- **Profilo apparecchio**

  Assegna utenti a un profilo e importa/esporta i dati del profilo.

4.1.5.6 Procedure guidate – Sicurezza

Le procedure guidate disponibili in **Sicurezza** supportano semplici funzioni di configurazione del firewall.

In **Sicurezza** sono disponibili le seguenti procedure guidate:

- **Firewall**

  Configura l'apertura della porta per limitare il traffico Internet.

4.1.5.7 Procedure guidate – UC Smart (solo con UC Smart)

Le procedure guidate in **UC Smart** facilitano la configurazione della soluzione di comunicazione unificata UC Smart.

Le seguenti procedure guidate sono disponibili in **UC Smart**:

- **UC Smart**

  Impostazioni di base e configurazione utente per UC Smart.

4.1.5.8 Procedure guidate – UC Suite (solo con UC Suite)

Le procedure guidate in UC Suite facilitano la configurazione della soluzione UC **UC Suite**.

In **UC Suite** sono disponibili le seguenti procedure guidate:

- **Rubrica utente**

  Configurazione degli utenti.
- **Reparti**

  Configurazione dei reparti.
- **Gruppi**

  Configurazione di gruppi casella vocale e casella fax.
- **Modelli**

  Configurazione dei modelli SMS.
- **Rubrica esterna**

  Aggiunta manuale di singoli contatti alla rubrica esterna.
- **Config provider esterni**

  Immissione dei dati di accesso dei server Exchange o LDAP.
- **Contact Center**

  Configurazione del Contact Center.
- **Pianificazioni**

  Configurazione delle pianificazioni.
- **Carica file**

  Caricamento di file audio per gli annunci e la musica in attesa.
- **Conferenza in corso**

  Configurazione di chiamate in conferenza.

- **Profili**

  Creazione di profili utente.
- **Intestazione fax**

  Configurazione della riga intestazione fax.

4.1.5.9 Procedure guidate - Rubrica unificata

Le procedure guidate disponibili in **Rubrica unificata** illustrano come eseguire l'importazione e la modifica dei contatti della rubrica.

In **Rubrica unificata** sono disponibili le seguenti procedure guidate:

- **Importa contatti**

  Questa procedura guidata assiste l'utente nell'operazione di importazione dei dati di contatto nella Rubrica globale da CSV.
- **Modifica contatti**

  Aggiungere o modificare voci manualmente nella Rubrica globale.

4.1.5.10 Procedure guidate - Servizi cloud

Le procedure guidate in **Servizi cloud** supportano le funzionalità supportate nel cloud.

In **Servizi cloud** sono disponibili le seguenti procedure guidate:

- **Plug-in client Microsoft Teams**

  Configurare e scaricare il plugin client di myPortal for Teams.
- **Connettività Unify Phone**

  Configurazione delle impostazioni di base per Unify Phone.
- **Istanza utente Unify Phone**

  Configurare l'istanza degli utenti di Unify Phone
- **Servizio Let's Encrypt**

  Configurare il servizio Let's Encrypt
- **CloudLink Service**

  Configura il CloudLink Service
- **Numeri pilota CloudLink**

  Configurare i numeri pilota per CloudLink

4.1.6 Centro assistenza

Il **Centro assistenza** del WBM offre diverse funzioni di manutenzione, avvia l'aggiornamento del software e rende disponibile la documentazione e il software.

4.1.6.1 Centro assistenza – Documenti

Documenti mette a disposizione la documentazione, i modelli CSV e collegamenti a informazioni più approfondite. La documentazione può essere richiamata in formato PDF in tutte le lingue supportate.

A seconda della configurazione del sistema, sono disponibili i seguenti contenuti:

Sommario	UC Smart	UC Suite
Documentazione per l'amministratore (PDF)	-	x
Documentazione per l'utente (PDF)	-	x
Collegamenti (Wiki)	x	x
Modelli (modelli CSV) per l'importazione di dati per • Utenti • Selezione breve del sistema • Rubrica esterna	x	x
Contratto di Licenza con l'utente finale (EULA)	x	x

Concetti correlati

Accounting Tools alla pagina 1223

4.1.6.2 Centro assistenza – Software

In **Software** sono disponibili il software per gli UC client, i driver USB e gli strumenti.

Sono disponibili i seguenti contenuti:

Indice	UC Smart	UC Suite
File di installazione per il software dei client UC	x	x
Driver USB	x	x
Strumenti	x	x
Collegamenti di accesso diretto ai file di installazione	-	x

4.1.6.3 Centro assistenza – Inventario > Sistema

Sistema fornisce una panoramica dei dati di configurazione di base del sistema.

4.1.6.4 Centro assistenza – Inventario > Numeri di telefono

Numeri di telefono fornisce un elenco di tutti i numeri di telefono assegnati.

4.1.6.5 Centro assistenza – Inventario > Descrizione rete

Descrizione rete fornisce un elenco con informazioni sui sistemi attualmente presenti nella rete.

4.1.6.6 Centro assistenza - Aggiornamento del software

Aggiornamento SW verifica se è disponibile un aggiornamento software sul server Web ed esegue l'aggiornamento.

4.1.6.7 Centro assistenza - Inoltro e-mail

Inoltro e-mail consente l'invio di e-mail con messaggi di sistema della UC Suite all'amministratore nonché l'invio di e-mail con allegati messaggi vocali e fax agli utenti.

4.1.6.8 Centro assistenza – Accesso remoto

L'accesso remoto consente la configurazione dell'accesso per l'amministrazione del sistema da qualsiasi luogo.

4.1.6.9 Centro assistenza - Riavvia/Ricarica

Riavvia/Ricaricaconsente di riavviare il sistema ed eventualmente ripristinare le impostazioni predefinite.

4.1.6.10 Centro assistenza – Diagnostica > Stato

Stato fornisce informazioni di stato su rete, utenti, connessione, ITSP e VPN.

Vedere anche Gestione inventario .

4.1.6.11 Centro assistenza – Diagnostica > Visualizzatore eventi

Visualizzatore eventi registra gli eventi del sistema.

Vedere anche Tracce .

4.1.6.12 Centro assistenza – Diagnostica > Traccia

Traccia consente la registrazione degli errori.

Vedere anche Tracce .

4.1.6.13 Centro assistenza – Diagnostica > Log servizi

Il log servizi registra diversi dati di sistema sotto forma di evento di HiPath 3000.

È necessario essere in modalità di visualizzazione WBM, per aggiornare o scaricare il file.

4.1.7 Modalità esperti

La Modalità esperti, offre a tecnici esperti (profilo **Expert**) i menu e le funzioni necessari per la configurazione e la manutenzione del sistema.

Per ulteriori informazioni, consultare il capitolo Modalità esperti.

4.1.8 Guida in linea

La guida in linea integrata descrive i concetti chiave e le istruzioni per l'uso. In ciascuna pagina WBM aperta è disponibile la guida sensibile al contesto corrispondente all'argomento della pagina.

Navigazione

I pulsanti nella Guida in linea offrono le seguenti funzioni:

- **Contenuto**

  fornisce una panoramica della struttura
- **Indice**

  fornisce accesso diretto a un argomento tramite parole chiave
- **Trova**

  consente con la ricerca a tutto testo di individuare in modo mirato tutti gli argomenti rilevanti

4.1.8.1 Come aprire la Guida in linea in modo sensibile al contesto

Prerequisiti

Si è connessi al WBM.

Procedura

- Fare clic nella finestra WBM aperta o sull'icona del punto interrogativo in alto a destra oppure sul pulsante della Guida in basso a sinistra.

4.2 Manager E

Manager E è uno strumento di manutenzione con Guida integrata funzionante in Windows per svolgere tutte quelle attività che non è possibile eseguire mediante il WBM.

Manager E può essere utilizzato per OpenScape Business X1, OpenScape Business X3, OpenScape Business X5 and OpenScape Business X8. OpenScape Business S non può essere amministrato usando Manager E.

Si raccomanda di effettuare le modifiche alla configurazione tramite Manager E solo quando non è possibile effettuarle tramite WBM, ad esempio, per l'attenuazione, la suoneria, la frequenza del tono, ecc. Le modifiche effettuate tramite Manager E devono essere inviate tramite la modalità delta.

Manager E è rivolto a personale di assistenza qualificato e comprende i seguenti blocchi funzionali:

- Generazione (anche generazione offline)
- Estrazione e salvataggio dati cliente
- Ordini di servizio, ad esempio riavvio dei moduli
- Reset di servizi attivi
- Creazione e stampa di:
  - Etichette tasti per optiPoint 500
  - Elenchi dati cliente
  - Assegnazioni permutatore
- Gestione utenti e password separata per il servizio post-vendita
- Routine di conversione per memoria dati cliente

Per l'accesso al sistema tramite Manager E viene richiesto un nome utente e una password. Per apportare delle piccole modifiche in modo rapido è disponibile la modalità online. La funzionalità della modalità online dipende dall'interfaccia di Assistant T.

Le seguenti funzioni non possono più essere gestite con Manager E:

- Concessione della licenza
- Rete
  - Partner SNMP
  - Partner PSTN
  - Routing
  - Mappat.
  - Gatekeeper
  - Int. H.323
  - Porte IP
- Manutenzione
  - Cronologia errori
  - Registro eventi
  - Impostazioni di traccia
  - Tabella reazione errori
  - Stato V.24
  - DMA
- Tracce

Modalità lavorativa con CDB (memoria dati cliente)

I passaggi di base sono i seguenti:

- Caricamento del CDB del sistema in Manager E
- Modifiche in Manager E
- Salvataggio del CDB di Manager nel sistema

4.2.1 Come caricare il CDB in Manager E

Procedere come descritto di seguito per eseguire le attività di configurazione in Manager E.

Passo a passo

1) Avviare Manager E sul PC Admin.
2) In **Nome utente** inserire il nome utente per Manager E.
3) In **Password** immettere la password per Manager E.
4) Fare clic su **File** > **Trasferisci**.
5) Fare clic sulla scheda **Comunicazioni**.
6) Nell'area **Accesso**, selezionare l'opzione richiesta in base al tipo di collegamento del PC Admin al sistema.
7) Selezionare l'opzione **Leggere/scrivere CDB**.
8) Fare clic su **Sistema -> PC**.
9) Fare clic su **OK**. Il CDB viene trasferito dal sistema a Manager E.
10) Terminato il trasferimento, fare clic su **OK**.
11) Fare clic su **Chiudi**.

4.2.2 Come ripristinare il CDB nel sistema

Per ripristinare nel sistema la configurazione eseguita con Manager E, procedere come descritto di seguito.

Passo a passo

1) Fare clic su **File** > **Trasferisci**.
2) Fare clic sulla scheda **Comunicazioni**.
3) Nell'area **Accesso**, selezionare l'opzione richiesta in base al tipo di collegamento del PC Admin al sistema.
4) Selezionare l'opzione **Leggere/scrivere CDB**.
5) Fare clic su **PC -> sistema**.
6) Fare clic su **OK**. Il CDB viene trasferito da Manager E al sistema.
7) Terminato il trasferimento, fare clic su **OK**.
8) Fare clic su **Chiudi**.

5 Configurazione iniziale di OpenScape Business X

Questa documentazione descrive la configurazione iniale di OpenScape Business X1/X3/X5/X8. Il sistema di comunicazione e i suoi componenti sono integrati in un'infrastruttura esistente costituita da una LAN del cliente e da una rete telefonica TDM. L'accesso a Internet e la connessione trunk sono stati configurati e le stazioni collegate sono state configurate.

La configurazione iniziale di OpenScape Business X1/X3/X5/X8 (ossia il sistema di comunicazione) viene eseguita con il programma di amministrazione OpenScape Business Assistant (gestione basata sul Web, denominata per brevità WBM).

Qui viene descritta la configurazione iniziale standard dei componenti comunemente utilizzati. Le fasi specifiche dell'installazione dipendono dal sistema di comunicazione e dai componenti coinvolti (ad esempio, la scheda UC Booster Card). Pertanto, alla configurazione iniziale, occorre scegliere tra più opzioni o configurazioni o saltare interamente alcune configurazioni. È anche possibile che i passaggi di installazione qui descritti non compaiano nel proprio sistema di comunicazione.

Le configurazioni dettagliate delle funzioni non coperte dalla configurazione iniziale standard sono descritte nei seguenti capitoli.

Requisito essenziale per la configurazione iniziale è la creazione di uno schema di indirizzi IP e di un piano di composizione.

I passaggi più importanti dell'installazione sono i seguenti:

- Indirizzi IP e impostazioni DHCP
- Impostazioni Paese e Ora
- Numeri di telefono completi e collegamento in rete
- Configurazione ISDN
- Accesso a Internet
- Telefonia Internet
- Configurazione utenti
- Licenza
- Rafforzamento del sistema
- Backup dei dati

Linee guida per l'aumento dell'intervallo di sottorete, al fine di prevenire potenziali errori di configurazione

Le considerazioni chiave da tenere presenti prima di procedere con tali modifiche includono:

Garantire che determinate reti non si sovrappongano ad altre reti di sistema. In particolare:

- Rete DSP
- Rete LAN1 (WAN)
- Rete LAN2
- Rete LAN3 (amministrazione)

Inoltre, è necessario assicurarsi che non vi siano conflitti con l'indirizzo IP del gateway predefinito e, se è presente una scheda Booster, l'interfaccia LAN2 del sistema deve trovarsi nella stessa sottorete dell'interfaccia LAN2 della scheda Booster.

5.1 Requisiti richiesti per l'installazione iniziale

Il rispetto dei requisiti richiesti per l'installazione iniziale garantisce il funzionamento corretto del sistema di comunicazione.

Generale

A seconda dell'hardware utilizzato (modulo, telefoni, ecc.) e delle infrastrutture esistenti, si applicano i seguenti requisiti generali:

- L'infrastruttura (LAN, rete telefonica TDM) è disponibile e utilizzabile.
- L'hardware è correttamente installato e collegato.
- Per l'integrazione della scheda madre e della UC Booster Card nella LAN del cliente è necessaria un'interfaccia LAN.
- Il sistema di comunicazione non è ancora collegato alla LAN.
- Se viene utilizzata la UC Booster Card, questa deve essere inserita prima dell'installazione iniziale.
- Un provider di servizi Internet fornisce accesso a Internet.
- Per l'uso di linee esterne ISDN è necessaria una connessione ISDN S_0 o un collegamento ISDN primario multiplex.
- Per l'uso di una linea esterna CAS è necessaria una connessione linea CAS.
- Per l'uso di una linea esterna analogica è necessaria una connessione di linea urbana analogica.
- Uno schema di indirizzi IP deve essere noto e disponibile (vedere Schema indirizzi IP).
- Un piano di composizione (anche detto piano di numerazione) è disponibile e noto (vedere Piano di composizione).

PC Admin

Il PC di amministrazione (PC Admin), da utilizzare per l'installazione iniziale e per la successiva amministrazione del sistema di comunicazione, deve soddisfare i seguenti requisiti:

- Interfaccia di rete:

  Il PC Admin richiede un'interfaccia LAN libera.
- Sistema operativo:

  Per l'eventuale configurazione del sistema di comunicazione con Manager E, è necessario un sistema operativo Windows (a partire da Windows XP).

  Per la configurazione con il WBM viene utilizzato il browser: la procedura è quindi indipendente dal sistema operativo.
- Browser Web:

  Sono supportati i seguenti browser:

  – Microsoft Internet Explorer dalla Versione 10.
  – Mozilla Firefox versione 17 e successive.
  – Microsoft Edge
  – Google Chrome

  Se è installata una versione precedente del browser Web, è necessario aggiornarla prima di procedere alla configurazione del sistema.

- Java:

  Sul PC deve essere installato Oracle Java 8 o versione successiva oppure, in alternativa, OpenJDK 8. Se è installata una versione precedente, è necessario aggiornarla prima di procedere alla configurazione del sistema.

5.2 Componenti

I componenti indicati nell'esempio di installazione sono descritti e schematizzati di seguito.

L'esempio di installazione comprende i seguenti componenti:

- OpenScape Business X

  Il sistema di comunicazione viene collegato alla LAN esistente del cliente tramite l'interfaccia LAN
- PC Admin

  Il PC Admin è inoltre collegato tramite un'interfaccia LAN al sistema di comunicazione.
- Utente IP (client IP)

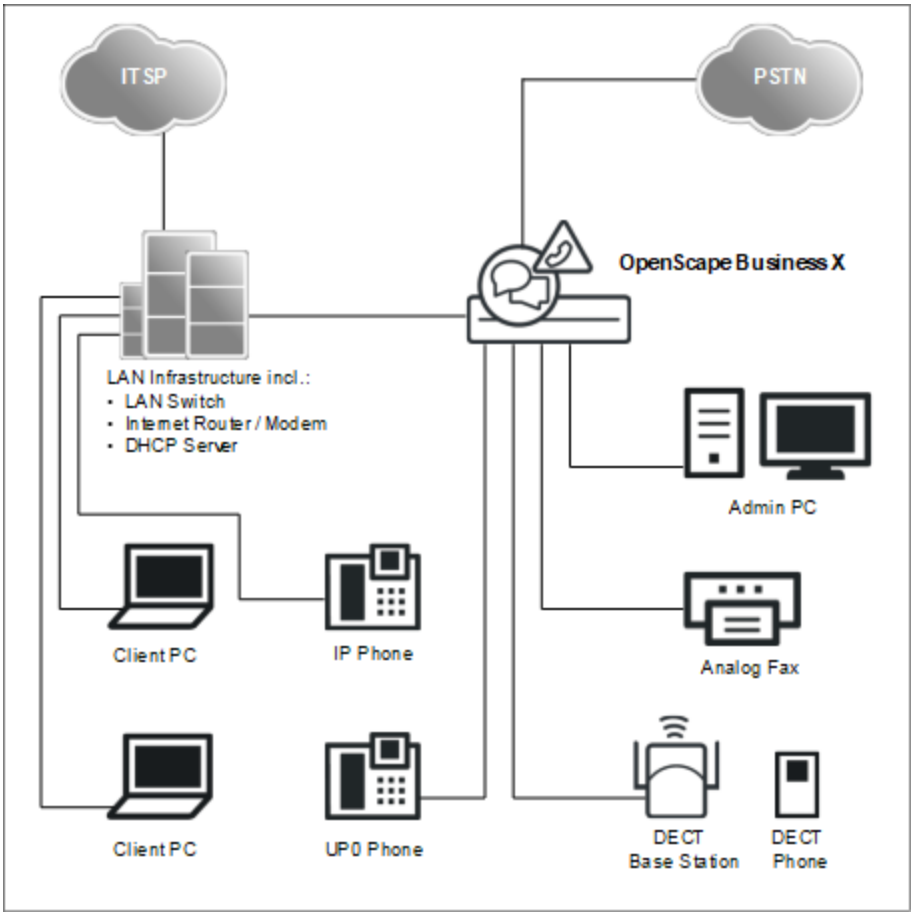
  Gli utenti IP (telefoni di sistema IP, PC client, punti di accesso WLAN ecc.) sono integrati tramite uno o più switch.
- Utente UP0

  Gli utenti UP0 (ad esempio telefono di sistema TDM OpenStage 60T) sono collegati direttamente al sistema di comunicazione.
- Utenti analogici

  Gli utenti analogici (ad esempio fax analogici) sono collegati direttamente al sistema di comunicazione.
- Utenti DECT

  Gli utenti DECT sono connessi tramite una stazione base al sistema di comunicazione.

I client IP ottengono il proprio indirizzo IP dinamico da un server DHCP interno o esterno (ad esempio un router Internet).



5.3 Piano di composizione

Un piano di composizione è una lista di tutti i numeri di telefono disponibili nel sistema di comunicazione. Contiene fra l'altro i numeri di telefoni interni, quelli di selezione passante e quelli dei gruppi.

Piano di composizione predefinito

Ai numeri di telefono interni sono preassegnati valori predefiniti. All'occorrenza, questi valori possono essere modificati in base ai propri requisiti (piano di composizione singolo).

Estratto dal piano di composizione predefinito:

Tipo di numero di telefono	**X1**	X3/X5/X8
Numeri di telefono dell'utente interno	11-30	100-742
Nr. di selezione passante	11-30	100-742
Numero di telefono linee	700-703	ab 7801

Tipo di numero di telefono	**X1**	X3/X5/X8
Codici del fascio (codici esterni): Fsc 1 (linea ISDN, analogica) Fsc 8 (UC Suite) Fsc 12-15 (linea ITSP) Fsc 16 (Rete)	 0 = mondo / 9 = USA - non preassegnati non preassegnati	 0 = mondo / 9 = USA 851 855-858 859
Numero di telefono per accesso remoto	non preassegnati	non preassegnati
Numero di telefono per i messaggi vocali UC Smart UC Suite	351 -	351 non preassegnati

Piano di composizione personalizzato

Durante la configurazione di base, è possibile importare un piano di composizione personalizzato in formato XML.

Il file XML contiene diverse schede. La scheda Cliente contiene, oltre al nome e al numero di telefono degli utenti, anche altri dati quali il tipo di utente e l'indirizzo e-mail degli utenti.

Nel WBM, disponibile in **Centro assistenza** > **Documenti** > **Modelli CSV**, è disponibile un esempio di file XML con relativa spiegazione. I file XML qui memorizzati possono essere utilizzati come modelli per i propri dati. Può essere modificato ad esempio in Microsoft Excel.

5.4 Schema indirizzi IP

Uno schema indirizzi IP definisce come vengono utilizzati gli indirizzi IP in una rete LAN. Comprende gli indirizzi IP di PC, server, router Internet, telefoni IP, sistema di comunicazione ecc.

Per una migliore visione d'insieme durante l'assegnazione degli indirizzi IP è necessario creare uno schema indirizzi IP.

Esempio di uno schema indirizzi IP nella gamma `192.168.1." -x`:

Intervallo di indirizzi IP	**Client**
Da **192.168.1.1** a **192.168.1.19**	Client con indirizzo IP fisso:
192.168.1.1	Router Internet (Gateway)
192.168.1.2	Sistema di comunicazione
192.168.1.3	Scheda applicazioni (opzionale)
192.168.1.10	Server e-mail
Da **192.168.1.50** a **192.168.1.254**	PC client e telefoni IP, unitamente all'intervallo indirizzi IP del server DHCP; l'assegnazione degli indirizzi IP avviene in modo dinamico

Il seguente intervallo di indirizzi IP è riservato per uso interno e non può essere occupato:

Intervallo di indirizzi IP riservato	Descrizione
10.0.0.1; 10.0.0.2	riservato per il server delle licenze
10.186.237.65; 10.186.237.66	Riservato per ISDN remota (obsoleto)
192.168.3.2	Indirizzo IP interno del sistema di comunicazione
192.168.2.1	Indirizzo IP della porta LAN3 (porta Admin)

Questo elenco è disponibile nel WBM selezionando il percorso **Centro assistenza** > **Diagnostica** > **Stato** > **Panoramica indirizzi IP**.

Estensione della maschera di rete quando si utilizza il segmento di rete predefinito

L'indirizzo IP interno del sistema di comunicazione e l'indirizzo IP della porta LAN3 (porta Admin) non possono trovarsi sullo stesso segmento di rete dell'indirizzo IP del sistema di comunicazione.

Configurazione predefinita per il segmento di rete:

- 192.168.1.2: Indirizzo IP del sistema di comunicazione
- 255.255.255.0: Maschera di rete
- 192.168.3.2: Indirizzo IP interno del sistema di comunicazione
- 192.168.2.1: Indirizzo IP della porta LAN3 (porta Admin)

Se si utilizza il segmento di rete predefinito e la maschera di rete deve essere estesa da 255.255.255.0 ad esempio a 255.255.0.0, è necessario modificare gli indirizzi IP sopra indicati:

Esempio di configurazione modificata:

- 192.168.1.2: Indirizzo IP del sistema di comunicazione
- 255.255.**0**.0: Maschera di rete
- 192.**169**.3.2: Indirizzo IP interno del sistema di comunicazione

  Modificabile tramite **Modalità esperti** > **Telefonia** > **Payload** > **Moduli HW** > **Modifica le impostazioni di DSP**
- 192.**170**.2.1: Indirizzo IP della porta LAN3 (porta Admin)

  Modificabile tramite **Modalità esperti** > **Telefonia** > **Interfacce di rete** > **Scheda madre** > **LAN 3 (Admin)**

5.5 Prima messa in servizio

La messa in servizio comprende l'avvio del sistema di comunicazione, il collegamento e la configurazione del PC Admin e il primo avio del programma di amministrazione OpenScape Business Administration Assistant (WBM).

La messa in servizio del sistema di comunicazione deve essere effettuata prima che il sistema di comunicazione venga integrato nella rete LAN interna. Possono insorgere problemi se l'indirizzo IP preconfigurato del sistema di comunicazione è già presente nella LAN interna e/o se è già in uso un server DHCP. Per questi casi, occorre prima deconfigurare l'indirizzo IP del sistema

di comunicazione e/o il server DHCP del sistema di comunicazione deve essere disattivato. Solo a questo punto, è possibile integrare il sistema di comunicazione nella LAN.

Nota: Prima della messa in servizio occorre rispettare le istruzioni sulla tutela e la sicurezza dei dati.

Pericolo: Prima di accendere OpenScape Business X8, verificare che il lato posteriore di tutti i box sia previsto dei pannelli ciechi e di connessione previsti.

Pericolo: OpenScape Business X3R/X5R non deve venire acceso se il lato frontale dell'alloggiamento è aperto. Gli slot non dotati di moduli vanno sempre chiusi con piastre vuote (C39165-A7027-B115).

Pericolo: OpenScape Business X1W/X3W/X5W non deve venire acceso se l'alloggiamento è aperto.

Connessione ai PC Admin

Per configurare il sistema di comunicazione, il PC Admin viene collegato direttamente all'interfaccia "LAN" del sistema di comunicazione e configurato per ottenere l'indirizzo IP dal server DHCP interno del sistema di comunicazione. Terminata l'installazione, il PC Admin può essere integrato nella LAN interna senza ulteriori configurazioni.

5.5.1 Come avviare il sistema di comunicazione

Prerequisiti

L'hardware è stato montato correttamente (vedere *Istruzioni di installazione di OpenScape Business*).

La scheda di memoria (con il software di sistema) è inserita.

Il sistema di comunicazione non è ancora integrato nella LAN del cliente.

Passo a passo

Collegare il sistema di comunicazione alla rete elettrica.

Attenzione:

Scossa elettrica per contatto con linee sotto tensione

Assicurarsi che il sistema di comunicazione (e nel caso di OpenScape Business X8, ogni box) sia messo a terra tramite un conduttore di protezione separato (vedere *OpenScape Business, Istruzioni di installazione*).

Il sistema di comunicazione verrà ora avviato. Durante questo processo, i LED del sistema si accendono con colori e sequenze diverse (per i dettagli vedere *OpenScape Business, Istruzioni di installazione*). Durante l'inizializzazione, il sistema di comunicazione non può essere disconnesso dall'alimentazione di rete.

Una volta avviato il sistema, il LED "Run" sulla scheda madre lampeggia con luce verde alla frequenza di 1 Hz (0,5 sec acceso/0,5 sec spento).

5.5.2 Come collegare il PC Admin al sistema di comunicazione

Prerequisiti

Il sistema di comunicazione è pronto all'uso.

Passo a passo

1) Avviare il PC Admin.

2) Verificare se al PC può essere assegnato un indirizzo IP dinamico. In caso negativo, è necessario cancellare la configurazione del PC Admin. A tale scopo sono necessari i diritti di amministratore.

Nota: Le impostazioni IP qui descritte valgono per Windows 7. Per ulteriori informazioni di configurazione in altri sistemi operativi Windows, consultare le istruzioni del sistema operativo corrispondente.

---

a) Selezionare **Start** > **Pannello di controllo**, quindi fare doppio clic su **Rete e Internet**, infine selezionare **Centro connessioni di rete e condivisione**.

b) Nella rete attiva corrispondente, fare clic su **Connessione LAN**, quindi su **Proprietà**.

c) Nella scheda **Rete** selezionare con il pulsante sinistro del mouse l'opzione **Protocollo Internet Versione 4 (TCP/IPv4)** e fare clic su **Proprietà**.

d) Fare clic sulla scheda **Generale** e verificare se il pulsante di opzione **Ottieni automaticamente indirizzo IP** è selezionato. Nel caso non lo sia, selezionarlo.

e) Chiudere tutte le finestre con **OK**.

3) Collegare l'interfaccia LAN appena configurata del PC Admin con l'interfaccia "LAN" del sistema di comunicazione utilizzando un cavo LAN. Tramite questa interfaccia viene assegnato al PC Admin un indirizzo IP dinamico.

Nota: È anche possibile collegare il PC Admin all'interfaccia LAN "Admin", quindi assegnare al PC Admin, un indirizzo IP fisso nell'intervallo 192.168.2.xxx (es. 192.168.2.40) e la maschera di rete 255.255.255.0. Tramite l'interfaccia LAN "Admin", il sistema di comunicazione ha l'indirizzo IP 192.168.2.1 - importante per l'accesso a WBM!

5.5.3 Come avviare WBM

Prerequisiti

Il sistema di comunicazione è pronto all'uso. Il LED "RUN" sulla scheda madre lampeggia con luce verde alla frequenza di 1 Hz (0,5 sec acceso/0,5 sec spento).

Il PC Admin e il sistema di comunicazione possono comunicare fra loro tramite LAN.

Passo a passo

1) Sul PC Admin, avviare il browser Web e richiamare la pagina di accesso di OpenScape Business Assistant (WBM) al seguente indirizzo:

`https://192.168.1.2`

Nota: Se il WBM non si avvia, verificare la connessione LAN e ripetere la procedura. Se il problema persiste, verificare se l'indirizzo IP viene bloccato dal proprio firewall PC interno. Per informazioni più precise, consultare la documentazione del firewall.

---

2) Se il browser Web segnala un problema con un certificato di sicurezza, installare il certificato (nell'esempio Internet Explorer V10).

a) Chiudere il browser Web.

b) Aprire il browser Web con i diritti di amministratore facendo clic con il pulsante destro del mouse sull'icona del browser, quindi nel menu di scelta rapida selezionare la voce **Esegui come amministratore**.

c) Consentire il controllo dell'ID utente.

d) Richiamare la pagina di accesso di OpenScape Business Assistant (WBM) al seguente indirizzo:

`https://192.168.1.2`

e) fare clic su **Continua caricamento del sito Web**.

f) Fare clic sul messaggio **Errore certificato** nella barra di navigazione del browser Web.

g) Fare clic su **Mostra certificati**.

h) Fare clic su **Installa certificato** (visibile solo con i privilegi di amministratore).

i) Selezionare l'opzione **Computer locale** e confermare con **Avanti**.

j) Selezionare l'opzione **Salva tutti i certificati nella seguente memoria**, fare clic su **Ricerca** e immettere le **Autorità di certificazione radice attendibili**.

k) Confermare con **OK** e successivamente con **Avanti** e **Fine**.

l) Confermare l'importazione del certificato con **OK** e chiudere la finestra del certificato con **OK**.

m) Chiudere il browser Web.

n) Avviare di nuovo il browser Web (senza i diritti di amministratore) e richiamare la pagina di accesso di OpenScape Business Assistant (WBM) al seguente indirizzo:

`https://192.168.1.2`

3) In alto a destra, fare clic sul codice della lingua e dal menu selezionare la lingua in cui deve essere visualizzata l'interfaccia del WBM. La pagina di registrazione viene visualizzata nella lingua desiderata.
4) Nel primo campo in **Accesso** immettere il nome utente predefinito `administrator@system` per accedere come amministratore.

   Nota: Se si digita il termine `administrator` nel campo **Password**, il sistema completa automaticamente la stringa con `@system`.

5) Nel secondo campo in **Accesso** immettere la password predefinita, `administrator`, per l'accesso come amministratore.
6) Fare clic su **Connetti**.
7) I seguenti passaggi sono necessari solo una volta al primo accesso al WBM:
   a) Nel campo **Password** immettere ancora la password predefinita, `administrator`.
   b) Per proteggere il sistema dall'uso improprio, nei campi **Nuova password** e **Conferma nuova password** immettere la nuova password. Prestare attenzione alle lettere maiuscole e minuscole e allo stato dei tasti `Num`e `CapsLock` (tasto bloc maiusc) La password viene visualizzata come una serie di asterischi (*).

      Nota: Tale password deve essere di almeno 8 caratteri e contenere un numero. Annotarsi esattamente la nuova password.

   c) Fare clic su **Accesso**.
   d) Selezionare la data corrente e inserire l'ora corretta.
   e) Fare clic su **OK & Avanti**. Si viene automaticamente disconnessi dal WBM.
   f) Nel primo campo in **Accesso** immettere il nome utente predefinito `administrator@system` per accedere come amministratore.

      Nota: Se si digita il termine `administrator` nel campo **Password**, il sistema completa automaticamente la stringa con `@system`.

   g) Nel secondo campo in **Accesso** immettere la nuova password definita per l'accesso come amministratore.
   h) Fare clic su **Accesso**. Viene visualizzata la pagina iniziale di WBM.

Passaggi successivi

Avvio della prima installazione.

5.6 Integrazione nella LAN del cliente

L'integrazione nella rete LAN del cliente viene eseguita con la procedura guidata **Configurazione di base** di WBM. La procedura guidata consente di definire le impostazioni fondamentali per il collegamento del sistema di comunicazione alla LAN esistente.

5.6.1 Come avviare la procedura guidata Prima installazione

Prerequisiti

WBM è avviato.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Fare clic su **Modifica**, per avviare la procedura guidata **Prima installazione**.

> **Nota:** Se con una bassa risoluzione dello schermo non è possibile visualizzare per intero l'area di lavoro nella finestra del browser, sono disponibili barre di scorrimento verticali o orizzontali per visualizzare il contenuto.

Passaggi successivi

Eseguire la prima installazione come descritto di seguito. I campi non descritti in questa sezione sono preimpostati su valori standard e devono essere modificati solo se non corrispondono ai dati della rete del cliente. Per informazioni più complete, fare riferimento alle descrizioni delle singole procedure guidate riportate nella Documentazione per l'amministratore.

5.6.2 Impostazioni di sistema

Nella finestra **Impostazioni di sistema**, configurare le impostazioni del sistema di comunicazione.

Procedere come segue:

1) Definizione del logo a display e del nome del prodotto

   È possibile definire un testo che verrà visualizzato sul display del telefono. Oltre a ciò, è possibile selezionare la designazione del prodotto.
2) Definire indirizzi IP (se necessario)

   Per impostazione predefinita, al sistema di comunicazione deve essere assegnato un indirizzo IP e una maschera di sottorete. Se necessario, l'indirizzo IP e/o la maschera di sottorete devono essere adattati al proprio intervallo di indirizzi IP.

   Inoltre è possibile indicare l'indirizzo IP di un router predefinito, ad esempio l'indirizzo IP del router Internet.

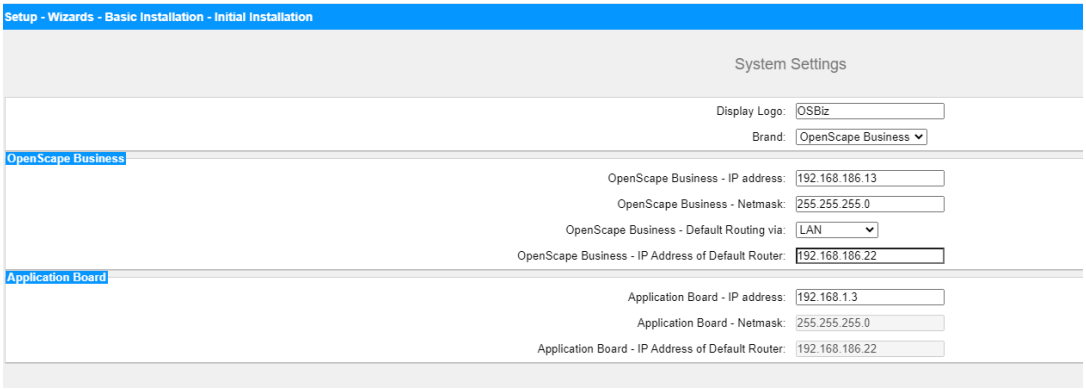
   La scheda applicazioni (UC Booster Card) richiede anche un indirizzo IP. Indipendentemente dal fatto che la scheda sia o meno montata, assegnare un indirizzo IP compreso nel proprio intervallo di indirizzi IP.

Se la maschera di rete deve essere estesa, ad esempio da 255.255.**255**.0 a 255.255.**0**.0, sia l'indirizzo IP interno del sistema di comunicazione sia l'indirizzo IP della porta LAN3 (porta Admin) devono essere modificati poiché questi non possono essere sullo stesso segmento di rete dell'indirizzo IP del sistema di comunicazione (vedere anche Schema indirizzi IP).

5.6.2.1 Come definire il logo sul display e la descrizione del prodotto

Prerequisiti

Si è nella finestra **Impostazioni di sistema**.



Passo a passo

1) Nel campo **Logo display**, immettere un testo a piacere (ad es. OpenScape Biz). Il testo può contenere fino a 16 caratteri. Evitare dieresi e caratteri speciali.
2) Nell'elenco a discesa **Brand** selezionare il brand desiderato.

Passaggi successivi

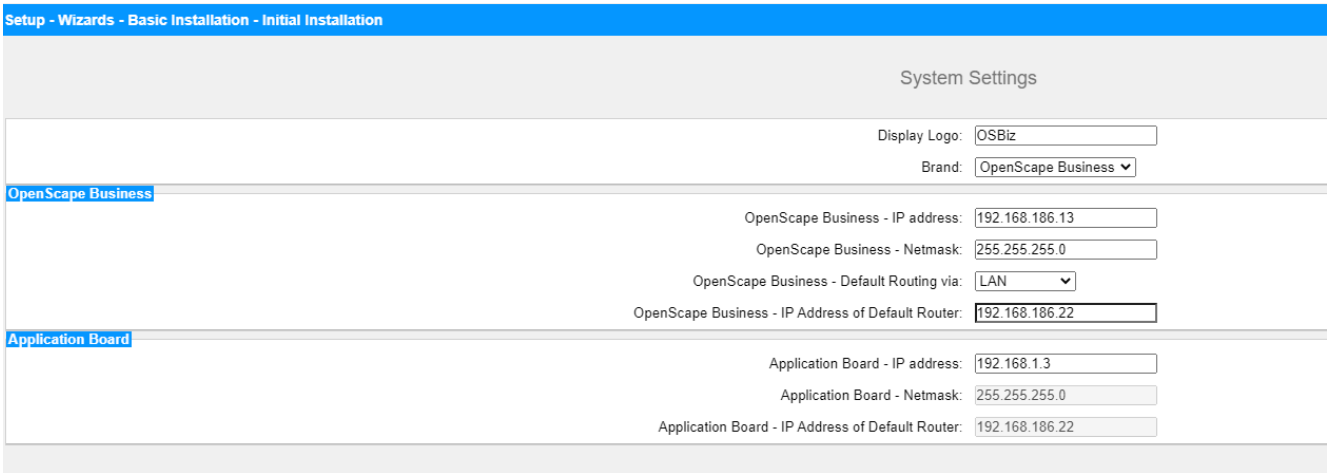
Modifica indirizzi IP (se necessario) o configurazione DHCP.

5.6.2.2 Come definire gli indirizzi IP (opzionale)

Prerequisiti

L'intervallo di indirizzi IP della propria rete interna è noto.

Si è nella finestra **Impostazioni di sistema**.



Passo a passo

1) Definire l'indirizzo IP del sistema di comunicazione:
   a) Nel campo **OpenScape Business - Indirizzo IP** inserire un indirizzo IP compreso nell'intervallo di indirizzi IP della rete interna (ad esempio, rete interna: `192.168.1.x`, OpenScape Business: `192.168.1.2`.

   Nota: L'indirizzo IP di OpenScape Business non deve essere assegnato ad alcun client della rete esistente, in quanto ciò produrrebbe un conflitto tra indirizzi IP.

   b) Nel campo **OpenScape Business - Maschera di rete** immettere la maschera di rete della propria rete interna (ad esempio, `255.255.255.0`).
2) Definire l'indirizzo IP del router predefinito:
   a) Nel campo **OpenScape Business - Routing predefinito tramite**, selezionare la voce **LAN**.
   b) Nel campo **OpenScape Business - Indirizzo IP del router predefinito** inserire l'indirizzo IP del router predefinito (ad esempio, rete interna: `192.168.1.x`, router Internet come router predefinito: `192.168.1.1`).
3) Definire l'indirizzo IP della UC Booster Card (necessario, se inserita):
4) Fare clic su **OK & Avanti**.

Passaggi successivi

Configurazione DHCP.

5.6.2.3 Come specificare il nome del dispositivo

Prerequisiti

Si è nella finestra **Impostazioni di sistema**.

Il sistema è in modalità DTAG.

Passo a passo

1) Selezionare la casella di controllo **Registrazione RSP.servicelink automatica**:

   Il campo **Nome dispositivo** è modificabile.
2) Specificare **Nome dispositivo**.

   Selezionando la registrazione automatica RSP.servicelink, il sistema cercherà automaticamente ogni 10 minuti di registrarsi e connettersi ai server RSP con il nome dispositivo fornito.
3) Fare clic su **OK & Avanti**.

Passaggi successivi

Configurazione DHCP.

5.6.3 Impostazioni DHCP

Nella finestra **Impostazioni globali di DHCP** attivare e configurare o disattivare il server DHCP interno del sistema di comunicazione.

Un server DHCP assegna automaticamente agli utenti IP (telefoni del sistema IP, PC ecc.) un indirizzo IP e fornisce i dati di rete, quali ad esempio l'indirizzo IP del gateway predefinito (router Internet).

Come server DHCP può essere usato un server DHCP esterno (ad esempio il server DHCP del router Internet) o un server DHCP interno, integrato nel sistema di comunicazione.

Per l'aggiornamento automatico del software dei telefoni IP di sistema, può essere utilizzato il DLI integrato nel sistema di comunicazione o un server DLS esterno (Servizio di distribuzione (DLI e DLS)). È necessario comunicare al server DHCP l'indirizzo IP del DLI integrato o del server DLS esterno.

Sono disponibili le seguenti opzioni:

- Attivazione e configurazione del server DHCP interno

  Se viene utilizzato il server DHCP interno del sistema di comunicazione, il server DHCP esterno (ad esempio il server DHCP del router Internet) deve essere disattivato. Se necessario, le impostazioni del server DHCP interno devono essere adattate alla rete LAN del cliente. Se viene utilizzato il server DHCP interno e il DLI interno, i telefoni di sistema vengono automaticamente aggiornati. Se viene usato un server DLS esterno, è necessario inserire il relativo indirizzo IP nel server DHCP interno tramite la Modalità esperti (Servizio di distribuzione (DLS e I).
- Disattivazione del server DHCP interno

  Se viene utilizzato un server DHCP esterno, il server DHCP interno del sistema di comunicazione deve essere disattivato. Per poter caricare automaticamente il software più nei telefoni IP di sistema, i dati specifici della rete devono essere inseriti nel server DHCP esterno, ad esempio l'indirizzo IP del server DLI interno o del server DLS esterno.

Nota: Non tutti i server DHCP esterni supportano l'inserimento dei dati di rete! In questo caso, occorre inserire i dati manualmente in tutti i telefoni di sistema IP.

5.6.3.1 Come disabilitare il server DHCP interno

Prerequisiti

Un server DHCP esterno (ad es. il server DHCP del router Internet) è abilitato nella rete interna.

Si è nella finestra **Impostazioni DHCP globali**.

Passo a passo

1) Deselezionare la casella di controllo **Abilita server DHCP**.
2) Fare clic su **OK & Avanti**.

Passaggi successivi

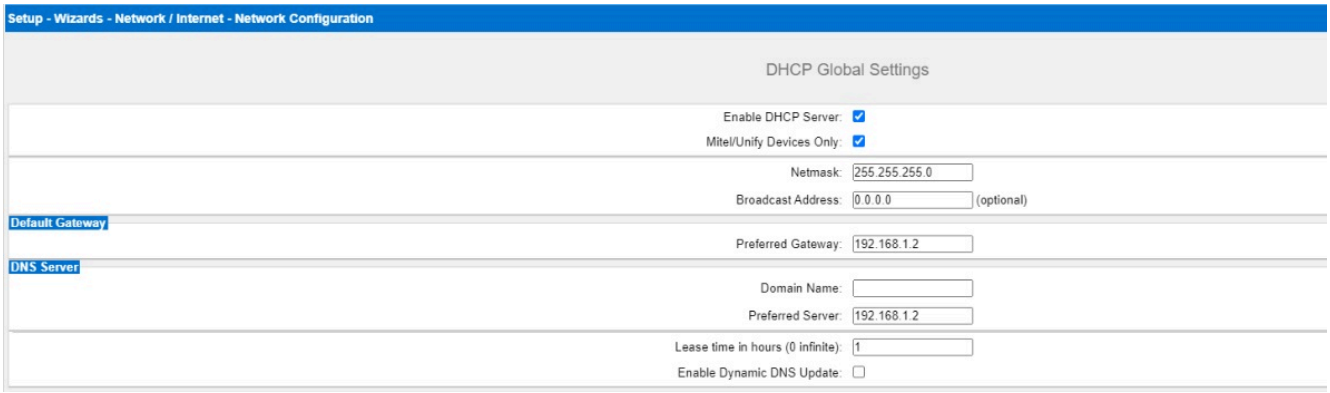
Configurare le impostazioni del paese e dell'ora.

5.6.3.2 Come abilitare e configurare il server DHCP interno

Prerequisiti

Il server DHCP esterno (ad es. il server DHCP del router Internet) è stato disabilitato nella rete interna.

Si è nella finestra **Impostazioni DHCP globali**.

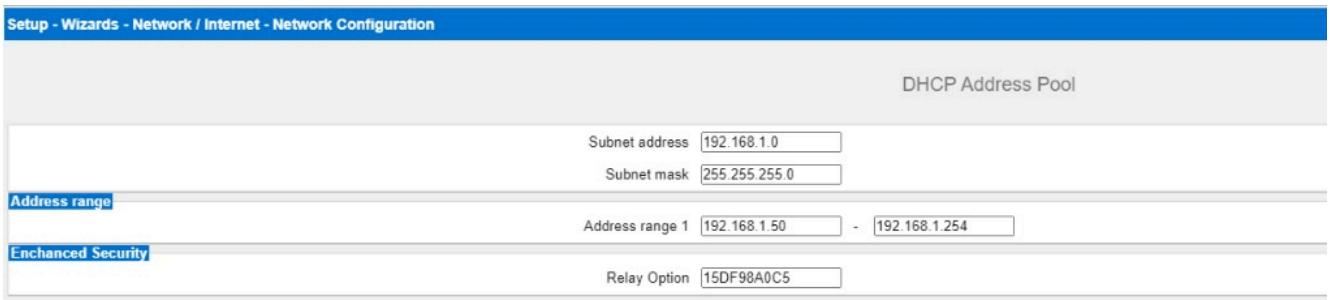


Passo a passo

1) Lasciare la casella di controllo **Abilita server DHCP** abilitata.
2) Se necessario, abilitare la casella di controllo **Solo dispositivi Mitel/Unify**.

   Nota: Questa opzione è disponibile solo per le schede madri V3.

3) Andare su **Netmask** e regolare la maschera di sottorete in base all'intervallo di indirizzi IP (ad esempio `255.255.255.0`).
4) Nel campo **Gateway preferito**, inserire l'indirizzo IP del router Internet (ad esempio `192.168.1.1`).
5) Nel campo **Server preferito**, inserire l'indirizzo IP del server DNS (ad esempio, l'indirizzo IP del router Internet, `192.168.1.1`.
6) Fare clic su **OK & Avanti**. Si apre la finestra **Pool di indirizzi DHCP**.



7) Specificare i valori per **Indirizzo di sottorete**, **Netmask** e **Intervallo indirizzi 1** per definire l'intervallo di indirizzi IP da gestire dal server DHCP interno.

   Se la rete interna utilizza indirizzi IP statici (ad esempio, per un server di stampa), l'intervallo di indirizzi IP (pool di indirizzi DHCP) deve essere selezionato in modo che gli indirizzi IP fissi non siano inclusi in questo intervallo.

   Esempio:

   Router Internet: `192.168.1.1`

   OpenScape Business: `192.168.1.2`

   UC Booster Card: `192.168.1.3`

   Indirizzo di sottorete: `192.168.1.0`

   Maschera di sottorete: `255.255.255.0`

   Server stampante: `192.168.1.10`

   Pool di indirizzi DHCP: da `192.168.1.50` a `192.168.1.254`

8) Se necessario, specificare il valore del campo **Opzione relè**.

   Nota: Questa opzione è disponibile solo per le schede madri V3.

9) Fare clic su **OK & Avanti**.

Passaggi successivi

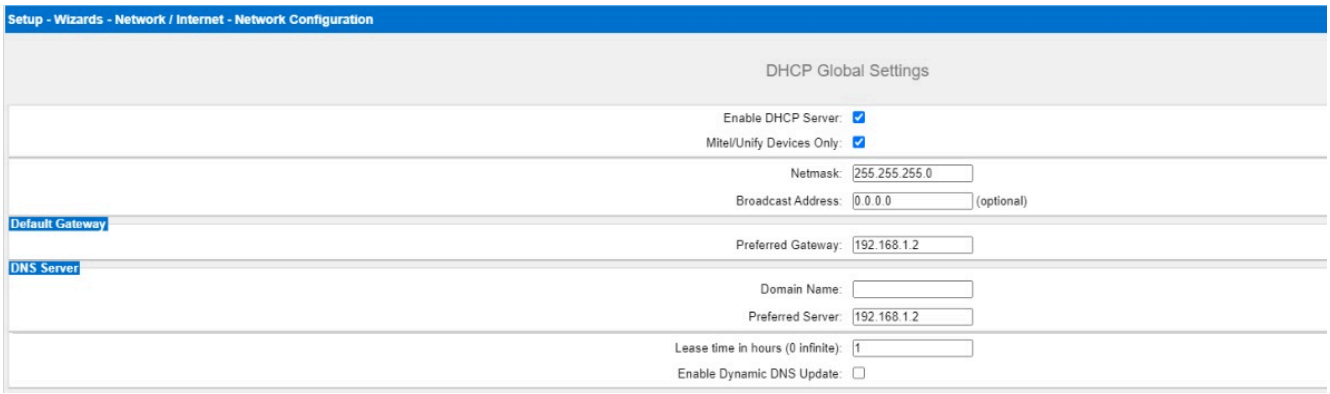
Configurare le impostazioni del paese e dell'ora.

5.6.3.3 Come abilitare il DHCP solo per i dispositivi Mitel/Unify

Questa opzione consente all'amministratore di sistema di attivare il servizio DHCP di OpenScape Business esclusivamente per i dispositivi Mitel e Unify.

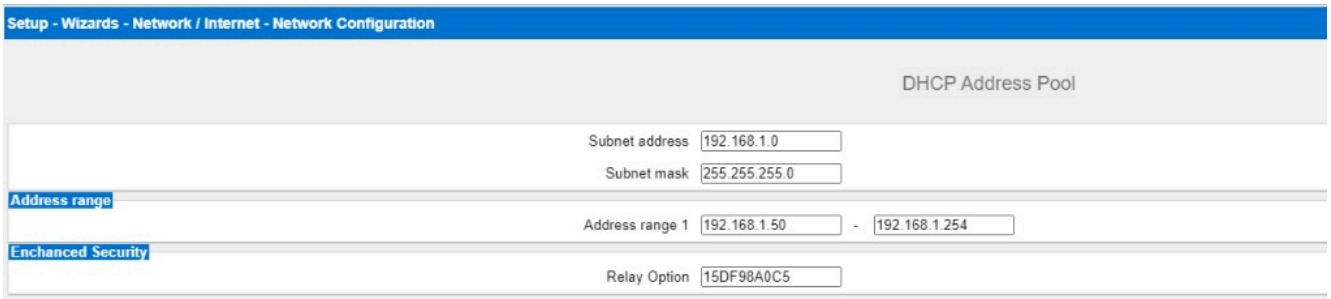
Prerequisiti

Si è nella finestra **Impostazioni DHCP globali**.



Passo a passo

1) Lasciare la casella di controllo **Abilita server DHCP** abilitata.
2) Fare clic per abilitare la casella di controllo **Solo dispositivi Mitel/Unify**. Per ulteriori informazioni su questa opzione, vedere la sezione Server DHCP > Parametri globali.
3) Andare su **Netmask** e regolare la maschera di sottorete in base all'intervallo di indirizzi IP (ad esempio `255.255.255.0`).
4) Nel campo **Gateway preferito**, inserire l'indirizzo IP del router Internet (ad esempio `192.168.1.1`).
5) Nel campo **Server preferito**, inserire l'indirizzo IP del server DNS (ad esempio, l'indirizzo IP del router Internet, `192.168.1.1`.
6) Fare clic su **OK & Avanti**. Si apre la finestra **Pool di indirizzi DHCP**.



7) Specificare i valori per **Indirizzo di sottorete**, **Maschera di sottorete** e **Intervallo indirizzi 1** per definire l'intervallo di indirizzi IP da gestire dal server DHCP interno.

   Se la rete interna utilizza indirizzi IP statici (ad esempio, per un server di stampa), l'intervallo di indirizzi IP (pool di indirizzi DHCP) deve essere selezionato in modo che gli indirizzi IP fissi non siano inclusi in questo intervallo.

   Esempio:

   Router Internet: `192.168.1.1`

   OpenScape Business: `192.168.1.2`

   UC Booster Card: `192.168.1.3`

   Indirizzo di sottorete: `192.168.1.0`

   Maschera di sottorete: `255.255.255.0`

   Server stampante: `192.168.1.10`

   Pool di indirizzi DHCP: da `192.168.1.50` a `192.168.1.254`
8) Specificare il valore del campo **Opzione relè**.
9) Fare clic su **OK & Avanti**.

Passaggi successivi

Configurare le impostazioni del paese e dell'ora.

5.6.4 Impostazioni temporali e del paese

Nella finestra **Configurazione base**, selezionare il paese e la lingua per i registri eventi e impostare la data e l'ora. Se si utilizza la soluzione cordless integrata, immettere qui l'ID DECT valido a livello di sistema.

Procedere come segue:

1) Selezionare il prefisso del paese e la lingua per i registri evento

Per una corretta inizializzazione del paese è necessario selezionare il paese in cui verrà utilizzato il sistema di comunicazione. Inoltre è possibile scegliere la lingua utilizzata per il registro eventi (registro degli eventi di sistema, errori ecc.).

2) Inserire l'identificativo di sistema DECT (solo con soluzione cordless integrata)

Se si utilizza la soluzione cordless integrata, immettere qui l'ID DECT valido a livello di sistema.

3) Impostazione di data e ora

- Come configurare manualmente data e ora

  Il sistema di comunicazione e gli utenti (telefoni IP, telefoni TDM, PC client) devono disporre di un riferimento temporale (data e ora) uniforme. Se per la sincronizzazione temporale non è noto alcun server SNTP, è possibile inserire la data e l'ora manualmente.

  Nota: Data e ora vengono aggiornate anche quando si instaura una connessione tramite linea ISDN.

- Fare riferimento alla data e all'ora di un server SNTP

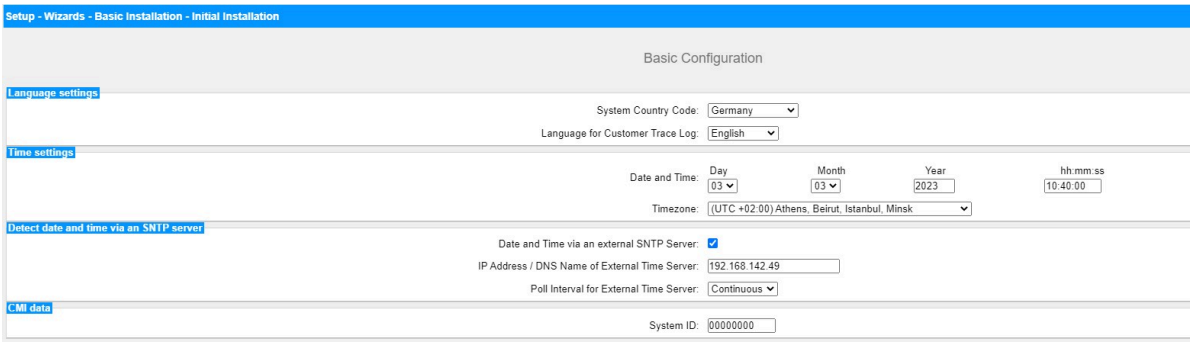
  Il sistema di comunicazione e gli utenti IP (telefoni IP, PC client) devono disporre di un riferimento temporale (data e ora) uniforme. Tale riferimento temporale può essere fornito da un server SNTP. Il server SNTP può trovarsi nella rete interna o in Internet.

I telefoni IP ottengono automaticamente la data e l'ora dal sistema di comunicazione. I PC client che utilizzano i client UC devono essere impostati in modo da avere l'orario sincronizzato con il sistema di comunicazione (consultare le istruzioni d'uso del sistema operativo dei PC client).

5.6.4.1 Come selezionare il prefisso nazionale e la lingua per i registri eventi

Prerequisiti

Si è nella finestra **Configurazione base**.



Passo a passo

1) Nell'elenco a discesa **Sigla internazionale del sistema**, selezionare il paese in cui viene utilizzato il sistema di comunicazione.
2) Nel campo **Lingua per log traccia cliente** definire la lingua da utilizzare per il registro eventi (registro degli eventi di sistema, errori ecc.).

Passaggi successivi

Inserire l'identificativo di sistema DECT (solo con soluzione cordless integrata)

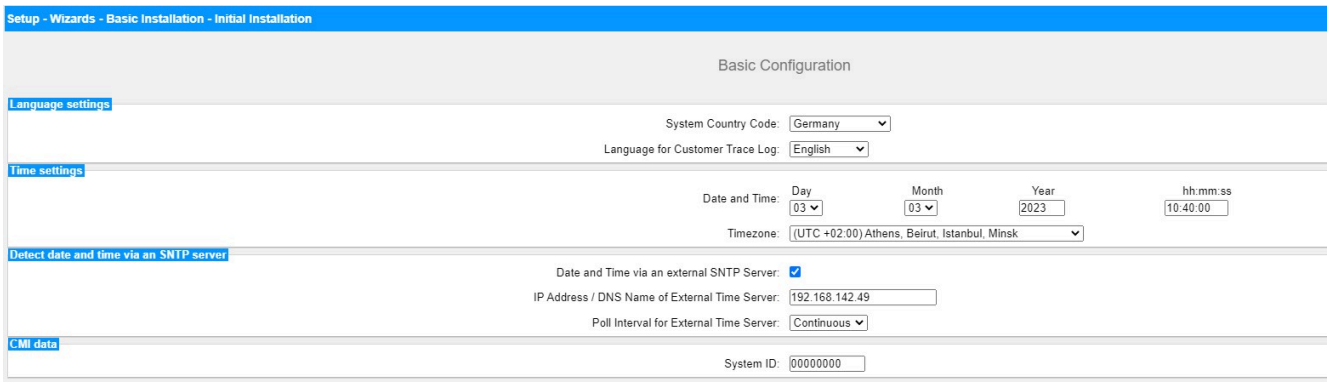
o

Impostare la data e l'ora manualmente o fare riferimento alla data e all'ora di un server SNTP.

5.6.4.2 Come immettere l'ID di sistema (EIC) DECT

Prerequisiti

Si è nella finestra **Configurazione base**.



Passo a passo

Nell'area **Dati CMI** in **EIC**, immettere il codice esadecimale a 8 cifre DECT ricevuto al momento dell'acquisto della soluzione cordless integrata.

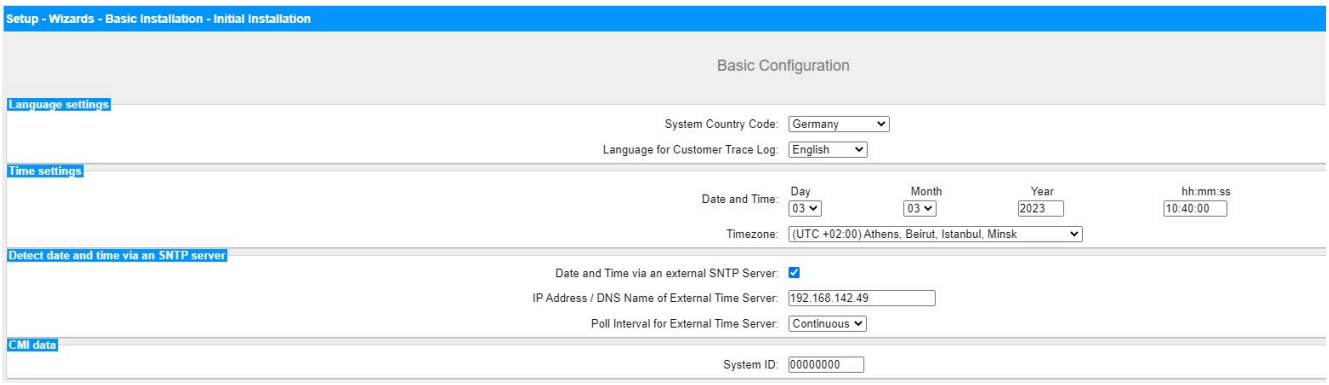
Passaggi successivi

Impostare la data e l'ora manualmente o fare riferimento alla data e all'ora di un server SNTP.

5.6.4.3 Come configurare manualmente data e ora

Prerequisiti

Si è nella finestra **Configurazione base**.



Passo a passo

1) Immettere i valori corretti per **Data e Ora**.
2) Nel campo **Fuso orario** indicare il fuso orario desiderato.
3) Fare clic su **OK & Avanti**.

Nota: Nel caso in cui l'impostazione del fuso orario venga modificata, all'ultimo passaggio della procedura guidata iniziale **il sistema verrà riavviato**.

Se l'impostazione del fuso orario rimane invariata, il sistema non verrà riavviato.

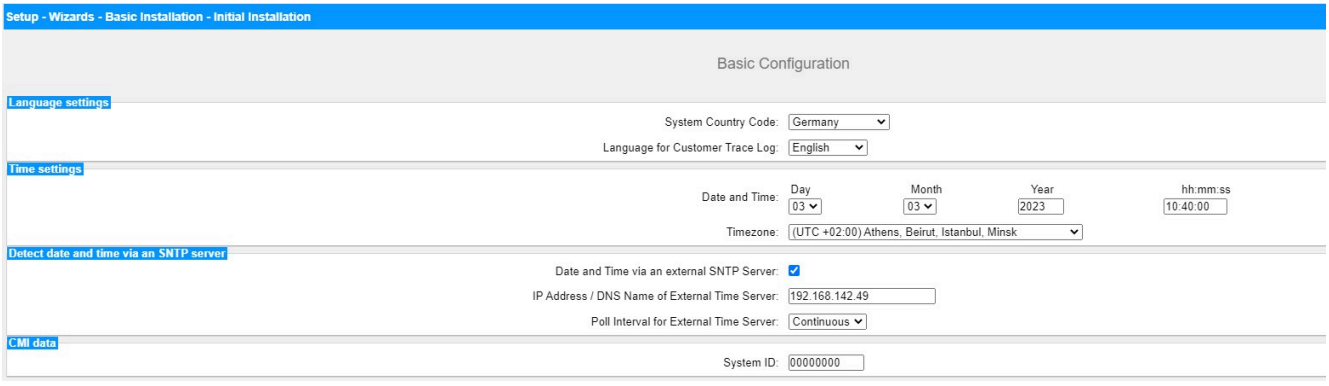
Passaggi successivi

Definire la soluzione UC.

5.6.4.4 Come fare riferimento alla data e all'ora di un server SNTP

Prerequisiti

Si è nella finestra **Configurazione base**.



Passo a passo

1) Selezionare la casella di controllo **Data e ora da server SNTP esterno**.
2) Nel campo **Indirizzo IP / nome DNS server di riferimento orario esterno** immettere l'indirizzo IP o il nome DNS del server SNTP (ad esempio, `0.de.pool.ntp.org`).
3) Nell'elenco a discesa **Tempo di polling del server dell'ora esterno**, indicare dopo quante ore, è necessario sincronizzare la data e l'ora del server SNTP (consigliato: `4 ore`).
4) Fare clic su **OK & Avanti**.

Passaggi successivi

Definire la soluzione UC.

5.6.5 Soluzione UC

Nella finestra **Selezione applicazione** è possibile scegliere quale soluzione UC usare.

Sono disponibili le seguenti opzioni:

- **Pacchetto con UC Smart**

  La soluzione UC Smart è integrata sulla scheda madre OpenScape Business X.
- **Pacchetto con UC Suite**

  La soluzione UC Suite è integrata sul modulo interno aggiuntivo "UC Booster Card".
- **Pacchetto con UC Suite su OSBiz UC Booster Server**

  La soluzione UC Smart è integrata sul server Linux "OpenScape Business UC Booster Server" esterno.
- **Pacchetto con UC Suite su OSBiz UC Booster Server**

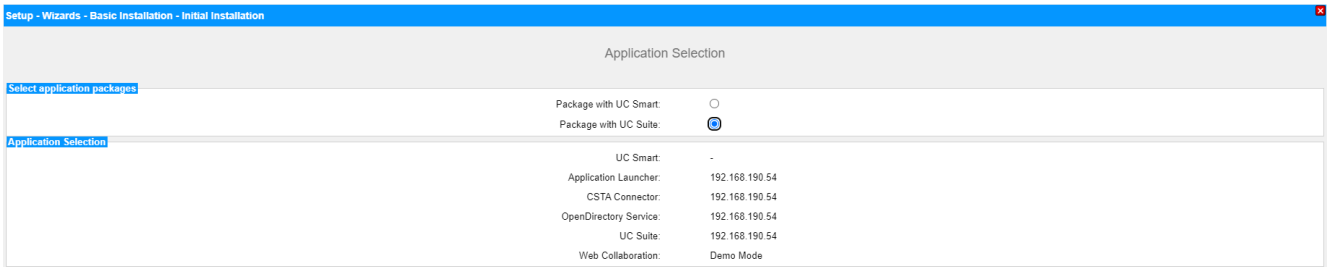
  La soluzione UC Suite è integrata sul server Linux "OpenScape Business UC Booster Server" esterno.

5.6.5.1 Come definire la soluzione UC

Prerequisiti

Si sono acquistate licenze per la soluzione UC Smart o UC Suite.

Si è nella finestra **Selezione applicazione**.



Passo a passo

1) Se si utilizza la soluzione di comunicazione unificata UC Smart senza UC Booster Server, fare clic su **Pacchetto con UC Smart**.
2) Se si utilizza la soluzione di comunicazione unificata UC Smart con UC Booster Server, fare clic su **Pacchetto con UC Smart su OSBiz UC Booster Server**. Nel campo **Indirizzo IP di OSBiz UC Booster Server** immettere l'indirizzo IP del server Linux esterno "OpenScape Business UC Booster Server".
3) Se si utilizza la soluzione di comunicazione unificata UC Suite con UC Booster Card, fare clic su **Pacchetto con UC Suite**.
4) Se si utilizza la soluzione di comunicazione unificata UC Suite con UC Booster Server, fare clic su **Pacchetto con UC Suite su OSBiz UC Booster Server**. Nel campo **Indirizzo IP di OSBiz UC Booster Server** immettere l'indirizzo IP del server Linux esterno "OpenScape Business UC Booster Server".
5) Fare clic su **OK & Avanti**.
6) La procedura guidata **Prima installazione** è conclusa. Fare clic su **Fine**.
7) Chiudere il WBM facendo clic in alto a destra sul collegamento **Disconnetti**, quindi chiudendo la finestra.

Nota: Se gli indirizzi IP o le impostazioni del server DHCP vengono modificati, il sistema di comunicazione si riavvia. La procedura può richiedere qualche minuto.

Passaggi successivi

Collegare il sistema di comunicazione alla LAN del cliente.

5.6.6 Connessione del sistema di comunicazione alla LAN del cliente

Terminata l'installazione iniziale, il sistema di comunicazione viene collegato alla LAN esistente del cliente.

5.6.6.1 Come collegare il sistema di comunicazione alla LAN del cliente

Prerequisiti

Il sistema di comunicazione è pronto all'uso.

Passo a passo

1) Rimuovere il cavo LAN del PC Admin dall'interfaccia LAN centrale "LAN" e integrare il PC Admin nella LAN del cliente, collegandolo ad esempio a uno switch.
2) Collegare un cavo LAN all'Interfaccia LAN centrale del sistema di comunicazione.
3) Integrare il sistema di comunicazione tramite il cavo LAN nella LAN del cliente, collegandolo ad esempio a uno switch.
4) Se è inserita una UC Booster Card (scheda applicazioni), collegare un altro cavo LAN alla porta "LAN2" della UC Booster Card (a destra/sotto le due

porte LAN) e integrare la UC Booster Card tramite questo cavo LAN nella rete LAN del cliente, collegandolo ad esempio a uno switch.

Passaggi successivi

Come avviare la configurazione di base.

5.7 Configurazione base

La configurazione base viene eseguita con la procedura guidata **Installazione di base** di WBM. La procedura guidata consente di definire le principali impostazioni per il funzionamento del sistema di comunicazione.

L'installazione guidata di base comprende un indicatore di avanzamento che mostra il passaggio corrente e quelli successivi.

5.7.1 Come avviare la procedura guidata Installazione di base

Prerequisiti

La procedura guidata **Prima installazione** è conclusa.

Il sistema di comunicazione viene integrato nella LAN del cliente.

Il sistema di comunicazione è pronto all'uso. Il LED "RUN" sulla scheda madre lampeggia con luce verde alla frequenza di 1 Hz (0,5 sec acceso/0,5 sec spento).

Passo a passo

1) Nel browser Web sul PC Admin, richiamare la pagina di accesso del WBM all'indirizzo:

   `https://<Indirizzo IP di OpenScape Business>`

   L'indirizzo IP predefinito di OpenScape Business è `192.168.1.2`, quindi ad esempio `https://192.168.1.2`
2) Nel campo **Nome utente** immettere il nome utente predefinito `administrator@system` per accedere come amministratore.
3) Nel campo **Password** immettere la password selezionata alla messa in funzione.
4) Fare clic su **Accesso**.
5) Nella barra di navigazione, fare clic su **Configurazione**.
6) Fare clic su **Modifica**, per avviare la procedura guidata **Installazione di base**.

Passaggi successivi

Eseguire l'installazione di base come descritto di seguito. I campi non descritti in questa sezione sono preimpostati su valori standard e devono essere modificati solo se non corrispondono ai dati della rete del cliente. Per informazioni più complete, fare riferimento alle descrizioni delle singole procedure guidate riportate nella Documentazione per l'amministratore.

5.7.2 Numeri di telefono completi e collegamento in rete

Nella finestra **Panoramica** inserire i numeri di telefono completi (numero PABX, codice paese e prefisso interurbano, prefisso internazionale) e determinare se OpenScape Business deve essere collegato in rete con altri sistemi OpenScape Business.

Procedere come segue:

1) Inserimento di numeri di telefono completi

- Inserimento di numeri di telefono completi per connessioni punto - punto

  Indicare qui il numero di sistema per la connessione al proprio sistema nonché i prefissi internazionale e interurbano.

  L'immissione del prefisso internazionale è obbligatoria per la telefonia Internet e per le funzionalità di server conferenza.

  Il prefisso internazionale dipende dal codice del paese selezionato in precedenza.
- Inserimento di numeri di telefono completi per connessioni punto - multipunto

  Inserire qui i prefissi internazionale e interurbano per la propria connessioni punto-multipunto.

  L'immissione del prefisso internazionale è obbligatoria per la telefonia Internet e per le conferenze Incontro.

  Il prefisso internazionale dipende dal codice del paese selezionato in precedenza.

2) Attivazione/disattivazione della connessione di rete

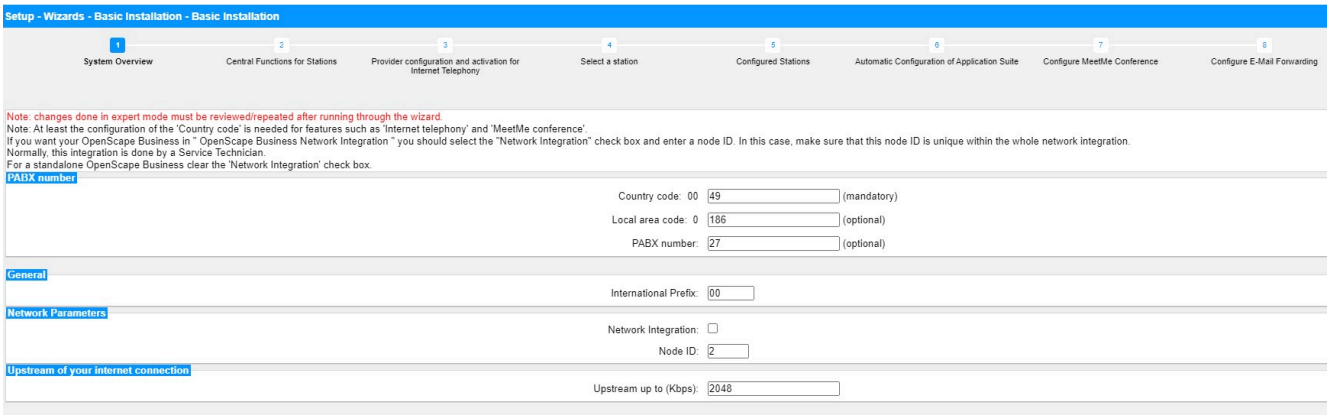
Se OpenScape Business deve essere collegato in rete con altri sistemi OpenScape Business, la connessione di rete deve essere attivata e a OpenScape Business deve essere assegnato un ID nodo. Ogni OpenScape Business nel sistema di reti deve disporre di un ID di nodo univoco.

5.7.2.1 Come inserire i numeri di telefono completi per una connessione punto - punto

Prerequisiti

Si dispone di una connessione punto - punto.

Si è nella finestra **Panoramica** della procedura guidata **Installazione di base**.



Passo a passo

1) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. `49` per la Germania o `1` per gli USA.
2) Nel campo **Prefisso interurbano**, immettere l'indicativo località, ad es. `051` per Bologna.
3) Nel campo **Numero del sistema** inserire il numero del sistema per la propria connessione linea esterna, ad esempio `7007` (il proprio numero della connessione).
4) Modificare il campo **Prefisso internazionale** solo quando necessario. Per la Germania si utilizza `00`, per gli Stati Uniti `011`

   Per le chiamate all'estero, il numero di telefono è preceduto dal prefisso internazionale e dal prefisso nazionale, ad esempio per telefonare dalla Germania agli USA "00-1-..." e dagli USA alla Germania "011-49-...".

Passaggi successivi

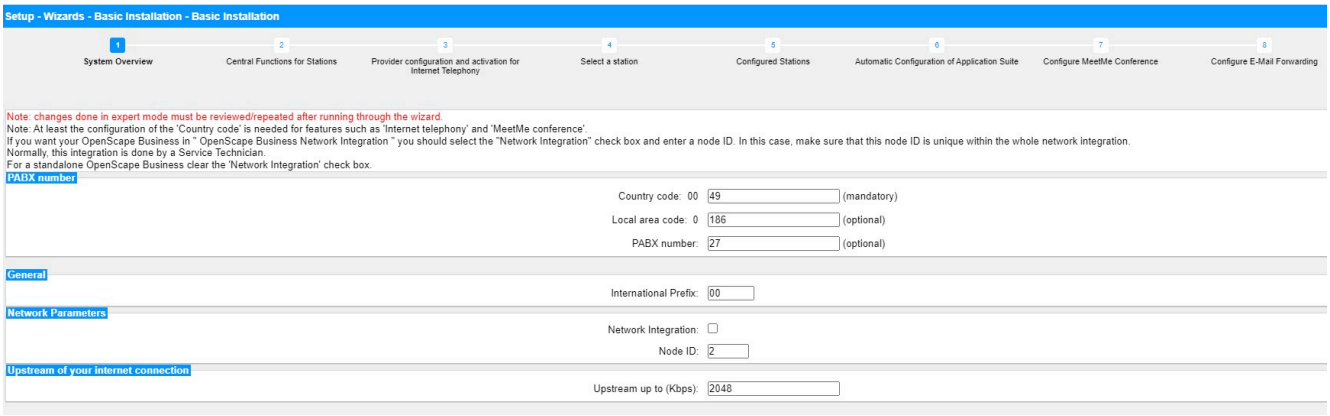
Attivazione/disattivazione della connessione di rete

5.7.2.2 Come inserire i numeri di telefono completi per una connessione punto - multipunto

Prerequisiti

Si dispone di una connessione punto - multipunto.

Si è nella finestra **Panoramica** della procedura guidata **Installazione di base**.



Passo a passo

1) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. `49` per la Germania o `1` per gli USA.
2) Nel campo **Prefisso interurbano**, immettere l'indicativo località, ad es. `051` per Bologna.
3) Lasciare vuoto il campo **Numero del sistema**.
4) Modificare il campo **Prefisso internazionale** solo quando necessario. Per la Germania si utilizza `00`, per gli Stati Uniti `011`.

   Per le chiamate all'estero, il numero di telefono è preceduto dal prefisso internazionale e dal prefisso nazionale, ad esempio per telefonare dalla Germania agli USA "00-1-..." e dagli USA alla Germania "011-49-...".

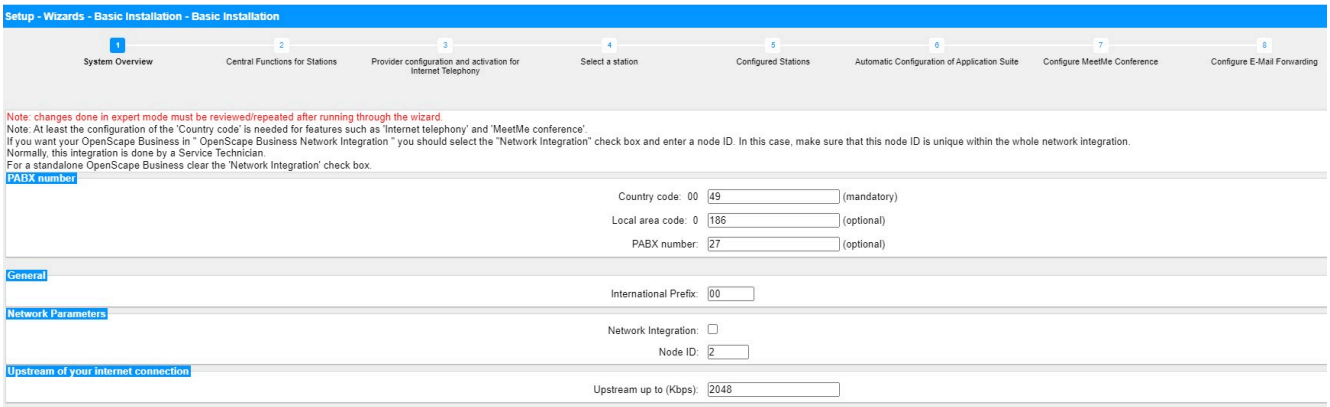
Passaggi successivi

Attivazione/disattivazione della connessione di rete

5.7.2.3 Come attivare o disattivare la connessione di rete

Prerequisiti

Si è nella finestra **Panoramica** della procedura guidata **Installazione di base**.



Passo a passo

1) Se il sistema di comunicazione deve essere collegato in rete con altri sistemi di comunicazione:
   a) Selezionare la casella di controllo **Integrazione rete**.
   b) Nel campo **ID nodo** del sistema di comunicazione, inserire un ID nodo univoco sul sistema di reti (cifre da `1` a `100`).
2) Se il sistema di comunicazione non deve essere collegato in rete con altri sistemi di comunicazione, lasciare deselezionata la casella di controllo **Integrazione in rete**.

Passaggi successivi

Configurare a monte della tua connessione Internet.

5.7.3 Dati dell'utente

Nella finestra **Funzioni centrali per gli utenti** è possibile configurare, se necessario, un proprio piano di composizione individuale al posto di quello predefinito e importare altri dati sugli utenti. Nel sistema di reti, il piano di composizione predefinito deve essere adeguato al piano di composizione specifico del sistema di reti.

Il piano di composizione predefinito contiene numeri predefiniti per i diversi tipi di utente (telefoni IP, telefoni analogici, ...) e per funzioni speciali (telefonia via Internet, casella vocale, AutoAttendant, ...).

I dati degli utenti contengono, tra l'altro, i numeri di telefono interni, i numeri di selezione passante e i nomi degli utenti. Con un file XML in formato UTF-8, questi dati e altri dati degli utenti possono essere importati nel sistema di comunicazione durante la configurazione di base.

Nota:

Nel WBM, disponibile in **Centro assistenza** > **Documenti** > **Modelli CSV**, è disponibile un modello XML con relativa spiegazione. In questi modelli è ad esempio possibile inserire i dati con Microsoft Excel.

Sono disponibili le seguenti opzioni:

- **Configurazione dei dati utente senza sistema di reti**

  Procedere come segue:

  1) Visualizzazione dei dati utente

  È possibile visualizzare tutti i numeri di telefono e i dati utente preconfigurati.

  2) Cancella tutti numeri di telefono (opzionale)

  Se si utilizza un piano di composizione personalizzato, occorre prima eliminare i numeri di telefono preconfigurati.

  3) Modificare i numeri di telefono preconfigurati in base al piano di composizione specifico (opzionale)

  Se si utilizza un piano di composizione personalizzato, è possibile modificare i numeri di telefono predefiniti per adattarli al piano di composizione stesso.

  Nota:

  Se l'utente passa attraverso **Modifica numeri di telefono e funzionali pre-configurati**, qualsiasi configurazione personalizzata esistente effettuata in UC Suite deve essere esaminata o ripetuta (ad es., code pilota)

  ---

  4) Importazione dei dati degli utenti tramite file XML (opzionale)

  I singoli numeri di telefono ed eventuali altri dati dell'utente possono essere facilmente importati tramite un file XML durante la configurazione di base.

- **Configurazione dei dati utente con sistema di reti**

  Procedere come segue:

  1) Cancella tutti i numeri di telefono

  Se nel sistema di reti viene utilizzata la UC Suite, è necessario un piano di numerazione chiuso, ovvero tutti i numeri di telefono del sistema di reti devono essere univoci. Pertanto, i numeri di telefono preconfigurati devono essere eliminati e devono essere utilizzati i numeri adattati per il sistema di reti.

  2) Importazione dei dati degli utenti tramite file XML

  I numeri di telefono modificati secondo il sistema di reti ed eventuali altri dati dell'utente possono essere facilmente importati tramite un file XML durante la configurazione di base. Questo file può contenere tutti gli utenti del sistema di reti. Durante l'impostazione vengono trasferiti solo i numeri e i dati degli utenti assegnati all'ID nodo del sistema di comunicazione specificato in precedenza.

Attività correlate

Come visualizzare i dati di massa alla pagina 162
Come resettare le voci LCR alla pagina 1410

Riferimenti correlati

LCR > Flag LCR alla pagina 1603

5.7.3.1 Come visualizzare i dati utente

Prerequisiti

Si è nella finestra **Funzioni centrali per gli utenti** della procedura guidata **Installazione di base**.

Passo a passo

1) Attivare il pulsante di opzione **Mostra configurazione utenti**.
2) Fare clic su **Esegui funzione**. Viene visualizzato un elenco degli utenti con numeri preconfigurati (piano di composizione predefinito).
3) Fare clic su **OK**. Si torna alla finestra **Funzioni centrali per gli utenti**.
4) Se non si desidera modificare dati degli utenti, fare clic su **OK & Avanti**.

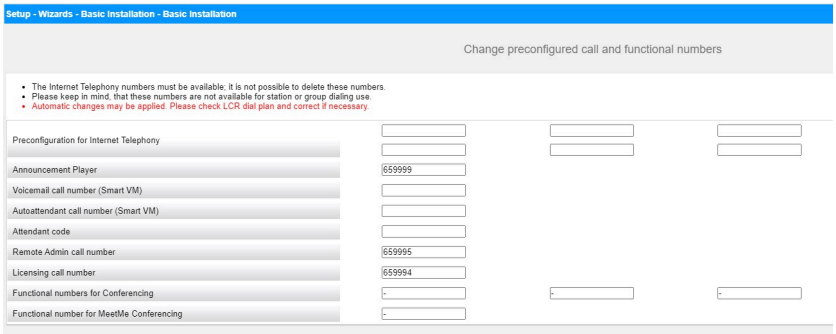
5.7.3.2 Come eliminare tutti i numeri di telefono

Prerequisiti

Si è nella finestra **Funzioni centrali per gli utenti** della procedura guidata **Installazione di base**.

Passo a passo

1) Selezionare **Cancella tutti numeri di telefono**.
2) Selezionare la casella di controllo **Cancella tutti numeri di telefono**.
3) Fare clic su **Esegui funzione**. Tutti i numeri preconfigurati vengono cancellati, tranne **Announcement Player, Numero di telefono Remote-Admin** e **Numero di telefono per concessione licenza**. Appare quindi la finestra **Modifica numeri di telefono e funzionali pre-configurati**.



4) Modificare i codici e i numeri speciali in base alle proprie esigenze, quindi fare clic su **OK**. Si torna alla finestra **Funzioni centrali per gli utenti**.
5) Se non si desidera configurare altri dati utente, fare clic su **OK & Avanti**.

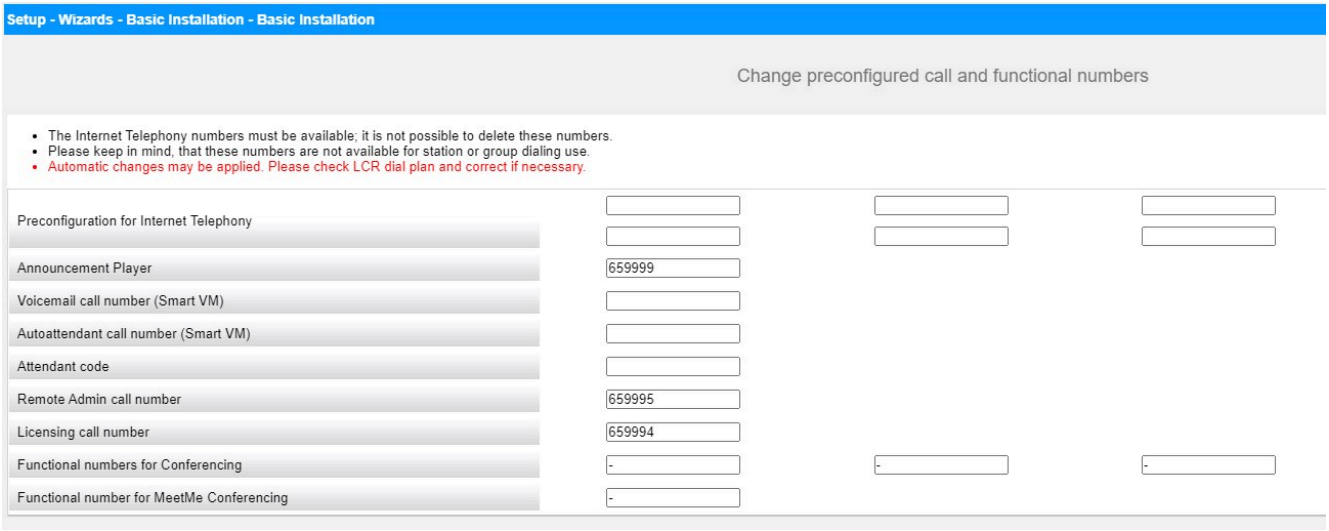
5.7.3.3 Modificare i numeri di telefono preconfigurati in base al piano di composizione specifico

Prerequisiti

Si è nella finestra **Funzioni centrali per gli utenti** della procedura guidata **Installazione di base**.

Passo a passo

1) Attivare **Modifica numeri di telefono e funzionali pre-configurati**.
2) Fare clic su **Esegui funzione**. Viene visualizzata la finestra **Modifica numeri di telefono e funzionali pre-configurati**.



3) Modificare i numeri preconfigurati in base alle proprie esigenze, quindi fare clic su **OK**. Si torna alla finestra **Funzioni centrali per gli utenti**.
4) Se non si desidera configurare altri dati utente, fare clic su **OK & Avanti**.

5.7.3.4 Come importare i dati degli utenti tramite un file XML

Prerequisiti

Si è nella finestra **Funzioni centrali per gli utenti** della procedura guidata **Installazione di base**.

Esiste un file XML in formato UTF-8 con i dati inseriti. Un modello XML è disponibile in **Centro assistenza** > **Documenti** > **Modelli CSV**.

Passo a passo

1) Attivare il pulsante di opzione **Configurazione utente importando file CSV/ XML**.
2) Fare clic su **Esegui funzione**.
3) Selezionare con **Sfoglia** il file XML creato e fare clic su **Apri**.
4) Fare quindi clic su **OK**. I dati utente vengono importati.
5) Fare clic su **OK & Avanti**.

5.7.3.5 Come visualizzare i dati di massa

Prerequisiti

- Si è nella finestra **Funzioni centrali per gli utenti** della procedura guidata **Installazione di base**.
- È possibile accedere alla procedura guidata **Dati di massa** da **Configurazione** > **Procedure guidate**.

Passo a passo

1) Attivare il pulsante **Procedura guidata dati di massa**.
2) Fare clic su **Esegui funzione**.
3) Nella finestra **Procedura guidata dati di massa** è possibile convalidare gli accessi del sistema facendo clic su **Convalida**. Esistono due tipi di convalida, il Controllo consistenza front end e il Controllo consistenza back end.
   Il colore verde nel campo di convalida indica solo le azioni convalidate di recente. La convalida dei dati non viene salvata, pertanto in caso di modifiche ai valori l'utente è tenuto a convalidare nuovamente i dati.
4) Durante il Controllo consistenza back end e una volta convalidati i dati non è possibile apportare modifiche nella finestra della **Procedura guidata dati di massa**. Se la convalida riesce, viene visualizzata l'opzione **OK&Avanti** in modalità di modifica con restrizioni. Se l'utente fa clic su **Indietro**, la modalità Modifica diventa disponibile ma l'opzione **OK&Avanti** non viene più visualizzata. Se la convalida non riesce, la modalità Modifica resta attiva e l'opzione **OK&Avanti** rimane nascosta.

   Nota: L'utente può fare clic su **Indietro** per modificare di nuovo i dati; la finestra torna alla modalità Modifica. La modalità di modifica con restrizioni fa sì che l'utente non possa fare clic su OK&Avanti e inviare modifiche non convalidate.

5) Una volta configurata correttamente la **Procedura guidata dati di massa**, fare clic su **Fine**. Nella pagina finale sono riassunte tutte le modifiche.

   I campi non sono modificabili e risultano già compilati con i valori corrispondenti ottenuti dal database. Pertanto, un'azione di Copia/Incolla non ha alcun effetto sui dati.

   Il campo Tipo è un menu a discesa selezionabile con funzionalità di modifica. Tuttavia, le sole opzioni accettate sono Nessuna porta, Client di sistema, Client SIP, Utente Deskshare e un possibile valore predefinito basato sul modulo a cui appartiene. Se l'utente tenta di inserire valori diversi, questi non vengono accettati e il menu a discesa rimane visualizzato e continua a presentare una voce appropriata.

   Un'ulteriore restrizione è rappresentata dalla non sostituibilità di alcune porte (ad esempio, per le porte che appartengono a una scheda analogica il tipo non può essere modificato e deve rimanere utente analogico). Tutti i limiti si applicano quando l'utente cerca di eseguire un'operazione di copia/incolla nella parte superiore della colonna Tipo. Se l'utente cerca di incollare dati non rilevanti, che non sono interessati dalle regole illustrate sopra, l'operazione non viene eseguita.

   L'operazione di copia/incolla può essere applicata all'intera tabella o solo a una parte di essa.

   Nota: Quando si selezionano due celle consecutive contenenti un valore numerico e si trascina il cursore del mouse verso il basso tenendo premuto il pulsante, nelle colonne seguenti non vengono inseriti numeri ascendenti ma una copia delle celle selezionate.

Concetti correlati

Dati dell'utente alla pagina 159

5.7.4 Configurazione ISDN

Nella finestra **Configurazione ISDN** si definisce se gli utenti ISDN devono essere connessi o se la connessione alla linea esterna deve avvenire mediante ISDN. Questa può essere impostata come connessione ISDN punto - punto e/o punto - multipunto. Per ciascun sistema di comunicazione ed eventualmente modulo utilizzato sono disponibili varie connessioni S_0.

Sono disponibili le seguenti opzioni:

- Attivazione della configurazione ISDN:
  1) Configurazione della connessione ISDN punto - punto

     È possibile configurare una connessione linea esterna ISDN come connessione punto - punto con numeri interni.
  2) Configurazione della connessione ISDN punto - multipunto

     È possibile configurare una connessione linea esterna ISDN come connessione punto - multipunto con numeri MSN.
  3) Configurazione della connessione di utenti ISDN (opzionale)

     Una o più interfacce S_0possono essere configurate come interfacce S_0 interne per il collegamento di utenti ISDN (telefono o fax ISDN). Per ogni utente ISDN, è necessaria una licenza apparecchio.
- Disattivazione della configurazione ISDN

  Se non si dispone di una connessione linea urbana ISDN, è necessario disattivare la configurazione ISDN. Tutte le interfacce S_0 vengono automaticamente configurate come connessioni interne S_0.

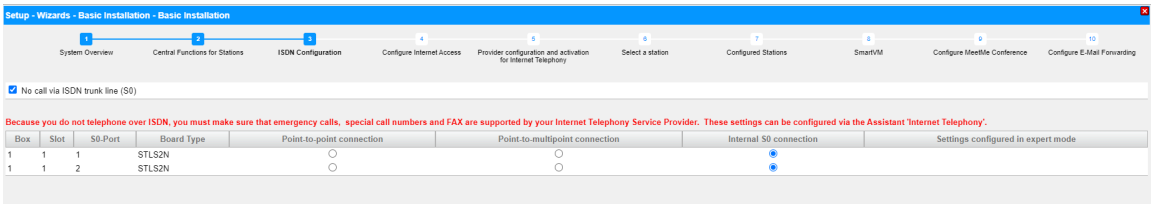
Ulteriori opzioni per gli attacchi linea urbana

Invece della linea esterna ISDN, è possibile disporre anche di una linea esterna analogica o di una linea esterna che utilizza un provider di telefonia Internet (provider ITSP, SIP). La configurazione dei collegamenti alla linea esterna analogica è possibile solo dopo l'installazione di base.

5.7.4.1 Come configurare il collegamento di utenti ISDN

Prerequisiti

Si è nella finestra **Configurazione ISDN** della procedura guidata **Installazione di base**.



Passo a passo

1) Lasciare disattivata la casella di controllo **Nessuna telefonia tramite linea esterna ISDN (S0)**.
2) Per l'interfaccia S_0 desiderata, selezionare il pulsante di opzione interfaccia **Connessione S0 interna**.

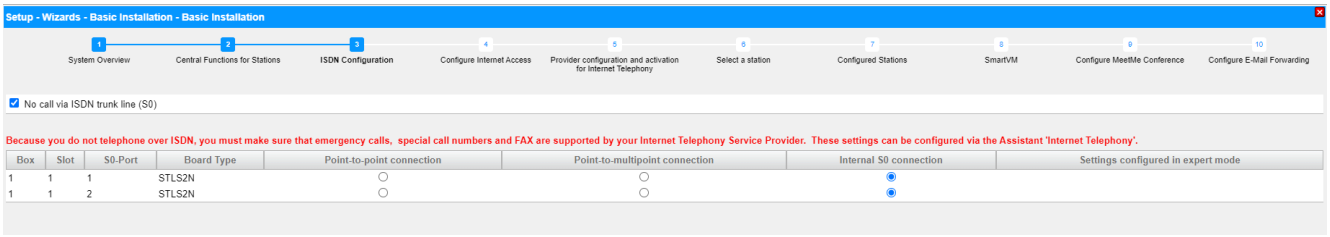
Passaggi successivi

Configurazione della connessione ISDN punto - punto e/o configurazione della connessione ISDN punto - multipunto.

5.7.4.2 Come configurare la linea esterna punto - punto ISDN

Prerequisiti

Si è nella finestra **Configurazione ISDN** della procedura guidata **Installazione di base**.



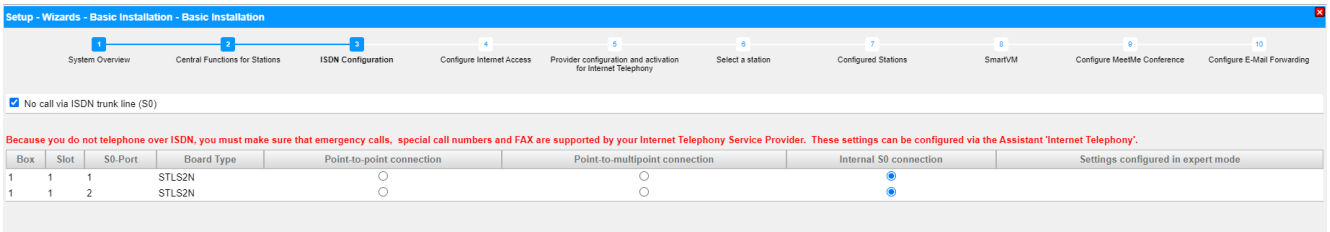
Passo a passo

1) Per configurare la linea esterna ISDN, lasciare deselezionata la casella di controllo **No telefonia tramite linea esterna ISDN (S0)**.
2) Per la porta S_0 desiderata, selezionare il pulsante di opzione **Connessione punto - punto**.
3) Fare clic su **OK & Avanti**.

5.7.4.3 Come configurare la linea esterna punto - multipunto ISDN

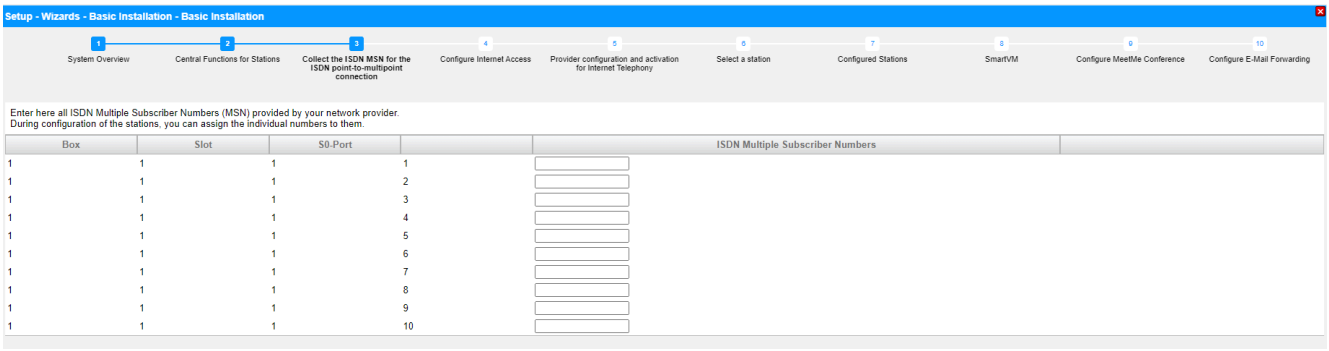
Prerequisiti

Si è nella finestra **Configurazione ISDN** della procedura guidata **Installazione di base**.



Passo a passo

1) Per configurare la linea esterna ISDN, lasciare deselezionata la casella di controllo **No telefonia tramite linea esterna ISDN (S0)**.
2) Per la porta S**0** desiderata, selezionare il pulsante di opzione **Connessione punto - multipunto**.
3) Fare clic su **OK & Avanti**.



4) Nella colonna **Numeri MSN ISDN** immettere tutti i numeri MSN comunicati dal gestore di rete. Per ciascuna porta S_0 si possono immettere fino a 10 numeri MSN. Il numero di porte S_0 dipende dal sistema di comunicazione ed eventualmente dal modulo utilizzato.
5) Fare clic su **OK & Avanti**.

5.7.4.4 Come disattivare la configurazione ISDN

Prerequisiti

Si è nella finestra **Configurazione ISDN** della procedura guidata **Installazione di base**.

Passo a passo

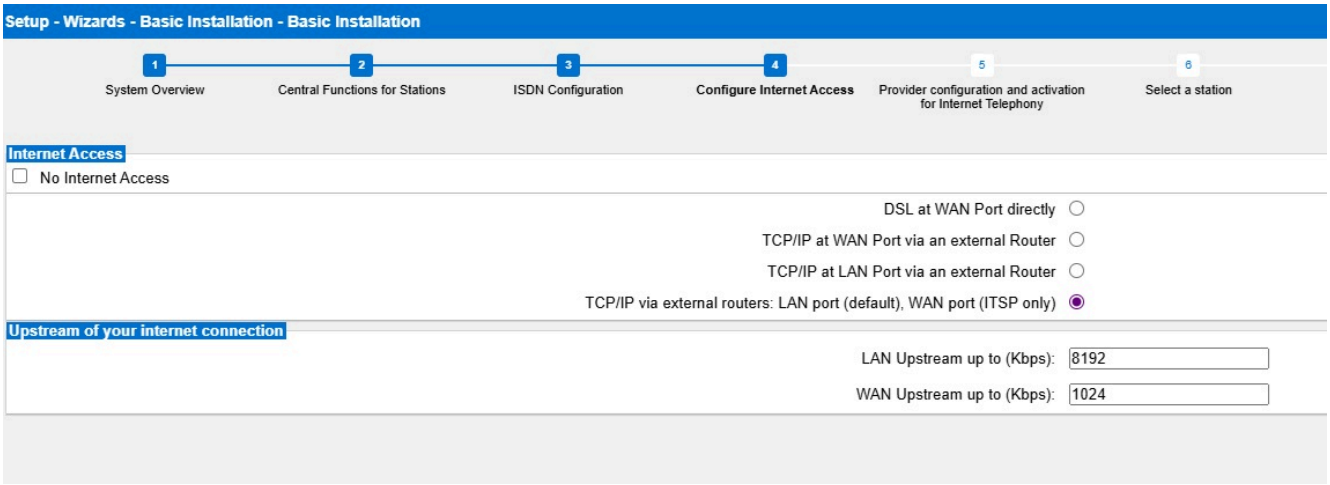
1) Selezionare la casella di controllo **No telefonia tramite linea esterna ISDN (S0)**.

> **Nota:** Le conversazioni si possono inoltre effettuare tramite un Provider di servizi di telefonia Internet, vedere Telefonia Internet.

2) Fare clic su **OK & Avanti**.

5.7.5 Accesso a Internet

È possibile utilizzare la finestra **Configurare l'accesso a Internet** per configurare l'accesso a Internet.



La configurazione dell'accesso a Internet nel WBM dipende dal fatto che la connessione a Internet sia già stata impostata in un router esterno o che avvenga tramite un modem Internet e quindi debba essere impostata nel WBM.

È possibile selezionare solo una delle opzioni elencate.

- Accesso a Internet tramite un modem Internet (**DSL direttamente sulla porta WAN**)

  Si desidera far funzionare il sistema di comunicazione direttamente con un modem Internet (DSL, cavo, UMTS...). OpenScape Business ha il router Internet integrato. Immettere i dati di accesso del Provider di servizi Internet (ISP) direttamente nel sistema di comunicazione e utilizzare la porta WAN del sistema di comunicazione.



Sono disponibili le seguenti opzioni:

– **Accesso a Internet tramite un ISP preconfigurato**
– **Accesso a Internet tramite l'ISP PPPoE standard**
– **Accesso a Internet tramite l'ISP PPTP standard**

Se il proprio ISP non è presente nell'elenco degli ISP preconfigurati, utilizzare l'ISP PPPoE o PPTP predefinito.

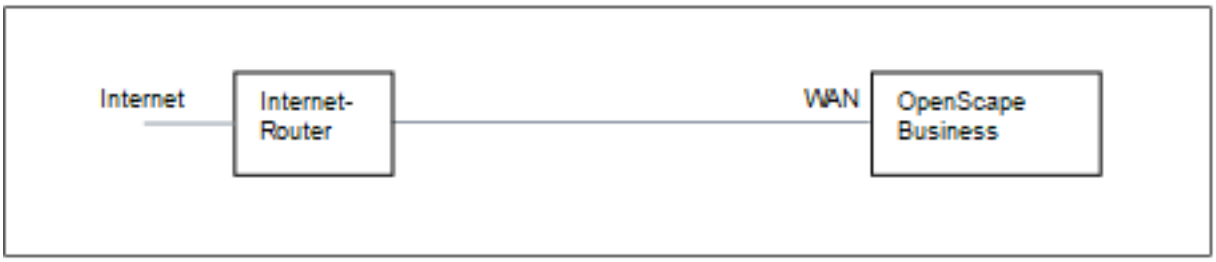
- Accesso a Internet tramite un router Internet esterno

  Si desidera utilizzare il sistema di comunicazione su un router Internet esterno. Il provider di servizi Internet è già configurato nel router Internet.

  Sono disponibili le seguenti opzioni:

  – **Accesso a Internet tramite un router Internet esterno sulla porta WAN**

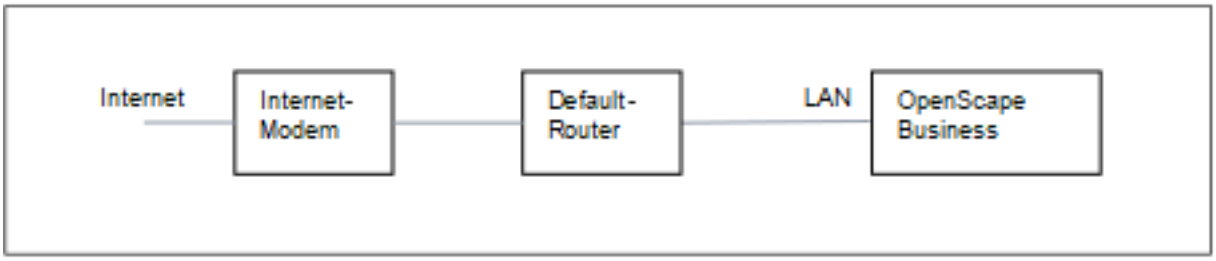
    (**TCP/IP sulla porta WAN attraverso un router esterno**)



    A tal fine, si utilizza la porta WAN del sistema di comunicazione. OpenScape Business conosce il router Internet o funziona come client DHCP. Questa opzione può essere utilizzata se il router Internet si trova in un altro segmento di rete e dispone di un proprio server DHCP.

  – **Accesso a Internet tramite un router Internet esterno sulla porta LAN**

    (**TCP/IP sulla porta LAN attraverso un router esterno**)

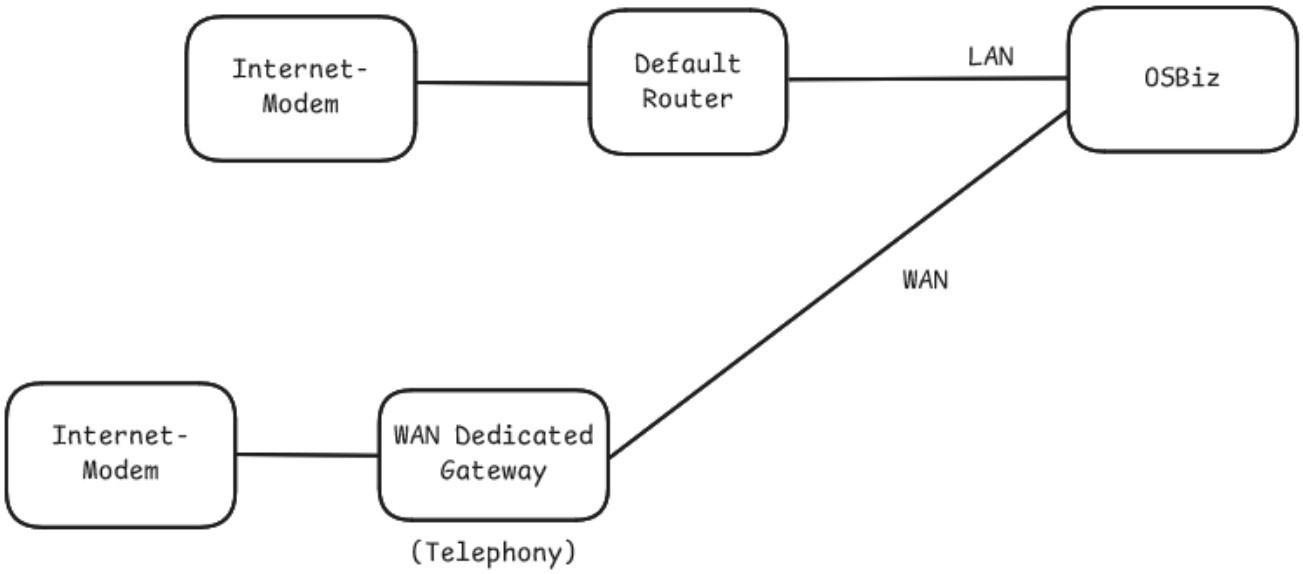


    A tal fine, si utilizza la porta LAN del sistema di comunicazione. OpenScape Business conosce solo il router predefinito e non l'infrastruttura sottostante. Per attivare la connessione al router Internet,

l'indirizzo IP del router predefinito e quello del server DNS devono essere resi noti al sistema di comunicazione.

– **Accesso a Internet tramite un router Internet esterno sulla porta LAN**

TCP/IP su porta LAN/WAN attraverso un router esterno con porta WAN dedicata all'ITSP



A tal fine, si utilizza la porta LAN del sistema di comunicazione, mentre la porta WAN è dedicata all'ITSP. OpenScape Business conosce solo il router predefinito e non l'infrastruttura sottostante. Per attivare la connessione al router Internet, l'indirizzo IP del router predefinito e quello del server DNS devono essere resi noti al sistema di comunicazione.

- Disattivare l'accesso a Internet (impostazione predefinita)

  Non si vuole utilizzare Internet.

5.7.5.1 Come configurare l'accesso a Internet tramite un router Internet esterno mediante una connessione LAN

Prerequisiti

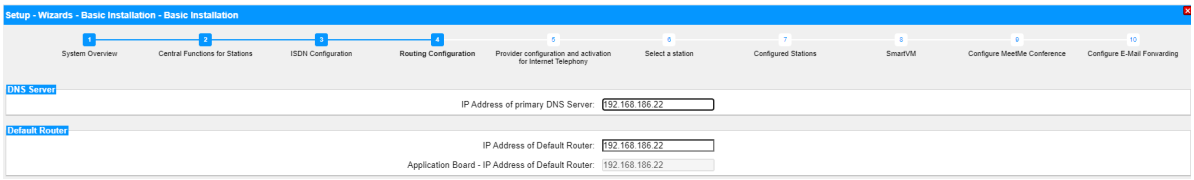
Il sistema di comunicazione deve essere collegato tramite l'interfaccia "LAN" alla LAN del cliente. La connessione non deve avvenire tramite WAN poiché questa è disattivata.

Si è nella finestra **Configurazione accesso a Internet** della procedura guidata **Installazione di base**.

Passo a passo

1) Deselezionare la casella di controllo **Nessun accesso ad Internet**.

2) Attivare il pulsante di opzione **TCP/IP alla porta LAN tramite router esterno**, immettere la velocità di caricamento della propria connessione a Internet nel campo **Upstream fino a (Kbps)** e fare clic su **OK & Avanti**.



3) Nel campo **Indirizzo IP dei server DNS** immettere l'indirizzo IP del server DNS locale (ad esempio il router Internet) o del server DNS Internet (ad esempio per telefonia Internet).
4) Nel campo **Indirizzo IP del router predefinito** immettere l'indirizzo IP del router Internet esterno.
5) Fare clic su **OK & Avanti**.

5.7.5.2 Come configurare l'accesso a Internet con un router Internet esterno mediante una connessione WAN

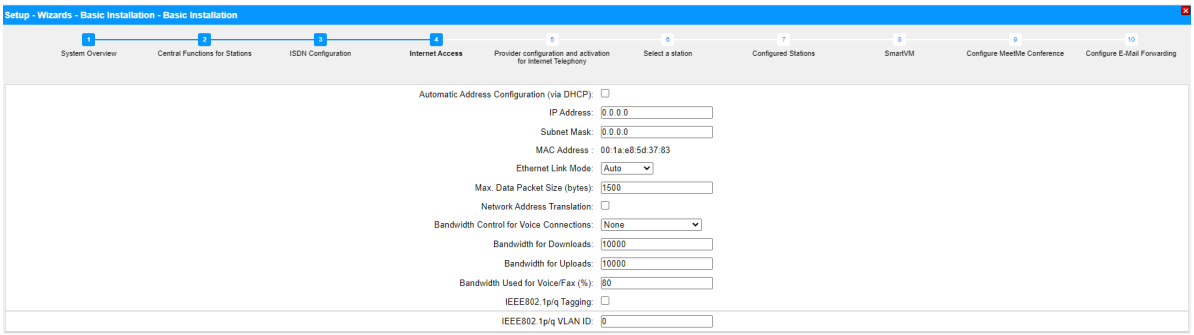
Prerequisiti

Il sistema di comunicazione deve essere collegato tramite l'interfaccia "LAN" al segmento LAN della LAN del cliente in cui si trova il router Internet.

Si è nella finestra **Configurazione accesso a Internet** della procedura guidata **Installazione di base**.

Passo a passo

1) Deselezionare la casella di controllo **Nessun accesso ad Internet**.
2) Selezionare **TCP/IP alla porta WAN tramite router esterno** quindi fare clic su **OK & Avanti**.



3) Se da un server DHCP già attivo devono essere ottenuti i dati specifici della rete per l'interfaccia WAN:
   a) Selezionare la casella di controllo **Configurazione automatica indirizzo (via DHCP)**.
   b) Selezionare la casella di controllo **Accetta indirizzo IP del router predefinito**.
   c) Se necessario, attivare la casella di controllo **Accetta indirizzo IP dei server DNS**.
   d) Se necessario, attivare la casella di controllo **Accetta indirizzo IP dei server SNTP**.

4) Se all'interfaccia WAN deve essere assegnato un indirizzo IP fisso:
   a) Deselezionare la casella di controllo **Configurazione automatica indirizzo (via DHCP)**.
   b) Inserire l'**Indirizzo IP** e la **Maschera di rete** desiderati per l'interfaccia WAN.
5) Selezionare la casella di controllo **Network Address Translation (NAT)**.
6) Se si desidera utilizzare anche la telefonia Internet, nell'elenco a discesa **Controllo della larghezza di banda per connessioni voce** selezionare **Solo upload** o **Upload e download**, come necessario. In caso di una larghezza di banda elevata per il download e più limitata per il caricamento, la regolazione della larghezza di banda deve essere attivata solo per il caricamento, affinché non venga inutilmente riservata molta larghezza di banda di download per la trasmissione voce.
7) Nei campi **Larghezza di banda per download** e **Larghezza di banda per upload** immettere la larghezza di banda per download e upload espressa in kbit/sec. messa a disposizione dal proprio provider di servizi Internet.
8) Fare clic su **OK & Avanti**.

5.7.5.3 Come configurare l'accesso a Internet tramite ISP preimpostato

Prerequisiti

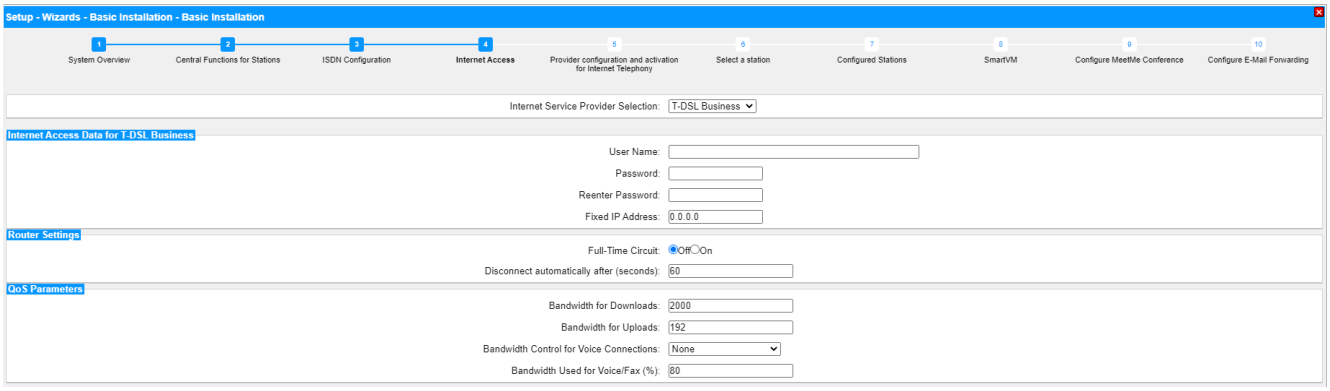
Si è nella finestra **Configurazione accesso a Internet** della procedura guidata **Installazione di base**.

I dati di accesso Internet del proprio ISP sono disponibili (ad es. ID utente, password, larghezza di banda in upload e download).

Opzionale: Sono disponibili i dati di un account DynDNS (nome, password, nome host, nome di dominio del provider DynDNS)

Passo a passo

1) Deselezionare la casella di controllo **Nessun accesso ad Internet**.
2) Selezionare il pulsante di opzione **DSL direttamente su porta WAN della scheda madre**, quindi fare clic su **OK & Avanti**.



3) Nell'elenco a discesa **Scelta del provider di servizi Internet**, selezionare il proprio ISP.
4) Nell'area **Dati di accesso ad Internet per** immettere i dati di accesso forniti dal provider. Le opzioni presenti in quest'area dipendono dal provider di servizi. Nell'immettere i dati rispettare maiuscole e minuscole.

5) In **Impostazioni router**, **Connessione permanente**, selezionare una delle seguenti opzioni in base al proprio modello tariffario:
   - In caso di tariffa Flatrate, selezionare **On**. Nel campo **Interruzione alle (hh:mm)**, immettere l'orario in cui interrompere la connessione a Internet (ad es. 01:30). In questo momento non devono essere scambiati dati su Internet (ad esempio, download di software o di telefonia Internet).
   - Se il modello tariffario è a tempo, selezionare **Off**. Nel campo **Disconnetti automaticamente dopo (secondi)**, immettere la durata dell'inattività trascorsa la quale viene interrotta la connessione Internet (ad es. 60 secondi).
6) Nell'area **Parametri QoS** immettere i seguenti valori:
   a) Nei campi **Larghezza di banda per download** e **Larghezza di banda per upload** immettere la larghezza di banda per download e upload espressa in kbit/sec. messa a disposizione dall'ISP.
   b) Se si desidera utilizzare anche la telefonia Internet, nell'elenco a discesa **Controllo della larghezza di banda per connessioni voce** selezionare **Solo upload** o **Upload e download**, come necessario. Nel campo **Larghezza di banda per connessioni voce/fax (%)** immettere la percentuale di larghezza di banda da riservare alle connessioni voce e fax (predefinito: 80%).
7) Fare clic su **OK & Avanti**. Si aprirà la finestra **Configura account DynDNS**.
8) Se si desidera utilizzare una VPN o la funzione di accesso remoto e non si dispone di un indirizzo IP statico, è necessario disporre di un account DynDNS (ad esempio, presso dyndns.org) e configurarlo.
   a) Se il provider DynDNS desiderato è disponibile nel menu a discesa **Nome del dominio**, selezionarlo dall'elenco (ad esempio dyndns.org).
   b) Se il provider del DynDNS desiderato non è compreso nell'elenco a discesa **Nome del dominio**, selezionare la casella di controllo **Dominio definito dall'utente**. Nel campo **Nome del dominio** immettere il provider del DynDNS desiderato e nel campo **URL aggiornamento** l'URL aggiornato del provider DynDNS. La struttura di tale URL dipende dal provider DynDNS. Inoltre, completare con i parametri specifici per il cliente (nell'esempio contrassegnati in *corsivo*).

      `http://www.anydns.info/update.php?user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`
   c) Inserire il **Nome utente** e la **Password** del proprio account DynDNS.
   d) Nel campo **Nome dell'host** immettere il nome host indicato dal fornitore DynDNS, senza nome di dominio, ad es. myhost. Il nome di dominio completo risulta myhost.dyndns.org.
   e) Testare l'account DynDNS utilizzando **Test connessione**.
   f) Se il test ha avuto esito positivo, fare clic su **OK**.
   g) Fare clic su **OK & Avanti**.
9) Se si dispone di un indirizzo IP statico pubblico o non si desidera utilizzare la VPN o l'accesso remoto, fare clic su **Nessun DynDNS**.
10) Fare clic su **OK & Avanti**.

5.7.5.4 Come configurare l'accesso a Internet tramite un ISP standard PPPoE

Prerequisiti

Si è nella finestra **Configurazione accesso a Internet** della procedura guidata **Installazione di base**.

L'ISP deve mettere a disposizione i seguenti dati per l'accesso a Internet:

Campo	Descrizione	Valore da ISP
Parametri IP (solo per indirizzi IP fissi)		
Indirizzo IP partner della connessione PPP	Indirizzo IP del server dell'ISP.	
Indirizzo IP locale della connessione PPP	Indirizzo IP comunicato dall'ISP per l'accesso a Internet.	
Autenticazione (tramite PAP o CHAP). PAP viene difficilmente utilizzata poiché l'autenticazione non è crittografata.		
Nome d'utente PPP	Nome utente per la connessione PPP, comunicato dall'ISP.	
Modalità di autenticazione PAP	Modalità di autenticazione per la connessione PPP su PAP: **Client PAP**, **Host PAP** o **Non utilizzato**.	
Password PAP	Password per l'autenticazione PAP, comunicata dall'ISP.	
Modalità di autenticazione CHAP	Modalità di autenticazione per la connessione PPP tramite CHAP: **Client CHAP**, **Host CHAP**, **Client e host CHAP** o **Non utilizzato**.	
Password CHAP	Password per l'autenticazione tramite CHAP, comunicata dall'ISP.	
Parametri QoS dell'interfaccia		
Larghezza di banda per download	Valore della larghezza di banda complessiva in kbit/sec. per il download dall'ISP.	
Larghezza di banda per upload	Valore della larghezza di banda complessiva in kbps per il caricamento fornito dall'ISP.	

Opzionale: Sono disponibili i dati di un account DynDNS (nome, password, nome host, nome di dominio del provider DynDNS)

Passo a passo

1) Deselezionare la casella di controllo **Nessun accesso ad Internet**.
2) Selezionare il pulsante di opzione **DSL direttamente su porta WAN**, quindi fare clic su **OK & Avanti**.
3) Nell'elenco a discesa **Scelta del provider di servizi Internet**, selezionare il tipo ISP standard **Provider PPPoE**.
4) Nell'area **Parametri IP**, selezionare la casella di controllo **Parametri IP** solo se l'ISP ha richiesto una modifica dei parametri. In questo caso,

nei campi **Indirizzo IP partner della connessione PPP**, **Indirizzo IP locale della connessione PPP** e **Lunghezza max. pacchetto dati (byte)** immettere i valori comunicati dall'ISP. Nell'elenco a discesa **Negoziazione dell'indirizzo IP** selezionare la voce **Utilizza indirizzo IP configurato**.

5) In **Impostazioni router**, **Connessione permanente**, selezionare una delle seguenti opzioni in base al proprio modello tariffario:

- In caso di tariffa Flatrate, selezionare **On**. Nel campo **Interruzione alle (hh:mm)**, immettere l'orario in cui interrompere la connessione a Internet (ad es. 01:30). In questo momento non devono essere scambiati dati su Internet (ad esempio, download di software o di telefonia Internet).
- Se il modello tariffario è a tempo, selezionare **Off**. Nel campo **Disconnetti automaticamente dopo (secondi)**, immettere la durata dell'inattività trascorsa la quale viene interrotta la connessione Internet (ad es. 60 secondi).

6) Le impostazioni nell'area **Autenticazione** dipendono dal fatto che l'ISP metta a disposizione o meno un'autenticazione tramite PPP.

- Se l'autenticazione viene fornita dall'ISP: Assicurarsi di selezionare la casella di controllo **Autenticazione PPP**. Come Nome utente PPP utilizzare il nome fornito dall'ISP per l'accesso a Internet. Lo standard utilizzato per la modalità di autenticazione è **CHAP-Client**.
- Se l'autenticazione non viene fornita dall'ISP: Assicurarsi di deselezionare la casella di controllo Autenticazione PPP.

7) Se si desidera utilizzare NAT, nell'area **Conversione indirizzi**, selezionare la casella di controllo **NAT** (per impostazione predefinita è già selezionata).

8) Nell'area **Parametri QoS dell'interfaccia** immettere i seguenti valori:

a) Nei campi **Larghezza di banda per download** e **Larghezza di banda per upload** immettere la larghezza di banda per download e upload espressa in kbit/sec. messa a disposizione dall'ISP.

b) Se si desidera utilizzare anche la telefonia Internet, nell'elenco a discesa **Controllo della larghezza di banda per connessioni voce** selezionare **Solo upload** o **Upload e download**, come necessario. Nel campo **Larghezza di banda per connessioni voce/fax (%)** immettere la percentuale di larghezza di banda da riservare alle connessioni voce e fax (predefinito: 80%).

9) Fare clic su **OK & Avanti**. Si aprirà la finestra **Configura account DynDNS**.

10) Se si desidera utilizzare una VPN o la funzione di accesso remoto e non si dispone di un indirizzo IP statico, è necessario disporre di un account DynDNS (ad esempio, presso dyndns.org) e configurarlo.

a) Se il provider DynDNS desiderato è disponibile nel menu a discesa **Nome del dominio**, selezionarlo dall'elenco (ad esempio dyndns.org).

b) Se il provider del DynDNS desiderato non è compreso nell'elenco a discesa **Nome del dominio**, selezionare la casella di controllo **Dominio definito dall'utente**. Nel campo **Nome del dominio** immettere il provider del DynDNS desiderato e nel campo **URL aggiornamento** l'URL aggiornato del provider DynDNS. La struttura di tale URL dipende dal provider DynDNS. Inoltre, completare con i parametri specifici per il cliente (nell'esempio contrassegnati in *corsivo*).

```
http://www.anydns.info/update.php?
user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>
```

c) Inserire il **Nome utente** e la **Password** del proprio account DynDNS.
d) Nel campo **Nome dell'host** immettere il nome host indicato dal fornitore DynDNS, senza nome di dominio, ad es. myhost. Il nome di dominio completo risulta myhost.dyndns.org.
e) Testare l'account DynDNS utilizzando **Test connessione**.
f) Se il test ha avuto esito positivo, fare clic su **OK**.
g) Fare clic su **OK & Avanti**.

11) Se si dispone di un indirizzo IP statico pubblico o non si desidera utilizzare la VPN o l'accesso remoto, fare clic su **Nessun DynDNS**.

12) Fare clic su **OK & Avanti**.

5.7.5.5 Come configurare l'accesso a Internet tramite un ISP standard PPTP

Prerequisiti

Si è nella finestra **Configurazione accesso a Internet** della procedura guidata **Installazione di base**.

L'ISP deve mettere a disposizione i seguenti dati per l'accesso a Internet:

Campo	Descrizione	Valore da ISP
Parametri IP (solo per indirizzi IP fissi)		
Indirizzo IP partner della connessione PPP	Indirizzo IP del server dell'ISP.	
Indirizzo IP locale della connessione PPP	Indirizzo IP comunicato dall'ISP per l'accesso a Internet.	
Parametri PPTP		
Indirizzo IP locale della connessione di controllo	Indirizzo IP comunicato dall'ISP per la connessione PPTP. Il valore predefinito è 10.0.0.140.	
Indirizzo IP partner della connessione di controllo	Indirizzo IP del server ISP destinato alla connessione PPTP. Il valore predefinito è 10.0.0.138.	
Maschera di rete partner della connessione di controllo	Maschera di rete comunicata dall'ISP per la connessione PPTP. Il valore predefinito è 255.255.255.248.	
Autenticazione (tramite PAP o CHAP). PAP viene difficilmente utilizzata poiché l'autenticazione non è crittografata.		
Nome utente PPP	Nome utente per la connessione PPP, comunicato dall'ISP.	
Modalità di autenticazione PAP	Modalità di autenticazione per la connessione PPP via PAP: **Client PAP**, **Host PAP** o **non utilizzata**.	
Password PAP	Password per l'autenticazione PAP, comunicata dall'ISP.	

Campo	Descrizione	Valore da ISP
Modalità di autenticazione CHAP	Modalità di autenticazione per la connessione PPP via CHAP: **Client CHAP**, **Host CHAP**, **Client e Host CHAP** o **non utilizzata**.	
Password CHAP	Password per l'autenticazione tramite CHAP, comunicata dall'ISP.	
Parametri QoS dell'interfaccia		
Larghezza di banda per download	Valore della larghezza di banda complessiva in kbit/sec. per il download dall'ISP.	
Larghezza di banda per upload	Valore della larghezza di banda complessiva in kbit/sec. per l'upload fornito dall'ISP.	

Opzionale: sono disponibili i dati di un account DynDNS (nome, password, nome host, nome di dominio del provider DynDNS)

Passo a passo

1) Deselezionare la casella di controllo **Nessun accesso ad Internet**.
2) Selezionare il campo opzione **DSL direttamente su porta WAN** quindi fare clic su **OK & Avanti**.
3) Nell'elenco a discesa **Scelta del provider di servizi Internet**, selezionare il tipo ISP standard **Provider PPTP**.
4) Nell'area **Parametri IP**, selezionare la casella di controllo **Parametri IP** solo se l'ISP ha richiesto una modifica dei parametri. In questo caso, nei campi **Indirizzo IP partner della connessione PPP**, **Indirizzo IP locale della connessione PPP** e **Lunghezza max. pacchetto dati (byte)** immettere i valori comunicati dall'ISP. Nell'elenco a discesa **Negoziazione dell'indirizzo IP** selezionare la voce **Utilizza indirizzo IP configurato**.
5) Nell'area **Parametri PPTP** immettere i valori indicati dall'ISP.
6) Se si utilizza una tariffazione a tempo, selezionare la casella di controllo **Modalità Short Hold**. Nel campo **Tempo Short Hold (s)**, immettere la durata dell'inattività trascorsa la quale viene interrotta la connessione Internet (ad es. 60 secondi).
7) Le impostazioni nell'area **Autenticazione** dipendono dal fatto che l'ISP metta a disposizione o meno un'autenticazione tramite PPP.
   - Se l'autenticazione viene fornita dall'ISP: assicurarsi di selezionare la casella di controllo **Autenticazione PPP**. Come Nome utente PPP utilizzare il nome fornito dall'ISP per l'accesso a Internet. Immettere le impostazioni PAP e CHAP, come indicato dall'ISP.
   - Se l'autenticazione non viene fornita dall'ISP: assicurarsi di deselezionare la casella di controllo Autenticazione PPP.
8) Se si desidera utilizzare NAT, nell'area **Conversione indirizzi**, selezionare la casella di controllo **NAT** (per impostazione predefinita è già selezionata).

9) Nell'area **Parametri QoS dell'interfaccia** immettere i seguenti valori:
   a) Nei campi **Larghezza di banda per download** e **Larghezza di banda per upload** immettere la larghezza di banda per download e upload espressa in kbit/sec. messa a disposizione dall'ISP.
   b) Se si desidera utilizzare anche la telefonia Internet, nell'elenco a discesa **Controllo della larghezza di banda per connessioni voce** selezionare **Solo upload** o **Upload e download**, come necessario. Nel campo **Larghezza di banda per connessioni voce/fax (%)** immettere la percentuale di larghezza di banda da riservare alle connessioni voce e fax (predefinito: 80%).
10) Fare clic su **OK & Avanti**. Si aprirà la finestra **Configura account DynDNS**.
11) Se si desidera utilizzare una VPN o la funzione di accesso remoto e non si dispone di un indirizzo IP statico, è necessario disporre di un account DynDNS (ad esempio, presso dyndns.org) e configurarlo.
   a) Se il provider DynDNS desiderato è disponibile nel menu a discesa **Nome del dominio**, selezionarlo dall'elenco (ad esempio dyndns.org).
   b) Se il provider del DynDNS desiderato non è compreso nell'elenco a discesa **Nome del dominio**, selezionare la casella di controllo **Dominio definito dall'utente**. Nel campo **Nome del dominio** immettere il provider del DynDNS desiderato e nel campo **URL aggiornamento** l'URL aggiornato del provider DynDNS. La struttura di tale URL dipende dal provider DynDNS. Inoltre, completare con i parametri specifici per il cliente (nell'esempio contrassegnati in *corsivo*).

      `http://www.anydns.info/update.php?`
      `user=<`*`nomeutente`*`>&password=<`*`password`*`>&host=<`*`dominio`*`>&ip=<`*`in`*
   c) Inserire il **Nome utente** e la **Password** del proprio account DynDNS.
   d) Nel campo **Nome dell'host** immettere il nome host indicato dal fornitore DynDNS, senza nome di dominio, ad es. myhost. Il nome di dominio completo risulta myhost.dyndns.org.
   e) Testare l'account DynDNS utilizzando **Test connessione**.
   f) Se il test ha avuto esito positivo, fare clic su **OK**.
   g) Fare clic su **OK & Avanti**.
12) Se si dispone di un indirizzo IP statico pubblico o non si desidera utilizzare la VPN o l'accesso remoto, fare clic su **Nessun DynDNS**.
13) Fare clic su **OK & Avanti**.

5.7.5.6 Come configurare l'accesso a Internet tramite un router Internet esterno sulla LAN con porta WAN dedicata all'ITSP

Prerequisiti

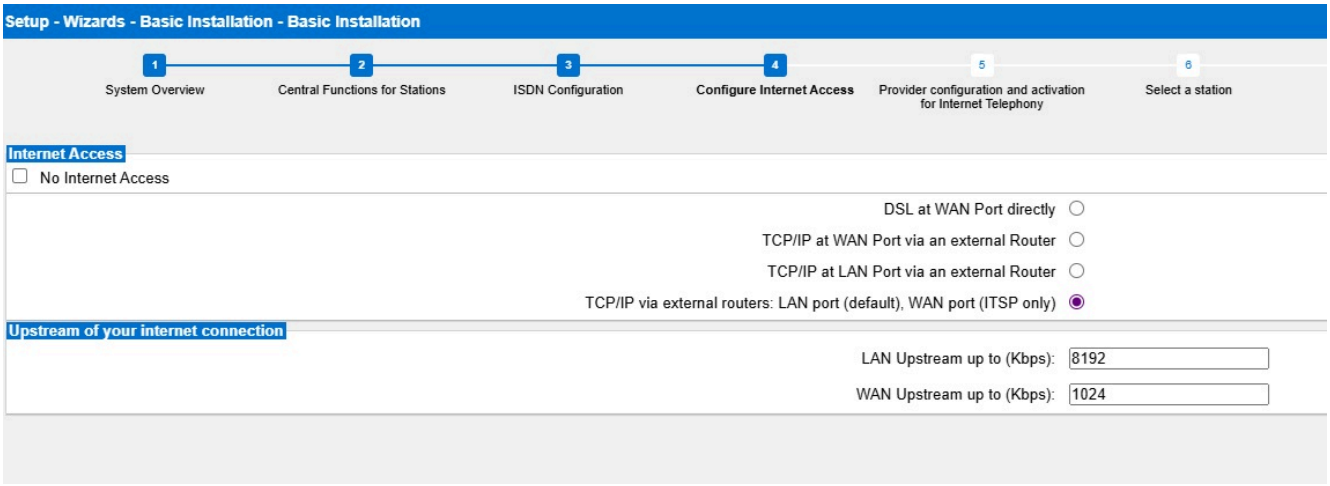
Si è nella finestra **Configurazione accesso a Internet** della procedura guidata **Installazione di base**.

Questa funzione è valida solo per gli ITSP che non richiedono l'uso di STUN nelle impostazioni del provider.

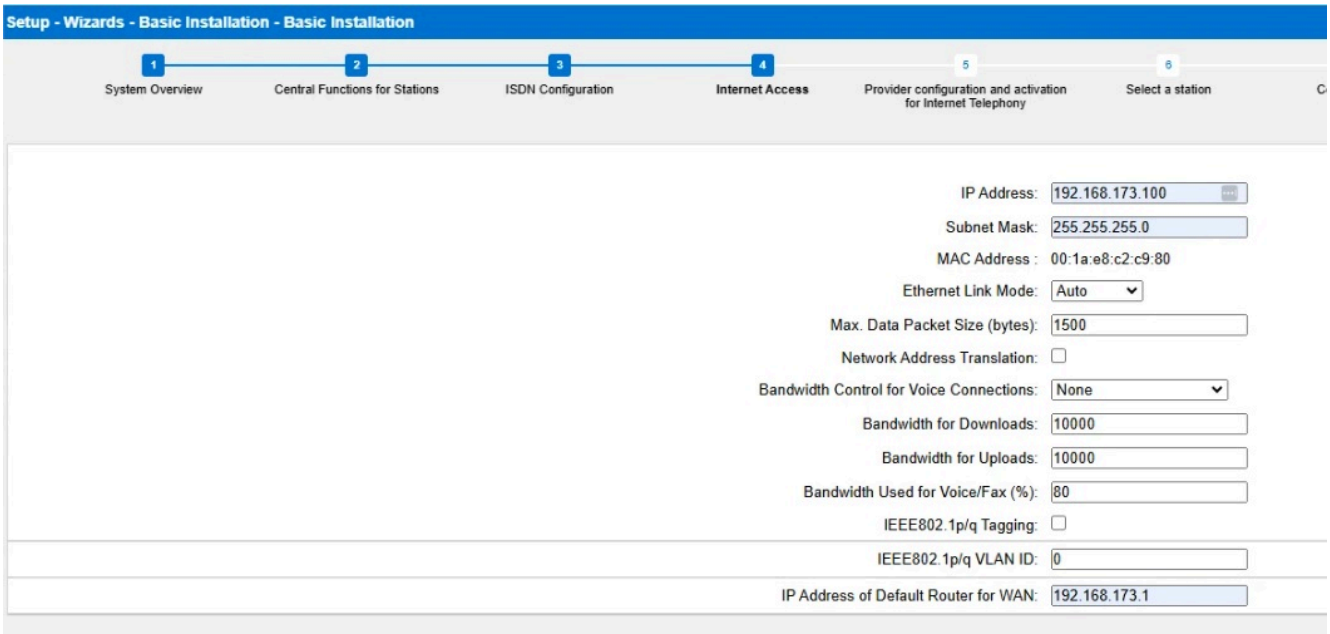
Non è possibile collegare contemporaneamente due ITSP identici (con lo stesso registrar/proxy) tramite LAN e WAN.

Passo a passo

1) Deselezionare la casella di controllo **Nessun accesso ad Internet**.
2) Attivare il pulsante di opzione **TCP/IP tramite router esterni: Porta LAN (predefinita), porta WAN (solo ITSP)**.



3) Configurare il valore massimo di Kbps in upstream nei campi **LAN upstream fino a (Kbps)** e **WAN upstream fino a (Kbps)** corrispondenti.
4) Fare clic su **OK & Avanti**.
5) Inserire la configurazione IP della porta WAN e anche l'indirizzo IP del router predefinito per la porta WAN.



6) Fare clic su **OK & Avanti**.

5.7.5.7 Come disattivare l'accesso a Internet

Prerequisiti

Si è nella finestra **Configurazione accesso a Internet** della procedura guidata **Installazione di base**.

Passo a passo

1) Lasciare selezionata la casella di controllo **Nessun accesso ad Internet**.
2) Fare clic su **OK & Avanti**.

5.7.6 Telefonia Internet

La finestra **Configurazione e attivazione provider per la telefonia Internet** consente di configurare la telefonia Internet. È possibile usare ITSP (Internet Telephony Service Provider) preconfigurati o configurarne di nuovi. Per ogni ITSP è possibile configurare uno o più account. È possibile attivare contemporaneamente fino a 8 ITSP.

Sono disponibili le seguenti opzioni:

- **Configurazione dell'ITSP predefinito**

  È possibile utilizzare modelli predefiniti di ITSP. A tal fine, nel modello vengono inseriti i propri dati e i numeri di telefono e questo viene successivamente attivato.
- **Configurazione di un nuovo ITSP**

  È possibile aggiungere e attivare nuovi ITSP.

  La configurazione di un nuovo ITSP è molto rara e richiede molto tempo. Pertanto, nella sezione dedicata alla prima installazione non viene descritta questa opzione. Per informazioni più dettagliate, consultare il capitolo Configurazione di un ITSP.
- **Disattivare la telefonia Internet**

  È possibile disattivare la telefonia Internet.

Nota:

Gli esempi di configurazione sono disponibili su Internet alla pagina **Unify Experts Wiki** in *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"* (disponibile solo in inglese e tedesco).

Assegnazione dei numeri di telefono ITSP

- Con una **connessione analogica di telefonia Internet** l'ITSP mette a disposizione singoli numeri di telefono, ad esempio 70005555, 70005556, ... Questi numeri vengono poi assegnati manualmente ai numeri interni degli utenti.
- Con una **connessione punto-punto di telefonia Internet** l'ITSP mette a disposizione una fascia di numeri (intervallo di numeri), ad esempio da (+39) 02 7007-100 a (+39) 02 7007-147. I numeri di telefono di questa fascia vengono successivamente assegnati manualmente ai numeri interni degli utenti.

I due tipi di connessione possono essere combinati.

In alternativa, per entrambi i tipi di collegamenti, i numeri di telefono dell'ITSP possono essere inseriti nella configurazione degli utenti come selezione passante dell'utente.

Numero di telefono interno	Servizio	DID
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

In questo modo, i numeri di telefono degli ITSP sono costituiti dal numero di sistema configurato (ad esempio il codice paese 49) e dal numero di selezione passante inserito in formato esteso. Ciò rappresenta un vantaggio nell'analisi del numero da comporre e nella gestione delle chiamate, anche in una rete. Quindi la connessione dell'ITSP è ad esempio estensibile anche a un altro nodo.

Eventuali ulteriori attacchi linea urbana via ISDN sono possibili solo con limitazioni (utile ad esempio per le chiamate di emergenza).

5.7.6.1 Come configurare un ITSP predefinito

Prerequisiti

Si è nella finestra **Configurazione del provider e attivazione della telefonia Internet** della procedura guidata **Installazione di base**.

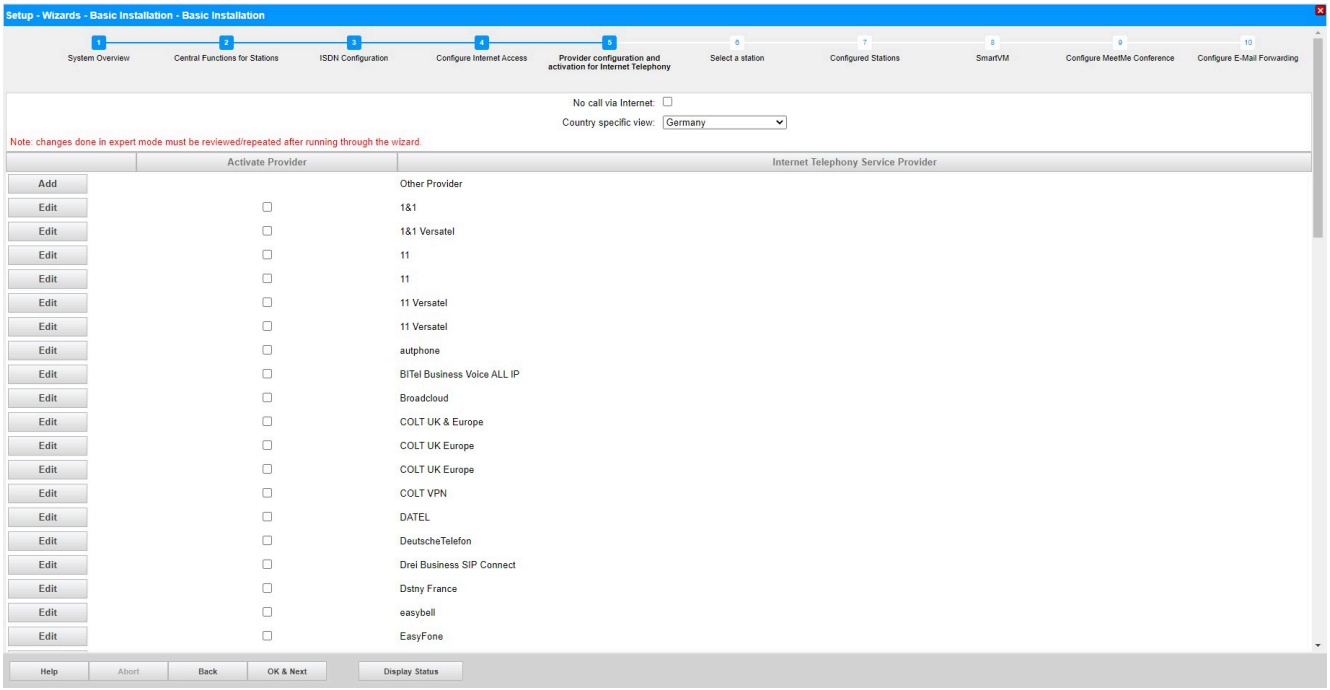
La connessione a Internet deve essere operativa.

I dati di accesso per la telefonia Internet del proprio ITSP sono disponibili (ad es. ID utente, password, numeri per telefonia Internet).

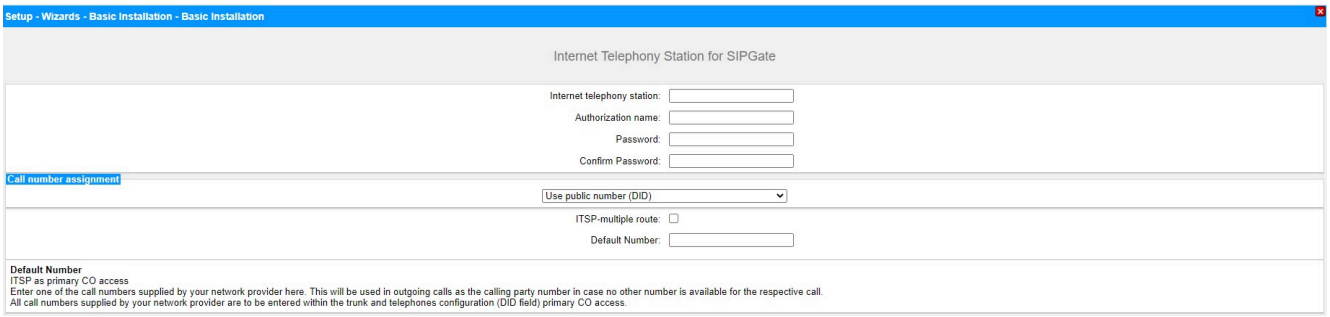
Passo a passo

1) Deselezionare la casella di controllo **No telefonia tramite Internet**. Viene visualizzata una lista degli ITSP possibili, in base al Paese. L'elenco

contiene gli ITSP predefiniti per il paese selezionato ed eventuali ITSP già creati.



2) Se si desidera modificare il Paese preimpostato, dall'elenco a discesa **Panoramica specifica del paese** selezionare il Paese desiderato. Verranno visualizzati gli ITSP disponibili per il Paese scelto.
3) Se necessario, fare clic su **Mostra stato**, per visualizzare quali sono gli ITSP già attivi e quali utenti di telefonia Internet sono configurati per i singoli ITSP. Si possono attivare fino a 8 ITSP. Fare quindi clic su **OK**.
4) Per configurare le stazioni di telefonia Internet, fare clic su **Modifica** nella riga associata all'ITSP corrispondente.
5) Selezionare la casella di controllo **Attiva provider**.
6) Fare clic su **OK & Avanti**.
7) Fare clic su **Aggiungi** per configurare il proprio account ITSP con i relativi numeri di telefonica Internet. I campi visualizzati dipendono dal provider.

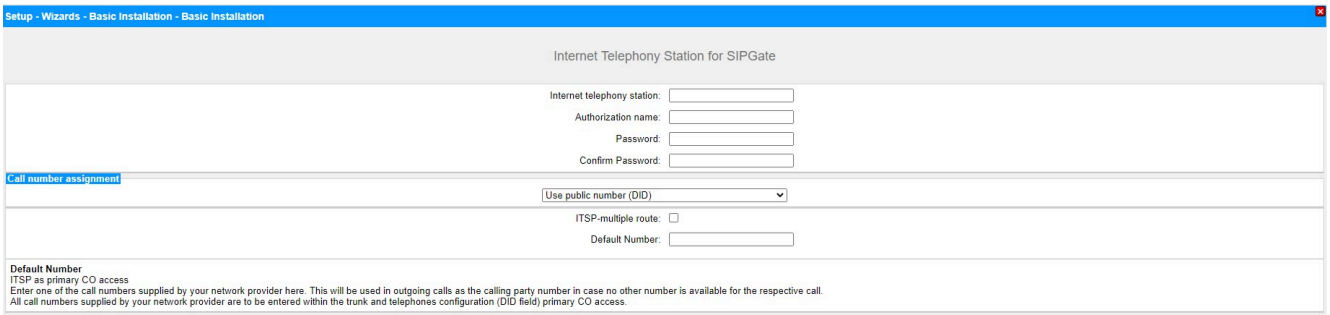


8) Nel campo **Utente di telefonia Internet** immettere i dati di accesso del proprio account. I dati sono stati forniti dall'ITSP. In base all'ITSP, possono venire utilizzati termini diversi, ad esempio: Utente SIP, ID SIP, ecc.
9) Nel campo **Nome autorizzazione** immettere il valore corrispondente. I dati sono stati forniti dall'ITSP. Se non si è ricevuto alcun nome autorizzazione, inserire gli stessi dati già indicati in **Utente di telefonia Internet**.

10) Nei campi **Nuova password** e **Ripeti password** immettere la password ricevuta dall'ITSP. In base all'ITSP, possono venire utilizzati termini diversi, ad esempio: Password, Password SIP, ecc.

11) Assegnazione dei numeri di telefonia Internet - Opzione 1:

Usa numero pubblico (DID): i numeri di telefonia via Internet della propria connessione utente o punto-punto di telefonia Internet non devono essere inseriti qui durante la configurazione dell'ITSP, ma durante la configurazione degli abbonati (nei campi **DID**).



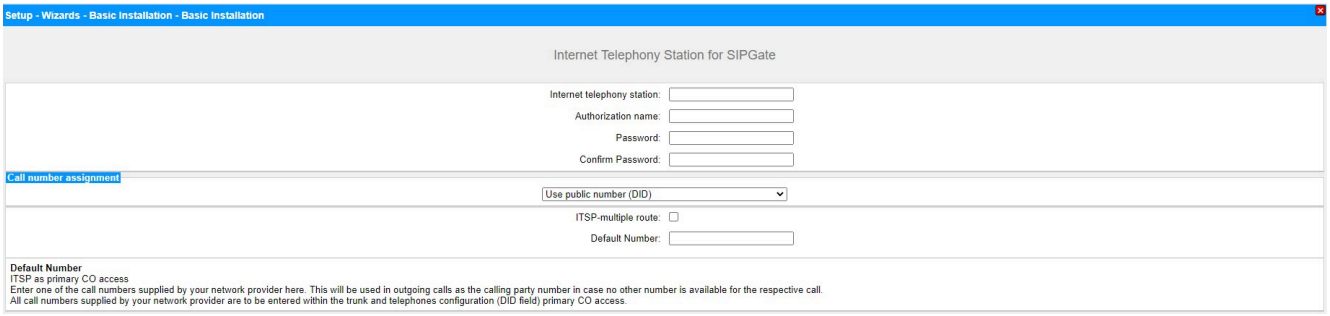
a) Nell'area **Assegnazione numero di telefono**, selezionare il pulsante di opzione **Usa numero pubblico (DID)**.

b) In **Numero predefinito**, inserire il numero di telefono da utilizzare per le chiamate in uscita quando non è disponibile un numero DID del chiamante.

c) Se il proprio ITSP supporta la funzione "Mobile Extension (MEX)", in **Numero MEX** inserire il numero MEX messo a disposizione dall'ITSP (8 cifre, solo numeri).

12) Assegnazione dei numeri di telefonia Internet - Opzione 2:

Usa numero interno (N° tel.) / singole voci: si dispone di una connessione stazione di telefonia Internet e si è ricevuto un numero di telefono singolo per la telefonia Internet (ad esempio, 70005555, 70005556,...). Questi numeri singoli vengono successivamente assegnati ai singoli numeri interni dell'utente.



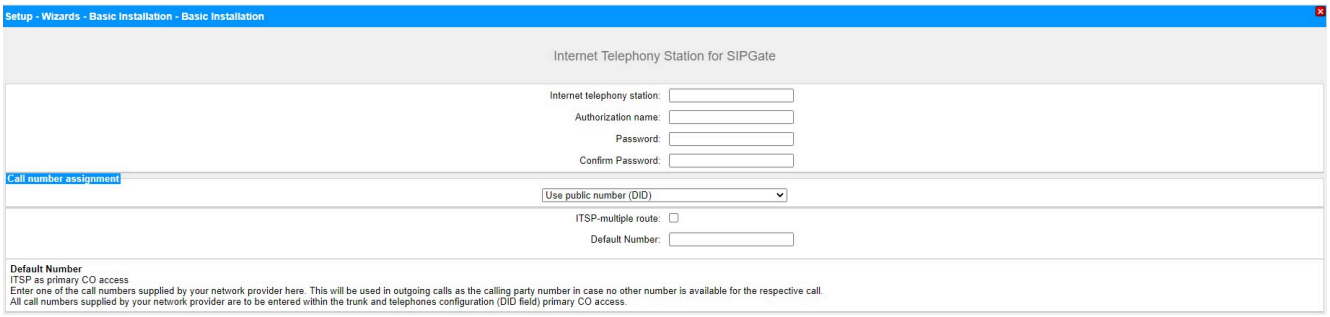
a) Nell'area **Assegnazione numero di telefono**, selezionare il pulsante di opzione **Usa numero interno (N° tel.) / singole registrazioni**.

b) Nell'area **Numeri telefonia Internet**, nel campo accanto al pulsante **Aggiungi** inserire uno dei numeri per telefonia Internet ricevuto dall'ITSP e fare clic su **Aggiungi**.

c) Se si desidera assegnare all'account altri numeri di telefonia Internet, ripetere il passo b).

13) Assegnazione dei numeri di telefonia Internet - Opzione 3:

Usa numero interno (N° tel.) / registrazione area: Si dispone di una connessione punto-punto di telefonia Internet e si è ricevuto un intervallo di numeri di telefono per la telefonia Internet, ad esempio da (+39) 02 7007-100 a (+39) 02 7007-147. I numeri di chiamata provenienti dall'intervallo di numeri di telefono vengono assegnati come numeri di chiamata interni degli utenti.



a) Nell'area **Assegnazione numero di telefono**, selezionare il pulsante di opzione **Usa numero interno (N° tel.) / registrazione area**.
b) In **Numero del sistema (prefisso)**, immettere il numero del sistema.
c) Nei campi **Fascia numeri interni diretti da** e **a**, immettere l'intervallo di numeri interni desiderato per l'utente di telefonia Internet. Di norma da 100 a 147.

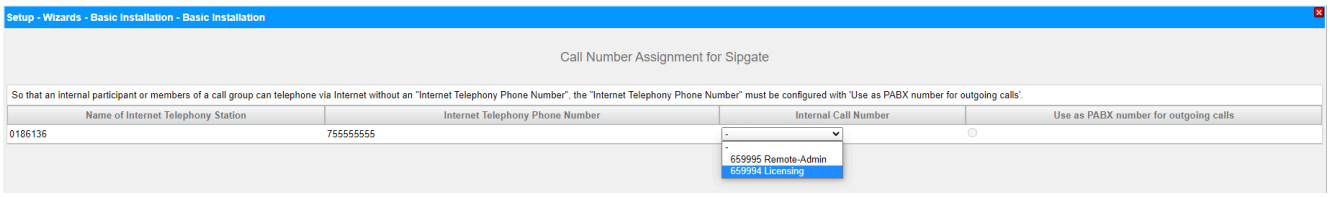
14) Fare clic su **OK & Avanti**.

15) Se si desidera configurare altri account con i numeri di telefonia Internet corrispondenti, ripetere i passaggi da 7 a 14.

16) Fare clic su **OK & Avanti**. Viene visualizzata una panoramica che riporta i numeri di telefono di telefonia Internet e gli account a cui sono assegnati.

17) Assegnare sempre tutti i numeri per telefonia Internet a un numero interno di un utente.

Questo passaggio non si applica se è stata selezionata l'opzione 1 per l'assegnazione dei numeri di telefono di telefonia Internet. In questo caso, l'assegnazione si effettua con la configurazione dell'utente nel campo **DID**.



a) Nella riga corrispondente dell'elenco a tendina **Numero interno** selezionare un numero di telefono interno.
b) Se un utente non dotato di numero di telefono per la telefonia Internet o membri di un gruppo di chiamata deve eseguire telefonate tramite Internet, è necessario selezionare il pulsante di opzione **Voce predefinita**. Il pulsante di opzione può essere selezionato solo per un singolo numero di telefonia Internet.

18) Fare clic su **OK & Avanti**. Qui viene visualizzato di nuovo l'elenco degli ITSP predefiniti e aggiunti di recente. Gli ITSP attivati sono contrassegnati con un segno di spunta nella colonna **Attiva provider**. Con **Riavvia ITSP** è possibile registrarsi nuovamente presso l'ITSP attivo in caso di problemi di connessione.

19) Fare clic su **OK & Avanti**.

20) Nel campo **Larghezza di banda della connessione (Kbit/s)** immettere il valore della velocità in upload della propria connessione Internet. Da non confondere con la velocità di download!

Nota: Nel campo **Numero conversazioni Internet simultanee** viene visualizzato il numero di conversazioni telefoniche Internet conducibili contemporaneamente. Se la qualità della conversazione peggiora a causa del sovraccarico della rete, è necessario ridurre il numero indicato.

Per ulteriori informazioni sul numero di chiamate Internet simultanee, fare riferimento a Limitazione del numero di chiamate simultanee tramite ITSP alla pagina 820.

---

21) Fare clic su **OK & Avanti**.

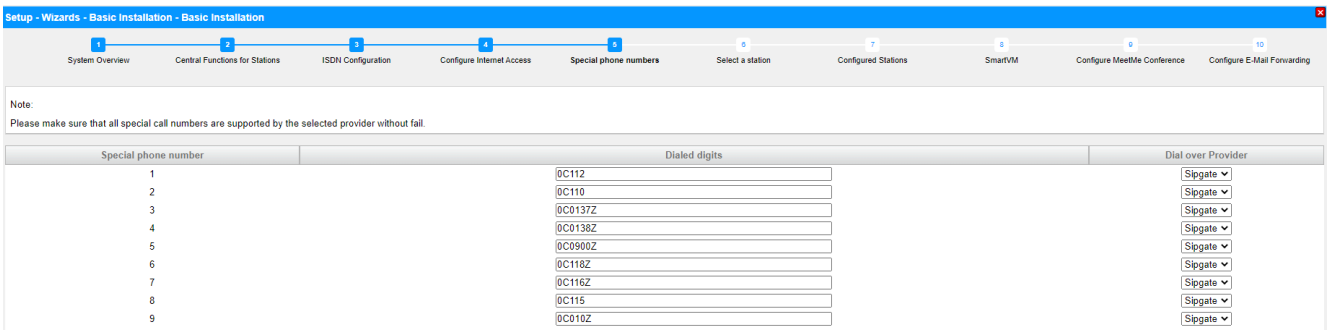
22) Nel caso durante la configurazione dell'accesso a Internet non sia stata ancora configurata la connessione permanente, è possibile farlo ora. Senza connessione permanente non è possibile ricevere alcuna chiamata tramite Internet. Se la connessione permanente è già configurata, non vengono visualizzati i campi descritti da a) a c).

a) In **Connessione permanente**, selezionare il pulsante di opzione **On**.

b) Nel campo **Interruzione alle (hh:mm)**, immettere l'orario in cui interrompere la connessione a Internet (ad es. 04:59).

c) Fare clic su **OK & Avanti**.

23) Nella colonna **Cifre selezionate** indicare i numeri di telefono speciali desiderati.



Sono valide le seguenti voci relative ai numeri di telefono:

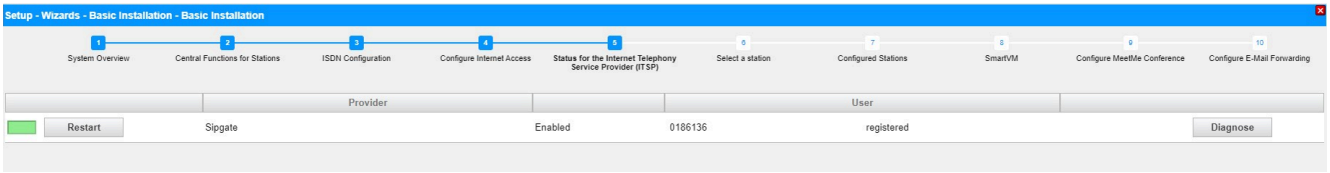
- 0 - 9: cifre consentite
- -: Separatore di campi
- X: Cifra a piacere fra 0 e 9
- N: Cifra a piacere fra 2 e 9
- Z: seguono una o più cifre fino alla fine della selezione
- C: Tono di selezione simulato (può essere specificato fino a tre volte)

24) Nella colonna **Chiama tramite provider**, selezionare se i numeri di telefono speciali devono essere selezionati via ISDN o tramite un ITSP. Vengono visualizzati solo gli ITSP attivi.

Nota: Assicurarsi che i numeri di emergenza possano sempre essere selezionati. Se i numeri di emergenza

devono essere selezionati tramite un Internet Telephony Service Provider, l'ITSP deve supportare questo servizio.

25) Fare clic su **OK & Avanti**. Viene visualizzato lo stato degli ITSP.



In verde sono indicati gli ITSP configurati presso i quali si è già registrati.

In arancione sono indicati gli ITSP configurati presso i quali non si è ancora registrati.

26) Fare clic su **Avanti**, quindi su **Fine**.

5.7.6.2 Come disattivare la telefonia Internet

Prerequisiti

Si è nella finestra **Configurazione e attivazione del provider di telefonia Internet** della procedura guidata **Installazione di base**.

Passo a passo

1) Lasciare selezionata la casella di controllo **No telefonia tramite Internet**.
2) Fare clic due volte su **OK & Avanti**.

5.7.7 Utenti

Nelle finestre **Seleziona utente / gruppo** configurare gli utenti collegati al sistema di comunicazione.

Procedere come segue:

1) Configurazione utenti ISDN

   Gli utenti ISDN sono telefoni ISDN o fax ISDN. L'utente ISDN può essere configurato solo se è stata configurata un'interfaccia S_0 come connessione interna S_0.
2) Configurazione degli utenti analogici

   Gli utenti analogici possono essere telefoni analogici o fax analogici.
3) Configurazione di utenti UP0

   Gli utenti UP0 sono telefoni di sistema quali OpenStage 60 T.
4) Configurazione utente DECT

   Gli utenti DECT sono telefoni cordless/DECT. Gli utenti DECT possono essere configurati solo se sono collegate una o più stazioni base cordless e se i telefoni DECT hanno effettuato l'accesso ad esse. La configurazione della stazione base viene eseguita con Manager E. Per informazioni più dettagliate sulla configurazione dei cordless, vedere Configurazione della soluzione cordless integrata

5) Configurazione di utenti IP e SIP

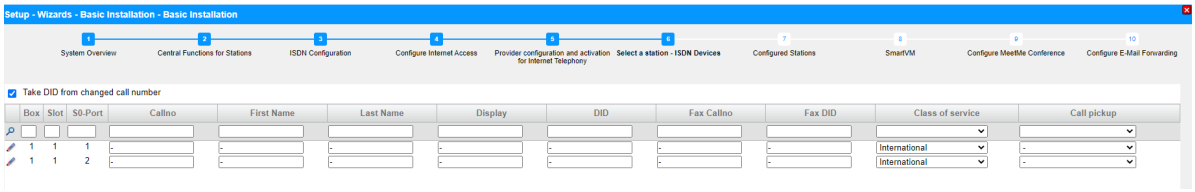
Gli utenti IP e gli utenti SIP sono ad esempio telefoni LAN o telefoni WLAN.

5.7.7.1 Come configurare gli utenti ISDN

Prerequisiti

Si è nella finestra **Seleziona utente - Terminali ISDN** della procedura guidata **Installazione di base**.

Le interfacce S_0 a cui sono collegati i telefoni ISDN devono essere configurate come interfacce S_0 interne.



Passo a passo

1) Se si desidera che il numero di selezione passante dell'utente sia diverso dal numero di telefono, nella riga dell'utente desiderato, in corrispondenza di **DID**, immettere un numero di selezione passante per l'utente:

- solo con connessioni punto - punto:

  Fare clic sul campo desiderato e immettere tramite tastiera il numero di selezione passante. Questo numero può coincidere con il numero interno.
- solo con connessioni punto - multipunto:

  Nell'elenco a discesa selezionare un MSN. L'utente può ad es. essere raggiunto da chiamate interne sul numero interno 101 e dall'esterno tramite l'MSN 654321.
- connessione punto - punto e connessione punto - multipunto:

  Nel campo desiderato selezionare una voce dall'elenco a discesa **xxx - modificabile** (xxx indica il numero interno) e immettere tramite tastiera il numero di selezione passante o selezionare un MSN dall'elenco a discesa.

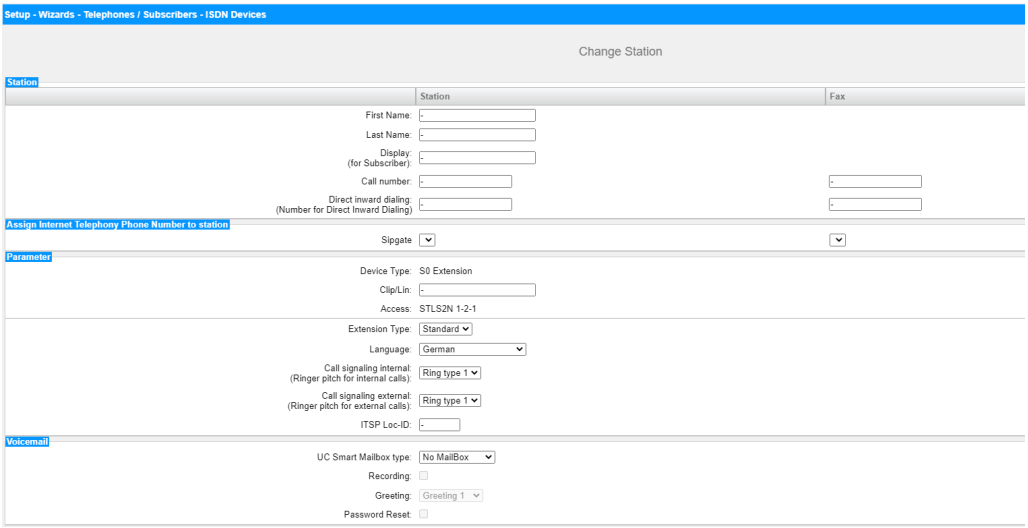
2) Nella riga appropriata dell'utente desiderato, immettere in **N° tel** un numero dell'utente interno. Si può utilizzare il numero di telefono pre-assegnato o immetterne uno diverso, ancora libero.

3) Nella riga dell'utente desiderato immettere in **Nome** un nome nel formato `Cognome, nome` o `Nome Cognome`.

Nota: Il nome può contenere fino a 16 caratteri, ma non sono consentiti umlaut o caratteri speciali.

---

4) Se per l'utente deve essere configurata una casella fax (utilizzabile ad esempio con i client UC **myPortal for Desktop** o **myPortal for Outlook**, procedere come segue:
   a) Nella riga dell'utente desiderato, nel campo **Fax N° tel**, inserire il numero di fax interno desiderato, mediante il quale l'utente potrà ricevere messaggi fax interni.
   b) Se per la casella fax viene configurato un numero DID, nella riga dell'utente desiderato inserire nel campo **Selezione passante fax** il numero di fax esterno a cui l'utente può ricevere fax dall'esterno.
5) Nella riga dell'utente selezionato, dall'elenco a discesa **Abilitazione**, selezionare il gruppo di abilitazione desiderato.
6) Per aggiungere l'utente a un gruppo di risposta, selezionare dall'elenco a discesa **Gruppo di risposta alle chiamate** nella riga dell'utente desiderato.
7) Solo se necessario, procedere a quanto descritto nel passo successivo:
   a) Nella riga del terminale ISDN desiderato, fare clic sull'icona a forma di matita **Modifica**.



   b) Nel campo **Clip/Lin** immettere un numero di telefono (selezione passante o MSN), che deve essere visualizzato sul display dell'utente chiamato al posto del proprio numero quando si effettua una chiamata esterna.

Nota: Questo servizio deve essere autorizzato dal gestore di rete.

Nota: Configurare almeno un numero DID. In caso contrario, il sistema non tiene conto del numero CLIP del chiamante e il numero interno della chiamata viene

formattato e inviato come numero di chiamata per la chiamata esterna.

c) Nell'elenco a discesa **Tipo stazione**, selezionare il tipo di terminale ISDN.

d) In **Interno per telefonia Internet** scegliere un numero interno dall'elenco a discesa. Per ciascun ITSP attivo viene visualizzato un elenco a discesa.

Nota: Il campo **Interno per telefonia DSL** non è visibile se la telefonia Internet non è stata configurata o non è attivo alcun Internet Telephony Service Provider.

e) Dall'elenco a discesa **Segnalazione della chiamata interna** assegnare all'utente uno degli otto possibili toni di segnalazione chiamate interne. In questo modo l'utente invia agli altri utenti interni un tono di chiamata diverso in base al quale può essere differenziato (standard: Suoneria 1).

f) Nell'elenco a discesa **Segnalazione della chiamata esterna**, selezionare e assegnare uno dei tre possibili toni di segnalazione chiamate esterne (standard: Suoneria 1).

g) Fare clic su **OK & Avanti**.

h) Modificare i flag utente in base alle necessità. Per una descrizione dei flag utente, vedere Utenti > Utenti > Parametri utente.

i) Fare clic su **OK & Avanti**.

8) Se si desidera configurare altri utenti ISDN, fare clic su **Salva i dati**, quindi ripetere i passi da 1 a 7.

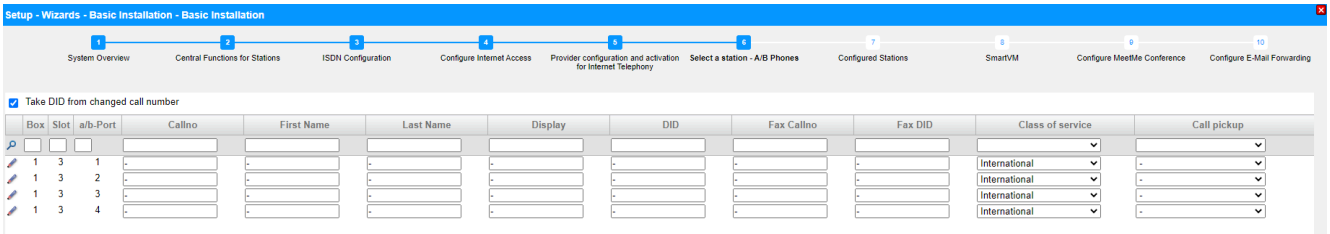
9) Fare clic su **OK & Avanti**.

5.7.7.2 Come configurare gli utenti analogici

Prerequisiti

Si è nella finestra **Seleziona utente - Telefoni A/B** della procedura guidata **Installazione di base**.

È disponibile una scheda madre o un modulo con interfaccia analogica.



Passo a passo

1) Se si desidera che il numero di selezione passante dell'utente sia diverso dal numero di telefono, nella riga dell'utente desiderato, in corrispondenza di **DID**, immettere un numero di selezione passante per l'utente:

- solo con connessioni punto - punto:

  Fare clic sul campo desiderato e immettere tramite tastiera il numero di selezione passante. Questo numero può coincidere con il numero interno.
- solo con connessioni punto - multipunto:

  Nell'elenco a discesa selezionare un MSN. L'utente può ad es. essere raggiunto da chiamate interne sul numero interno 101 e dall'esterno tramite l'MSN 654321.
- connessione punto - punto e connessione punto - multipunto:

  Nel campo desiderato selezionare una voce dall'elenco a discesa **xxx - modificabile** (xxx indica il numero interno) e immettere tramite tastiera il numero di selezione passante o selezionare un MSN dall'elenco a discesa.

2) Nella riga appropriata dell'utente desiderato, immettere in **N° tel** un numero dell'utente interno. Si può utilizzare il numero di telefono pre-assegnato o immetterne uno diverso, ancora libero.

3) Nella riga dell'utente desiderato immettere in **Nome** un nome nel formato `Cognome, nome` o `Nome Cognome`.

Nota: Il nome può contenere fino a 16 caratteri, ma non sono consentiti umlaut o caratteri speciali.

---

4) Se per l'utente deve essere configurata una casella fax (utilizzabile ad esempio con i client UC **myPortal for Desktop** o **myPortal for Outlook**, procedere come segue:

a) Nella riga dell'utente desiderato, nel campo **Fax N° tel**, inserire il numero di fax interno desiderato, mediante il quale l'utente potrà ricevere messaggi fax interni.

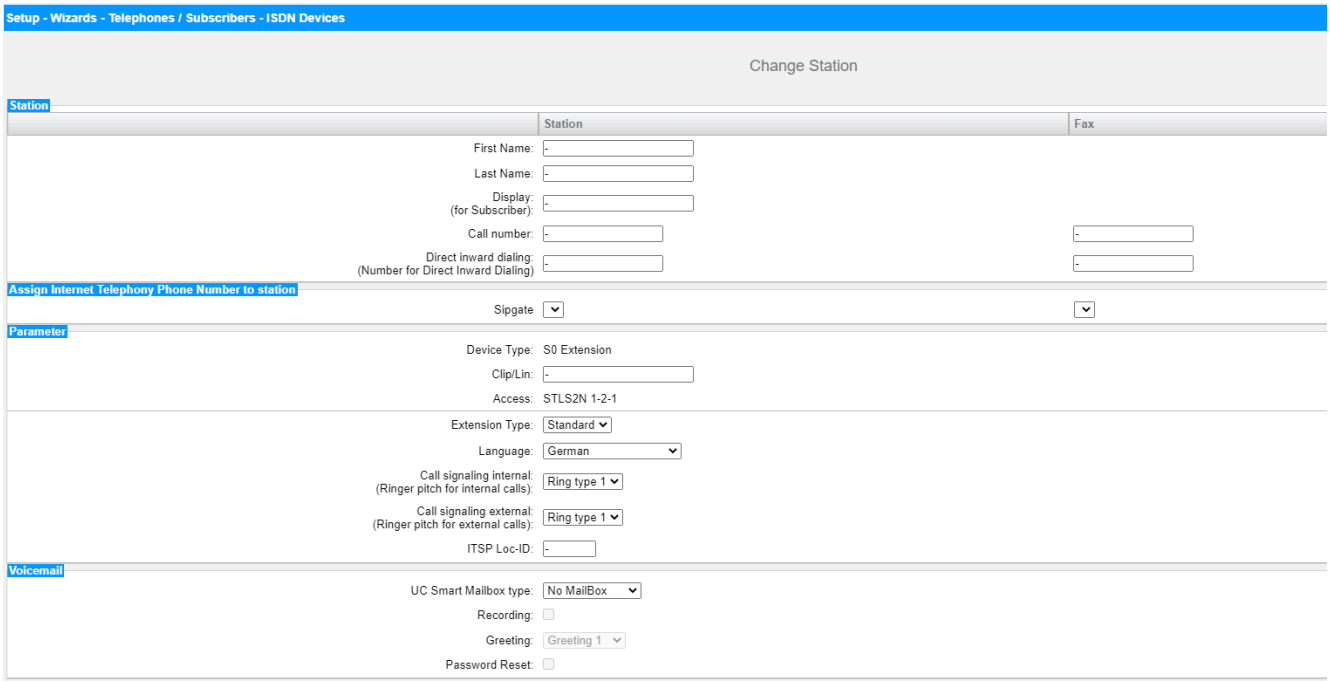
b) Se per la casella fax deve essere configurato un numero interno, nella riga dell'utente desiderato, nel campo **DID fax**, inserire il numero di fax esterno desiderato, mediante il quale l'utente potrà ricevere messaggi fax esterni.

5) Nella riga dell'utente selezionato, dall'elenco a discesa **Abilitazione**, selezionare il gruppo di abilitazione desiderato.

6) Per aggiungere l'utente a un gruppo di risposta, selezionare dall'elenco a discesa **Gruppo di risposta alle chiamate** nella riga dell'utente desiderato.

7) Solo se necessario, procedere a quanto descritto nel passo successivo:

a) Nella riga del terminale analogico desiderato, fare clic sull'icona a forma di matita **Modifica**.



b) Nel campo **Clip/Lin** immettere un numero di telefono (selezione passante o MSN), che deve essere visualizzato sul display dell'utente chiamato al posto del proprio numero quando si effettua una chiamata esterna.

Nota: Questo servizio deve essere autorizzato dal gestore di rete.

Nota: Configurare almeno un numero DID. In caso contrario, il sistema non tiene conto del numero CLIP del chiamante e il numero interno della chiamata viene formattato e inviato come numero di chiamata per la chiamata esterna.

---

c) Nell'elenco a discesa **Tipo di periferica**, selezionare il tipo di terminale analogico (ad es. fax).

d) In **Interno per telefonia Internet** scegliere un numero interno dall'elenco a discesa. Per ciascun ITSP attivo viene visualizzato un elenco a discesa.

Nota: Il campo **Interno per telefonia DSL** non è visibile se la telefonia Internet non è stata configurata o non è attivo alcun Internet Telephony Service Provider.

---

e) Dall'elenco a discesa **Segnalazione della chiamata interna** assegnare all'utente uno degli otto possibili toni di segnalazione chiamate interne.

In questo modo l'utente invia agli altri utenti interni un tono di chiamata diverso in base al quale può essere differenziato (standard: Suoneria 1).

f) Nell'elenco a discesa **Segnalazione della chiamata esterna**, selezionare e assegnare uno dei tre possibili toni di segnalazione chiamate esterne (standard: Suoneria 1).

g) Fare clic su **OK & Avanti**.

h) Modificare i flag utente in base alle necessità. Per una descrizione dei flag utente, vedere Utenti > Utenti > Parametri utente.

i) Fare clic su **OK & Avanti**.

8) Se si desidera configurare altri utenti analogici, fare clic su **Salva i dati**, quindi ripetere i passi da 1 a 7.

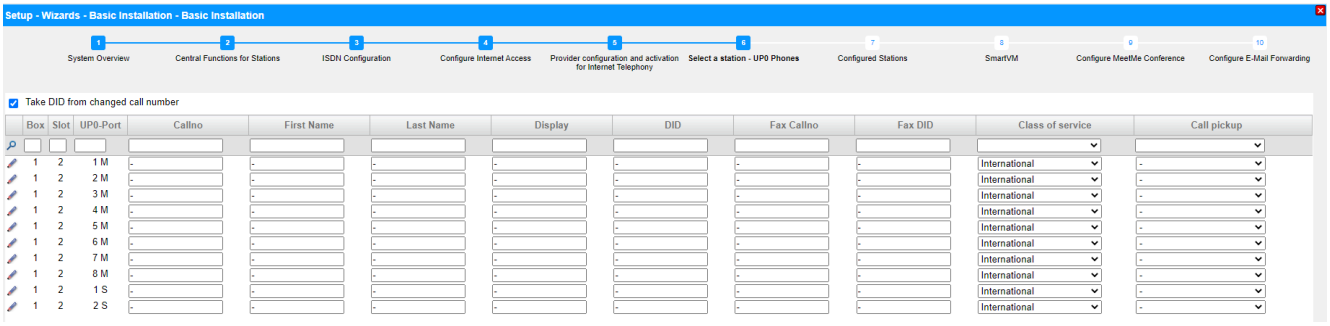
9) Fare clic su **OK & Avanti**.

5.7.7.3 Come configurare gli utenti UP0

Prerequisiti

Si è nella finestra **Seleziona utente - Utenti UP0** della procedura guidata **Installazione di base**.

È disponibile una scheda madre o un modulo con interfaccia UP0.



Passo a passo

1) Se si desidera che il numero di selezione passante dell'utente sia diverso dal numero di telefono, nella riga dell'utente desiderato, in corrispondenza di **DID**, immettere un numero di selezione passante per l'utente:

- solo con connessioni punto - punto:

  Fare clic sul campo desiderato e immettere tramite tastiera il numero di selezione passante. Questo numero può coincidere con il numero interno.
- solo con connessioni punto - multipunto:

  Nell'elenco a discesa selezionare un MSN. L'utente può ad es. essere raggiunto da chiamate interne sul numero interno 101 e dall'esterno tramite l'MSN 654321.
- connessione punto - punto e connessione punto - multipunto:

  Nel campo desiderato selezionare una voce dall'elenco a discesa **xxx - modificabile** (xxx indica il numero interno) e immettere tramite tastiera il numero di selezione passante o selezionare un MSN dall'elenco a discesa.

2) Nella riga appropriata dell'utente desiderato, immettere in **N° tel** un numero dell'utente interno. Si può utilizzare il numero di telefono pre-assegnato o immetterne uno diverso, ancora libero.
3) Nella riga dell'utente desiderato immettere in **Nome** un nome nel formato `Cognome, nome` o `Nome Cognome`.

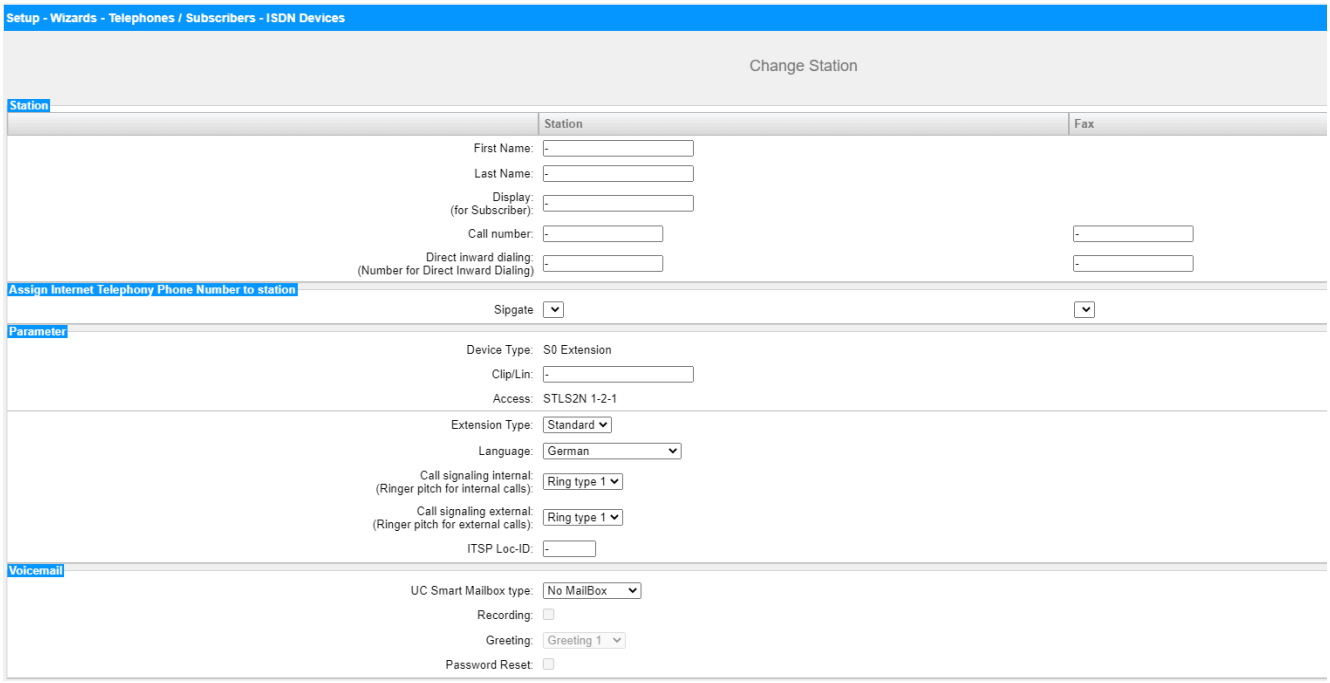
Nota: Il nome può contenere fino a 16 caratteri, ma non sono consentiti umlaut o caratteri speciali.

---

4) Se per l'utente deve essere configurata una casella fax (utilizzabile ad esempio con i client UC **myPortal for Desktop** o **myPortal for Outlook**, procedere come segue:
   a) Nella riga dell'utente desiderato, nel campo **Fax N° tel**, inserire il numero di fax interno desiderato, mediante il quale l'utente potrà ricevere messaggi fax interni.
   b) Se per la casella fax viene configurato un numero DID, nella riga dell'utente desiderato inserire nel campo **Selezione passante fax** il numero di fax esterno a cui l'utente può ricevere fax dall'esterno.
5) Nella riga dell'utente selezionato, dall'elenco a discesa **Abilitazione**, selezionare il gruppo di abilitazione desiderato.
6) Per aggiungere l'utente a un gruppo di risposta, selezionare dall'elenco a discesa **Gruppo di risposta alle chiamate** nella riga dell'utente desiderato.

7) Solo se necessario, procedere a quanto descritto nel passo successivo:

a) Nella riga del terminale desiderato, fare clic sull'icona a forma di matita **Modifica**.



b) Nel campo **Clip/Lin** immettere un numero di telefono (selezione passante o MSN), che deve essere visualizzato sul display dell'utente chiamato al posto del proprio numero quando si effettua una chiamata esterna.

Nota: Questo servizio deve essere autorizzato dal gestore di rete.

Nota: Configurare almeno un numero DID. In caso contrario, il sistema non tiene conto del numero CLIP del chiamante e il numero interno della chiamata viene formattato e inviato come numero di chiamata per la chiamata esterna.

---

c) Nell'elenco a discesa **Tipo di periferica**, selezionare il tipo di terminale TDM.

d) Mantenere la selezione predefinita nell'elenco a discesa **Lingua**. Per i terminali TDM, questa impostazione non ha alcun significato.

e) In **Interno per telefonia Internet** scegliere un numero interno dall'elenco a discesa. Per ciascun ITSP attivo viene visualizzato un elenco a discesa.

Nota: Il campo **Interno per telefonia DSL** non è visibile se la telefonia Internet non è stata configurata o non è attivo alcun Internet Telephony Service Provider.

---

f) Dall'elenco a discesa **Segnalazione della chiamata interna** assegnare all'utente uno degli otto possibili toni di segnalazione chiamate interne.

In questo modo l'utente invia agli altri utenti interni un tono di chiamata diverso in base al quale può essere differenziato (standard: Suoneria 1).

g) Nell'elenco a discesa **Segnalazione della chiamata esterna**, selezionare e assegnare uno dei tre possibili toni di segnalazione chiamate esterne (standard: Suoneria 1).

h) Fare clic su **OK & Avanti**.

i) Modificare i flag utente in base alle necessità. Per una descrizione dei flag utente, vedere Utenti > Utenti > Parametri utente.

j) Fare clic su **OK & Avanti**.

8) Se si desidera configurare altri utenti UP0, fare clic su **Salva i dati**, quindi ripetere i passi da 1 a 7.

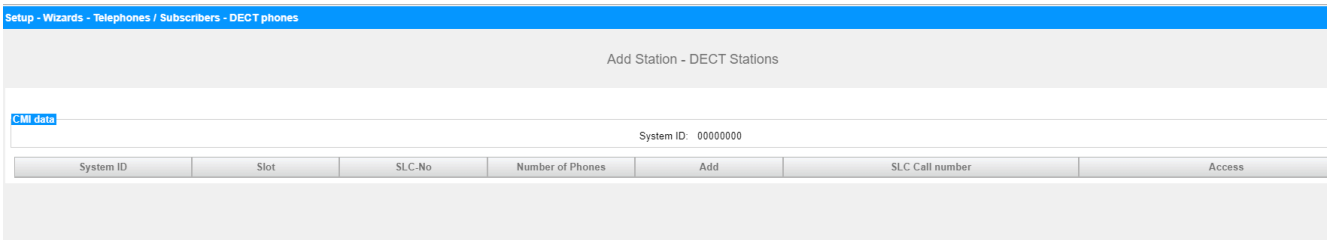
9) Fare clic su **OK & Avanti**.

5.7.7.4 Come configurare gli utenti DECT

Prerequisiti

Si è nella finestra **Seleziona utente - Utenti DECT** della procedura guidata **Installazione di base**.

Per la configurazione degli utenti DECT è necessario collegare un utente base e accedere ad esso col telefono DECT. In caso contrario, ignorare questa finestra. È inoltre possibile configurare successivamente l'utente DECT (vedere Configurazione degli utenti).



Passo a passo

1) Se si desidera che il numero di selezione passante dell'utente sia diverso dal numero di telefono, nella riga dell'utente desiderato, in corrispondenza di **DID**, immettere un numero di selezione passante per l'utente:

- solo con connessioni punto - punto:

  Fare clic sul campo desiderato e immettere tramite tastiera il numero di selezione passante. Questo numero può coincidere con il numero interno.
- solo con connessioni punto - multipunto:

  Nell'elenco a discesa selezionare un MSN. L'utente può ad es. essere raggiunto da chiamate interne sul numero interno 101 e dall'esterno tramite l'MSN 654321.
- connessione punto - punto e connessione punto - multipunto:

  Nel campo desiderato selezionare una voce dall'elenco a discesa **xxx - modificabile** (xxx indica il numero interno) e immettere tramite tastiera il numero di selezione passante o selezionare un MSN dall'elenco a discesa.

2) Nella riga appropriata dell'utente desiderato, immettere in **N° tel** un numero dell'utente interno. Si può utilizzare il numero di telefono pre-assegnato o immetterne uno diverso, ancora libero.

3) Se per l'utente deve essere configurata una casella fax (utilizzabile ad esempio con i client UC **myPortal for Desktop** o **myPortal for Outlook**, procedere come segue:

   a) Nella riga dell'utente desiderato, nel campo **Fax N° tel**, inserire il numero di fax interno desiderato, mediante il quale l'utente potrà ricevere messaggi fax interni.

   b) Se per la casella fax viene configurato un numero DID, nella riga dell'utente desiderato inserire nel campo **Selezione passante fax** il numero di fax esterno a cui l'utente può ricevere fax dall'esterno.

4) Nella riga dell'utente desiderato immettere in **Nome** un nome nel formato `Cognome, nome` o `Nome Cognome`.

Nota: Il nome può contenere fino a 16 caratteri, ma non sono consentiti umlaut o caratteri speciali.

---

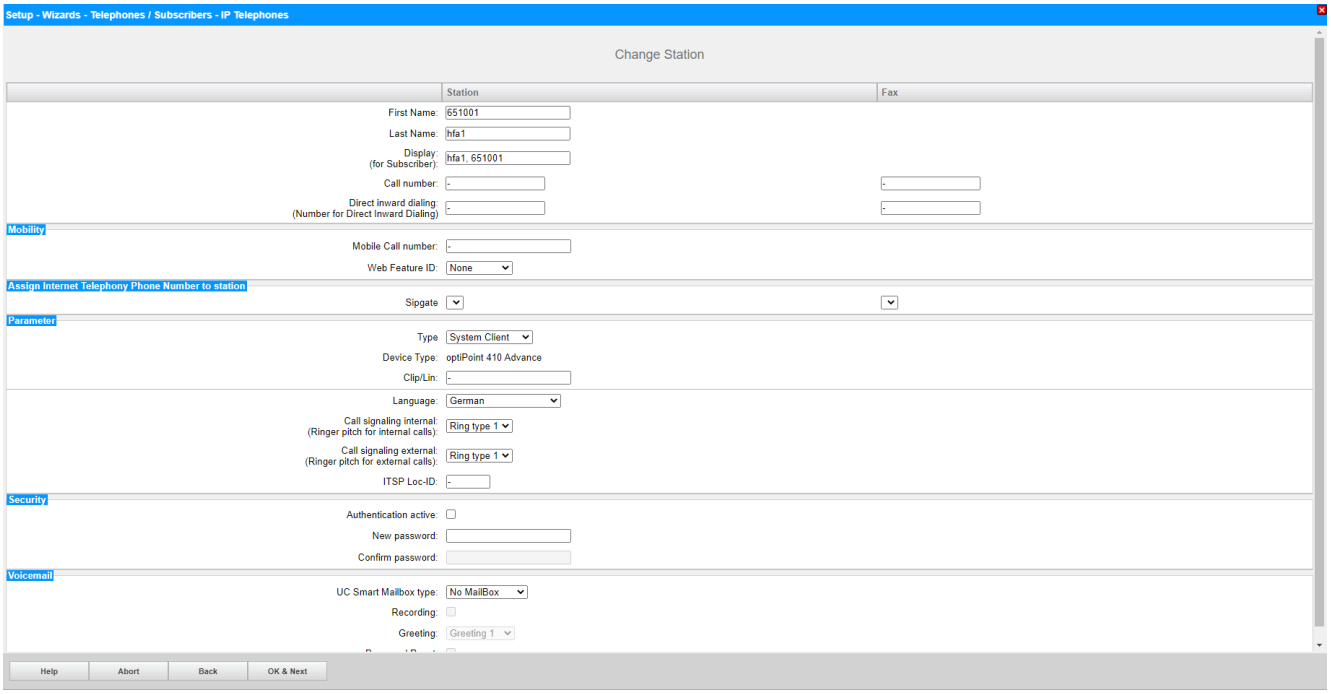
5) Nella riga dell'utente selezionato, dall'elenco a discesa **Abilitazione**, selezionare il gruppo di abilitazione desiderato.

6) Per aggiungere l'utente a un gruppo di risposta, selezionare dall'elenco a discesa **Gruppo di risposta alle chiamate** nella riga dell'utente desiderato.

7) Se si desidera modificare il codice (PIN) del telefono DECT, immettere il nuovo codice nella riga dell'utente desiderato in **Codice mobile**. L'utente DECT deve accedere all'utente base con questo codice.

8) Solo se necessario, procedere a quanto descritto nel passo successivo:

   a) Nella riga del terminale desiderato, fare clic sull'icona a forma di matita **Modifica**.



   b) Nel campo **Clip/Lin** immettere un numero di telefono (selezione passante o MSN), che deve essere visualizzato sul display dell'utente

chiamato al posto del proprio numero quando si effettua una chiamata esterna.

Nota: Questo servizio deve essere autorizzato dal gestore di rete.

Nota: Configurare almeno un numero DID. In caso contrario, il sistema non tiene conto del numero CLIP del chiamante e il numero interno della chiamata viene formattato e inviato come numero di chiamata per la chiamata esterna.

c) Nell'elenco a discesa **Tipo stazione**, selezionare il tipo di terminale cordless.
d) Mantenere la selezione predefinita nell'elenco a discesa **Lingua**. Nel caso di dispositivi cordless, questa impostazione non ha alcun significato.
e) In **Interno per telefonia Internet** scegliere un numero interno dall'elenco a discesa. Per ciascun ITSP attivo viene visualizzato un elenco a discesa.

Nota: Il campo **Interno per telefonia DSL** non è visibile se la telefonia Internet non è stata configurata o non è attivo alcun Internet Telephony Service Provider.

f) Dall'elenco a discesa **Segnalazione della chiamata interna** assegnare all'utente uno degli otto possibili toni di segnalazione chiamate interne. In questo modo l'utente invia agli altri utenti interni un tono di chiamata diverso in base al quale può essere differenziato (standard: Suoneria 1).
g) Nell'elenco a discesa **Segnalazione della chiamata esterna**, selezionare e assegnare uno dei tre possibili toni di segnalazione chiamate esterne (standard: Suoneria 1).
h) Fare clic su **OK & Avanti**.
i) Modificare i flag utente in base alle necessità. Per una descrizione dei flag utente, vedere Utenti > Utenti > Parametri utente.
j) Fare clic su **OK & Avanti**.

9) Se si desidera configurare altri utenti, fare clic su **Salva i dati**, quindi ripetere i passi da 1 a 8.

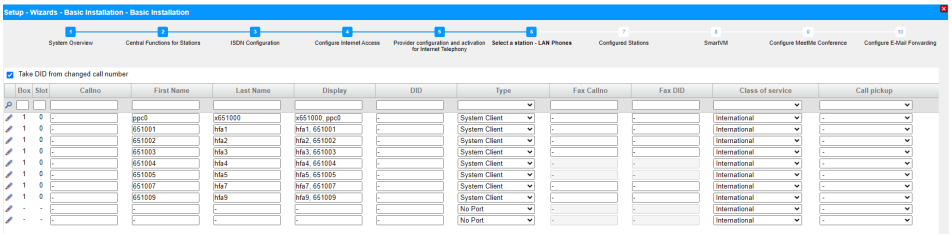
10) Fare clic su **OK & Avanti**.

5.7.7.5 Come configurare utenti IP e SIP

Prerequisiti

Si è nella finestra **Seleziona utente - Telefoni LAN** della procedura guidata **Installazione di base**.

Per il funzionamento dei telefoni WLAN è necessaria una rete LAN wireless operativa.



Passo a passo

1) Se si desidera che il numero di selezione passante dell'utente sia diverso dal numero di telefono, nella riga dell'utente desiderato, in corrispondenza di **DID**, immettere un numero di selezione passante per l'utente:

- solo con connessioni punto - punto:

  Fare clic sul campo desiderato e immettere tramite tastiera il numero di selezione passante. Questo numero può coincidere con il numero interno.
- solo con connessioni punto - multipunto:

  Nell'elenco a discesa selezionare un MSN. L'utente può ad es. essere raggiunto da chiamate interne sul numero interno 101 e dall'esterno tramite l'MSN 654321.
- connessione punto - punto e connessione punto - multipunto:

  Nel campo desiderato selezionare una voce dall'elenco a discesa **xxx - modificabile** (xxx indica il numero interno) e immettere tramite tastiera il numero di selezione passante o selezionare un MSN dall'elenco a discesa.

2) Nella riga appropriata dell'utente desiderato, immettere in **N° tel** un numero dell'utente interno. Si può utilizzare il numero di telefono pre-assegnato o immetterne uno diverso, ancora libero.

3) Nella riga dell'utente desiderato immettere in **Nome** un nome nel formato `Cognome, nome`.

Nota: Il nome può contenere fino a 16 caratteri, ma non sono consentiti umlaut o caratteri speciali. Il nome è quello qui indicato nei client UC come cognome, ma può essere modificato.

---

4) Nella riga dell'utente desiderato, selezionare dall'elenco a discesa **Tipo** il tipo di utente IP (ad es."Client di sistema" o "Client SIP").

5) Se per l'utente deve essere configurata una casella fax (utilizzabile ad esempio con i client UC **myPortal for Desktop** o **myPortal for Outlook**, procedere come segue:

a) Nella riga dell'utente desiderato, nel campo **Fax N° tel**, inserire il numero di fax interno desiderato, mediante il quale l'utente potrà ricevere messaggi fax interni.

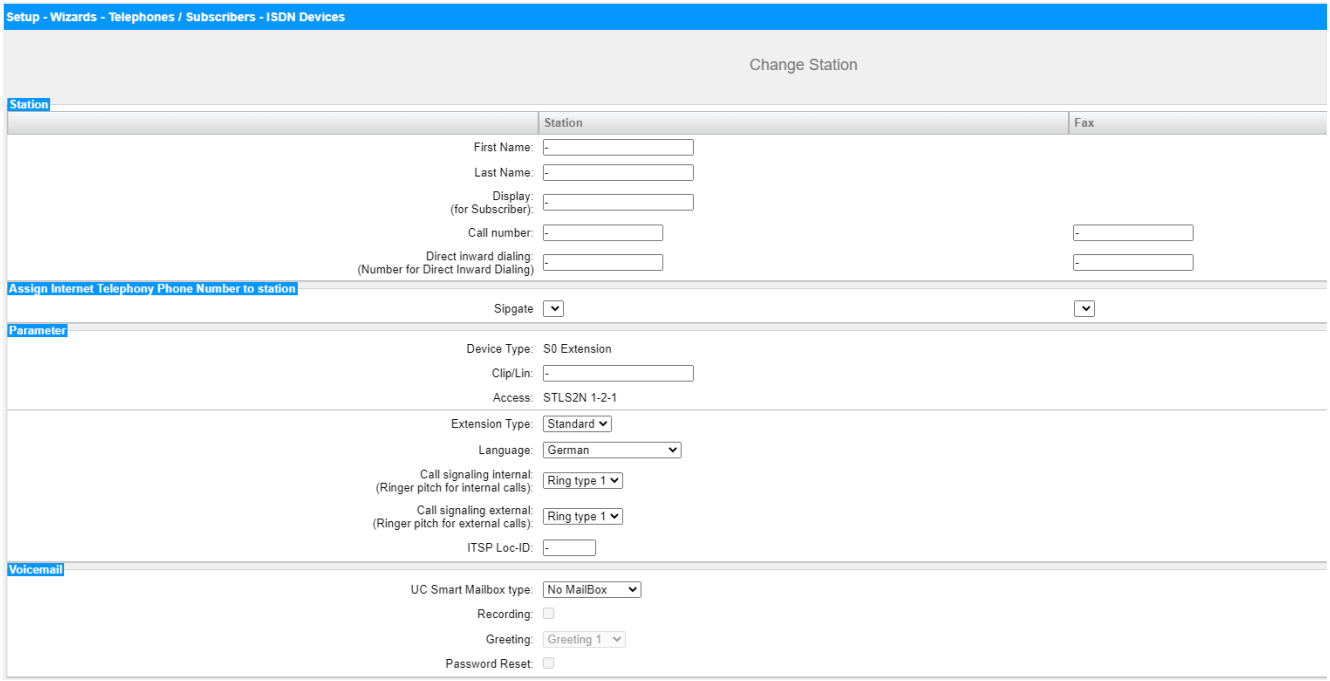
b) Se per la casella fax viene configurato un numero DID, nella riga dell'utente desiderato inserire nel campo **Selezione passante fax** il numero di fax esterno a cui l'utente può ricevere fax dall'esterno.

6) Nella riga dell'utente selezionato, dall'elenco a discesa **Abilitazione**, selezionare il gruppo di abilitazione desiderato.

7) Per aggiungere l'utente a un gruppo di risposta, selezionare dall'elenco a discesa **Gruppo di risposta alle chiamate** nella riga dell'utente desiderato.

8) Eseguire le impostazioni descritte di seguito solo in caso di necessità o per un telefono SIP:

a) Nella riga del terminale desiderato, fare clic sull'icona a forma di matita **Modifica**.



b) Per telefoni SIP: Se il telefono SIP deve essere utilizzato insieme a un telefono cellulare dual-mode, inserire nell'area **Mobility** in **Num. cellulare** il codice linea esterna e di seguito il numero di telefono del cellulare (es. `0016012345678`). Inoltre, nell'elenco a discesa **Web Feature ID**, selezionare questo client SIP. (Vedere Telefonia dual mode).

c) Nel campo **Clip/Lin** immettere un numero di telefono (selezione passante o MSN), che deve essere visualizzato sul display dell'utente chiamato al posto del proprio numero quando si effettua una chiamata esterna.

Nota: Questo servizio deve essere autorizzato dal gestore di rete.

Nota: Configurare almeno un numero DID. In caso contrario, il sistema non tiene conto del numero CLIP del chiamante e il numero interno della chiamata viene formattato e inviato come numero di chiamata per la chiamata esterna.

---

d) Nell'elenco a discesa **Lingua** selezionare la lingua da utilizzare per i comandi dei menu del telefono.

e) Dall'elenco a discesa **Segnalazione della chiamata interna** assegnare all'utente uno degli otto possibili toni di segnalazione chiamate interne.

In questo modo l'utente invia agli altri utenti interni un tono di chiamata diverso in base al quale può essere differenziato (standard: Suoneria 1).

f) Nell'elenco a discesa **Segnalazione della chiamata esterna**, selezionare e assegnare uno dei tre possibili toni di segnalazione chiamate esterne (standard: Suoneria 1).

g) Consentiti solo per telefoni SIP: inserire la password di autenticazione nei campi **Password** e **Conferma password**.

h) Consentiti solo per telefoni SIP: nel campo **SIP ID d'utente/Nome d'utente** immettere l'identificativo utente per l'autenticazione.

i) Consentiti solo per telefoni SIP: nel campo **Realm** immettere la zona corrispondente per l'autenticazione.

j) Fare clic su **OK & Avanti**.

k) Modificare i flag utente in base alle necessità. Per una descrizione dei flag utente, vedere Utenti > Utenti > Parametri utente.

l) Fare clic su **OK & Avanti**.

9) Se si desidera configurare altri utenti IP, fare clic su **Salva i dati**, quindi ripetere i passi da 1 a 8.

10) Fare clic su **OK & Avanti**. Viene visualizzato l'elenco di tutti gli utenti configurati. Tale elenco corrisponde a un piano di composizione.

11) Se necessario, fare clic su **Stampa**, per stampare le informazioni sull'utente configurato.

12) Fare clic su **OK & Avanti**.

Concetti correlati

Testo in più lingue alla pagina 1230

5.7.8 Configurazione della UC Suite

Nella finestra Configurazione automatica della suite applicazioni è possibile eseguire la **configurazione automatica della soluzione UC (UC Suite)**.

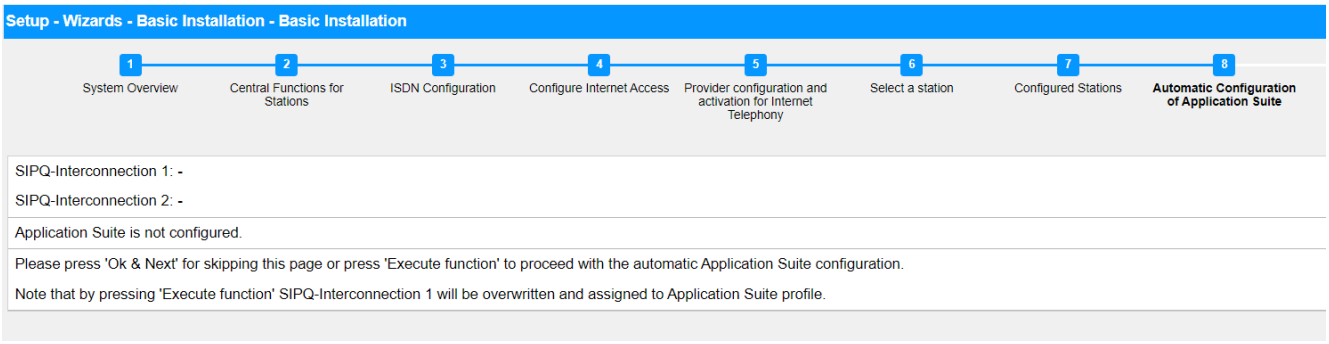
Nota: Questa finestra viene visualizzata solo se nella procedura guidata **Installazione iniziale** è stato selezionato **Pacchetto con UC Suite**.

La configurazione automatica della soluzione UC UC Suite richiede un numero di linee urbane libere che saranno occupate staticamente per l'applicazione. Questo numero dipende dalle capacità delle specifiche del sistema ed è elencato nella sezione Valori massimi per le linee alla pagina 1436 (Vedere *Canali di linea MEB per UC Suite* nelle tabelle). In caso di superamento del limite complessivo di 250 linee, la configurazione di UC Suite non è possibile.

5.7.8.1 Come configurare la UC Suite

Prerequisiti

Si è nella finestra **Configurazione automatica della suite di applicazioni** della procedura guidata **Installazione di base**.



Passo a passo

1) Se nel sistema di comunicazione non è integrata alcuna UC Booster Card, fare clic su **OK & Avanti**. La configurazione verrà ignorata.
2) Se la UC Booster Card è integrata nel sistema di comunicazione, fare clic su **Esegui funzione**. La UC Suite viene configurata automaticamente. Una volta che la barra di avanzamento indica 100%, fare clic su **OK & Avanti**.

Nota:

Per OpenScape Business X, la procedura guidata genera automaticamente 76 canali multimediali.

5.7.9 Configurazione delle caselle vocali UC Smart

Nella finestra **Configurazione automatica di Smart VM** è possibile eseguire la configurazione automatica delle caselle vocali UC Smart (Smart VM, Smart VoiceMail), se viene utilizzata la soluzione UC Smart.

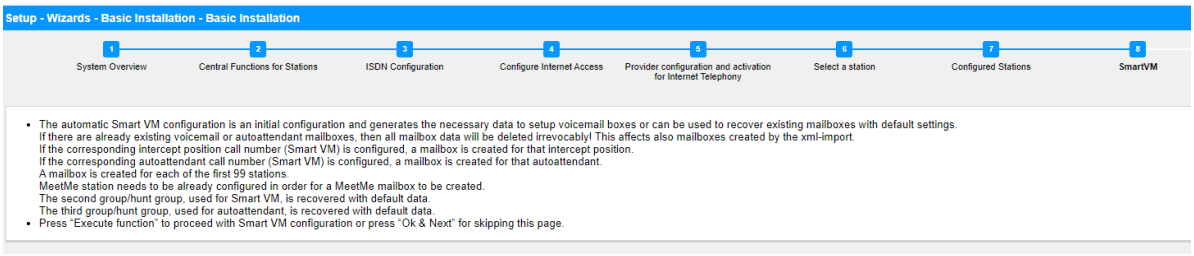
Nota:

Questa finestra viene visualizzata solo se nella procedura guidata **Configurazione di base nella selezione dell'applicazione** è stato selezionato **Pacchetto con UC Smart**.

5.7.9.1 Come configurare le caselle vocali UC Smart

Prerequisiti

Si è nella finestra **Configurazione automatica di Smart VM** della procedura guidata **Installazione di base**.



Passo a passo

1) Se non devono essere usate le caselle vocali UC Smart, fare clic su **OK & Avanti**. La configurazione delle caselle vocali viene ignorata.
2) Se devono essere usate le caselle vocali UC Smart, fare clic su **Esegui funzione**. Per i primi 100 utenti vengono automaticamente configurate le caselle vocali. Una volta che la barra di avanzamento indica 100%, fare clic su **OK & Avanti**.

Nota: Le caselle vocali UC Smart o UC Smart AutoAttendant già presenti vengono definitivamente cancellate.

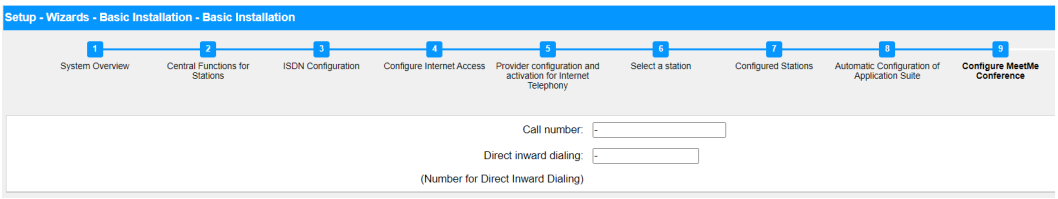
5.7.10 Impostazioni del server conferenze

Nella finestra **Configura conferenza MeetMe** è possibile immettere il numero di telefono e il numero di accesso per le conferenze.

5.7.10.1 Come modificare le impostazioni server conferenza

Prerequisiti

Si è nella finestra **Configura conferenza MeetMe** della procedura guidata **Installazione di base**.



Passo a passo

1) Nel campo **Numero di telefono** immettere un numero di telefono per la conferenza.
2) Nel campo **Selezione passante** immettere il numero di accesso alla conferenza (DID conferenza) con il quale gli utenti possono connettersi a una conferenza esistente.
3) Fare clic su **OK & Avanti**.

5.7.11 Invio per e-mail (opzionale)

Nella finestra **Modifica inoltro e-mail** è possibile definire i dettagli dell'inoltro di e-mail. In questo modo gli utenti vengono informati di nuovi messaggi vocali e fax e gli amministratori ricevono i messaggi di sistema.

Sono disponibili le seguenti opzioni:

- Configurazione dell'invio di e-mail

  È possibile definire un server di posta elettronica esterno tramite il quale è possibile inviare le e-mail con OpenScape Business. I messaggi vocali e fax o i messaggi di sistema interni vengono inoltrati tramite questo server di posta elettronica ad uno o più indirizzi e-mail diversamente configurabili.

  Nota: La definizione di un server di posta è importante se gli utenti della UC Suite devono essere indirizzati ai file di installazione automaticamente tramite un link inviato per e-mail.

5.7.11.1 Come configurare l'invio di e-mail

Prerequisiti

Se il server e-mail esterno è stato configurato per utilizzare l'autenticazione di base, assicurarsi che esista un account e-mail con una password con un provider e-mail e di conoscere i dati di accesso per questo account.

Se il server e-mail esterno è stato configurato per utilizzare l'autenticazione moderna (autorizzazione basata su token Microsoft OAuth 2.0), come nel caso di Exchange Online, assicurarsi che:

- L'account e-mail del mittente deve essere autorizzato a utilizzare SMTP autenticato (per impostazione predefinita questa opzione è inattiva nel tenant di Microsoft 365). Una volta attivato il protocollo SMTP autenticato, l'inoltro e-mail OAUTH 2.0 funziona normalmente con tutte le schede madri OpenScape Business.
- Un'applicazione con le autorizzazioni necessarie è stata registrata in Microsoft Azure Active Directory (Azure AD) per consentire al sistema OpenScape Business di inviare e-mail.
- Si conosce l'ID applicazione (client) e l'ID directory (tenant) dell'applicazione registrata.

  Chiedere all'amministratore di Azure AD di fornire questi valori, se necessario.
- L'indirizzo e-mail che verrà visualizzato come mittente delle e-mail appartiene allo stesso Azure AD o al tenant dell'applicazione registrata.

Si è nella finestra **Configura inoltro e-mail** della procedura guidata **Installazione di base**.

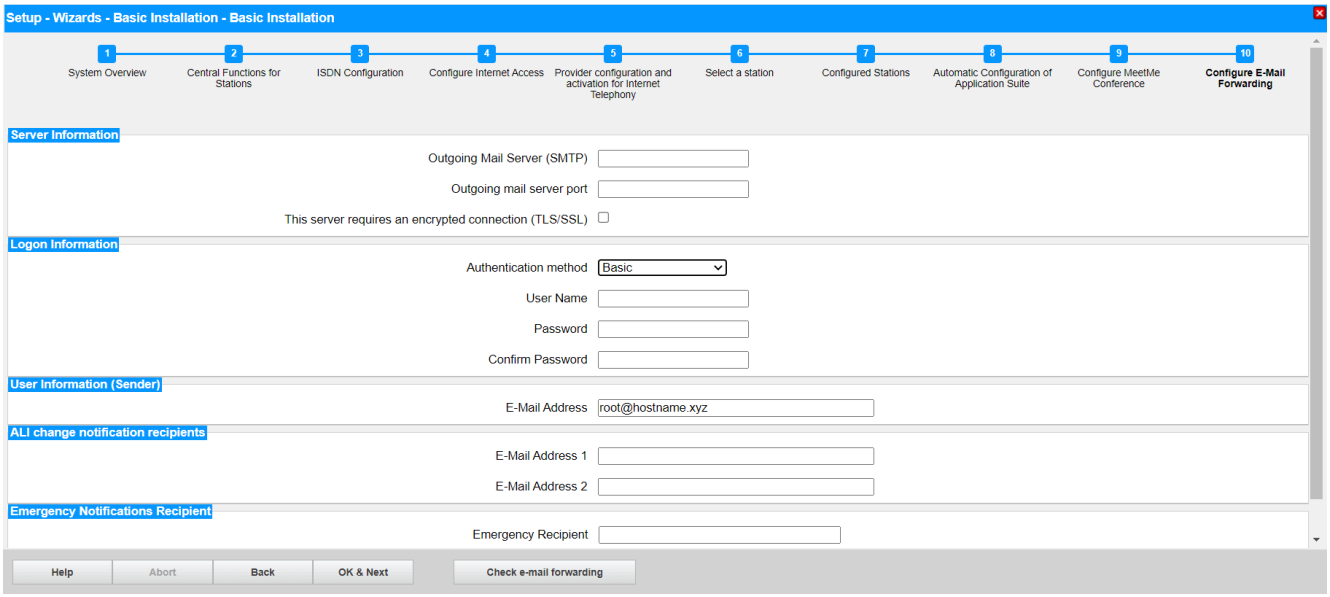


Figura 6: Opzioni di inoltro e-mail quando è selezionato il metodo di autenticazione di base

Passo a passo

1) Inserire il **Server della posta in uscita (SMTP)** per il server e-mail, da utilizzare per l'invio delle e-mail, ad esempio, `smtp.web.de`. Eventualmente richiedere il server della posta in uscita al proprio provider e-mail.

Nota: Assicurarsi che il nome del server di posta in uscita possa essere risolto. In caso negativo, avviare la procedura guidata per l'invio di e-mail tramite **Centro assistenza** > **Inoltro e-mail** e immettere l'indirizzo IP del server della posta in uscita anziché il nome.

---

2) Inserire il **Server della posta in uscita** per la porta del server da utilizzare per l'invio delle e-mail. Eventualmente richiedere il server della posta in uscita al proprio provider e-mail.

3) Se è necessario stabilire una connessione sicura, selezionare la casella di controllo **Questo server richiede una connessione criptata (TLS/SSL)**. Chiedere al proprio provider e-mail se questa opzione deve essere selezionata.

4) Se il server e-mail esterno è stato configurato per utilizzare l'autenticazione di base, procedere come segue:

a) Dall'elenco a discesa **Metodo di autenticazione**, selezionare **Base**.

b) Immettere il **Nome utente** dell'account e-mail, ad esempio, `bruno.rossi`.

c) In **Nuova password** e **Confermare password** immettere la password dell'account e-mail.

5) Se il server e-mail esterno è stato configurato per utilizzare l'autenticazione moderna, procedere come segue:

a) Dall'elenco a discesa **Metodo di autenticazione**, selezionare **Microsoft OAuth 2.0**.

b) Immettere l'ID applicazione (client) ottenuto dal portale Microsoft Azure nel campo **ID applicazione**.

c) Immettere l'ID directory (tenant) ottenuto dal portale di Microsoft Azure nel campo **Tenant**.

6) Inserire l'**Indirizzo e-mail** che comparirà come mittente delle e-mail, ad esempio: `bruno.rossi@web.it`.

7) Inserire l'**Indirizzo e-mail 1** per ricevere un'e-mail di notifica quando viene utilizzata la tolleranza ALI. È anche possibile inserire un secondo indirizzo e-mail nel campo **Indirizzo e-mail 2**.

8) Nel campo **Destinatario di emergenza**, inserire l'indirizzo e-mail di un responsabile della sicurezza in loco a cui viene inviata un'e-mail quando si seleziona un numero di emergenza.

L'oggetto dell'e-mail sarà "Nuova chiamata di emergenza". Il numero di telefono e il nome del chiamante, se configurati, sono inclusi nell'e-mail e recuperati dal database del sistema.

9) Se è stato selezionato **Microsoft OAuth 2.0** come metodo di autenticazione procedere come segue:

a) Fare clic su **OK & Avanti**.

b) Attendere che vengano visualizzati un collegamento di autorizzazione e un codice utente.

Il codice di autorizzazione scade dopo alcuni minuti.

c) Aprire il collegamento di autorizzazione e inserire il codice utente nel popup.

d) Accedere con l'indirizzo e-mail inserito al passaggio 6 alla pagina 204 (**Indirizzo e-mail**).

L'indirizzo e-mail deve trovarsi nello stesso Azure AD o tenant dell'applicazione registrata.

e) Dopo l'autenticazione riuscita, il popup visualizza un messaggio come di seguito:

```
Hai effettuato l'accesso a <nome-applicazione> sul
tuo dispositivo. Ora puoi chiudere questa finestra.
```

f) Chiudere il popup e tornare a WBM. Se l'autenticazione è andata a buon fine, sarà visualizzato il messaggio `L'autenticazione è andata a buon fine!`.

10) Per controllare le impostazioni e-mail configurate, procedere come segue:

a) Fare clic su **Controllo inoltro e-mail**.

b) Nel campo **Invia a un indirizzo e-mail** inserire l'indirizzo e-mail del servizio a cui si ha accesso. A questo indirizzo e-mail verrà inviata l'email di prova.

c) Nel campo **Oggetto dell'e-mail** inserire un testo descrittivo per identificare l'e-mail una volta ricevuta.

d) Fare clic su **Invia e-mail di prova**. Vengono testate le impostazioni e l'e-mail viene inviata alla casella e-mail indicata.

e) Verificare se il messaggio e-mail è presente nella propria casella.

f) Se l'invio dell'e-mail ha avuto esito positivo, fare clic su **Indietro** e passare alla fase seguente.

g) Se l'invio dell'e-mail non ha avuto esito positivo, fare clic su **Indietro** e verificare nuovamente le impostazioni e-mail.

11) Fare clic su **OK & Avanti**, quindi su **Fine**. L'installazione di base è conclusa. Attivare le licenze prima di eseguire il backup dei dati previsto dalla procedura guidata.

5.8 Attività finali

Una volta conclusa l'installazione iniziale e l'installazione di base eseguita con il WBM, è necessario eseguire ancora alcune importanti impostazioni per l'uso di OpenScape Business.

Procedere come segue:

1) Attivazione e assegnazione licenze

Le licenze acquistate con OpenScape Business devono essere attivate entro 30 giorni. L'intervallo di tempo inizia al primo accesso al WBM. Alla scadenza del periodo il sistema di comunicazione è utilizzabile solo in modo limitato. Dopo l'attivazione, le licenze devono essere assegnate agli utenti e alle linee. In un sistema indipendente, le funzioni a livello di sistema sono già automaticamente abilitate all'attivazione.

2) Preparazione di UC Smart Client per l'installazione (solo per UC Smart)

3) Come preparare i client UC Suite all'installazione (solo per UC Suite)

I client UC sono componenti integranti della UC Suite. I file di installazione per i client UC sono accessibili tramite il WBM e possono essere messi a disposizione degli utenti IP in modo automatico o manuale.

Inoltre, per l'amministratore è disponibile l'opzione Installazione Silent. Si tratta di un metodo basato su riga di comando per l'installazione/disinstallazione e la modifica automatiche su client della UC Suite senza necessità di inserire altri comandi. Per ulteriori informazioni, vedere Installazione/disinstallazione Silent per client PC UC Suite.

4) Esecuzione del backup dei dati

Le modifiche apportate a OpenScape Business devono essere salvate. Per il backup può essere memorizzato ad esempio su un supporto USB un set di backup.

5.8.1 Come attivare e assegnare le licenze

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Il LAC (codice di autorizzazione licenza) per il rilascio della licenza è noto e si dispone di un ID utente e di una password per l'accesso al server delle licenze.

Per la connessione al server delle licenze è necessario l'accesso a Internet.

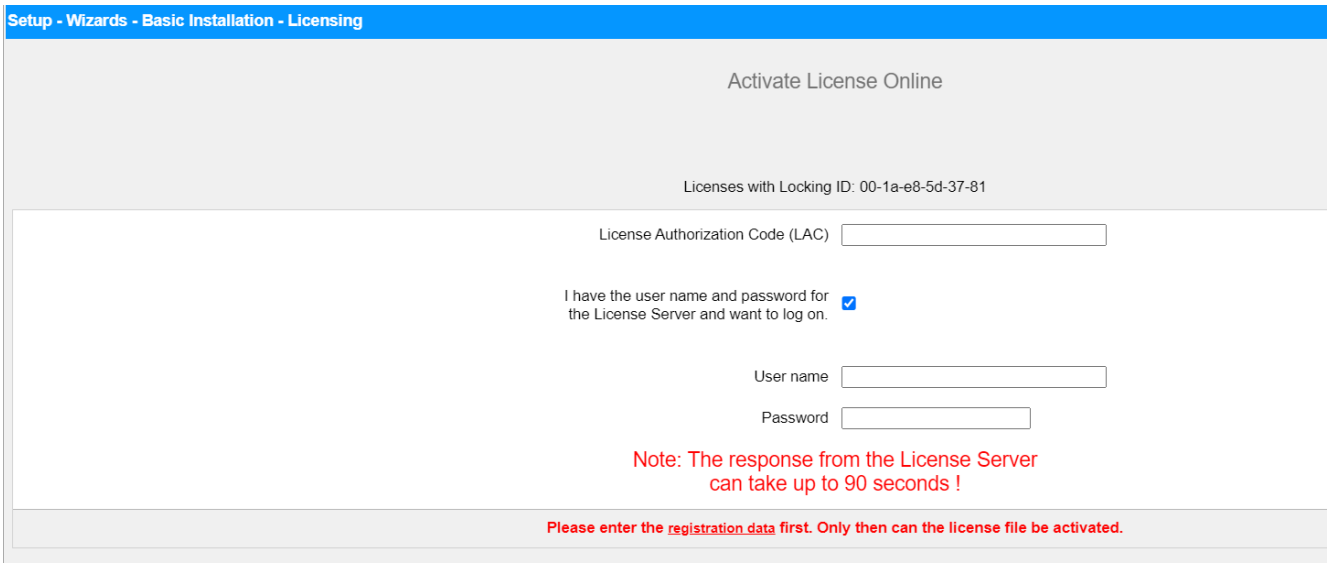
Passo a passo

1) Attivare le licenze online:

a) Nella barra di navigazione fare clic su **Configurazione**.

b) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.

c) Fare clic su **Modifica**, per avviare la procedura guidata **Concessione della licenza**.



d) Nel campo **Codice autorizzazione licenza (LAC)** immettere il LAC.

e) Selezionare la casella di controllo **Dispongo del nome utente e della password per il server delle licenze e desidero accedere**.

f) In **Nome utente** e **Password**, inserire i rispettivi dati per l'accesso al server delle licenze.

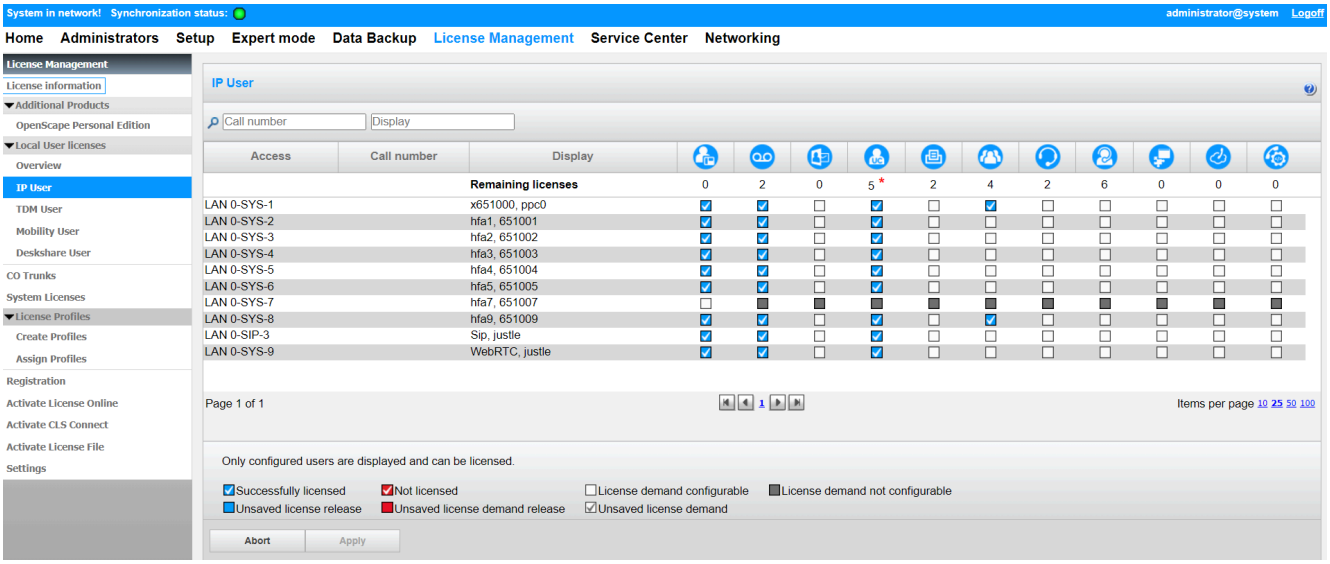
g) Fare clic su **OK & Avanti**. Viene stabilita la connessione al server delle licenze e le licenze vengono attivate.

2) Assegnazione delle licenze agli utenti:

a) Nella barra di navigazione fare clic su **Gestione delle licenze**.

b) Nella struttura di navigazione, selezionare **Licenze di utenti locali** > **...** fino al tipo di utente desiderato. Viene visualizzato un elenco di tutti gli utenti del tipo selezionato.

c) Nella riga dell'utente desiderato, selezionare la casella di controllo nella colonna **Licenza utente** (prima colonna con caselle di controllo).



d) Nella riga dell'utente desiderato, attivare le licenze orientate all'utente selezionando le caselle di controllo desiderate.

Nota: Le licenze orientate all'utente possono essere assegnate a un'apparecchio solo se è stata in precedenza assegnata una licenza all'apparecchio (licenza utente) (punto c).

---

e) Fare clic su **OK & Avanti**. Il sistema verifica che per la propria assegnazione siano disponibili licenze sufficienti.

Se le licenze disponibili sono sufficienti, la concessione delle licenze dell'utente è completata.

f) In caso di mancanza di licenze, viene segnalato l'errore con una casella di controllo rossa ombreggiata. Correggere l'errore e ripetere il passo e.

3) Assegnazione delle licenze alle linee:

a) Nella struttura di navigazione fare clic su **Linee urbane**. Nell'area **Linee urbane** viene visualizzato il numero di licenze acquistate per le linee.

b) Per linee SIP: nell'area **Richiesta licenze per numero di chiamante simultanee via Internet in questo nodo**, inserire il numero di chiamate

Internet che possono essere eseguite contemporaneamente tramite un ITSP.

c) Per linee S_{2M}: nell'area **S2M**, nella riga degli slot desiderati nell'elenco a discesa della colonna **Demands**, selezionare il numero di canali B desiderato.
d) Per linee T1 (solo per gli USA): nell'area **T1**, nella riga degli slot desiderati nell'elenco a discesa della colonna **Demands**, selezionare il numero di canali B desiderato.
e) Fare clic su **OK & Avanti**.

Nota: Il numero di linee SIP con licenza e il numero di linee S_{2M}/T1 con licenza non può superare il numero di licenze acquistate per le linee.

5.8.2 Come preparare i client UC Smart all'installazione

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

L'hardware e il software per l'uso di UC @work sono disponibili.

Nota: Per l'utilizzo del client UC Smart myPortal @work sono necessarie le relative licenze.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione, fare clic su **Software**.
3) Fare clic sull'icona **myPortal @work** e salvare il file di installazione su un'unità di rete condivisa.
4) Inviare agli utenti di myPortal @work i due file di installazione.
5) In alternativa, è anche possibile inviare agli utenti di myPortal @work il collegamento per accedere direttamente al file di installazione:

```
https://<Indirizzo IP del sistema di comunicazione>/
management/downloads/myPortalAtWorkSetup.exe
```

5.8.3 Come preparare i client UC Suite all'installazione

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

L'hardware e il software per l'uso della UC Suite sono disponibili.

Nota: Per l'utilizzo dei client UC Suite sono necessarie le licenze.

Passo a passo

1) Al fine di rendere automaticamente disponibili a un utente i file di installazione, assicurarsi di avere eseguito le seguenti azioni:
   a) Gli indirizzi e-mail degli utenti devono essere stati importati assieme ai dati dell'utente tramite un file XML o inseriti selezionando il percorso **Configurazione** > **UC Suite** > **Rubrica utente**.
   b) È necessario che sia stato configurato un server di posta elettronica.

   Nota: Il server di posta può essere inserito anche successivamente in **Centro assistenza** > **Inoltro e-mail**.

   Tutti i client con indirizzi e-mail noti ricevono un'e-mail con il collegamento alla cartella di installazione di client UC nonché istruzioni per i primi passi. Nella cartella di installazione si trova inoltre un file Readme con informazioni sull'installazione del software su PC client.
2) Nel caso in cui non vengano eseguite le fasi necessarie per l'avviso automatico, è possibile mettere a disposizione manualmente i file di installazione. A tale riguardo, procedere nel modo seguente:
   a) Nella barra di navigazione fare clic su **Centro assistenza**.
   b) Nella struttura di navigazione, fare clic su **Software**.
   c) Fare clic sul client UC desiderato e salvare il file di installazione zippato su un'unità di rete condivisa.
   d) Nella struttura di navigazione, fare clic su **Documenti** e selezionare l'elenco a discesa **Istruzioni per l'uso**.
   e) Fare clic sulla documentazione per il client UC desiderata e salvare il file della documentazione su un'unità di rete condivisa.
   f) Inviare agli utenti dei client UC Suite il file di installazione zippato e il file della documentazione via e-mail o comunicare agli utenti il percorso in cui risiedono i file.
   g) Nel file zip contenente i file di installazione è presente anche un file Readme. Informare gli utenti che l'installazione dei client UC deve essere eseguita secondo le indicazioni riportate nel file Readme.
3) In alternativa, è anche possibile inviare agli utenti UC collegamenti per accedere direttamente ai file di installazione dei client UC.
   a) Nella barra di navigazione fare clic su **Centro assistenza**.
   b) Nella struttura di navigazione, fare clic su **Software**.
   c) Fare clic sul pulsante **Visualizza collegamenti applicazione**. Vengono visualizzati più collegamenti, a seconda del sistema operativo e del client UC desiderato. Ad esempio:

   ```
   https://<Indirizzo IP del sistema di comunicazione>/
   management/downloads/install-common.zip
   ```

5.8.4 Come eseguire il backup dei dati

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Per effettuare un backup dei dati su un supporto USB (chiavetta o disco rigido USB) è necessario che tale supporto sia collegato a un'interfaccia server USB.

Nota: Per ulteriori informazioni sul backup dei dati, vedere Salvataggio immediato .

Passo a passo

1) Nella barra di navigazione fare clic su **Backup dei dati**.
2) Nella struttura di navigazione fare clic su **Backup - immediato**.
3) Nell'area **Nome**, nel campo **Commento**, immettere un commento per il set di backup per facilitare l'identificazione in caso di ripristino dei dati. Non utilizzare dieresi e caratteri speciali.
4) Nell'area **Dispositivi**, selezionare l'unità di destinazione sulla quale si vuole salvare il set di backup.
5) Fare clic su **OK & Avanti**. Viene visualizzata una finestra che mostra l'avanzamento del backup.
6) Il backup ha esito positivo se viene visualizzato il messaggio **Backup completato**. Fare clic su **Chiudi**.
7) Se per il backup si utilizza un supporto USB, attendere fino a quando il LED di tale supporto non smette di lampeggiare. A questo punto il backup sulla chiave USB è stato eseguito. Rimuovere la chiave USB.
8) La messa in servizio con il WBM è ora completata. Chiudere il WBM facendo clic in alto a destra sul collegamento **Disconnetti**, quindi chiudendo la finestra.

Nota: Nel caso sia presente una nuova versione software per il sistema di comunicazione, ciò verrà comunicato nella pagina iniziale del WBM, a condizione che l'accesso a Internet sia stato configurato correttamente. Se è disponibile una nuova versione software, eseguire un aggiornamento (vedere Aggiornamento del sistema di comunicazione).

5.9 Messa in servizio dei telefoni IP

Per una pratica messa in funzione dei telefoni IP, è necessario un server DHCP che fornisce ai telefoni IP i dati richiesti per l'accesso al sistema di comunicazione dati (dati di rete).

Dati specifici della rete

Per l'accesso al sistema di comunicazione, un telefono IP deve disporre dei dati di rete. Questi dati possono essere archiviati nel server DHCP o inseriti direttamente nel telefono IP. Il vantaggio di un server DHCP è costituito dal fatto che tutti i telefoni IP collegati ricevono automaticamente i dati.

Per il telefono IP sono necessari i seguenti dati:

- Indirizzo IP del sistema di comunicazione
- Indirizzo IP del server DLS

Inoltre il telefono IP richiede anche il proprio numero di telefono. Durante l'accesso, deve essere digitato manualmente nel telefono.

Registrazione dei telefoni SIP

Per motivi di sicurezza si consiglia di registrare i telefoni SIP presso il sistema di comunicazione. A tal fine, i dati di registrazione nel telefono IP e nel sistema di comunicazione devono corrispondere.

Per l'accesso sono necessari i seguenti dati:

- ID utente SIP
- Password SIP
- SIP realm (opzionale)

Non utilizzare password SIP semplici, ma assicurarsi che la password rispetti le seguenti regole:

- Almeno 8 caratteri
- Almeno una lettera maiuscola (A - Z)
- Almeno una lettera minuscola (a - z)
- Almeno una cifra (0-9)
- Almeno un carattere speciale

Utilizzare un ID utente SIP che non comprenda il numero di telefono.

Nota: Per ulteriori informazioni sulla configurazione dei telefoni SIP, visitare l'indirizzo Web `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Uso del server DHCP interno

Se viene utilizzato il server DHCP interno del sistema di comunicazione, i dati specifici della rete sono già memorizzati qui. Per poter registrare un telefono IP sul sistema di comunicazione, è necessario immettere nel telefono IP solo il numero di telefono definito. Per un telefono SIP, occorre inoltre che i dati per la registrazione SIP sul telefono SIP e nel sistema di comunicazione corrispondano.

Uso di un server DHCP esterno con dati specifici della rete

Se viene utilizzato un server DHCP esterno, i dati specifici della rete devono essere salvati qui. Per poter registrare un telefono IP sul sistema di comunicazione, è necessario immettere nel telefono IP solo il numero di telefono definito. Per un telefono SIP, occorre inoltre che i dati per la registrazione SIP sul telefono SIP e nel sistema di comunicazione corrispondano.

Uso di un server DHCP esterno senza dati specifici della rete

Se si utilizza un server DHCP esterno, in cui non possono essere conservati i dati specifici della rete, questi devono essere inseriti sul telefono IP. Per poter registrare un telefono IP sul sistema di comunicazione, è necessario immettere nel telefono IP il numero di telefono definito, l'indirizzo IP del sistema di comunicazione ed eventualmente modificare le impostazioni per il Deployment Service. Per un telefono SIP, occorre inoltre che i dati per la registrazione SIP sul telefono SIP e nel sistema di comunicazione corrispondano.

5.9.1 Come configurare il telefono IP

Prerequisiti

Il telefono IP è collegato alla rete interna e operativo.

Nota: Qui viene descritta la configurazione di esempio per un telefono di sistema IP OpenStage 40/60/80. Per un altro telefono IP le impostazioni devono essere eseguite in modo analogo. Consultare le istruzioni del telefono IP.

Passo a passo

1) Per accedere alla modalità di amministrazione del telefono di sistema IP, premere, sul telefono, il tasto corrispondente al menu delle impostazioni/ applicazioni.

2) Sfogliare nella scheda da `Impostazioni` a `Admin` e confermare con il tasto OK.

3) Immettere la password di amministratore (predefinita: `123456`) e confermare con il tasto OK.

4) Se sulla rete interna si utilizza il server DHCP del sistema di comunicazione, saltare il passo successivo.

5) Se sulla rete interna non si utilizza il server DHCP del sistema di comunicazione, è necessario inserire l'indirizzo IP del Deployment server (DLS) e del sistema di comunicazione per consentire l'aggiornamento automatico del software dei telefoni IP di sistema. Questo si applica solo per i telefoni IP del sistema. Procedere come segue:

a) Sfogliare fino a `Network` (Rete) e confermare con il tasto OK.
b) Sfogliare fino a `Update service (DLS)` (Servizio di aggiornamento – DLS) e confermare con il tasto OK.
c) Sfogliare fino a `DLS address` (Indirizzo DLS) e confermare con il tasto OK.
d) Per il Deployment server, immettere l'indirizzo IP del sistema di comunicazione (predefinito: `192.168.1.2`) e confermare con il tasto OK.
e) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.
f) Sfogliare fino a `IPv4 configuration` (Configurazione IPv4) e confermare con il tasto OK.
g) Sfogliare fino a `Route (default)` (Route predefinita) e confermare con il tasto OK.
h) Immettere l'indirizzo IP del sistema di comunicazione (predefinito: `192.168.1.2`) e confermare con il tasto OK.
i) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.
j) Per tornare un livello di menu superiore usare il tasto Indietro.

6) Definire il numero del telefono:
   a) Sfogliare fino a `System` (Sistema) e confermare con il tasto OK.
   b) Sfogliare fino a `Identity` (Identità) e confermare con il tasto OK.
   c) Sfogliare fino a `Terminal number` (Numero terminale) e confermare con il tasto OK.
   d) Immettere il numero di telefono configurato (ad esempio, `120`) e confermare con il tasto OK.
   e) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.

7) Per tornare un livello di menu superiore usare il tasto Indietro.

8) Quando il telefono di sistema richiede un riavvio in seguito alle modifiche apportate, nel menu `Admin` viene visualizzata la voce `Riavvia`. Confermare `Riavvia` con il tasto OK e poi `Sì` sempre con il tasto OK. Il telefono di sistema effettua un riavvio e accede al sistema di comunicazione.

5.9.2 Come configurare un telefono SIP

Prerequisiti

Il telefono SIP è collegato alla LAN del cliente e operativo.

Nota: Qui viene descritta la configurazione di esempio per un telefono di sistema OpenStage 40/60/80 SIP. Per un altro telefono SIP le impostazioni devono essere eseguite in modo analogo. Consultare le istruzioni del telefono SIP.

Passo a passo

1) Per accedere alla modalità di amministrazione del telefono di sistema SIP, premere, sul telefono, il tasto corrispondente al menu delle impostazioni/applicazioni.

2) Sfogliare nella scheda da `Impostazioni` a `Amministratore (Admin)` e confermare con il tasto OK.

3) Immettere la password di amministratore (predefinita: `123456`) e confermare con il tasto OK.

4) Se sulla rete interna si utilizza il server DHCP del sistema di comunicazione, saltare il passo successivo.

5) Se sulla rete interna non si utilizza il server DHCP del sistema di comunicazione, è necessario inserire l'indirizzo IP del Deployment server (DLS) e del sistema di comunicazione per consentire l'aggiornamento automatico del software dei telefoni SIP di sistema. Questo si applica solo per i telefoni SIP del sistema. Procedere come segue:
   a) Sfogliare fino a `Network` (Rete) e confermare con il tasto OK.
   b) Sfogliare fino a `Update service (DLS)` (Servizio di aggiornamento – DLS) e confermare con il tasto OK.
   c) Sfogliare fino a `DLS address` (Indirizzo DLS) e confermare con il tasto OK.
   d) Per il Deployment server, immettere l'indirizzo IP del sistema di comunicazione (predefinito: `192.168.1.2`) e confermare con il tasto OK.

e) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.
f) Sfogliare fino a `IPv4 configuration` (Configurazione IPv4) e confermare con il tasto OK.
g) Sfogliare fino a `Route (default)` (Route predefinita) e confermare con il tasto OK.
h) Immettere l'indirizzo IP del sistema di comunicazione (predefinito: `192.168.1.2`) e confermare con il tasto OK.
i) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.
j) Per tornare un livello di menu superiore usare il tasto Indietro.

6) Definire le impostazioni temporali SNTP:
a) Sfogliare fino a `Date and time` (Data e ora) e confermare con il tasto OK.
b) Sfogliare fino a `Time source` (Origine ora) e confermare con il tasto OK.
c) Sfogliare fino a `SNTP IP address` (Indirizzo IP SNTP) e confermare con il tasto OK.
d) Immettere l'indirizzo IP del sistema di comunicazione (predefinito: `192.168.1.2`) e confermare con il tasto OK.
e) Sfogliare fino a `Timezone offset` (Offset fuso orario) e confermare con il tasto OK.
f) Inserire la deviazione tra l'ora locale e UTC (Universal Time Coordinated) espressa in ore (Germania: `1`) e confermare con il tasto OK.
g) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.
h) Per tornare un livello di menu superiore usare il tasto Indietro.

7) Definire il numero del telefono:
a) Sfogliare fino a `System` (Sistema) e confermare con il tasto OK.
b) Sfogliare fino a `Identity` (Identità) e confermare con il tasto OK.
c) Sfogliare fino a `Terminal number` (Numero terminale) e confermare con il tasto OK.
d) Immettere il numero di telefono configurato (ad esempio, `120`) e confermare con il tasto OK.
e) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.

8) Definire i dati di autenticazione SIP:
a) Sfogliare fino a `Registration` (Registrazione) e confermare con il tasto OK.
b) Sfogliare fino a `SIP session` (Sessione SIP) e confermare con il tasto OK.
c) Prendere nota del `Realm` o se richiesto inserire un nuovo realm (ad esempio `OSBIZ-SIP`).
d) Prendere nota dell'`ID utente` o se richiesto inserire un nuovo ID utente (ad esempio `SIP-120`).
e) Immettere la `Password` per la registrazione presso il server SIP.
f) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.

9) Utilizzando il pulsante Indietro, tornare al menu `Admin`.

10) Quando il telefono di sistema richiede un riavvio in seguito alle modifiche apportate, nel menu `Admin` viene visualizzata la voce `Riavvia`. Confermare `Riavvia` con il tasto OK e poi `Sì` sempre con il tasto OK. Il telefono di sistema effettua un riavvio e accede al sistema di comunicazione.

5.10 Come raccogliere tracce diagnostiche per un evento di errore

È possibile raccogliere automaticamente le tracce diagnostiche necessarie per un evento di errore. The **Error Management** wizard will guide you through the whole process.

You must run the **Error Management** wizard twice: before and after the execution of the problematic scenario. During the first run (Phase 1), you activate the diagnostic traces collection. After execution of the problematic scenario, run the wizard again to collect the diagnostic trace data (Phase 2). Once the Phase 2 is complete, you can download the trace file to include them in the ticket system.

Eseguire i passaggi seguenti per raccogliere i dati della traccia diagnostica per l'evento di errore:

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.

2) Fare clic su **Modifica** vicino a **Gestione errori**.

3) Click on **OK & Next**

4) If you want to collect the Default Traces click on the **Default Traces** check-box.

5) If you want to specify the types of traces to collect, select the desired ones from the list of traces. More than one selection is possible.

Per ulteriori informazioni sulle tracce, vedere la Guida alla risoluzione dei problemi.

6) Fare clic su **OK & Avanti**.

7) Viene visualizzato un elenco con informazioni aggiuntive, documentazione rilevante e suggerimenti. Fare clic su **OK & Avanti**.

8) Vengono visualizzati gli scenari e il tipo di tracce da raccogliere. Fare clic su **Fine**.

9) Continuare eseguendo lo scenario problematico.

10) Dopo aver completato lo scenario, andare di nuovo a **Configurazione > Gestione errori** e fare clic su **Modifica**.

Si viene reindirizzati al Passaggio 2 della raccolta tracce di diagnostica. Per interrompere il processo e riavviarlo, è possibile fare clic sul pulsante **Annulla**.

11) Fare clic su **OK & Avanti**.

12) Inserire le informazioni richieste e fare clic su **OK & Avanti**.

13) Viene visualizzato un elenco con le informazioni necessarie e alcune altre azioni aggiuntive.

14) Fare clic su **OK & Avanti**.

15) Fare clic su **Fine** per avviare il download dei dati della traccia diagnostica.

5.11 Reflashing

Seguendo i passaggi indicati di seguito è possibile modificare facilmente il tipo di software di un dispositivo.

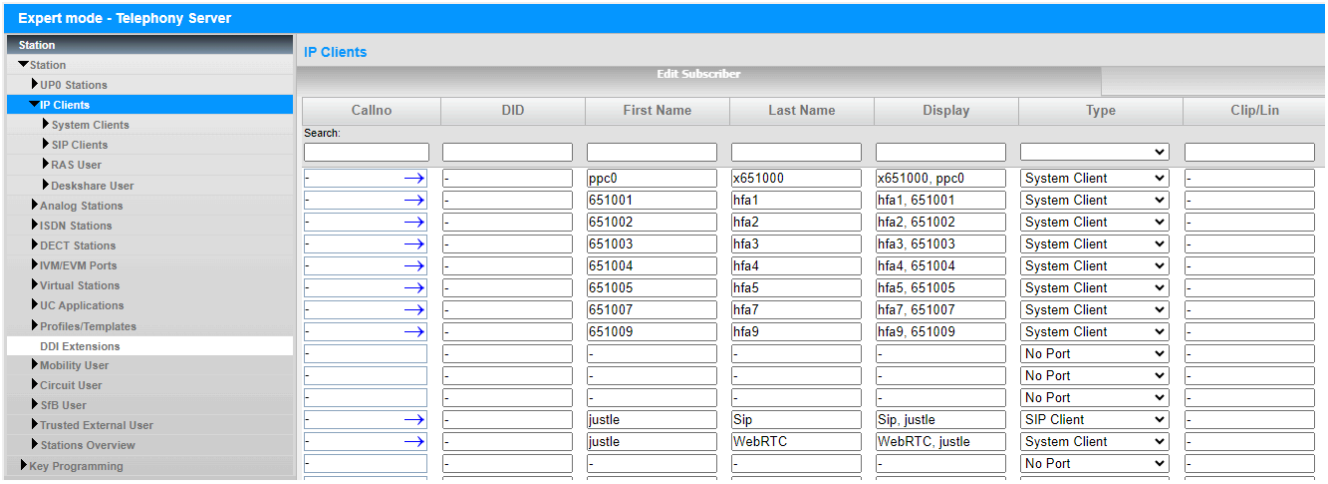
L'idea alla base di questa funzione è quella di semplificare il modo in cui ottenere un dispositivo SIP (pronto all'uso) e registrarlo nel sistema OSBiz come dispositivo HFA. Gli unici requisiti sono che:

- il telefono deve ottenere l'indirizzo DLI (dal server DHCP o manualmente)
- l'amministratore deve inserire il numero del telefono (che deve essere preconfigurato come client di sistema)

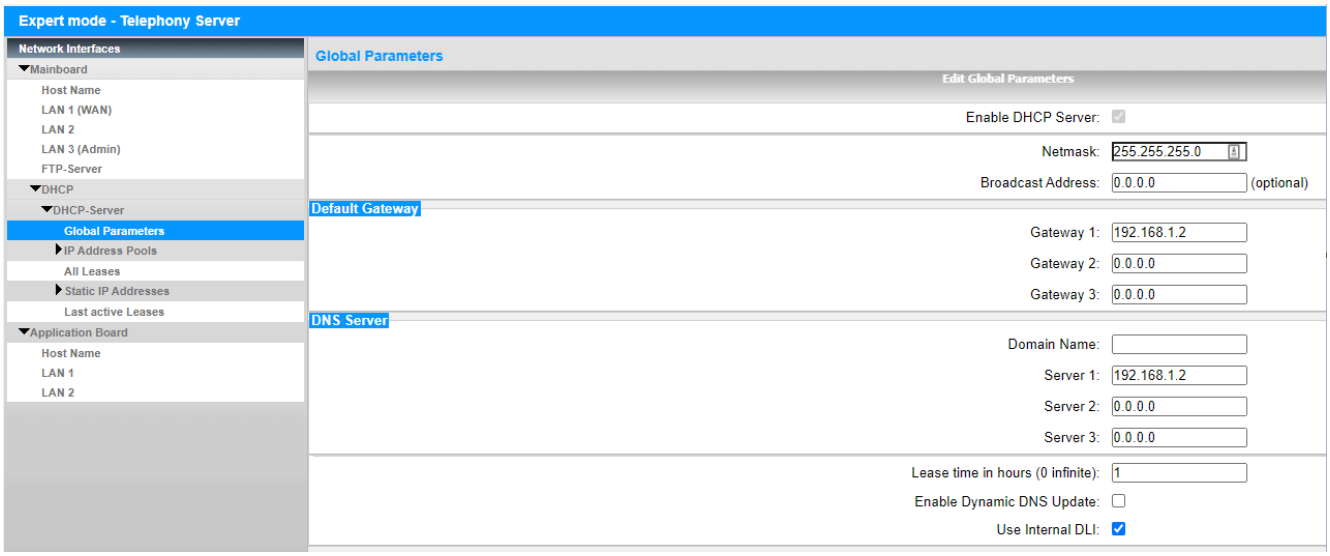
Quando il cliente riceve un nuovo dispositivo, questo viene preconfigurato come dispositivo SIP (impostazioni di fabbrica). I passaggi da seguire per eseguire il reflashing del dispositivo e trasformarlo in un dispositivo HFA sono i seguenti:

Passo a passo

1) Configurare nel database OSBIZ il numero di telefono desiderato come client di sistema (HFA).



2) Configurare il server DHCP per inviare l'indirizzo IP del DLI. Questa operazione può essere eseguita sul server DHCP esterno o sul server DHCP interno.



3) Se non viene utilizzato un server DHCP, è necessario configurare manualmente l'IP di DLI sul telefono.

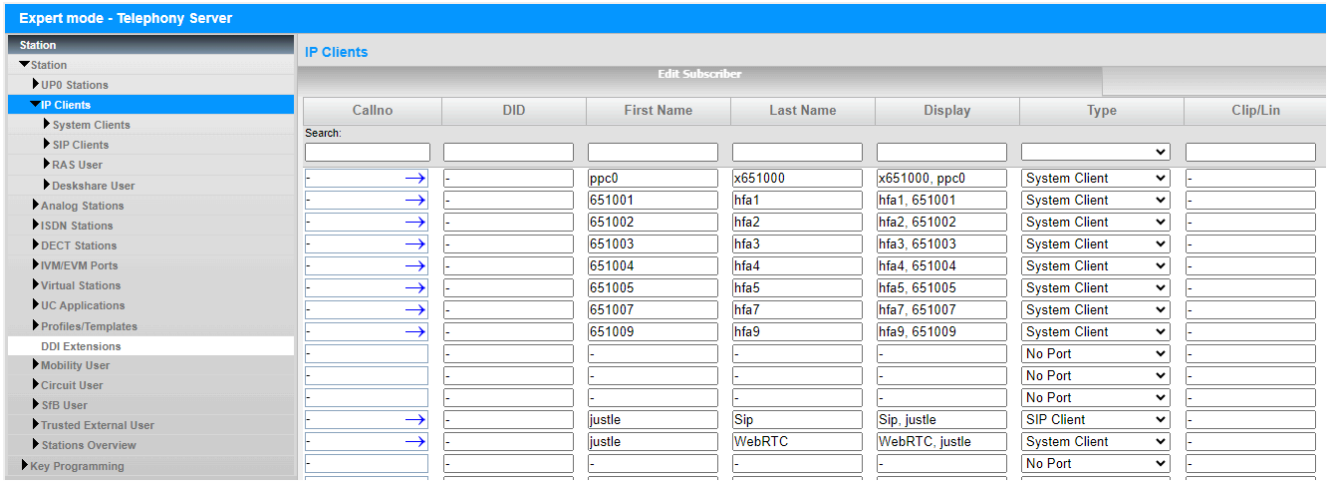
4) Una volta che il telefono SIP ha ottenuto un IP e l'IP DLI, il dispositivo telefonico verrà registrato nel database DLI e verrà visualizzato un prompt per l'immissione del numero di interno.

5) Immettere il numero di terminale del telefono (il numero deve essere lo stesso configurato nel primo passaggio, ad esempio 4111).

6) Il reflashing si avvia e la nuova immagine HFA viene scaricata sul telefono. Al suo riavvio, il telefono verrà registrato come telefono HFA e i dati plug and play saranno inviati dal sistema al telefono.

7) **Per eseguire il reflashing di un telefono SIP già registrato:**

8) Cambiare il dispositivo SIP funzionante in "Client di sistema".



9) Riavviare il telefono

10) Il reflashing si avvia e la nuova immagine HFA viene scaricata sul telefono. Al suo riavvio, il telefono verrà registrato come telefono HFA e i dati plug and play saranno inviati dal sistema al telefono.

6 Configurazione iniziale di OpenScape Business S

Viene descritta la configurazione iniziale di OpenScape Business S (indicato anche come Soft switch in breve). Il softswitch e i relativi componenti sono integrati nella rete LAN esistente del cliente. Vengono configurati l'accesso a Internet per la telefonia Internet e gli utenti collegati.

Per OpenScape Business S, il software di comunicazione OpenScape Business viene installato sul sistema operativo Linux SLES 12 SP5 a 64 bit o SLES 15 SP6 a 64 bit. Il software di comunicazione può essere messo in funzione direttamente su un server Linux o in un ambiente virtuale con VMware VSphere o Microsoft Hyper-V. L'installazione del sistema operativo Linux è descritta nelle istruzioni di installazione *OpenScape Business, Installazione del server Linux*.

La configurazione iniziale di OpenScape Business S viene eseguita con il programma di amministrazione OpenScape Business Assistant (gestione basata sul Web, denominata per brevità WBM).

Questa sezione descrive come configurare i componenti più comunemente utilizzati. Non è necessario utilizzare tutti i componenti. Pertanto, alla configurazione iniziale, occorre scegliere tra più opzioni o configurazioni o saltare interamente alcune configurazioni, a seconda di quali componenti sono inclusi nella propria applicazione.

L'amministrazione dettagliata delle funzioni non coperte dalla configurazione iniziale è descritta nei seguenti capitoli.

Requisito essenziale per la configurazione iniziale è la creazione di uno schema di indirizzi IP e di un piano di composizione.

Panoramica dei principali passaggi di installazione:

- Impostazioni di sistema
- Numeri di telefono completi e collegamento in rete
- Telefonia Internet
- Configurazione utenti
- Licenza
- Rafforzamento del sistema
- Backup dei dati

6.1 Requisiti richiesti per la configurazione iniziale

Soddisfare i prerequisiti per la configurazione iniziale serve a garantire il corretto funzionamento di OpenScape Business S.

Generale

A seconda dell'hardware utilizzato (telefoni, ...) e dell'infrastruttura esistente, si applicano le seguenti condizioni generali:

- L'infrastruttura LAN (router Internet, switch, ecc.) è presente e utilizzabile.
- I telefoni IP sono connessi alla LAN del cliente.
- Il server Linux necessario per OpenScape Business S è stato installato seguendo le istruzioni presenti nella *Guida all'installazione del server Linux per OpenScape Business*, è stato integrato nella LAN del cliente ed è pronto per l'uso.

- Tutte le licenze necessarie per OpenScape Business S sono presenti (ad esempio, client UC, servizi di directory, ecc.).
- Uno schema di indirizzi IP esiste già ed è noto.
- Un piano di composizione (chiamato anche piano di numerazione) è presente e noto.

Software

Per l'installazione di OpenScape Business S è necessario il seguente software:

- DVD o immagine .ISO con il software di comunicazione il OpenScape Business

  Contiene il software di comunicazione OpenScape Business. Questo DVD o questa immagine .ISO sono inclusi nel pacchetto di consegna.
- DVD o chiavetta USB con il sistema operativo Linux SLES 12 SP5 o SLES 15 SP6.

  Il DVD Linux potrebbe essere necessario durante l'installazione del software di comunicazione OpenScape Business, poiché alcuni pacchetti software (RPM) necessari per il software di comunicazione potrebbero dover essere installati successivamente da questo DVD o file .ISO.

Amministrazione

Per la configurazione iniziale di OpenScape Business S con OpenScape Business Assistant (WBM), è possibile utilizzare il server Linux o il PC amministratore. Il WBM è basato su browser e, quindi, dipende dal sistema operativo.

- Browser Web:

  Sono supportati i seguenti browser Web abilitati per HTML 5:

  – Microsoft Internet Explorer versione 11 e successive (PC amministratore).
  – Microsoft Edge
  – Mozilla Firefox versioni 37.x e 38.x
  – Mozilla Firefox ESR versioni 24.x e 31.x
  – Google Chrome

  Se è installata una versione precedente del browser Web, è necessario installare una versione aggiornata prima di poter avviare la configurazione iniziale del sistema.
- Java:

  occorre installare Oracle Java 8 o versione superiore oppure, in alternativa, OpenJDK 8. Se è installata una versione precedente, è necessario aggiornarla alla versione più recente prima di poter iniziare a configurare il sistema per la prima volta.

- Risoluzione dello schermo: 1024x768 o superiore

Firewall

Se si è connessi a Internet, è necessario un firewall per il server Linux al fine di impedire l'accesso non autorizzato dall'esterno. Dopo l'installazione di Linux, il firewall di Linux è abilitato. L'installatore del software di comunicazione regola le impostazioni del firewall in modo che il software di comunicazione possa funzionare correttamente. Le porte per il software di comunicazione sono aperte e tutte le altre porte sono chiuse.

Se viene utilizzato un firewall esterno nella rete, il firewall Linux deve essere disabilitato e gli indirizzi e le porte necessari per il software di comunicazione devono essere aperti (vedere Porte usate).

Accesso a Internet

Il PC server deve disporre dell'accesso a Internet a banda larga per:

- Patch di sicurezza e aggiornamenti generali del software Linux

OpenScape Business richiede una connessione a Internet per:

- Aggiornamenti del software OpenScape Business
- Funzionalità di OpenScape Business quali la telefonia Internet, ad esempio
- OpenScape Business Mobility Client come myPortal to go, ad esempio
- Assistenza remota

Server di posta elettronica (opzionale)

OpenScape Business richiede l'accesso a un server di posta elettronica per poter inviare e-mail. A tale scopo, i dati di accesso al server di posta elettronica devono essere inseriti in OpenScape Business e i relativi account (indirizzo IP, URL, dati di accesso del server di posta elettronica) devono essere configurati nel server di posta elettronica.

Se la funzionalità e-mail non viene usata in OpenScape Business, non è necessario inserire questi dati.

Telefonia Internet, VoIP (opzionale)

Se all'interno di OpenScape Business viene utilizzata la telefonia tramite Internet, è necessario che OpenScape Business disponga di un accesso a Internet a banda larga e di un provider di servizi di telefonia tramite Internet (provider ITSP, SIP) per la telefonia SIP su Internet. A tal fine, è necessario ottenere gli account appropriati dall'ITSP e configurare in OpenScape Business i dati di accesso per l'ITSP (indirizzo IP, URL, dati di accesso del provider SIP).

Seconda porta LAN

Se OpenScape Business S (o il server Linux) possiede una seconda porta LAN, questa può essere utilizzata come un'interfaccia WAN per l'accesso a Internet e la telefonia via Internet tramite un provider ITSP. La prima porta LAN viene utilizzata come interfaccia LAN per i telefoni interni e i computer. La configurazione dell'accesso a Internet viene effettuata nel router Internet esterno della LAN del cliente. La configurazione della seconda porta LAN viene effettuata direttamente durante la configurazione iniziale di Linux o può essere eseguita in un secondo momento con YaST. Nel WBM, la seconda porta LAN deve essere attivata solo come interfaccia WAN.

Fax in formato PDF

Se i fax devono essere salvati in formato PDF, il PC server richiede almeno 4 GB di RAM. Se OpenScape Business S verrà utilizzato in un ambiente virtuale, anche alla macchina virtuale devono essere assegnati 4 GB di RAM.

6.2 Componenti

I componenti indicati nell'esempio di installazione sono descritti e schematizzati di seguito.

L'esempio di installazione comprende i seguenti componenti:

- OpenScape Business S

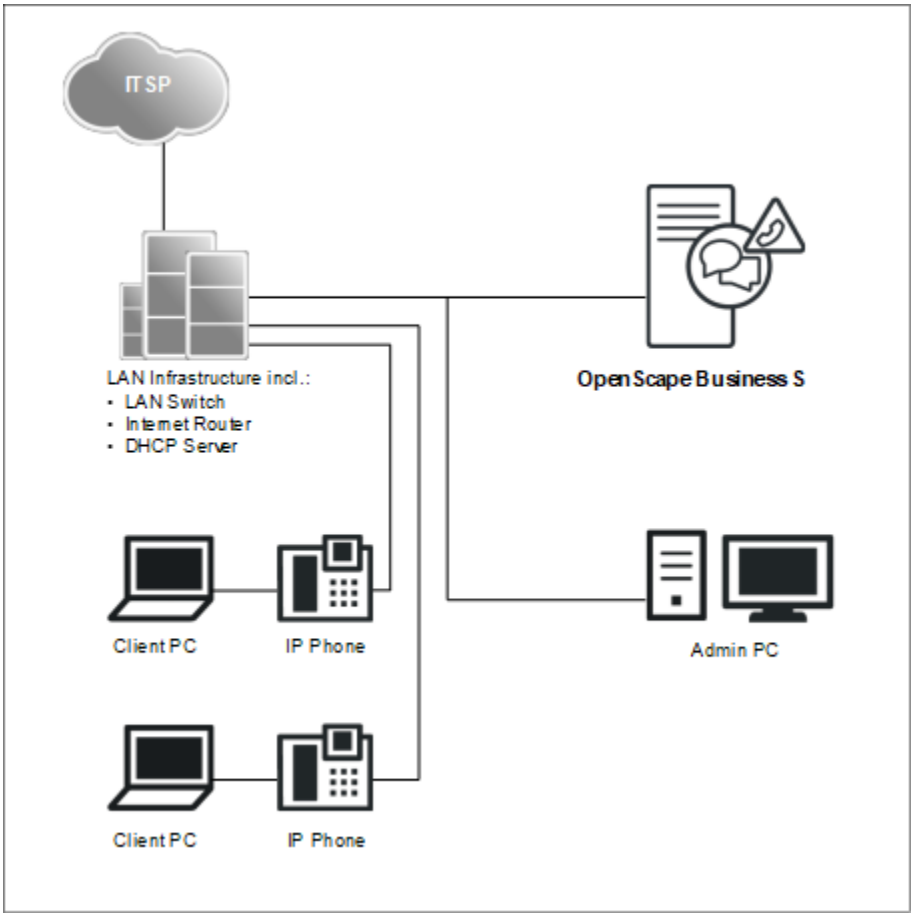
  Il server Linux con cui il software di comunicazione OpenScape Business S è integrato nella LAN esistente del cliente tramite la propria interfaccia LAN.
- PC Admin

  Anche il PC Admin è integrato nella LAN esistente del cliente tramite la propria interfaccia LAN.
- Utente IP (client IP)

  Gli utenti IP (telefoni di sistema IP, PC client, punti di accesso WLAN ecc.) sono integrati tramite uno o più switch.

I client IP ottengono il proprio indirizzo IP in modo dinamico da un server DHCP interno (server DHCP del server Linux) o da un server DHCP esterno (ad esempio il server DHCP del router Internet).

L'accesso a Internet è configurato nel router Internet.



6.3 Schema indirizzi IP

Uno schema indirizzi IP definisce come vengono utilizzati gli indirizzi IP in una rete LAN. Comprende gli indirizzi IP di PC, server, router Internet, telefoni IP ecc.

Per una migliore visione d'insieme durante l'assegnazione degli indirizzi IP è necessario creare uno schema indirizzi IP.

Esempio di uno schema indirizzi IP nella gamma `192.168.5.x`:

Intervallo di indirizzi IP	Client
192.168.5.1 a **192.168.5.49**	Client con indirizzo IP fisso
192.168.5.1	Router Internet (Gateway)
192.168.5.10	PC server (OpenScape Business S)
192.168.5.20	Server e-mail
192.168.5.100 a **192.168.5.254**	PC client e telefoni IP, unitamente all'intervallo indirizzi IP del server DHCP; l'assegnazione degli indirizzi IP avviene in modo dinamico

6.4 Piano di composizione

Un piano di composizione è una lista di tutti i numeri di telefono disponibili nel sistema di comunicazione. Comprende numeri interni, di selezione passante e per chiamate di gruppo.

Piano di composizione predefinito

Ai numeri di telefono interni sono preassegnati valori predefiniti. All'occorrenza, questi valori possono essere modificati in base ai propri requisiti (piano di composizione singolo).

Estratto dal piano di composizione predefinito:

Tipo di numero di telefono	Numeri di telefono predefiniti
Numeri di telefono dell'utente interno	100-349, 500-709
Nr. di selezione passante	100-349, 500-709
Numeri di telefono dei gruppi	350-439
Numero casella vocale	71
Numero di telefono Announcement Player	72
Codici del fascio (codici esterni): Linea urbana ITSP	855-858
Numero di telefono per conferenze	7400-7404

Tipo di numero di telefono	Numeri di telefono predefiniti
Numero di telefono per parcheggio	7405
Numero di telefono per AutoAttendant	7410-7429
Numero di telefono per conferenza Incontro	7430

Piano di composizione personalizzato

Durante la configurazione di base, è possibile importare un piano di composizione personalizzato nel WBM in formato XML.

Il file XML contiene diverse schede. La scheda Cliente contiene, oltre al nome e al numero di telefono degli utenti, anche altri dati quali il tipo di utente e l'indirizzo e-mail degli utenti.

Nel WBM, disponibile in **Centro assistenza** > **Documenti** > **Modelli** > **ModelliCSV**, è disponibile un esempio di file XML con relativa spiegazione. I file XML qui memorizzati possono essere utilizzati come modelli per i propri dati. Può essere modificato ad esempio in Microsoft Excel.

6.5 Installazione del software di comunicazione

Il software di comunicazione OpenScape Business S è installato sul server Linux.

Assicurarsi che gli indirizzi IP e le maschere di rete da configurare siano adeguati alla LAN del cliente.

Server DHCP

Un server DHCP assegna automaticamente un indirizzo IP univoco a ciascuna stazione IP (telefoni IP, PC, ecc.) e fornisce alle stazioni IP dati specifici della rete, come ad esempio l'indirizzo IP del gateway predefinito.

È possibile utilizzare come server DHCP un server DHCP esterno (ad esempio, il server DHCP del router Internet o del sistema di comunicazione) o il server DHCP del server Linux. Se si utilizza il server DHCP del server Linux, il server DHCP esterno deve essere disabilitato. La configurazione del server DHCP Linux può essere eseguita durante l'installazione del software di comunicazione OpenScape Business.

Nota: Si dovrebbe attivare il DHCP da yast o da WBM, ma non da entrambi. Se si attiva il DHCP durante l'installazione iniziale di OpenScape Business S, è equivalente all'attivazione del DHCP tramite yast. Se si desidera attivare il DHCP su OpenScape Business S da WBM, il DHCP non deve essere attivato durante l'installazione iniziale del software di comunicazione.

Ambiente virtuale

Il software di comunicazione può essere eseguito in un ambiente virtuale. Sono disponibili due modi per eseguire l'installazione:

- Installazione separata di Linux e del software di comunicazione

  A tal fine, il software di virtualizzazione (sistema operativo host) deve essere prima installato e configurato sul PC server. Linux è installato nell'ambiente virtuale come sistema operativo guest. All'interno del sistema operativo Linux, il software di comunicazione viene installato per ultimo con l'aiuto del DVD o del file .ISO di OpenScape Business (per maggiori dettagli, vedere *Server Linux per OpenScape Business, Guida all'installazione*).
- Installazione combinata di Linux e del software di comunicazione (solo VMWare)

  A tal fine, il software di virtualizzazione (sistema operativo host) deve essere prima installato e configurato sul PC server. Un'immagine OVA (Open Virtualization Appliance), che include Linux e il software di comunicazione, viene installata nell'ambiente virtuale. L'immagine OVA viene fornita attraverso il server di fornitura del software (SWS).

  Per più di 50 utenti, la partizione home deve essere ridimensionata dopo l'installazione a 100 GB (per 50-100 utenti) o 200 GB (per un massimo di 500 utenti o per OpenScape Business Contact Center) o 500 GB (per più di 500 utenti).

  Per gli aggiornamenti di Linux, è necessaria anche la chiave di aggiornamento OpenScape Business SLES per potersi registrare con Linux.

Uso delle istantanee sulle macchine virtuali (VM):

Le istantanee possono essere un valido meccanismo di manutenzione, ad esempio per eseguire un rapido rollback a uno stato operativo predefinito della macchina virtuale dopo il fallimento di uno script di distribuzione di massa.

- Le istantanee non possono essere create durante il normale funzionamento. Durante l'acquisizione di un'istantanea, lo stato operativo attuale della macchina virtuale viene congelato. Di conseguenza, i terminali e le applicazioni collegate, come i telefoni IP o i client UC, potrebbero perdere la connessione al server.
- Le istantanee possono causare la perdita di sincronizzazione dei processi interni del server, il che significa che non è più possibile garantire il funzionamento stabile del sistema di comunicazione. Pertanto, anche il riavvio del server dopo lo snapshot deve essere pianificato nell'arco di tempo della manutenzione.
- Le istantanee precedenti non devono rimanere nell'ambiente di produzione durante il normale funzionamento.
- Le istantanee possono essere eseguite durante una finestra di manutenzione pianificata o nell'ambito dell'installazione.
- Le istantanee sono utilizzate internamente da strumenti di backup come VDP o VDR. È necessario assicurarsi che queste operazioni di backup siano pianificate al di fuori dell'orario di lavoro e che le istantanee generate da questi strumenti siano eliminate al termine dell'operazione.

Ulteriori informazioni sulle snapshot sono disponibili nella Knowledge Base (KB) di VMware. Un buon punto di partenza è l'articolo KB 1025279 - Best Practices for virtual machine snapshots in the VMware environment (`http://kb.vmware.com/kb/1025279`).

Tutte le informazioni sulle istantanee in Microsoft Hyper-V sono disponibili nella libreria technet all'indirizzo technet.microsoft.com nel capitolo Hyper-V.

6.5.1 Come installare il software di comunicazione

Prerequisiti

- Il sistema operativo SLES 12 SP5 o SLES 15 SP6 è stato installato e avviato correttamente sul server Linux.
- DVD o file .ISO con software di comunicazione OpenScape Business.
- DVD, file .ISO o chiavetta USB con sistema operativo Linux SLES 12 SP5 a 64 bit o SLES 15 SP6 a 64 bit, per un'eventuale successiva installazione di pacchetti software (RPM), in caso di necessità.
- Sono disponibili i dati dell'accesso root (nome utente e password) per accedere al server Linux.

Importante: Durante l'installazione, il software di comunicazione OpenScape Business sovrascrive qualsiasi file di configurazione esistente (ad esempio, per DHCP, FTP, Postfix, ecc.).

Passo a passo

1) Accedere al server Linux con i privilegi root.

2) Inserire il DVD o il file .ISO di OpenScape Business nell'unità DVD.

3) Confermare il messaggio con **Esegui**. Viene visualizzata la finestra "Welcome".

4) Selezionare la lingua di configurazione desiderata (ad es, **Inglese**) e fare clic su **Avvia**. Qui viene descritto il resto dell'installazione per la lingua inglese.

5) Selezionare il prodotto desiderato dall'elenco e fare clic su **Seleziona**. Viene eseguito un controllo per determinare se l'hardware soddisfa tutti i requisiti per l'installazione. In caso di carenze di poca importanza nei requisiti, viene visualizzato un avviso. Dopo la conferma, è possibile proseguire con l'installazione. In caso di carenze gravi, l'installazione viene annullata automaticamente.

6) Viene eseguito un controllo per determinare se devono essere installati altri pacchetti RPM. In tal caso, confermare con **Conferma**. A questo punto sarà necessario tornare a SLES 12 o SLES 15, su DVD o file .ISO, in un secondo momento.

7) Viene visualizzata una finestra con i termini della licenza (ossia il Contratto di licenza per l'utente finale o EULA). Leggere i termini della licenza e accettare il contratto di licenza con **Sì**.

8) Se è già presente un server DHCP nella LAN del cliente (ad esempio, il server DHCP del router Internet), interrompere qui la configurazione del server DHCP Linux con **No** e procedere on il passaggio 12 per continuare.

Nota: Per garantire che il software dei telefoni di sistema possa essere aggiornato automaticamente anche quando si utilizza un server DHCP esterno, si hanno due possibilità:

a) L'indirizzo IP del server Linux deve essere inserito come indirizzo DLS in ogni telefono di sistema.

b) I dati specifici della rete devono essere inseriti nel server DHCP esterno. I parametri si trovano in `/var/log/OPTI.txt`.

---

9) Se si desidera utilizzare il server DHCP Linux, fare clic su **Sì** per abilitare e configurare il server DHCP Linux.

10) Inserire i seguenti valori (preimpostati con valori predefiniti):

- **Instradamento predefinito**: l'indirizzo IP del gateway predefinito; come regola, l'indirizzo IP del router Internet, ad esempio `192.168.5.1`.
- **Dominio** (opzionale): il dominio specificato durante l'installazione di Linux, ad esempio `<cliente>.com`
- **Server DNS** (opzionale): l'indirizzo IP del server DNS specificato durante l'installazione di Linux. Se nella rete interna non è disponibile nessun server DNS, inserire qui l'indirizzo IP del router Internet (ad esempio, `192.168.5.1`).
- **Server SNTP**: indirizzo IP del server NTP interno o esterno.
- **Server DLS/DLI**: l'indirizzo IP del server DLS, ovvero l'indirizzo IP del server Linux (ad esempio, `192.168.5.10`).
- **Sottorete**: sottorete appropriata per l'intervallo di indirizzi IP, ad esempio: `192.168.5.0`.
- **Maschera di rete**: la maschera di sottorete del server Linux specificata durante l'installazione di Linux, ad esempio: `255.255.255.0`.
- **Inizio intervallo IP** e **Fine intervallo IP**: l'intervallo di indirizzi IP dal quale il server DHCP può assegnare gli indirizzi IP, ad esempio: da `192.168.5.100` a `192.168.5.254`.

11) Fare clic su **Continua**.

12) Dopo l'installazione, è necessario riavviare il sistema operativo Linux. Selezionare la casella di controllo **Riavvio PC** e confermare con **Continua**.

13) Se è necessario installare ulteriori pacchetti RPM, verrà chiesto di inserire il DVD SLES 12 o la chiavetta USB SLES 15. Inserire il DVD o la chiavetta USB e confermare con **Continua**. Dopo aver installato correttamente i pacchetti RPM, reinserire il DVD o il file .ISO di OpenScape Business e confermare con **Continua**, seguito da **Esegui**.

14) Il software di comunicazione OpenScape Business viene installato. Il sistema operativo esegue automaticamente un riavvio.

15) Dopo il riavvio, accedere con l'account utente configurato in precedenza durante l'installazione di Linux.

16) Fare clic con il tasto destro del mouse sull'icona dell'unità DVD sul desktop e selezionare la voce di menu **Espelli**. Rimuovere il DVD di OpenScape Business dall'unità DVD.

Nota: Sono necessari alcuni minuti prima che tutti i componenti del software di comunicazione OpenScape Business siano attivi.

6.6 Messa in servizio

Con la procedura guidata **Configurazione di base** del WBM vengono eseguite le impostazioni di base.

6.6.1 Come avviare la procedura guidata Prima installazione

Prerequisiti

WBM è avviato.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.

2) Fare clic su **Modifica**, per avviare la procedura guidata **Prima installazione**.

Nota: Se con una bassa risoluzione dello schermo non è possibile visualizzare per intero l'area di lavoro nella finestra del browser, sono disponibili barre di scorrimento verticali o orizzontali per visualizzare il contenuto.

Passaggi successivi

Eseguire la prima installazione come descritto di seguito. I campi non descritti in questa sezione sono preimpostati su valori standard e devono essere modificati solo se non corrispondono ai dati della rete del cliente. Per informazioni più complete, fare riferimento alle descrizioni delle singole procedure guidate riportate nella Documentazione per l'amministratore.

6.6.2 Impostazioni di sistema

Nella finestra **Impostazioni di sistema**, configurare le impostazioni del sistema di comunicazione.

Procedere come segue:

1) Definizione del logo a display e del nome del prodotto

È possibile definire un testo che verrà visualizzato sul display del telefono. Oltre a ciò, è possibile selezionare la designazione del prodotto.

2) Selezionare il prefisso del paese e la lingua per i registri evento

Per una corretta inizializzazione del paese è necessario selezionare il paese in cui verrà utilizzato il sistema di comunicazione. Inoltre è possibile

scegliere la lingua utilizzata per il registro eventi (registro degli eventi di sistema, errori ecc.).

3) Solo se necessario: attivare ulteriori porte LAN come interfaccia WAN

   Se OpenScape Business S (o il server Linux) possiede una seconda porta LAN, questa può essere utilizzata come un'interfaccia WAN per l'accesso a Internet e la telefonia via Internet tramite un provider ITSP. La prima porta LAN viene utilizzata come interfaccia LAN per i telefoni interni e i computer.

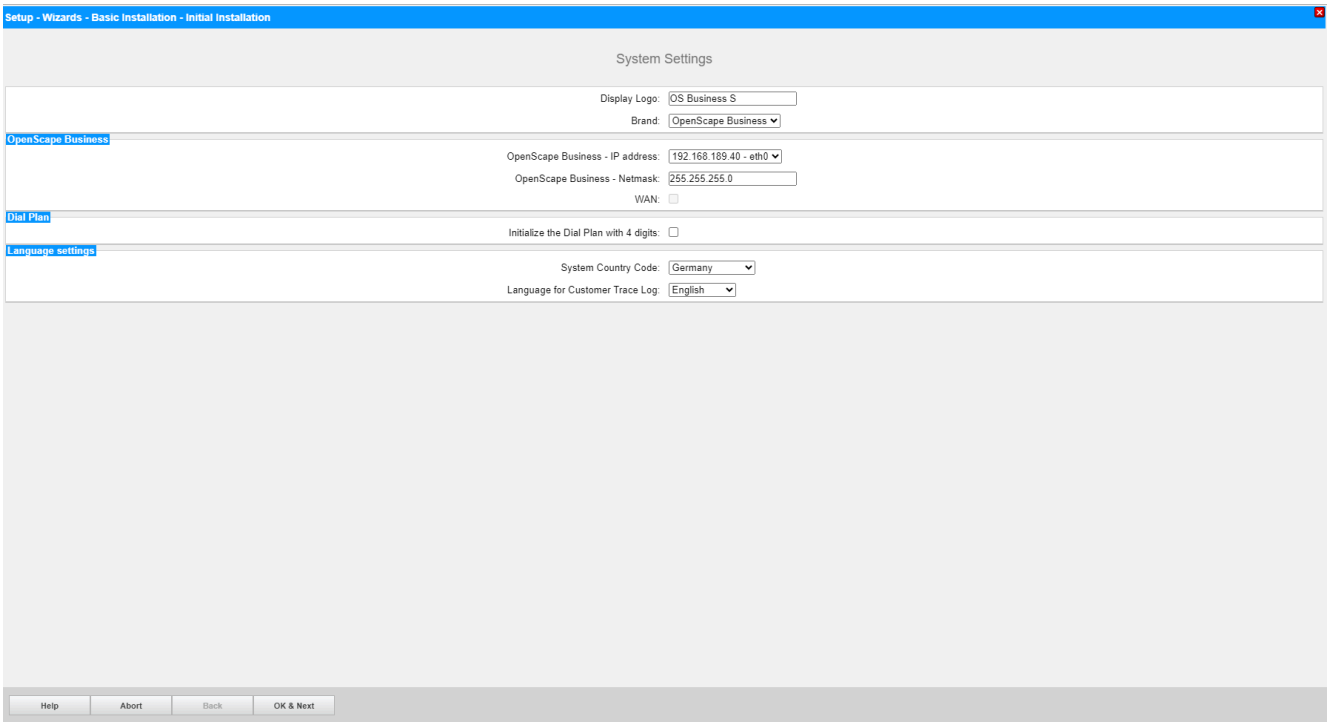
4) Modifica del piano di composizione predefinito con numeri a 4 cifre (disponibile solo per OSBiz S)

   In una nuova installazione del sistema, è possibile inizializzare il piano di composizione con 4 cifre, anziché 3. In questo modo, i numeri predefiniti del sistema passano da 100, 101, 102, ..., a 1000, 1001, 1002 e così via. Ciò consente l'assegnazione automatica del numero di chiamata per un numero elevato di stazioni utente. Tenere presente che, dopo aver abilitato questo flag, il sistema si riavvia.

6.6.2.1 Come impostare il logo sul display e il nome del prodotto

Prerequisiti

Si è nella finestra **Impostazioni di sistema**.



Passo a passo

1) Nel campo **Logo display**, immettere un testo a piacere (ad es. OS Business S). Il testo può contenere fino a 16 caratteri. Evitare dieresi e caratteri speciali.
2) Nell'elenco a discesa **Marchio** selezionare il marchio desiderato.

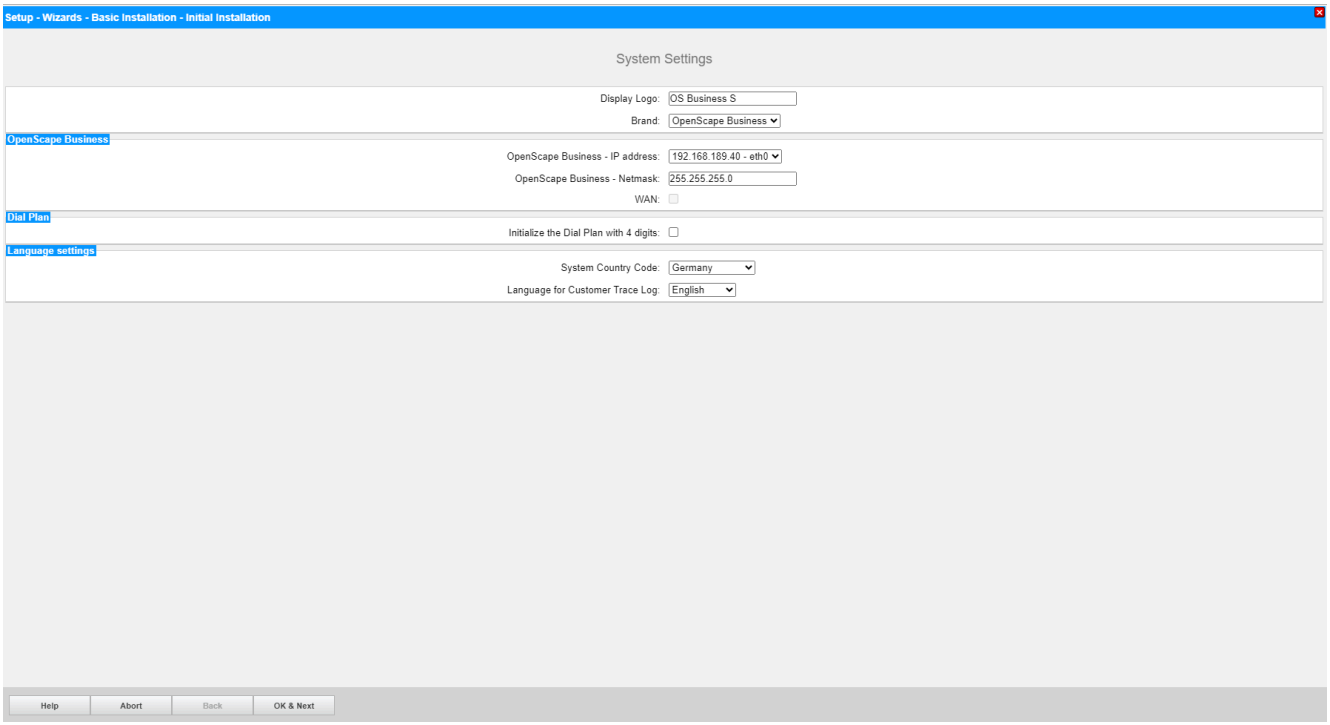
Passaggi successivi

Selezionare il prefisso del Paese e la lingua per i registri di traccia.

6.6.2.2 Come selezionare il prefisso nazionale e la lingua per i registri di traccia

Prerequisiti

Si è nella finestra **Impostazioni di sistema**.



Passo a passo

1) Nell'elenco a discesa **Prefisso internazionale del sistema**, selezionare il Paese in cui viene utilizzato il sistema di comunicazione.
2) Nel campo **Lingua per registro traccia cliente** definire la lingua da utilizzare per il registro eventi (registro degli eventi di sistema, registro degli errori ecc.).

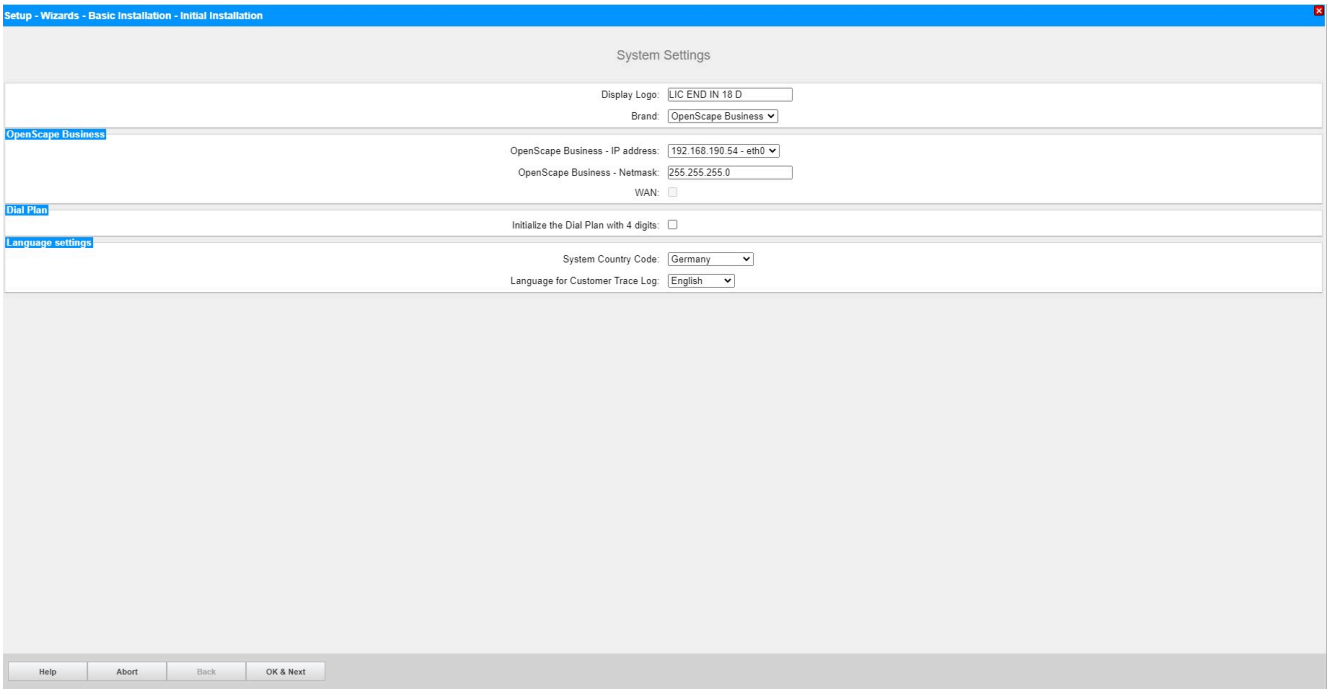
Passaggi successivi

Come avviare la configurazione di base.

6.6.2.3 Come attivare una porta LAN aggiunta come interfaccia WAN

Prerequisiti

Si è nella finestra **Impostazioni di sistema**.



Passo a passo

1) Selezionare la casella di controllo **WAN**.
2) Selezionare la porta LAN desiderata (ad es. `eth1` o `eth2`) dall'elenco a discesa **OpenScape Business - Indirizzo IP (WAN)**. Se sono disponibili solo due porte LAN, la seconda porta LAN `eth1` viene attivata automaticamente.

Importante: Assicurarsi di selezionare l'interfaccia di rete effettiva, anziché localhost.

Nota: L'assegnazione degli indirizzi IP e delle maschera di sottorete alle porte LAN avviene durante l'installazione iniziale di Linux o successivamente tramite YaST.

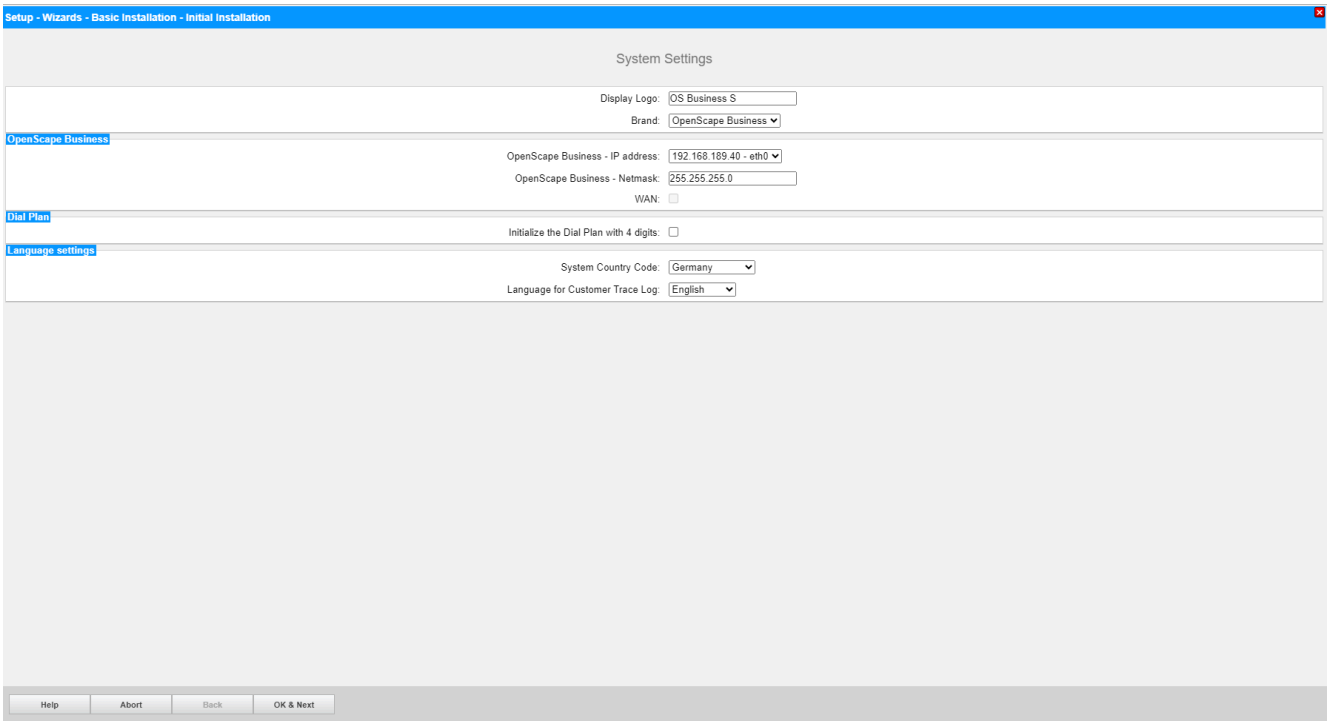
Passaggi successivi

Specificare la soluzione UC.

6.6.2.4 Come modificare il piano di composizione con numeri a 4 cifre

Prerequisiti

Si è nella finestra **Impostazioni di sistema**.



Passo a passo

Fare clic sulla casella di controllo del campo **Inizializzare il piano di composizione con 4 cifre**.

Passaggi successivi

Il sistema si riavvia

6.6.3 Soluzione UC

Nella finestra **Selezione applicazione** è possibile scegliere quale soluzione UC usare.

Sono disponibili le seguenti opzioni:

- **Pacchetto con UC Smart**

  La soluzione UC Smart è integrata in OpenScape Business S.
- **Pacchetto con UC Suite**

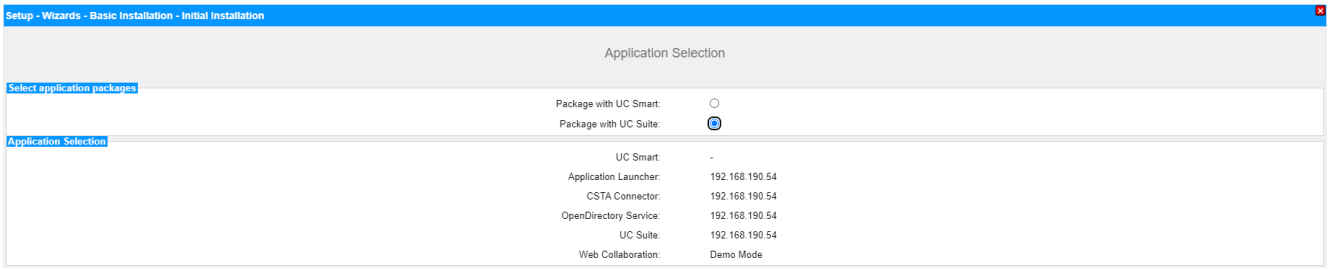
  La soluzione UC Suite è integrata in OpenScape Business S.

6.6.3.1 Come definire la soluzione UC

Prerequisiti

Si sono acquistate licenze per la soluzione UC Smart o UC Suite.

Si è nella finestra **Selezione applicazione**.



Passo a passo

1) Se si utilizza la soluzione di comunicazione unificata Smart UC, fare clic su **Pacchetto con Smart UC**.
2) Se si utilizza la soluzione di comunicazione unificata UC Suite, fare clic su **Pacchetto con UC Suite**.
3) Fare clic su **OK & Avanti**.
4) La procedura guidata **Prima installazione** è conclusa. Fare clic su **Fine**.

Passaggi successivi

Come avviare la configurazione di base.

6.7 Configurazione base

La configurazione base viene eseguita con la procedura guidata **Installazione di base** di WBM. La procedura guidata consente di definire le principali impostazioni per il funzionamento del sistema di comunicazione.

L'installazione guidata di base comprende un indicatore di avanzamento che mostra il passaggio corrente e quelli successivi.

6.7.1 Come avviare la procedura guidata Installazione di base

Prerequisiti

La procedura guidata **Prima installazione** è conclusa.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Fare clic su **Modifica**, per avviare la procedura guidata **Installazione di base**.

Passaggi successivi

Eseguire l'installazione di base come descritto di seguito. I campi non descritti in questa sezione sono preimpostati su valori standard e devono essere modificati solo se non corrispondono ai dati della rete del cliente. Per informazioni più complete, fare riferimento alle descrizioni delle singole procedure guidate riportate nella Documentazione per l'amministratore.

6.7.2 Numeri di telefono completi e collegamento in rete

Nella finestra **Panoramica** inserire i numeri di telefono completi (numero PABX, codice paese e prefisso interurbano, prefisso internazionale) e determinare se OpenScape Business deve essere collegato in rete con altri sistemi OpenScape Business.

Procedere come segue:

1) Inserimento di numeri di telefono completi

- Inserimento di numeri di telefono completi per connessioni punto - punto

  Indicare qui il numero di sistema per la connessione al proprio sistema nonché i prefissi internazionale e interurbano.

  L'immissione del prefisso internazionale è obbligatoria per la telefonia Internet e per le funzionalità di server conferenza.

  Il prefisso internazionale dipende dal codice del paese selezionato in precedenza.
- Inserimento di numeri di telefono completi per connessioni punto - multipunto

  Inserire qui i prefissi internazionale e interurbano per la propria connessioni punto-multipunto.

  L'immissione del prefisso internazionale è obbligatoria per la telefonia Internet e per le conferenze Incontro.

  Il prefisso internazionale dipende dal codice del paese selezionato in precedenza.

2) Attivazione/disattivazione della connessione di rete

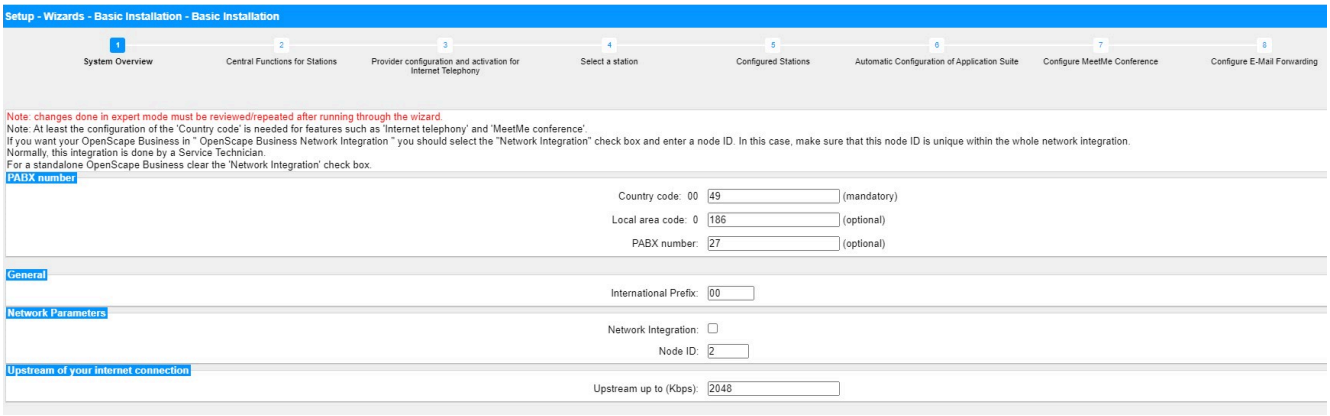
Se OpenScape Business deve essere collegato in rete con altri sistemi OpenScape Business, la connessione di rete deve essere attivata e a OpenScape Business deve essere assegnato un ID nodo. Ogni OpenScape Business nel sistema di reti deve disporre di un ID di nodo univoco.

6.7.2.1 Come inserire i numeri di telefono completi per una connessione punto - punto

Prerequisiti

Si dispone di una connessione punto - punto.

Si è nella finestra **Panoramica** della procedura guidata **Installazione di base**.



Passo a passo

1) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. `49` per la Germania o `1` per gli USA.
2) Nel campo **Prefisso interurbano**, immettere l'indicativo località, ad es. `051` per Bologna.
3) Nel campo **Numero del sistema** inserire il numero del sistema per la propria connessione linea esterna, ad esempio `7007` (il proprio numero della connessione).
4) Modificare il campo **Prefisso internazionale** solo quando necessario. Per la Germania si utilizza `00`, per gli Stati Uniti `011`

   Per le chiamate all'estero, il numero di telefono è preceduto dal prefisso internazionale e dal prefisso nazionale, ad esempio per telefonare dalla Germania agli USA "00-1-..." e dagli USA alla Germania "011-49-...".

Passaggi successivi

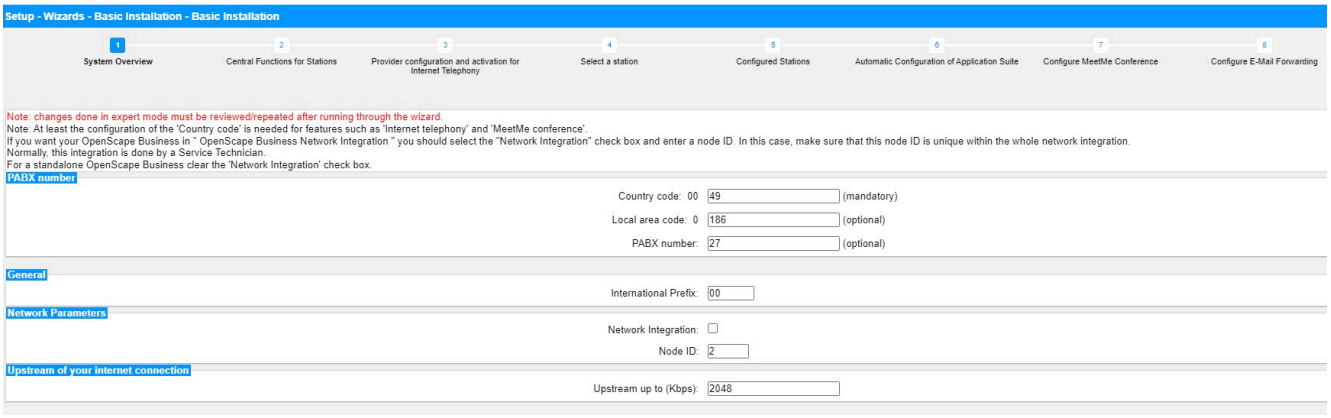
Attivazione/disattivazione della connessione di rete

6.7.2.2 Come inserire i numeri di telefono completi per una connessione punto - multipunto

Prerequisiti

Si dispone di una connessione punto - multipunto.

Si è nella finestra **Panoramica** della procedura guidata **Installazione di base**.



Passo a passo

1) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. `49` per la Germania o `1` per gli USA.
2) Nel campo **Prefisso interurbano**, immettere l'indicativo località, ad es. `051` per Bologna.
3) Lasciare vuoto il campo **Numero del sistema**.
4) Modificare il campo **Prefisso internazionale** solo quando necessario. Per la Germania si utilizza `00`, per gli Stati Uniti `011`.

   Per le chiamate all'estero, il numero di telefono è preceduto dal prefisso internazionale e dal prefisso nazionale, ad esempio per telefonare dalla Germania agli USA "00-1-..." e dagli USA alla Germania "011-49-...".

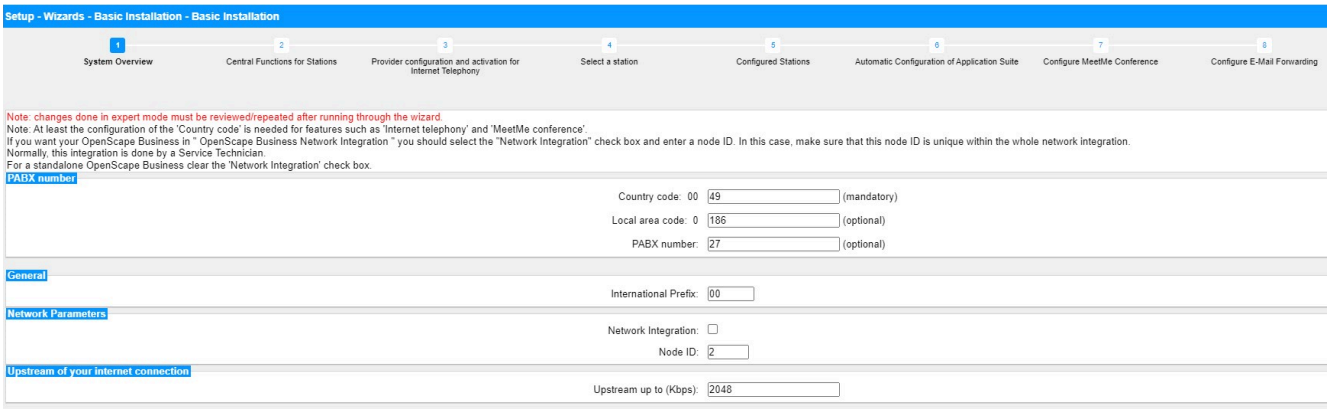
Passaggi successivi

Attivazione/disattivazione della connessione di rete

6.7.2.3 Come attivare o disattivare la connessione di rete

Prerequisiti

Si è nella finestra **Panoramica** della procedura guidata **Installazione di base**.



Passo a passo

1) Se il sistema di comunicazione deve essere collegato in rete con altri sistemi di comunicazione:
   a) Selezionare la casella di controllo **Integrazione rete**.
   b) Nel campo **ID nodo** del sistema di comunicazione, inserire un ID nodo univoco sul sistema di reti (cifre da `1` a `100`).
2) Se il sistema di comunicazione non deve essere collegato in rete con altri sistemi di comunicazione, lasciare deselezionata la casella di controllo **Integrazione in rete**.

Passaggi successivi

Configurare a monte della tua connessione Internet.

6.7.2.4 Come configurare l'upstream della connessione a Internet

Prerequisiti

Si è nella finestra **Panoramica**.

Passo a passo

1) Nel campo **Upstream fino a (Kbps)**, immettere la velocità della propria connessione a Internet.
2) Fare clic su **OK & Avanti**.

Passaggi successivi

Configurare i dati degli utenti.

6.7.3 Dati dell'utente

Nella finestra **Funzioni centrali per gli utenti** è possibile configurare, se necessario, un proprio piano di composizione individuale al posto di quello predefinito e importare altri dati sugli utenti. Nel sistema di reti, il piano di composizione predefinito deve essere adeguato al piano di composizione specifico del sistema di reti.

Il piano di composizione predefinito contiene numeri predefiniti per i diversi tipi di utente (telefoni IP, telefoni analogici, ...) e per funzioni speciali (telefonia via Internet, casella vocale, AutoAttendant, ...).

I dati degli utenti contengono, tra l'altro, i numeri di telefono interni, i numeri di selezione passante e i nomi degli utenti. Con un file XML in formato UTF-8, questi dati e altri dati degli utenti possono essere importati nel sistema di comunicazione durante la configurazione di base.

Nota:

Nel WBM, disponibile in **Centro assistenza** > **Documenti** > **Modelli CSV**, è disponibile un modello XML con relativa spiegazione. In questi modelli è ad esempio possibile inserire i dati con Microsoft Excel.

Sono disponibili le seguenti opzioni:

- **Configurazione dei dati utente senza sistema di reti**

  Procedere come segue:

  1) Visualizzazione dei dati utente

  È possibile visualizzare tutti i numeri di telefono e i dati utente preconfigurati.

  2) Cancella tutti numeri di telefono (opzionale)

  Se si utilizza un piano di composizione personalizzato, occorre prima eliminare i numeri di telefono preconfigurati.

  3) Modificare i numeri di telefono preconfigurati in base al piano di composizione specifico (opzionale)

  Se si utilizza un piano di composizione personalizzato, è possibile modificare i numeri di telefono predefiniti per adattarli al piano di composizione stesso.

  Nota:

  Se l'utente passa attraverso **Modifica numeri di telefono e funzionali pre-configurati**, qualsiasi configurazione personalizzata esistente effettuata in UC Suite deve essere esaminata o ripetuta (ad es., code pilota)

  ---

  4) Importazione dei dati degli utenti tramite file XML (opzionale)

  I singoli numeri di telefono ed eventuali altri dati dell'utente possono essere facilmente importati tramite un file XML durante la configurazione di base.

- **Configurazione dei dati utente con sistema di reti**

  Procedere come segue:

  1) Cancella tutti i numeri di telefono

  Se nel sistema di reti viene utilizzata la UC Suite, è necessario un piano di numerazione chiuso, ovvero tutti i numeri di telefono del sistema di reti devono essere univoci. Pertanto, i numeri di telefono preconfigurati devono essere eliminati e devono essere utilizzati i numeri adattati per il sistema di reti.

  2) Importazione dei dati degli utenti tramite file XML

  I numeri di telefono modificati secondo il sistema di reti ed eventuali altri dati dell'utente possono essere facilmente importati tramite un file XML durante la configurazione di base. Questo file può contenere tutti gli utenti del sistema di reti. Durante l'impostazione vengono trasferiti solo i numeri e i dati degli utenti assegnati all'ID nodo del sistema di comunicazione specificato in precedenza.

Attività correlate

Come visualizzare i dati di massa alla pagina 162
Come resettare le voci LCR alla pagina 1410

Riferimenti correlati

LCR > Flag LCR alla pagina 1603

6.7.3.1 Come visualizzare i dati utente

Prerequisiti

Si è nella finestra **Funzioni centrali per gli utenti** della procedura guidata **Installazione di base**.

Passo a passo

1) Attivare il pulsante di opzione **Mostra configurazione utenti**.
2) Fare clic su **Esegui funzione**. Viene visualizzato un elenco degli utenti con numeri preconfigurati (piano di composizione predefinito).
3) Fare clic su **OK**. Si torna alla finestra **Funzioni centrali per gli utenti**.
4) Se non si desidera modificare dati degli utenti, fare clic su **OK & Avanti**.

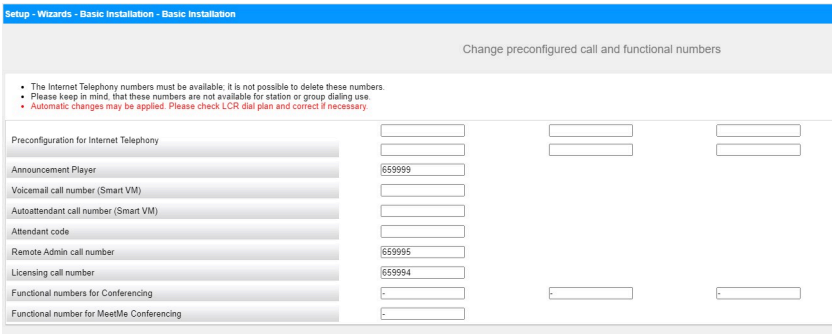
6.7.3.2 Come eliminare tutti i numeri di telefono

Prerequisiti

Si è nella finestra **Funzioni centrali per gli utenti** della procedura guidata **Installazione di base**.

Passo a passo

1) Selezionare **Cancella tutti numeri di telefono**.
2) Selezionare la casella di controllo **Cancella tutti numeri di telefono**.
3) Fare clic su **Esegui funzione**. Tutti i numeri preconfigurati vengono cancellati, tranne **Announcement Player, Numero di telefono Remote-Admin** e **Numero di telefono per concessione licenza**. Appare quindi la finestra **Modifica numeri di telefono e funzionali pre-configurati**.



4) Modificare i codici e i numeri speciali in base alle proprie esigenze, quindi fare clic su **OK**. Si torna alla finestra **Funzioni centrali per gli utenti**.
5) Se non si desidera configurare altri dati utente, fare clic su **OK & Avanti**.

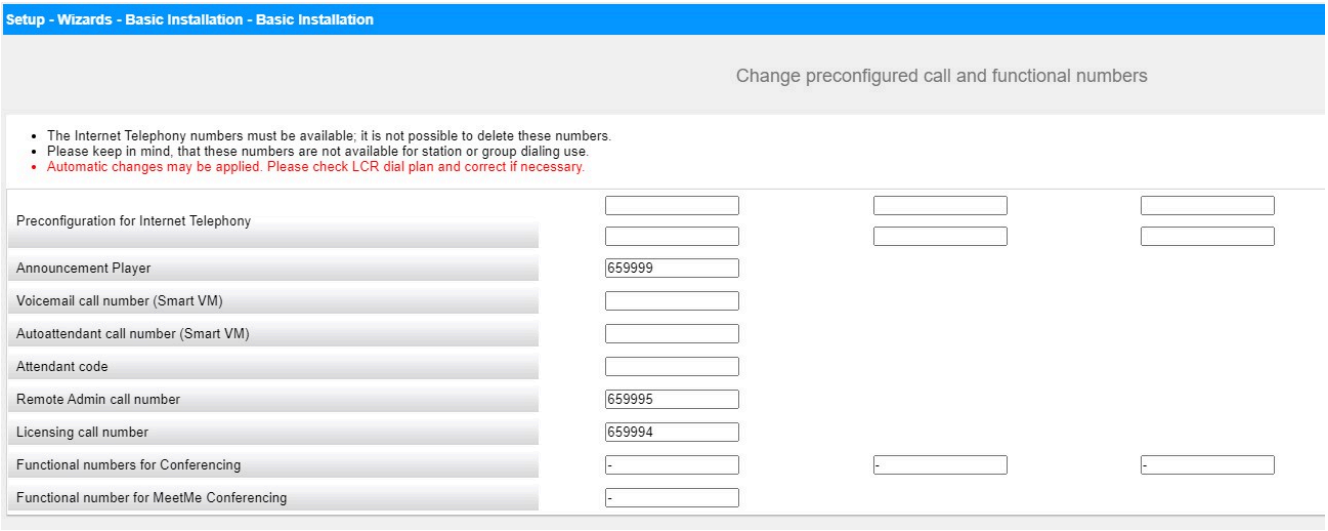
6.7.3.3 Modificare i numeri di telefono preconfigurati in base al piano di composizione specifico

Prerequisiti

Si è nella finestra **Funzioni centrali per gli utenti** della procedura guidata **Installazione di base**.

Passo a passo

1) Attivare **Modifica numeri di telefono e funzionali pre-configurati**.
2) Fare clic su **Esegui funzione**. Viene visualizzata la finestra **Modifica numeri di telefono e funzionali pre-configurati**.



3) Modificare i numeri preconfigurati in base alle proprie esigenze, quindi fare clic su **OK**. Si torna alla finestra **Funzioni centrali per gli utenti**.
4) Se non si desidera configurare altri dati utente, fare clic su **OK & Avanti**.

6.7.3.4 Come importare i dati degli utenti tramite un file XML

Prerequisiti

Si è nella finestra **Funzioni centrali per gli utenti** della procedura guidata **Installazione di base**.

Esiste un file XML in formato UTF-8 con i dati inseriti. Un modello XML è disponibile in **Centro assistenza** > **Documenti** > **Modelli CSV**.

Passo a passo

1) Attivare il pulsante di opzione **Configurazione utente importando file CSV/ XML**.
2) Fare clic su **Esegui funzione**.
3) Selezionare con **Sfoglia** il file XML creato e fare clic su **Apri**.
4) Fare quindi clic su **OK**. I dati utente vengono importati.
5) Fare clic su **OK & Avanti**.

6.7.4 Accesso a Internet

6.7.4.1 Come configurare l'accesso a Internet tramite un router Internet esterno sulla LAN con porta WAN dedicata all'ITSP

Prerequisiti

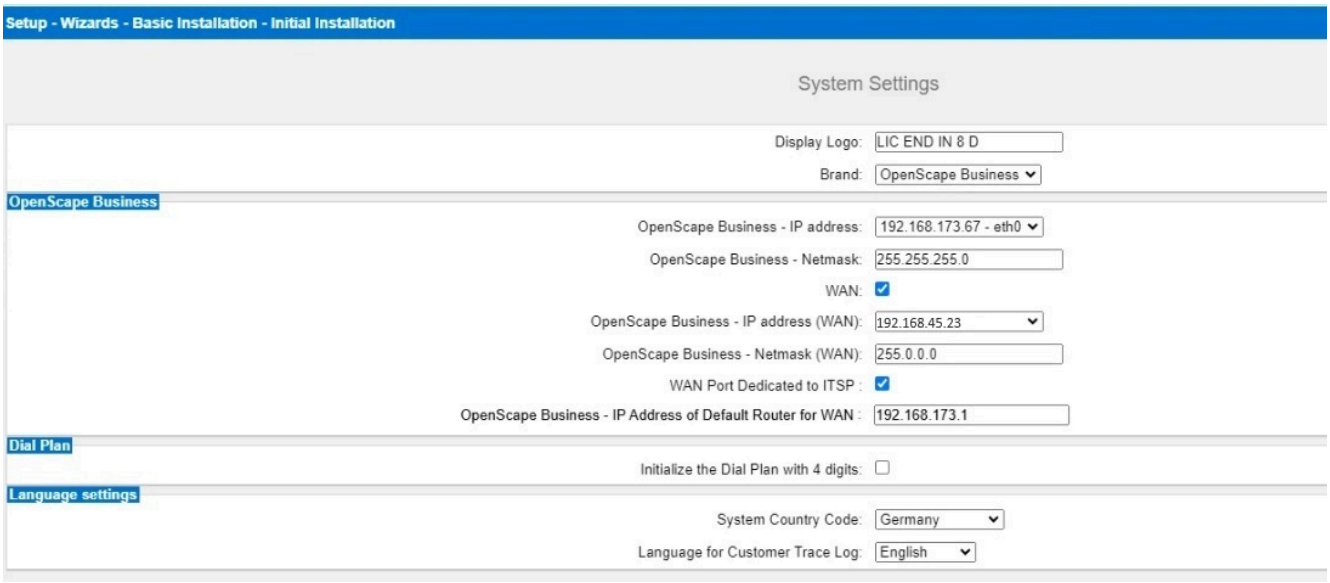
È stata creata una nuova interfaccia di rete in SLES.

Si è nella finestra **Impostazioni di sistema** della procedura guidata **Installazione iniziale**.

Tenere presente che questa funzione è valida solo per gli ITSP che non richiedono l'uso di STUN nelle impostazioni del provider.

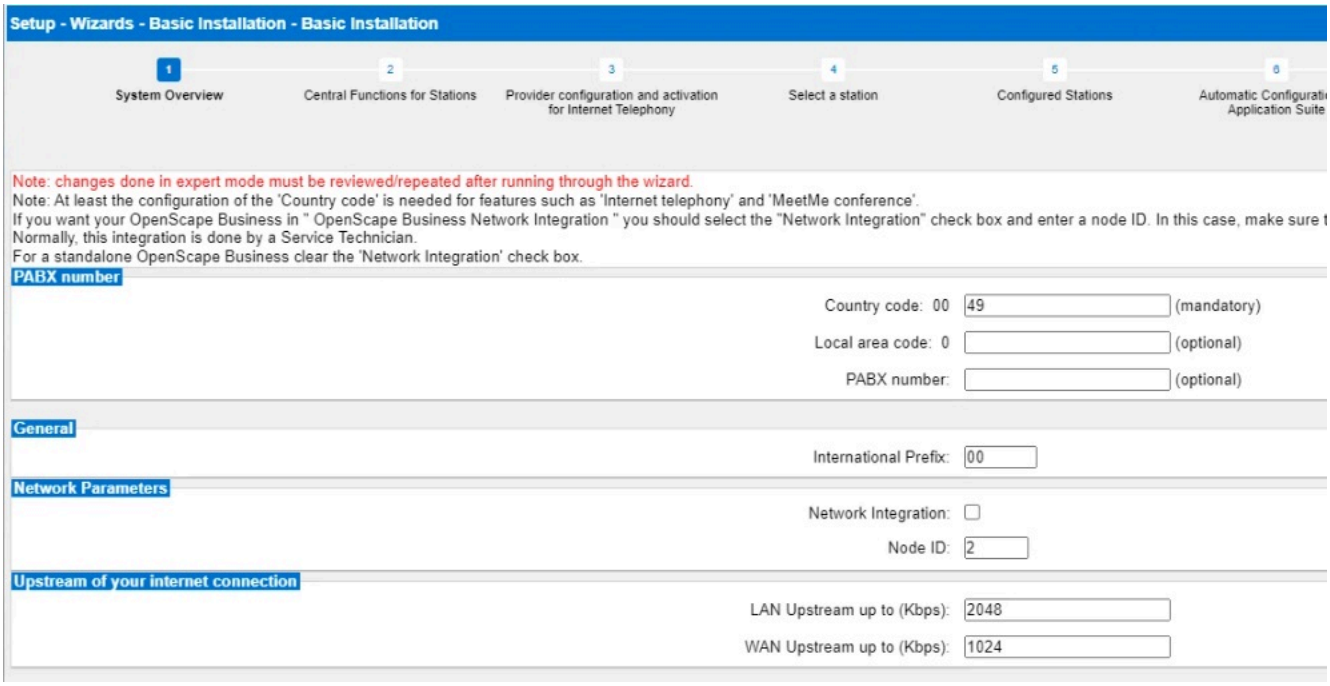
Passo a passo

1) Attivare la casella di controllo **WAN** e selezionare l'interfaccia di rete appropriata.
   L'opzione **Interfaccia WAN dedicata all'ITSP** diventerà disponibile.
2) Fare clic per abilitare la casella di controllo **Interfaccia WAN dedicata all'ITSP**.



3) Fare clic su **OK & Avanti**.
4) Spostarsi su **Configurazione > Installazione di base** e lanciare la procedura guidata **Installazione di base**.

5) Configurare i valori massimi di upstream nei campi **LAN upstream fino a (Kbps)** e **WAN upstream fino a (Kbps)** corrispondenti.



6) Fare clic su **OK & Avanti**.

7) Dopo aver applicato la configurazione, è necessario riavviare il sistema.

6.7.5 Telefonia Internet

La finestra **Configurazione e attivazione provider per la telefonia Internet** consente di configurare la telefonia Internet. È possibile usare ITSP (Internet Telephony Service Provider) preconfigurati o configurarne di nuovi. Per ogni ITSP è possibile configurare uno o più account. È possibile attivare contemporaneamente fino a 8 ITSP.

Sono disponibili le seguenti opzioni:

- **Configurazione dell'ITSP predefinito**

  È possibile utilizzare modelli predefiniti di ITSP. A tal fine, nel modello vengono inseriti i propri dati e i numeri di telefono e questo viene successivamente attivato.
- **Configurazione di un nuovo ITSP**

  È possibile aggiungere e attivare nuovi ITSP.

  La configurazione di un nuovo ITSP è molto rara e richiede molto tempo. Pertanto, nella sezione dedicata alla prima installazione non viene descritta questa opzione. Per informazioni più dettagliate, consultare il capitolo Configurazione di un ITSP.
- **Disattivare la telefonia Internet**

  È possibile disattivare la telefonia Internet.

Nota:

Gli esempi di configurazione sono disponibili su Internet alla pagina **Unify Experts Wiki** in *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"* (disponibile solo in inglese e tedesco).

Assegnazione dei numeri di telefono ITSP

- Con una **connessione analogica di telefonia Internet** l'ITSP mette a disposizione singoli numeri di telefono, ad esempio 70005555, 70005556, ... Questi numeri vengono poi assegnati manualmente ai numeri interni degli utenti.
- Con una **connessione punto-punto di telefonia Internet** l'ITSP mette a disposizione una fascia di numeri (intervallo di numeri), ad esempio da (+39) 02 7007-100 a (+39) 02 7007-147. I numeri di telefono di questa fascia vengono successivamente assegnati manualmente ai numeri interni degli utenti.

I due tipi di connessione possono essere combinati.

In alternativa, per entrambi i tipi di collegamenti, i numeri di telefono dell'ITSP possono essere inseriti nella configurazione degli utenti come selezione passante dell'utente.

Numero di telefono interno	Servizio	DID
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

In questo modo, i numeri di telefono degli ITSP sono costituiti dal numero di sistema configurato (ad esempio il codice paese 49) e dal numero di selezione passante inserito in formato esteso. Ciò rappresenta un vantaggio nell'analisi del numero da comporre e nella gestione delle chiamate, anche in una rete. Quindi la connessione dell'ITSP è ad esempio estensibile anche a un altro nodo.

Eventuali ulteriori attacchi linea urbana via ISDN sono possibili solo con limitazioni (utile ad esempio per le chiamate di emergenza).

6.7.5.1 Come configurare un ITSP predefinito

Prerequisiti

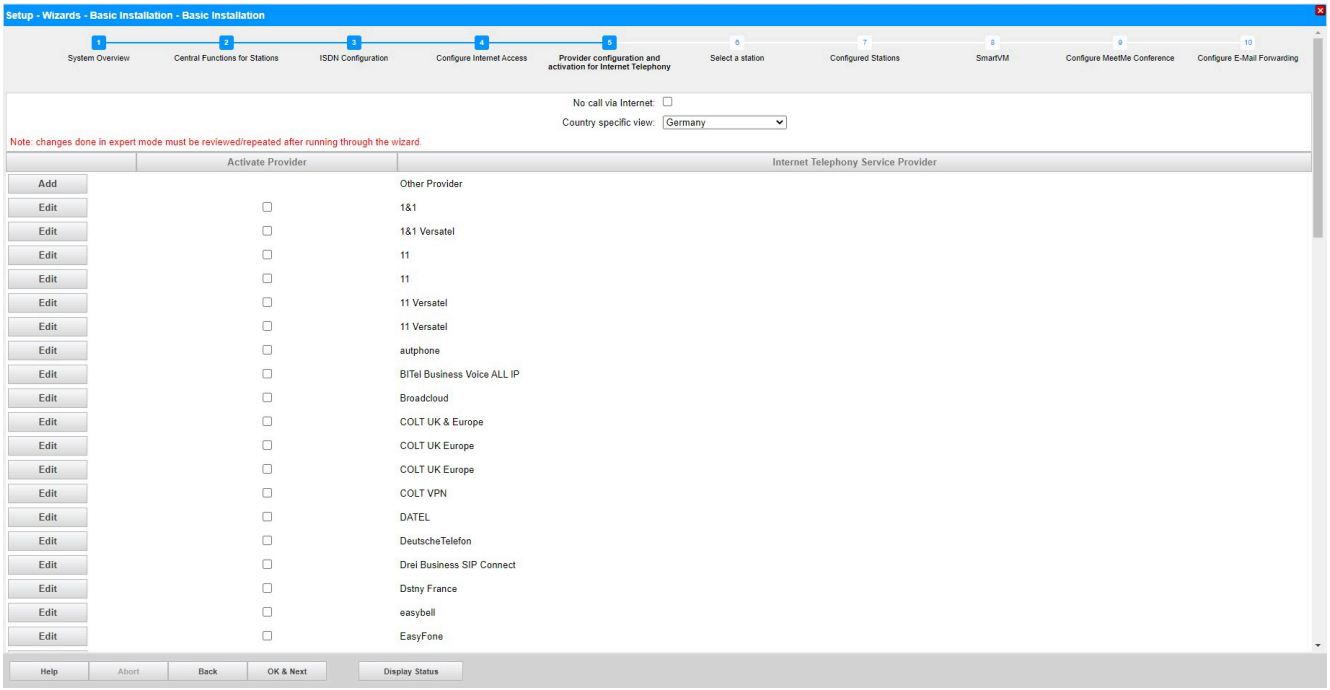
Si è nella finestra **Configurazione del provider e attivazione della telefonia Internet** della procedura guidata **Installazione di base**.

La connessione a Internet deve essere operativa.

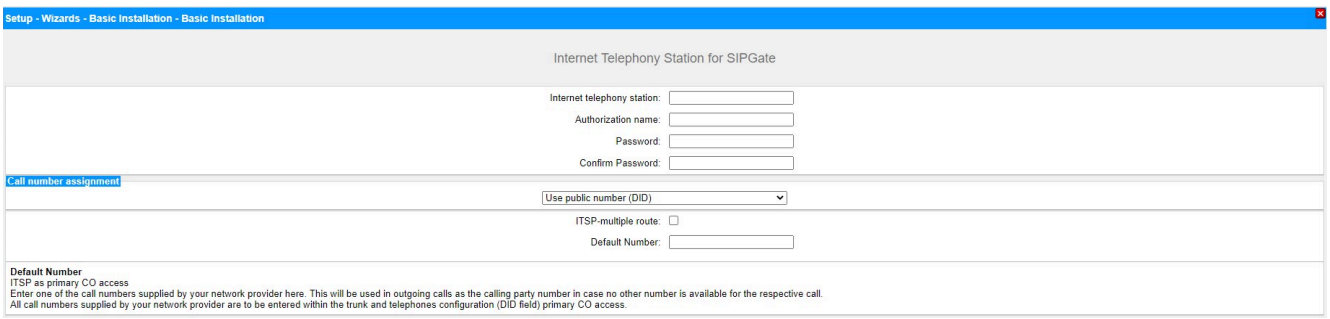
I dati di accesso per la telefonia Internet del proprio ITSP sono disponibili (ad es. ID utente, password, numeri per telefonia Internet).

Passo a passo

1) Deselezionare la casella di controllo **No telefonia tramite Internet**. Viene visualizzata una lista degli ITSP possibili, in base al Paese. L'elenco contiene gli ITSP predefiniti per il paese selezionato ed eventuali ITSP già creati.



2) Se si desidera modificare il Paese preimpostato, dall'elenco a discesa **Panoramica specifica del paese** selezionare il Paese desiderato. Verranno visualizzati gli ITSP disponibili per il Paese scelto.
3) Se necessario, fare clic su **Mostra stato**, per visualizzare quali sono gli ITSP già attivi e quali utenti di telefonia Internet sono configurati per i singoli ITSP. Si possono attivare fino a 8 ITSP. Fare quindi clic su **OK**.
4) Per configurare le stazioni di telefonia Internet, fare clic su **Modifica** nella riga associata all'ITSP corrispondente.
5) Selezionare la casella di controllo **Attiva provider**.
6) Fare clic su **OK & Avanti**.
7) Fare clic su **Aggiungi** per configurare il proprio account ITSP con i relativi numeri di telefonica Internet. I campi visualizzati dipendono dal provider.



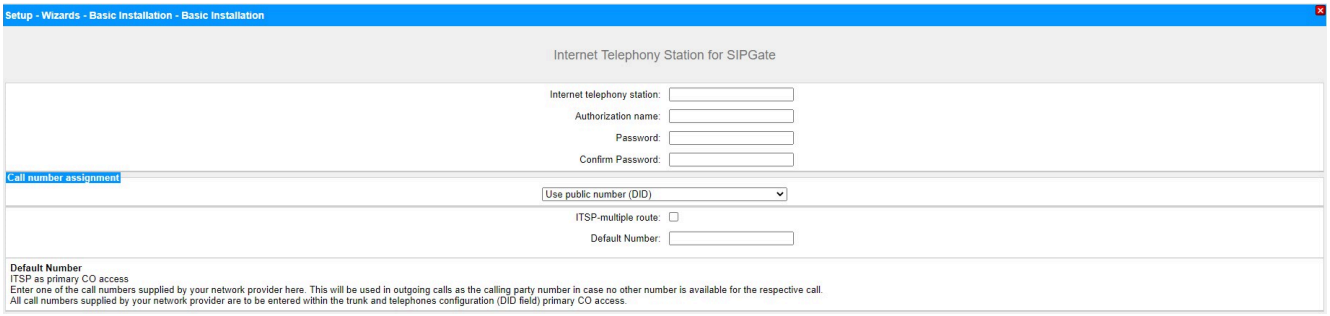
8) Nel campo **Utente di telefonia Internet** immettere i dati di accesso del proprio account. I dati sono stati forniti dall'ITSP. In base all'ITSP, possono venire utilizzati termini diversi, ad esempio: Utente SIP, ID SIP, ecc.

9) Nel campo **Nome autorizzazione** immettere il valore corrispondente. I dati sono stati forniti dall'ITSP. Se non si è ricevuto alcun nome autorizzazione, inserire gli stessi dati già indicati in **Utente di telefonia Internet**.

10) Nei campi **Nuova password** e **Ripeti password** immettere la password ricevuta dall'ITSP. In base all'ITSP, possono venire utilizzati termini diversi, ad esempio: Password, Password SIP, ecc.

11) Assegnazione dei numeri di telefonia Internet - Opzione 1:

Usa numero pubblico (DID): i numeri di telefonia via Internet della propria connessione utente o punto-punto di telefonia Internet non devono essere inseriti qui durante la configurazione dell'ITSP, ma durante la configurazione degli abbonati (nei campi **DID**).



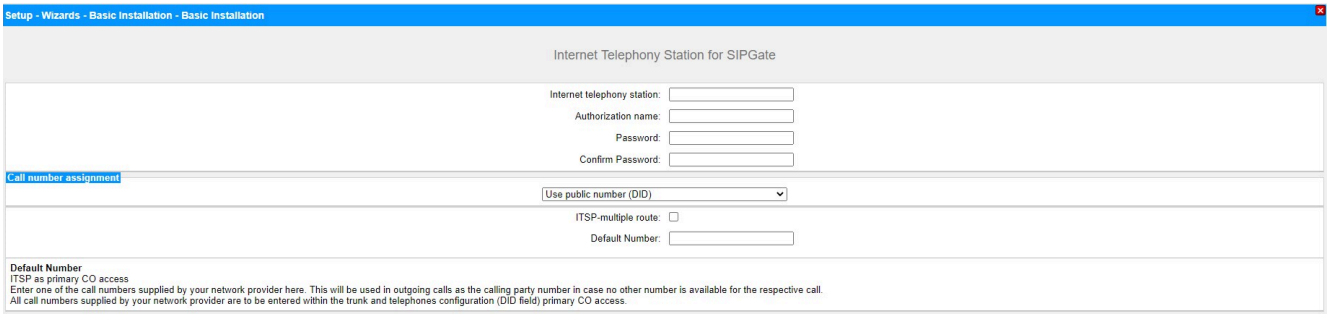
a) Nell'area **Assegnazione numero di telefono**, selezionare il pulsante di opzione **Usa numero pubblico (DID)**.

b) In **Numero predefinito**, inserire il numero di telefono da utilizzare per le chiamate in uscita quando non è disponibile un numero DID del chiamante.

c) Se il proprio ITSP supporta la funzione "Mobile Extension (MEX)", in **Numero MEX** inserire il numero MEX messo a disposizione dall'ITSP (8 cifre, solo numeri).

12) Assegnazione dei numeri di telefonia Internet - Opzione 2:

Usa numero interno (N° tel.) / singole voci: si dispone di una connessione stazione di telefonia Internet e si è ricevuto un numero di telefono singolo per la telefonia Internet (ad esempio, 70005555, 70005556,...). Questi numeri singoli vengono successivamente assegnati ai singoli numeri interni dell'utente.



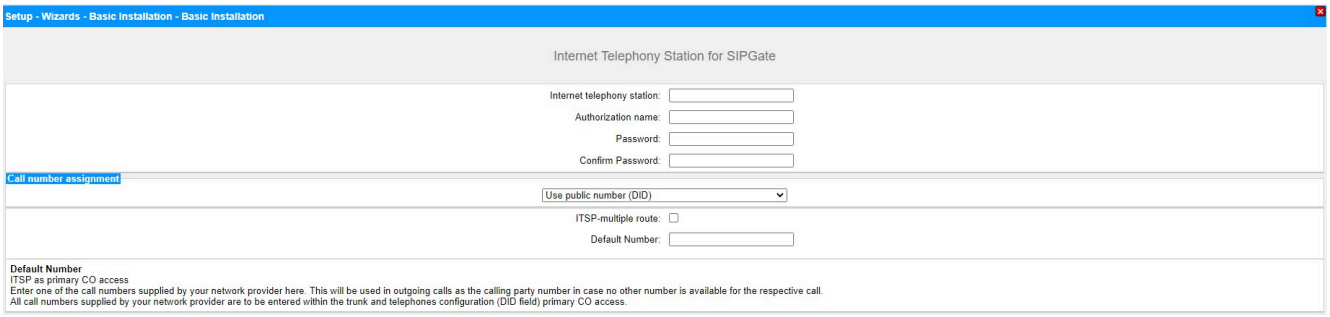
a) Nell'area **Assegnazione numero di telefono**, selezionare il pulsante di opzione **Usa numero interno (N° tel.) / singole registrazioni**.

b) Nell'area **Numeri telefonia Internet**, nel campo accanto al pulsante **Aggiungi** inserire uno dei numeri per telefonia Internet ricevuto dall'ITSP e fare clic su **Aggiungi**.

c) Se si desidera assegnare all'account altri numeri di telefonia Internet, ripetere il passo b).

13) Assegnazione dei numeri di telefonia Internet - Opzione 3:

Usa numero interno (N° tel.) / registrazione area: Si dispone di una connessione punto-punto di telefonia Internet e si è ricevuto un intervallo di numeri di telefono per la telefonia Internet, ad esempio da (+39) 02 7007-100 a (+39) 02 7007-147. I numeri di chiamata provenienti dall'intervallo di numeri di telefono vengono assegnati come numeri di chiamata interni degli utenti.



a) Nell'area **Assegnazione numero di telefono**, selezionare il pulsante di opzione **Usa numero interno (N° tel.) / registrazione area**.

b) In **Numero del sistema (prefisso)**, immettere il numero del sistema.

c) Nei campi **Fascia numeri interni diretti da** e **a**, immettere l'intervallo di numeri interni desiderato per l'utente di telefonia Internet. Di norma da 100 a 147.

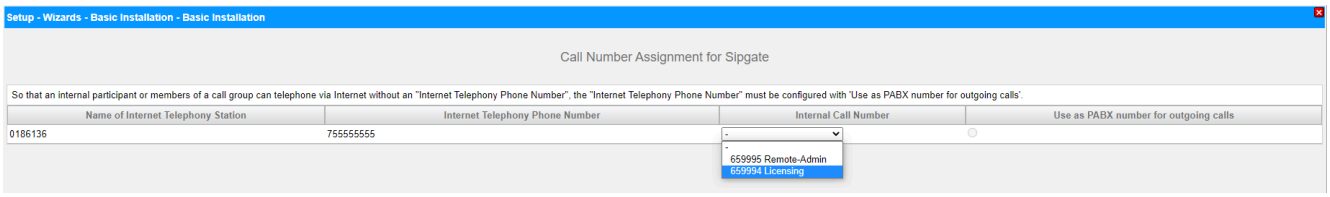
14) Fare clic su **OK & Avanti**.

15) Se si desidera configurare altri account con i numeri di telefonia Internet corrispondenti, ripetere i passaggi da 7 a 14.

16) Fare clic su **OK & Avanti**. Viene visualizzata una panoramica che riporta i numeri di telefono di telefonia Internet e gli account a cui sono assegnati.

17) Assegnare sempre tutti i numeri per telefonia Internet a un numero interno di un utente.

Questo passaggio non si applica se è stata selezionata l'opzione 1 per l'assegnazione dei numeri di telefono di telefonia Internet. In questo caso, l'assegnazione si effettua con la configurazione dell'utente nel campo **DID**.



a) Nella riga corrispondente dell'elenco a tendina **Numero interno** selezionare un numero di telefono interno.

b) Se un utente non dotato di numero di telefono per la telefonia Internet o membri di un gruppo di chiamata deve eseguire telefonate tramite Internet, è necessario selezionare il pulsante di opzione **Voce predefinita**. Il pulsante di opzione può essere selezionato solo per un singolo numero di telefonia Internet.

18) Fare clic su **OK & Avanti**. Qui viene visualizzato di nuovo l'elenco degli ITSP predefiniti e aggiunti di recente. Gli ITSP attivati sono contrassegnati con un segno di spunta nella colonna **Attiva provider**. Con **Riavvia ITSP** è possibile registrarsi nuovamente presso l'ITSP attivo in caso di problemi di connessione.

19) Fare clic su **OK & Avanti**.

20) Nel campo **Larghezza di banda della connessione (Kbit/s)** immettere il valore della velocità in upload della propria connessione Internet. Da non confondere con la velocità di download!

Nota: Nel campo **Numero conversazioni Internet simultanee** viene visualizzato il numero di conversazioni telefoniche Internet conducibili contemporaneamente. Se la qualità della conversazione peggiora a causa del sovraccarico della rete, è necessario ridurre il numero indicato.

Per ulteriori informazioni sul numero di chiamate Internet simultanee, fare riferimento a Limitazione del numero di chiamate simultanee tramite ITSP alla pagina 820.

---

21) Fare clic su **OK & Avanti**.

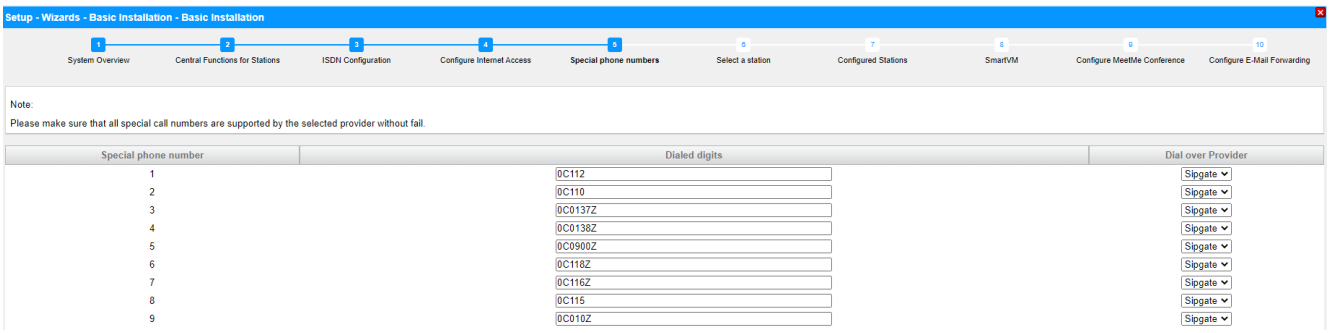
22) Nel caso durante la configurazione dell'accesso a Internet non sia stata ancora configurata la connessione permanente, è possibile farlo ora. Senza connessione permanente non è possibile ricevere alcuna chiamata tramite Internet. Se la connessione permanente è già configurata, non vengono visualizzati i campi descritti da a) a c).

a) In **Connessione permanente**, selezionare il pulsante di opzione **On**.

b) Nel campo **Interruzione alle (hh:mm)**, immettere l'orario in cui interrompere la connessione a Internet (ad es. 04:59).

c) Fare clic su **OK & Avanti**.

23) Nella colonna **Cifre selezionate** indicare i numeri di telefono speciali desiderati.



Sono valide le seguenti voci relative ai numeri di telefono:

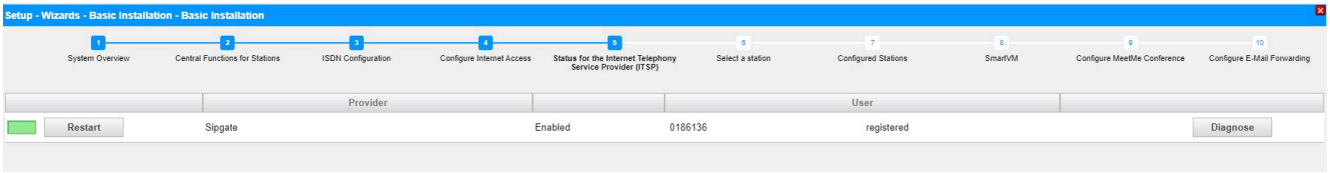
- 0 - 9: cifre consentite
- -: Separatore di campi
- X: Cifra a piacere fra 0 e 9
- N: Cifra a piacere fra 2 e 9
- Z: seguono una o più cifre fino alla fine della selezione
- C: Tono di selezione simulato (può essere specificato fino a tre volte)

24) Nella colonna **Chiama tramite provider**, selezionare se i numeri di telefono speciali devono essere selezionati via ISDN o tramite un ITSP. Vengono visualizzati solo gli ITSP attivi.

Nota: Assicurarsi che i numeri di emergenza possano sempre essere selezionati. Se i numeri di emergenza

devono essere selezionati tramite un Internet Telephony Service Provider, l'ITSP deve supportare questo servizio.

25) Fare clic su **OK & Avanti**. Viene visualizzato lo stato degli ITSP.



In verde sono indicati gli ITSP configurati presso i quali si è già registrati.

In arancione sono indicati gli ITSP configurati presso i quali non si è ancora registrati.

26) Fare clic su **Avanti**, quindi su **Fine**.

6.7.5.2 Come disattivare la telefonia Internet

Prerequisiti

Si è nella finestra **Configurazione e attivazione del provider di telefonia Internet** della procedura guidata **Installazione di base**.

Passo a passo

1) Lasciare selezionata la casella di controllo **No telefonia tramite Internet**.
2) Fare clic due volte su **OK & Avanti**.

6.7.6 Utenti

Nelle finestre **Seleziona utente / gruppo** configurare gli utenti collegati al sistema di comunicazione.

Procedere come segue:

1) Configurazione di utenti IP e SIP

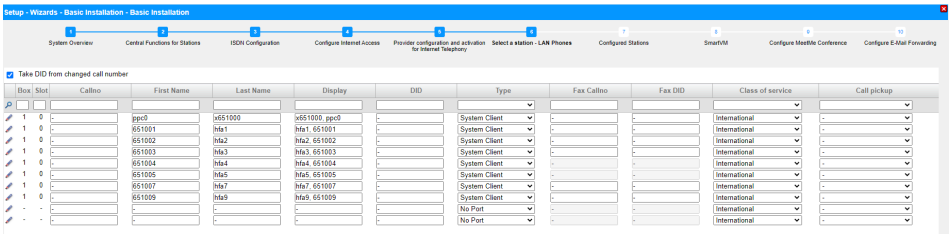
   Gli utenti IP e gli utenti SIP sono ad esempio telefoni LAN o telefoni WLAN.

6.7.6.1 Come configurare utenti IP e SIP

Prerequisiti

Si è nella finestra **Seleziona utente - Telefoni LAN** della procedura guidata **Installazione di base**.

Per il funzionamento dei telefoni WLAN è necessaria una rete LAN wireless operativa.



Passo a passo

1) Se si desidera che il numero di selezione passante dell'utente sia diverso dal numero di telefono, nella riga dell'utente desiderato, in corrispondenza di **DID**, immettere un numero di selezione passante per l'utente:

- solo con connessioni punto - punto:

  Fare clic sul campo desiderato e immettere tramite tastiera il numero di selezione passante. Questo numero può coincidere con il numero interno.
- solo con connessioni punto - multipunto:

  Nell'elenco a discesa selezionare un MSN. L'utente può ad es. essere raggiunto da chiamate interne sul numero interno 101 e dall'esterno tramite l'MSN 654321.
- connessione punto - punto e connessione punto - multipunto:

  Nel campo desiderato selezionare una voce dall'elenco a discesa **xxx - modificabile** (xxx indica il numero interno) e immettere tramite tastiera il numero di selezione passante o selezionare un MSN dall'elenco a discesa.

2) Nella riga appropriata dell'utente desiderato, immettere in **N° tel** un numero dell'utente interno. Si può utilizzare il numero di telefono pre-assegnato o immetterne uno diverso, ancora libero.

3) Nella riga dell'utente desiderato immettere in **Nome** un nome nel formato `Cognome, nome`.

Nota: Il nome può contenere fino a 16 caratteri, ma non sono consentiti umlaut o caratteri speciali. Il nome è quello qui indicato nei client UC come cognome, ma può essere modificato.

---

4) Nella riga dell'utente desiderato, selezionare dall'elenco a discesa **Tipo** il tipo di utente IP (ad es."Client di sistema" o "Client SIP").

5) Se per l'utente deve essere configurata una casella fax (utilizzabile ad esempio con i client UC **myPortal for Desktop** o **myPortal for Outlook**, procedere come segue:

a) Nella riga dell'utente desiderato, nel campo **Fax N° tel**, inserire il numero di fax interno desiderato, mediante il quale l'utente potrà ricevere messaggi fax interni.

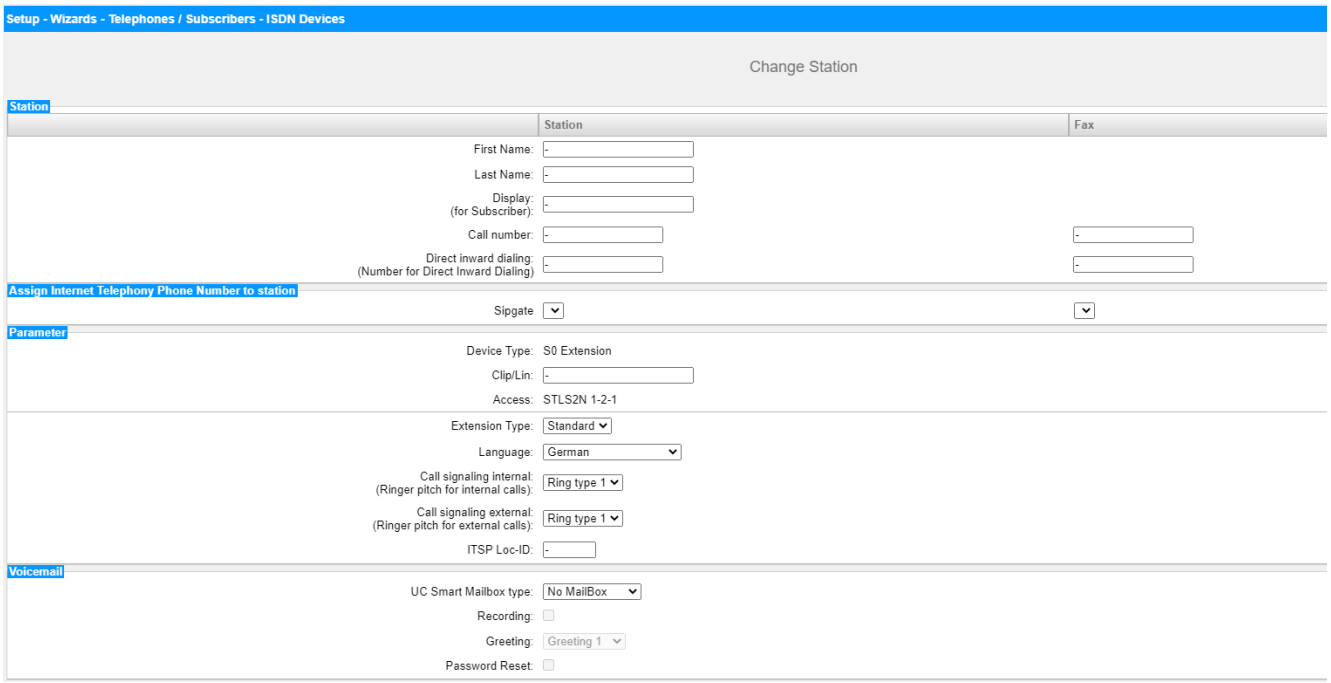
b) Se per la casella fax viene configurato un numero DID, nella riga dell'utente desiderato inserire nel campo **Selezione passante fax** il numero di fax esterno a cui l'utente può ricevere fax dall'esterno.

6) Nella riga dell'utente selezionato, dall'elenco a discesa **Abilitazione**, selezionare il gruppo di abilitazione desiderato.

7) Per aggiungere l'utente a un gruppo di risposta, selezionare dall'elenco a discesa **Gruppo di risposta alle chiamate** nella riga dell'utente desiderato.

8) Eseguire le impostazioni descritte di seguito solo in caso di necessità o per un telefono SIP:

a) Nella riga del terminale desiderato, fare clic sull'icona a forma di matita **Modifica**.



b) Per telefoni SIP: Se il telefono SIP deve essere utilizzato insieme a un telefono cellulare dual-mode, inserire nell'area **Mobility** in **Num. cellulare** il codice linea esterna e di seguito il numero di telefono del cellulare (es. `0016012345678`). Inoltre, nell'elenco a discesa **Web Feature ID**, selezionare questo client SIP. (Vedere Telefonia dual mode).

c) Nel campo **Clip/Lin** immettere un numero di telefono (selezione passante o MSN), che deve essere visualizzato sul display dell'utente chiamato al posto del proprio numero quando si effettua una chiamata esterna.

Nota: Questo servizio deve essere autorizzato dal gestore di rete.

Nota: Configurare almeno un numero DID. In caso contrario, il sistema non tiene conto del numero CLIP del chiamante e il numero interno della chiamata viene formattato e inviato come numero di chiamata per la chiamata esterna.

---

d) Nell'elenco a discesa **Lingua** selezionare la lingua da utilizzare per i comandi dei menu del telefono.

e) Dall'elenco a discesa **Segnalazione della chiamata interna** assegnare all'utente uno degli otto possibili toni di segnalazione chiamate interne.

In questo modo l'utente invia agli altri utenti interni un tono di chiamata diverso in base al quale può essere differenziato (standard: Suoneria 1).

f) Nell'elenco a discesa **Segnalazione della chiamata esterna**, selezionare e assegnare uno dei tre possibili toni di segnalazione chiamate esterne (standard: Suoneria 1).

g) Consentiti solo per telefoni SIP: inserire la password di autenticazione nei campi **Password** e **Conferma password**.

h) Consentiti solo per telefoni SIP: nel campo **SIP ID d'utente/Nome d'utente** immettere l'identificativo utente per l'autenticazione.

i) Consentiti solo per telefoni SIP: nel campo **Realm** immettere la zona corrispondente per l'autenticazione.

j) Fare clic su **OK & Avanti**.

k) Modificare i flag utente in base alle necessità. Per una descrizione dei flag utente, vedere Utenti > Utenti > Parametri utente.

l) Fare clic su **OK & Avanti**.

9) Se si desidera configurare altri utenti IP, fare clic su **Salva i dati**, quindi ripetere i passi da 1 a 8.

10) Fare clic su **OK & Avanti**. Viene visualizzato l'elenco di tutti gli utenti configurati. Tale elenco corrisponde a un piano di composizione.

11) Se necessario, fare clic su **Stampa**, per stampare le informazioni sull'utente configurato.

12) Fare clic su **OK & Avanti**.

Concetti correlati

Testo in più lingue alla pagina 1230

6.7.7 Configurazione della UC Suite

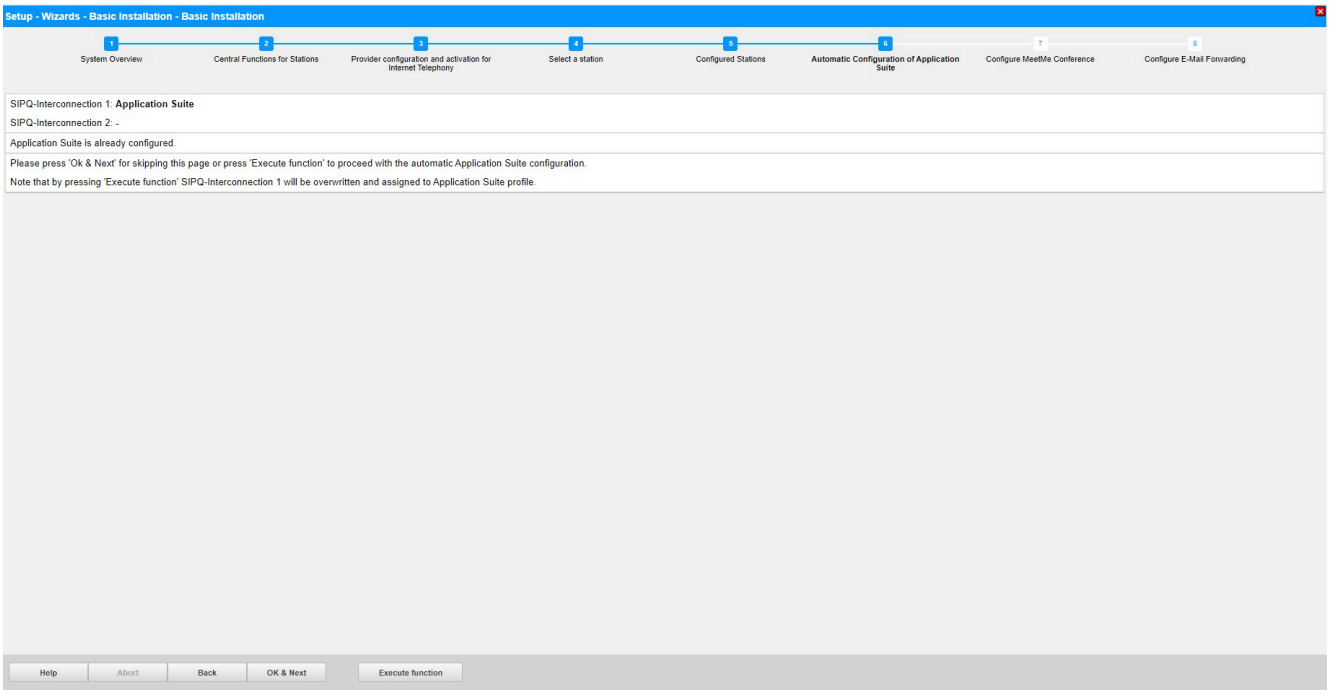
Nella finestra **Configurazione automatica della suite applicazioni** è possibile eseguire la configurazione automatica della soluzione UC (Suite UC).

Nota: Questa finestra viene visualizzata solo se nella procedura guidata è stato selezionato **Configurazione di base** nella selezione dell'applicazione **Pacchetto con UC Suite**.

6.7.7.1 Come configurare la UC Suite

Prerequisiti

Si è nella finestra **Configurazione automatica della suite di applicazioni**.



Passo a passo

Fare clic su **Esegui funzione**. La UC Suite viene configurata automaticamente. Una volta che la barra di avanzamento indica 100%, fare clic su **OK & Avanti**.

Nota:

Per OpenScape Business s, la procedura guidata genera automaticamente 60 canali multimediali in UC Suite. In parallelo è possibile utilizzare 16 canali per gli annunci senza configurare canali multimediali aggiuntivi.

6.7.8 Configurazione delle caselle vocali UC Smart

Nella finestra **Configurazione automatica di Smart VM** è possibile eseguire la configurazione automatica delle caselle vocali UC Smart (Smart VM, Smart VoiceMail), se viene utilizzata la soluzione UC Smart.

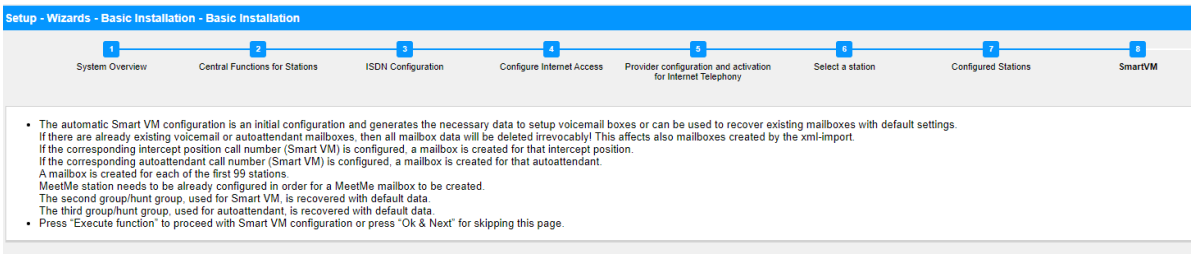
Nota:

Questa finestra viene visualizzata solo se nella procedura guidata **Configurazione di base nella selezione dell'applicazione** è stato selezionato **Pacchetto con UC Smart**.

6.7.8.1 Come configurare le caselle vocali UC Smart

Prerequisiti

Si è nella finestra **Configurazione automatica di Smart VM**.



Passo a passo

1) Se non devono essere usate le caselle vocali UC Smart, fare clic su **OK & Avanti**. La configurazione delle caselle vocali viene ignorata.
2) Se devono essere usate le caselle vocali UC Smart, fare clic su **Esegui funzione**. Per i primi 100 utenti vengono automaticamente configurate le caselle vocali. Una volta che la barra di avanzamento indica 100%, fare clic su **OK & Avanti**.

Nota: Le caselle vocali UC Smart o UC Smart AutoAttendant già presenti vengono definitivamente cancellate.

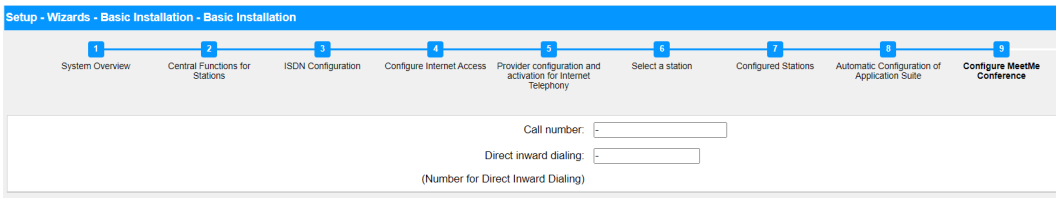
6.7.9 Impostazioni del server conferenze

Nella finestra **Configura conferenza MeetMe** è possibile immettere il numero di telefono e il numero di accesso per le conferenze.

6.7.9.1 Come modificare le impostazioni server conferenza

Prerequisiti

Si è nella finestra **Configura conferenza MeetMe** della procedura guidata **Installazione di base**.



Passo a passo

1) Nel campo **Numero di telefono** immettere un numero di telefono per la conferenza.
2) Nel campo **Selezione passante** immettere il numero di accesso alla conferenza (DID conferenza) con il quale gli utenti possono connettersi a una conferenza esistente.
3) Fare clic su **OK & Avanti**.

6.7.10 Invio per e-mail (opzionale)

Nella finestra **Modifica inoltro e-mail** è possibile definire i dettagli dell'inoltro di e-mail. In questo modo gli utenti vengono informati di nuovi messaggi vocali e fax e gli amministratori ricevono i messaggi di sistema.

Sono disponibili le seguenti opzioni:

- Configurazione dell'invio di e-mail

  È possibile definire un server di posta elettronica esterno tramite il quale è possibile inviare le e-mail con OpenScape Business. I messaggi vocali e fax o i messaggi di sistema interni vengono inoltrati tramite questo server di posta elettronica ad uno o più indirizzi e-mail diversamente configurabili.

Nota: La definizione di un server di posta è importante se gli utenti della UC Suite devono essere indirizzati ai file di installazione automaticamente tramite un link inviato per e-mail.

6.7.10.1 Come configurare l'invio di e-mail

Prerequisiti

Se il server e-mail esterno è stato configurato per utilizzare l'autenticazione di base, assicurarsi che esista un account e-mail con una password con un provider e-mail e di conoscere i dati di accesso per questo account.

Se il server e-mail esterno è stato configurato per utilizzare l'autenticazione moderna (autorizzazione basata su token Microsoft OAuth 2.0), come nel caso di Exchange Online, assicurarsi che:

- L'account e-mail del mittente deve essere autorizzato a utilizzare SMTP autenticato (per impostazione predefinita questa opzione è inattiva nel tenant di Microsoft 365). Una volta attivato il protocollo SMTP autenticato, l'inoltro e-mail OAUTH 2.0 funziona normalmente con tutte le schede madri OpenScape Business.
- Un'applicazione con le autorizzazioni necessarie è stata registrata in Microsoft Azure Active Directory (Azure AD) per consentire al sistema OpenScape Business di inviare e-mail.
- Si conosce l'ID applicazione (client) e l'ID directory (tenant) dell'applicazione registrata.

  Chiedere all'amministratore di Azure AD di fornire questi valori, se necessario.
- L'indirizzo e-mail che verrà visualizzato come mittente delle e-mail appartiene allo stesso Azure AD o al tenant dell'applicazione registrata.

Si è nella finestra **Configura inoltro e-mail** della procedura guidata **Installazione di base**.

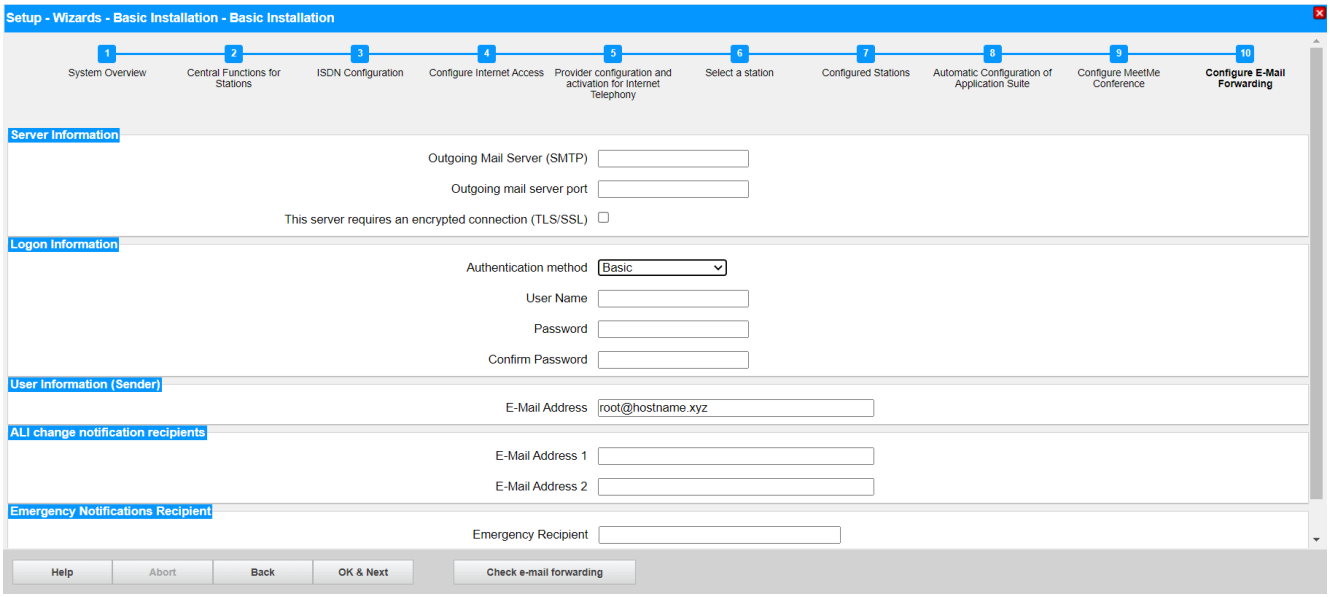


Figura 7: Opzioni di inoltro e-mail quando è selezionato il metodo di autenticazione di base

Passo a passo

1) Inserire il **Server della posta in uscita (SMTP)** per il server e-mail, da utilizzare per l'invio delle e-mail, ad esempio, `smtp.web.de`. Eventualmente richiedere il server della posta in uscita al proprio provider e-mail.

   Nota: Assicurarsi che il nome del server di posta in uscita possa essere risolto. In caso negativo, avviare la procedura guidata per l'invio di e-mail tramite **Centro assistenza** > **Inoltro e-mail** e immettere l'indirizzo IP del server della posta in uscita anziché il nome.

   ---

2) Inserire il **Server della posta in uscita** per la porta del server da utilizzare per l'invio delle e-mail. Eventualmente richiedere il server della posta in uscita al proprio provider e-mail.
3) Se è necessario stabilire una connessione sicura, selezionare la casella di controllo **Questo server richiede una connessione criptata (TLS/SSL)**. Chiedere al proprio provider e-mail se questa opzione deve essere selezionata.
4) Se il server e-mail esterno è stato configurato per utilizzare l'autenticazione di base, procedere come segue:
   a) Dall'elenco a discesa **Metodo di autenticazione**, selezionare **Base**.
   b) Immettere il **Nome utente** dell'account e-mail, ad esempio, `bruno.rossi`.
   c) In **Nuova password** e **Confermare password** immettere la password dell'account e-mail.

5) Se il server e-mail esterno è stato configurato per utilizzare l'autenticazione moderna, procedere come segue:

a) Dall'elenco a discesa **Metodo di autenticazione**, selezionare **Microsoft OAuth 2.0**.

b) Immettere l'ID applicazione (client) ottenuto dal portale Microsoft Azure nel campo **ID applicazione**.

c) Immettere l'ID directory (tenant) ottenuto dal portale di Microsoft Azure nel campo **Tenant**.

6) Inserire l'**Indirizzo e-mail** che comparirà come mittente delle e-mail, ad esempio: `bruno.rossi@web.it`.

7) Inserire l'**Indirizzo e-mail 1** per ricevere un'e-mail di notifica quando viene utilizzata la tolleranza ALI. È anche possibile inserire un secondo indirizzo e-mail nel campo **Indirizzo e-mail 2**.

8) Nel campo **Destinatario di emergenza**, inserire l'indirizzo e-mail di un responsabile della sicurezza in loco a cui viene inviata un'e-mail quando si seleziona un numero di emergenza.

L'oggetto dell'e-mail sarà "Nuova chiamata di emergenza". Il numero di telefono e il nome del chiamante, se configurati, sono inclusi nell'e-mail e recuperati dal database del sistema.

9) Se è stato selezionato **Microsoft OAuth 2.0** come metodo di autenticazione procedere come segue:

a) Fare clic su **OK & Avanti**.

b) Attendere che vengano visualizzati un collegamento di autorizzazione e un codice utente.

Il codice di autorizzazione scade dopo alcuni minuti.

c) Aprire il collegamento di autorizzazione e inserire il codice utente nel popup.

d) Accedere con l'indirizzo e-mail inserito al passaggio 6 alla pagina 255 (**Indirizzo e-mail**).

L'indirizzo e-mail deve trovarsi nello stesso Azure AD o tenant dell'applicazione registrata.

e) Dopo l'autenticazione riuscita, il popup visualizza un messaggio come di seguito:

```
Hai effettuato l'accesso a <nome-applicazione> sul
tuo dispositivo. Ora puoi chiudere questa finestra.
```

f) Chiudere il popup e tornare a WBM. Se l'autenticazione è andata a buon fine, sarà visualizzato il messaggio `L'autenticazione è andata a buon fine!`.

10) Per controllare le impostazioni e-mail configurate, procedere come segue:

a) Fare clic su **Controllo inoltro e-mail**.

b) Nel campo **Invia a un indirizzo e-mail** inserire l'indirizzo e-mail del servizio a cui si ha accesso. A questo indirizzo e-mail verrà inviata l'email di prova.

c) Nel campo **Oggetto dell'e-mail** inserire un testo descrittivo per identificare l'e-mail una volta ricevuta.

d) Fare clic su **Invia e-mail di prova**. Vengono testate le impostazioni e l'e-mail viene inviata alla casella e-mail indicata.

e) Verificare se il messaggio e-mail è presente nella propria casella.

f) Se l'invio dell'e-mail ha avuto esito positivo, fare clic su **Indietro** e passare alla fase seguente.

g) Se l'invio dell'e-mail non ha avuto esito positivo, fare clic su **Indietro** e verificare nuovamente le impostazioni e-mail.

11) Fare clic su **OK & Avanti**, quindi su **Fine**. L'installazione di base è conclusa. Attivare le licenze prima di eseguire il backup dei dati previsto dalla procedura guidata.

6.8 Attività finali

Una volta conclusa l'installazione iniziale e l'installazione di base eseguita con il WBM, è necessario eseguire ancora alcune importanti impostazioni per l'uso di OpenScape Business.

Procedere come segue:

1) Attivazione e assegnazione licenze

Le licenze acquistate con OpenScape Business devono essere attivate entro 30 giorni. L'intervallo di tempo inizia al primo accesso al WBM. Alla scadenza del periodo il sistema di comunicazione è utilizzabile solo in modo limitato. Dopo l'attivazione, le licenze devono essere assegnate agli utenti e alle linee. Le funzioni a livello di sistema sono già abilitate all'attivazione.

2) Preparazione di UC Smart Client per l'installazione (solo per UC Smart)

3) Preparare i client UC all'installazione

I client UC sono componenti della UC Suite. I file di installazione per i client UC sono accessibili tramite il WBM e possono essere messi a disposizione degli utenti IP in modo automatico o manuale.

Inoltre, per l'amministratore è disponibile l'opzione Installazione Silent. Si tratta di un metodo basato su riga di comando per l'installazione/disinstallazione e la modifica automatiche su client della UC Suite senza necessità di inserire altri comandi. Per ulteriori informazioni, vedere Installazione/disinstallazione Silent per client PC UC Suite.

4) Esecuzione del backup dei dati

Le modifiche apportate a OpenScape Business devono essere salvate. Il backup può essere salvato come set di backup ad esempio sulla rete interna.

6.8.1 Come attivare e assegnare le licenze

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Il LAC (codice di autorizzazione licenza) per il rilascio della licenza è noto e si dispone di un ID utente e di una password per l'accesso al server delle licenze.

Per la connessione al server delle licenze è necessario l'accesso a Internet.

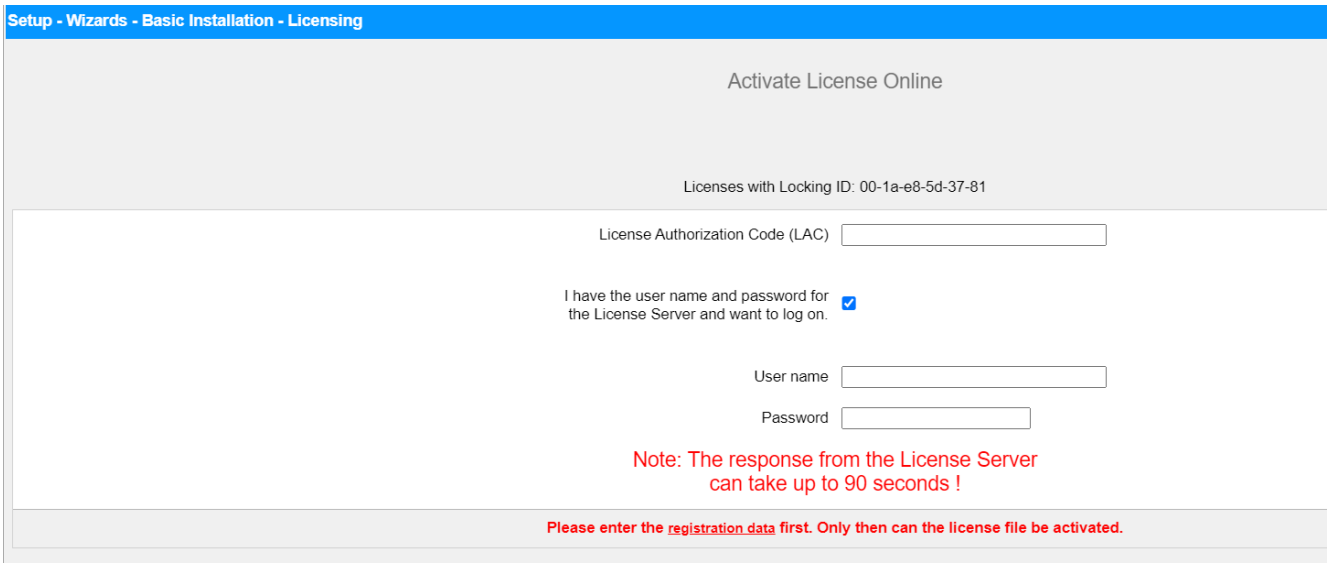
Passo a passo

1) Attivare le licenze online:

a) Nella barra di navigazione fare clic su **Configurazione**.

b) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.

c) Fare clic su **Modifica**, per avviare la procedura guidata **Concessione della licenza**.



d) Nel campo **Codice autorizzazione licenza (LAC)** immettere il LAC.

e) Selezionare la casella di controllo **Dispongo del nome utente e della password per il server delle licenze e desidero accedere**.

f) In **Nome utente** e **Password**, inserire i rispettivi dati per l'accesso al server delle licenze.

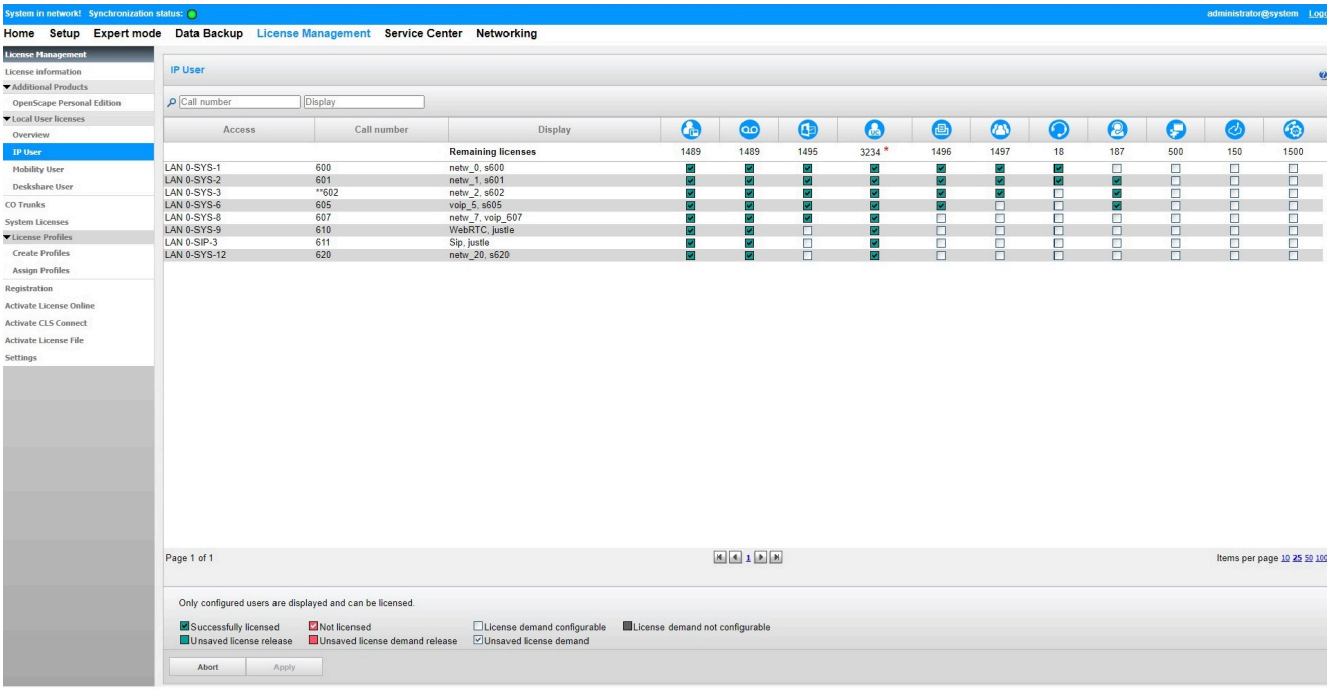
g) Fare clic su **OK & Avanti**. Viene stabilita la connessione al server delle licenze e le licenze vengono attivate.

2) Assegnazione delle licenze agli utenti:

a) Nella barra di navigazione fare clic su **Gestione delle licenze**.

b) Nella struttura di navigazione, selezionare **Licenze di utenti locali** > **...** fino al tipo di utente desiderato. Viene visualizzato un elenco di tutti gli utenti del tipo selezionato.

c) Nella riga dell'utente desiderato, selezionare la casella di controllo nella colonna **Licenza utente** (prima colonna con caselle di controllo).



d) Nella riga dell'utente desiderato, attivare le licenze orientate all'utente selezionando le caselle di controllo desiderate.

Nota: Le licenze orientate all'utente possono essere assegnate a un'apparecchio solo se è stata in precedenza assegnata una licenza all'apparecchio (licenza utente) (punto c).

---

e) Fare clic su **OK & Avanti**. Il sistema verifica che per la propria assegnazione siano disponibili licenze sufficienti.

Se le licenze disponibili sono sufficienti, la concessione delle licenze dell'utente è completata.

f) In caso di mancanza di licenze, viene segnalato l'errore con una casella di controllo rossa ombreggiata. Correggere l'errore e ripetere il passo e.

3) Assegnazione delle licenze alle linee:

a) Nella struttura di navigazione fare clic su **Linee urbane**. Nell'area **Linee urbane** viene visualizzato il numero di licenze acquistate per le linee.

b) Per linee SIP: nell'area **Richiesta licenze per numero di chiamante simultanee via Internet in questo nodo**, inserire il numero di chiamate Internet che possono essere eseguite contemporaneamente tramite un ITSP.

c) Fare clic su **OK & Avanti**.

6.8.2 Come preparare i client UC Smart all'installazione

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

L'hardware e il software per l'uso di UC @work sono disponibili.

Nota: Per l'utilizzo del client UC Smart myPortal @work sono necessarie le relative licenze.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione, fare clic su **Software**.
3) Fare clic sull'icona **myPortal @work** e salvare il file di installazione su un'unità di rete condivisa.
4) Inviare agli utenti di myPortal @work i due file di installazione.
5) In alternativa, è anche possibile inviare agli utenti di myPortal @work il collegamento per accedere direttamente al file di installazione:

   ```
   https://<Indirizzo IP del sistema di comunicazione>/
   management/downloads/myPortalAtWorkSetup.exe
   ```

6.8.3 Come preparare i client UC Suite all'installazione

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

L'hardware e il software per l'uso della UC Suite sono disponibili.

Nota: Per l'utilizzo dei client UC Suite sono necessarie le licenze.

Passo a passo

1) Al fine di rendere automaticamente disponibili a un utente i file di installazione, assicurarsi di avere eseguito le seguenti azioni:
   a) Gli indirizzi e-mail degli utenti devono essere stati importati assieme ai dati dell'utente tramite un file XML o inseriti selezionando il percorso **Configurazione** > **UC Suite** > **Rubrica utente**.
   b) È necessario che sia stato configurato un server di posta elettronica.

      Nota: Il server di posta può essere inserito anche successivamente in **Centro assistenza** > **Inoltro e-mail**.

   Tutti i client con indirizzi e-mail noti ricevono un'e-mail con il collegamento alla cartella di installazione di client UC nonché istruzioni per i primi passi. Nella cartella di installazione si trova inoltre un file Readme con informazioni sull'installazione del software su PC client.

2) Nel caso in cui non vengano eseguite le fasi necessarie per l'avviso automatico, è possibile mettere a disposizione manualmente i file di installazione. A tale riguardo, procedere nel modo seguente:
   a) Nella barra di navigazione fare clic su **Centro assistenza**.
   b) Nella struttura di navigazione, fare clic su **Software**.
   c) Fare clic sul client UC desiderato e salvare il file di installazione zippato su un'unità di rete condivisa.
   d) Nella struttura di navigazione, fare clic su **Documenti** e selezionare l'elenco a discesa **Istruzioni per l'uso**.
   e) Fare clic sulla documentazione per il client UC desiderata e salvare il file della documentazione su un'unità di rete condivisa.
   f) Inviare agli utenti dei client UC Suite il file di installazione zippato e il file della documentazione via e-mail o comunicare agli utenti il percorso in cui risiedono i file.
   g) Nel file zip contenente i file di installazione è presente anche un file Readme. Informare gli utenti che l'installazione dei client UC deve essere eseguita secondo le indicazioni riportate nel file Readme.
3) In alternativa, è anche possibile inviare agli utenti UC collegamenti per accedere direttamente ai file di installazione dei client UC.
   a) Nella barra di navigazione fare clic su **Centro assistenza**.
   b) Nella struttura di navigazione, fare clic su **Software**.
   c) Fare clic sul pulsante **Visualizza collegamenti applicazione**. Vengono visualizzati più collegamenti, a seconda del sistema operativo e del client UC desiderato. Ad esempio:

   ```
   https://<Indirizzo IP del sistema di comunicazione>/
   management/downloads/install-common.zip
   ```

6.8.4 Come eseguire il backup dei dati

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Nota: Per ulteriori informazioni sul backup dei dati, vedere Salvataggio immediato .

Passo a passo

1) Nella barra di navigazione fare clic su **Backup dei dati**.
2) Nella struttura di navigazione fare clic su **Backup - immediato**.
3) Nell'area **Nome**, nel campo **Commento**, immettere un commento per il set di backup per facilitare l'identificazione in caso di ripristino dei dati. Non utilizzare dieresi e caratteri speciali.
4) Nell'area **Dispositivi**, selezionare l'unità di destinazione sulla quale si vuole salvare il set di backup (ad esempio, sull'unità di rete).
5) Fare clic su **OK & Avanti**. Viene visualizzata una finestra che mostra l'avanzamento del backup.
6) Il backup ha esito positivo se viene visualizzato il messaggio **Backup completato**. Fare clic su **Chiudi**.

7) La messa in servizio con il WBM è ora completata. Chiudere il WBM facendo clic in alto a destra sul collegamento **Disconnetti**, quindi chiudendo la finestra.

6.9 Messa in servizio dei telefoni IP

Per una pratica messa in funzione dei telefoni IP, è necessario un server DHCP che fornisce ai telefoni IP i dati richiesti per l'accesso al sistema di comunicazione dati (dati di rete).

Dati specifici della rete

Per l'accesso al sistema di comunicazione, un telefono IP deve disporre dei dati di rete. Questi dati possono essere archiviati nel server DHCP o inseriti direttamente nel telefono IP. Il vantaggio di un server DHCP è costituito dal fatto che tutti i telefoni IP collegati ricevono automaticamente i dati.

Per il telefono IP sono necessari i seguenti dati:

- Indirizzo IP del sistema di comunicazione
- Indirizzo IP del server DLS

Inoltre il telefono IP richiede anche il proprio numero di telefono. Durante l'accesso, deve essere digitato manualmente nel telefono.

Registrazione dei telefoni SIP

Per motivi di sicurezza si consiglia di registrare i telefoni SIP presso il sistema di comunicazione. A tal fine, i dati di registrazione nel telefono IP e nel sistema di comunicazione devono corrispondere.

Per l'accesso sono necessari i seguenti dati:

- ID utente SIP
- Password SIP
- SIP realm (opzionale)

Non utilizzare password SIP semplici, ma assicurarsi che la password rispetti le seguenti regole:

- Almeno 8 caratteri
- Almeno una lettera maiuscola (A - Z)
- Almeno una lettera minuscola (a - z)
- Almeno una cifra (0-9)
- Almeno un carattere speciale

Utilizzare un ID utente SIP che non comprenda il numero di telefono.

Nota: Per ulteriori informazioni sulla configurazione dei telefoni SIP, visitare l'indirizzo Web `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Uso del server DHCP interno

Se viene utilizzato il server DHCP interno del sistema di comunicazione, i dati specifici della rete sono già memorizzati qui. Per poter registrare un telefono IP sul sistema di comunicazione, è necessario immettere nel telefono IP solo il numero di telefono definito. Per un telefono SIP, occorre inoltre che i

dati per la registrazione SIP sul telefono SIP e nel sistema di comunicazione corrispondano.

Uso di un server DHCP esterno con dati specifici della rete

Se viene utilizzato un server DHCP esterno, i dati specifici della rete devono essere salvati qui. Per poter registrare un telefono IP sul sistema di comunicazione, è necessario immettere nel telefono IP solo il numero di telefono definito. Per un telefono SIP, occorre inoltre che i dati per la registrazione SIP sul telefono SIP e nel sistema di comunicazione corrispondano.

Uso di un server DHCP esterno senza dati specifici della rete

Se si utilizza un server DHCP esterno, in cui non possono essere conservati i dati specifici della rete, questi devono essere inseriti sul telefono IP. Per poter registrare un telefono IP sul sistema di comunicazione, è necessario immettere nel telefono IP il numero di telefono definito, l'indirizzo IP del sistema di comunicazione ed eventualmente modificare le impostazioni per il Deployment Service. Per un telefono SIP, occorre inoltre che i dati per la registrazione SIP sul telefono SIP e nel sistema di comunicazione corrispondano.

6.9.1 Come configurare il telefono IP

Prerequisiti

Il telefono IP è collegato alla rete interna e operativo.

Nota: Qui viene descritta la configurazione di esempio per un telefono di sistema IP OpenStage 40/60/80. Per un altro telefono IP le impostazioni devono essere eseguite in modo analogo. Consultare le istruzioni del telefono IP.

Passo a passo

1) Per accedere alla modalità di amministrazione del telefono di sistema IP, premere, sul telefono, il tasto corrispondente al menu delle impostazioni/ applicazioni.
2) Sfogliare nella scheda da `Impostazioni` a `Admin` e confermare con il tasto OK.
3) Immettere la password di amministratore (predefinita: `123456`) e confermare con il tasto OK.
4) Se sulla rete interna si utilizza il server DHCP del sistema di comunicazione, saltare il passo successivo.
5) Se sulla rete interna non si utilizza il server DHCP del sistema di comunicazione, è necessario inserire l'indirizzo IP del Deployment server (DLS) e del sistema di comunicazione per consentire l'aggiornamento automatico del software dei telefoni IP di sistema. Questo si applica solo per i telefoni IP del sistema. Procedere come segue:
   a) Sfogliare fino a `Network` (Rete) e confermare con il tasto OK.
   b) Sfogliare fino a `Update service (DLS)` (Servizio di aggiornamento – DLS) e confermare con il tasto OK.

c) Sfogliare fino a `DLS address` (Indirizzo DLS) e confermare con il tasto OK.
d) Per il Deployment server, immettere l'indirizzo IP del sistema di comunicazione (predefinito: `192.168.1.2`) e confermare con il tasto OK.
e) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.
f) Sfogliare fino a `IPv4 configuration` (Configurazione IPv4) e confermare con il tasto OK.
g) Sfogliare fino a `Route (default)` (Route predefinita) e confermare con il tasto OK.
h) Immettere l'indirizzo IP del sistema di comunicazione (predefinito: `192.168.1.2`) e confermare con il tasto OK.
i) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.
j) Per tornare un livello di menu superiore usare il tasto Indietro.

6) Definire il numero del telefono:
a) Sfogliare fino a `System` (Sistema) e confermare con il tasto OK.
b) Sfogliare fino a `Identity` (Identità) e confermare con il tasto OK.
c) Sfogliare fino a `Terminal number` (Numero terminale) e confermare con il tasto OK.
d) Immettere il numero di telefono configurato (ad esempio, `120`) e confermare con il tasto OK.
e) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.

7) Per tornare un livello di menu superiore usare il tasto Indietro.

8) Quando il telefono di sistema richiede un riavvio in seguito alle modifiche apportate, nel menu `Admin` viene visualizzata la voce `Riavvia`. Confermare `Riavvia` con il tasto OK e poi `Sì` sempre con il tasto OK. Il telefono di sistema effettua un riavvio e accede al sistema di comunicazione.

6.9.2 Come configurare un telefono SIP

Prerequisiti

Il telefono SIP è collegato alla LAN del cliente e operativo.

Nota: Qui viene descritta la configurazione di esempio per un telefono di sistema OpenStage 40/60/80 SIP. Per un altro telefono SIP le impostazioni devono essere eseguite in modo analogo. Consultare le istruzioni del telefono SIP.

Passo a passo

1) Per accedere alla modalità di amministrazione del telefono di sistema SIP, premere, sul telefono, il tasto corrispondente al menu delle impostazioni/applicazioni.

2) Sfogliare nella scheda da `Impostazioni` a `Amministratore (Admin)` e confermare con il tasto OK.

3) Immettere la password di amministratore (predefinita: `123456`) e confermare con il tasto OK.

4) Se sulla rete interna si utilizza il server DHCP del sistema di comunicazione, saltare il passo successivo.

5) Se sulla rete interna non si utilizza il server DHCP del sistema di comunicazione, è necessario inserire l'indirizzo IP del Deployment server (DLS) e del sistema di comunicazione per consentire l'aggiornamento automatico del software dei telefoni SIP di sistema. Questo si applica solo per i telefoni SIP del sistema. Procedere come segue:

a) Sfogliare fino a `Network` (Rete) e confermare con il tasto OK.
b) Sfogliare fino a `Update service (DLS)` (Servizio di aggiornamento – DLS) e confermare con il tasto OK.
c) Sfogliare fino a `DLS address` (Indirizzo DLS) e confermare con il tasto OK.
d) Per il Deployment server, immettere l'indirizzo IP del sistema di comunicazione (predefinito: `192.168.1.2`) e confermare con il tasto OK.
e) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.
f) Sfogliare fino a `IPv4 configuration` (Configurazione IPv4) e confermare con il tasto OK.
g) Sfogliare fino a `Route (default)` (Route predefinita) e confermare con il tasto OK.
h) Immettere l'indirizzo IP del sistema di comunicazione (predefinito: `192.168.1.2`) e confermare con il tasto OK.
i) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.
j) Per tornare un livello di menu superiore usare il tasto Indietro.

6) Definire le impostazioni temporali SNTP:

a) Sfogliare fino a `Date and time` (Data e ora) e confermare con il tasto OK.
b) Sfogliare fino a `Time source` (Origine ora) e confermare con il tasto OK.
c) Sfogliare fino a `SNTP IP address` (Indirizzo IP SNTP) e confermare con il tasto OK.
d) Immettere l'indirizzo IP del sistema di comunicazione (predefinito: `192.168.1.2`) e confermare con il tasto OK.
e) Sfogliare fino a `Timezone offset` (Offset fuso orario) e confermare con il tasto OK.
f) Inserire la deviazione tra l'ora locale e UTC (Universal Time Coordinated) espressa in ore (Germania: `1`) e confermare con il tasto OK.
g) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.
h) Per tornare un livello di menu superiore usare il tasto Indietro.

7) Definire il numero del telefono:
   a) Sfogliare fino a `System` (Sistema) e confermare con il tasto OK.
   b) Sfogliare fino a `Identity` (Identità) e confermare con il tasto OK.
   c) Sfogliare fino a `Terminal number` (Numero terminale) e confermare con il tasto OK.
   d) Immettere il numero di telefono configurato (ad esempio, `120`) e confermare con il tasto OK.
   e) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.

8) Definire i dati di autenticazione SIP:
   a) Sfogliare fino a `Registration` (Registrazione) e confermare con il tasto OK.
   b) Sfogliare fino a `SIP session` (Sessione SIP) e confermare con il tasto OK.
   c) Prendere nota del `Realm` o se richiesto inserire un nuovo realm (ad esempio `OSBIZ-SIP`).
   d) Prendere nota dell'`ID utente` o se richiesto inserire un nuovo ID utente (ad esempio `SIP-120`).
   e) Immettere la `Password` per la registrazione presso il server SIP.
   f) Sfogliare fino a `Save & Exit` (Salva ed esci) e confermare con il tasto OK.

9) Utilizzando il pulsante Indietro, tornare al menu `Admin`.

10) Quando il telefono di sistema richiede un riavvio in seguito alle modifiche apportate, nel menu `Admin` viene visualizzata la voce `Riavvia`. Confermare `Riavvia` con il tasto OK e poi `Sì` sempre con il tasto OK. Il telefono di sistema effettua un riavvio e accede al sistema di comunicazione.

6.10 Disinstallazione del software di comunicazione

Per la disinstallazione del software di comunicazione viene utilizzata una console di tipo testuale.

6.10.1 Come disinstallare il software di comunicazione

Passo a passo

1) Aprire un terminale (ad esempio, terminale GNOME).

2) Inserire nell'interfaccia shell il comando `su` (a indicare superuser = utente root) e confermare con Invio.

3) Inserire nell'interfaccia shell la password per l'utente "root" e confermare con Invio.

4) Inserire nell'interfaccia shell il comando `oso_deinstall.sh` e confermare con Invio. Seguire le istruzioni fornite dal programma di disinstallazione.

6.11 Porte usate

I componenti del sistema OpenScape Business utilizzano porte diverse, che potrebbero dover essere aperte nel firewall in base alle necessità. Per le porte

dei client basati sul Web (ad esempio, myPortal to go), è necessario configurare l'inoltro delle porte nel router.

L'elenco completo di tutte le porte utilizzate da OpenScape Business è disponibile nel "Database di gestione delle interfacce" (IFMD), accessibile tramite il Portale partner di Unify (https://unify.com/en/partners/partner-portal.

Nota: Le porte identificate nell'elenco seguente con "O" sono opzionali, cioè non sono aperte in modo permanente nel firewall.

Descrizione	TCP	UDP	Numero di porta	OpenScape Business X	Scheda UC Booster	OpenScape Business S	Server UC Booster
Componenti del sistema							
Portale di amministrazione (https)	X		443	X	X	X	X
Verifiche CAR Alive	X		12062	X		X	
CLA	X		61740	A		A	A
CLA Auto Discovery		X	23232	X		X	X
CLS	X		7780, 7790 (fino alla versione V3R3) 7780, 7791 (dalla versione V3R3.1 in poi)	A		A	
Programma di installazione del client di comunicazione	X		8101	X	X	X	X
Csta Message Dispatcher (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	
Csta Service Provider (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	A		A	
FTP Passive	X		40000-40040	A		A	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Messaggistica istantanea (http)	X		8101	X	X	X	X
JSFT	X		8771		X	X	X

Descrizione	TCP	UDP	Numero di porta	OpenScape Business X	Scheda UC Booster	OpenScape Business S	Server UC Booster
JSFT	X		8772		X	X	X
LAS Cloud Service	X		8602	X			
Server LDAP	X		389		X	X	X
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
NAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
Openfire Admin (https)	X		9091		X	X	X
OpenScape Business Auto Update Service (http)	X		8101	X	X	X	X
OpenScape Business Multisite	X		8778		X	X	X
OpenScape Business myReports (http)	X		8101		X	X	X
Server stato OpenScape Business	X		8808	X		X	X
Portale utenti OpenScape Business	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (integrato)		X	29100-30530	X	X	X	X
RTP (server)		X	29100-30888	X	X	X	X
SIP (server)	X	X	5060	X		X	
SIP TLS SIPQ (server)	X		5061	X		X	
SIP TLS Subscriber (server)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (traps)		X	162	X		X	
VSL	X		8770-8780		X	X	X
Webadmin per client	X		8803	X	X	X	X
Client basati sul Web							
Client basati sul Web (http)	X		8801	X	X	X	X
Client basati sul Web (https)	X		8802	X	X	X	X

Nota: Per motivi di sicurezza, si consiglia di utilizzare solo https per i client basati sul Web e di impostare l'inoltro delle porte da TCP/443 esterno a TCP/8802 interno.

Certificato CLS

A partire dalla V3R3.1, viene fornito un nuovo certificato CLS con un nome comune (CN) aggiornato tramite una porta di nuova introduzione. Ciò offre un algoritmo digest migliorato e più forte, nonché entità legali aggiornate. I sistemi con licenza online tramite la modalità CLS Connect richiedono i seguenti due prerequisiti:

- L'indirizzo IP 188.64.16.4 è abilitato per il traffico in uscita nel firewall.
- Le porte 7780 e 7791 sono abilitate per il traffico in uscita nel firewall.

La porta 7790 usata in precedenza può essere rimossa dalla configurazione del firewall dopo l'aggiornamento alla V3R3.1 per aumentare la sicurezza.

6.12 Come raccogliere tracce diagnostiche per un evento di errore

È possibile raccogliere automaticamente le tracce diagnostiche necessarie per un evento di errore. The **Error Management** wizard will guide you through the whole process.

You must run the **Error Management** wizard twice: before and after the execution of the problematic scenario. During the first run (Phase 1), you activate the diagnostic traces collection. After execution of the problematic scenario, run the wizard again to collect the diagnostic trace data (Phase 2). Once the Phase 2 is complete, you can download the trace file to include them in the ticket system.

Eseguire i passaggi seguenti per raccogliere i dati della traccia diagnostica per l'evento di errore:

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Fare clic su **Modifica** vicino a **Gestione errori**.
3) Click on **OK & Next**
4) If you want to collect the Default Traces click on the **Default Traces** check-box.
5) If you want to specify the types of traces to collect, select the desired ones from the list of traces. More than one selection is possible.

   Per ulteriori informazioni sulle tracce, vedere la Guida alla risoluzione dei problemi.
6) Fare clic su **OK & Avanti**.
7) Viene visualizzato un elenco con informazioni aggiuntive, documentazione rilevante e suggerimenti. Fare clic su **OK & Avanti**.
8) Vengono visualizzati gli scenari e il tipo di tracce da raccogliere. Fare clic su **Fine**.
9) Continuare eseguendo lo scenario problematico.

10) Dopo aver completato lo scenario, andare di nuovo a **Configurazione > Gestione errori** e fare clic su **Modifica**.

    Si viene reindirizzati al Passaggio 2 della raccolta tracce di diagnostica. Per interrompere il processo e riavviarlo, è possibile fare clic sul pulsante **Annulla**.

11) Fare clic su **OK & Avanti**.

12) Inserire le informazioni richieste e fare clic su **OK & Avanti**.

13) Viene visualizzato un elenco con le informazioni necessarie e alcune altre azioni aggiuntive.

14) Fare clic su **OK & Avanti**.

15) Fare clic su **Fine** per avviare il download dei dati della traccia diagnostica.

6.13 Reflashing

Seguendo i passaggi indicati di seguito è possibile modificare facilmente il tipo di software di un dispositivo.

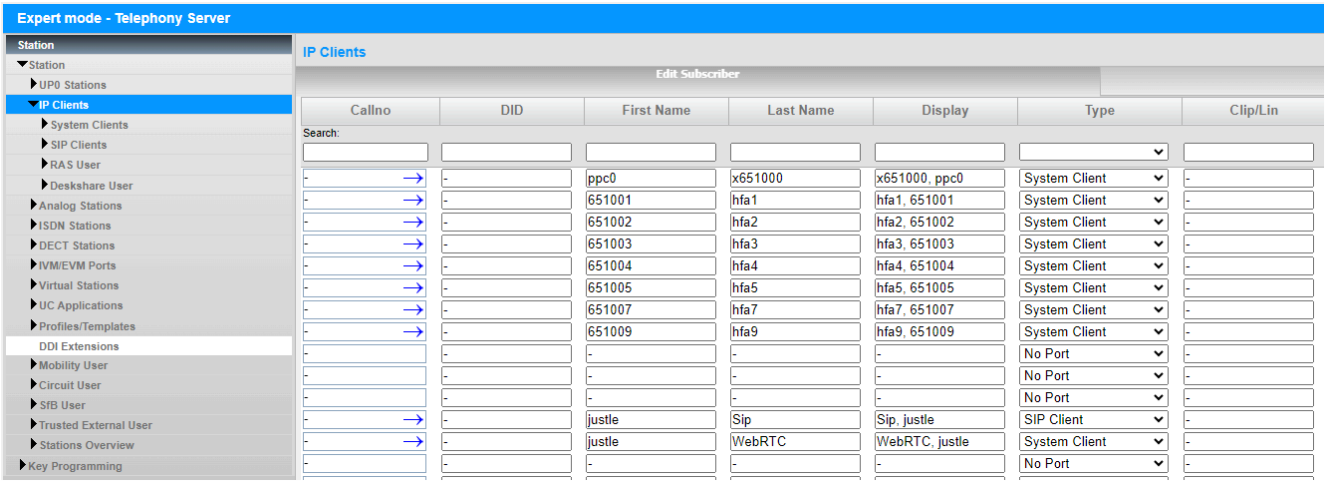
L'idea alla base di questa funzione è quella di semplificare il modo in cui ottenere un dispositivo SIP (pronto all'uso) e registrarlo nel sistema OSBiz come dispositivo HFA. Gli unici requisiti sono che:

- il telefono deve ottenere l'indirizzo DLI (dal server DHCP o manualmente)
- l'amministratore deve inserire il numero del telefono (che deve essere preconfigurato come client di sistema)

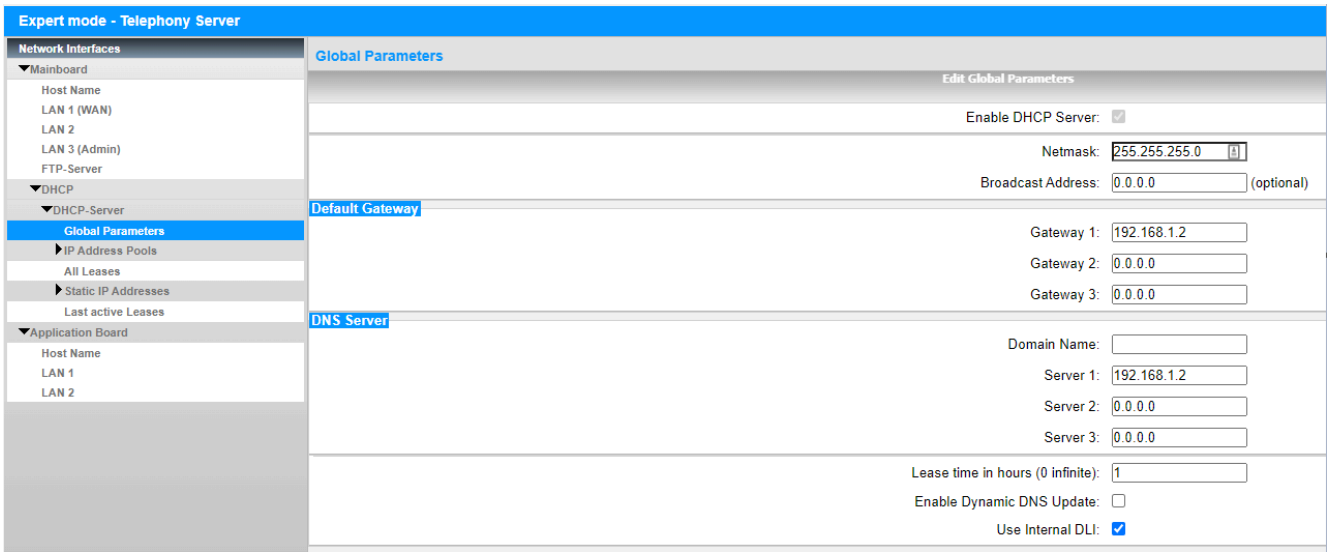
Quando il cliente riceve un nuovo dispositivo, questo sarà preconfigurato come dispositivo SIP (impostazioni di fabbrica). I passaggi da seguire per eseguire il reflashing del dispositivo e trasformarlo in un dispositivo HFA sono i seguenti:

Passo a passo

1) Configurare nel database OSBIZ il numero di telefono desiderato come client di sistema (HFA).



2) Configurare il server DHCP per inviare l'indirizzo IP del DLI. Questa operazione può essere eseguita sul server DHCP esterno o sul server DHCP interno.



3) Se non viene utilizzato un server DHCP, è necessario configurare manualmente l'IP di DLI sul telefono.

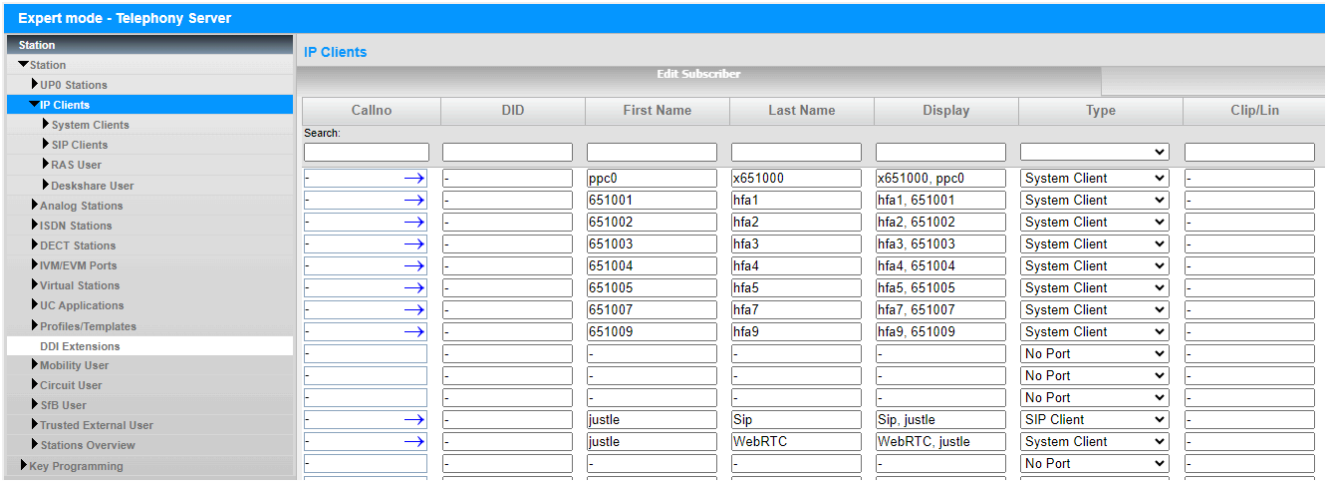
4) Una volta che il telefono SIP ha ottenuto un IP e l'IP DLI, il dispositivo telefonico verrà registrato nel database DLI e verrà visualizzato un prompt per l'immissione del numero di interno.

5) Immettere il numero di terminale del telefono (il numero deve essere lo stesso configurato nel primo passaggio, ad esempio 4111).

6) Il reflashing si avvia e la nuova immagine HFA viene scaricata sul telefono. Al suo riavvio, il telefono verrà registrato come telefono HFA e i dati plug and play saranno inviati dal sistema al telefono.

7) **Per eseguire il reflashing di un telefono SIP già registrato:**

8) Cambiare il tipo di dispositivo SIP funzionante in "Client di sistema".



9) Riavviare il telefono.

10) Il reflashing si avvia e la nuova immagine HFA viene scaricata sul telefono. Al suo riavvio, il telefono verrà registrato come telefono HFA e i dati plug and play saranno inviati dal sistema al telefono.

7 Configurazione iniziale di OpenScape Business UC Booster

Questa sezione descrive l'installazione e la configurazione iniziali di OpenScape Business UC Booster nel sistema di comunicazione OpenScape Business X3/X5/X8. Tenere presente che c'è una differenza se si utilizza la OpenScape Business UC Booster Card o l'OpenScape Business UC Booster Server per la funzionalità UC Booster.

La configurazione iniziale di OpenScape Business UC Booster viene eseguita con il programma di amministrazione OpenScape Business Assistant (gestione basata sul Web, denominata per brevità WBM).

L'amministrazione dettagliata delle funzioni non coperte dalla configurazione iniziale è descritta nei seguenti capitoli.

Configurazione iniziale della OpenScape Business UC Booster Card

Viene installata la OpenScape Business UC Booster Card nel sistema di comunicazione OpenScape Business X3/X5/X8 e ne viene configurato il funzionamento. Segue la configurazione delle funzionalità di OpenScape Business UC Booster.

I passaggi di installazione specifici necessari per la configurazione iniziale differiscono a seconda che la scheda UC Booster venga messa in funzione per la prima volta con il sistema di comunicazione OpenScape Business X3/X5/X8 o che venga integrata in seguito in un sistema di comunicazione OpenScape Business X3/X5/X8 esistente e già configurato.

Panoramica delle fasi di installazione per entrambe le opzioni:

Integrazione in un nuovo sistema di comunicazione	Integrazione in un sistema di comunicazione esistente
	Backup dei dati di configurazione del sistema di comunicazione
Installazione della scheda UC Booster La scheda UC Booster viene installata nel sistema di comunicazione OpenScape Business X3/X5/X8. Per una descrizione, consultare la Documentazione di servizio di OpenScape Business, Installazione dell'hardware - Descrizione delle schede.	Installazione della scheda UC Booster La scheda UC Booster viene installata nel sistema di comunicazione OpenScape Business X3/X5/X8. Per una descrizione, consultare la Documentazione di servizio di OpenScape Business, Installazione dell'hardware - Descrizione delle schede.
Configurazione della scheda UC Booster La configurazione della scheda UC Booster viene eseguita insieme all'installazione iniziale del sistema di comunicazione OpenScape Business X3/X5/X8. Per una descrizione, vedere Integrazione nella LAN del cliente.	Configurazione della scheda UC Booster La configurazione della scheda UC Booster viene eseguita successivamente su un sistema di comunicazione OpenScape Business X3/X5/X8 già configurato. Per una descrizione, vedere Integrazione nella LAN del cliente. Per le specifiche della configurazione, vedere Configurazione della scheda UC Booster

Integrazione in un nuovo sistema di comunicazione	Integrazione in un sistema di comunicazione esistente
Configurazione di base La configurazione di base viene eseguita insieme all'installazione iniziale del sistema di comunicazione OpenScape Business X3/X5/X8. Per una descrizione, vedere Configurazione di base.	Configurazione di base La configurazione di base viene eseguita in seguito su un sistema di comunicazione OpenScape Business X3/X5/X8 già configurato. Per una descrizione, vedere Configurazione di base. Per le funzionalità speciali della configurazione di base, vedere Configurazione di base
Attività di chiusura Le attività di chiusura (compresa la concessione della licenza dei client UC) vengono eseguite insieme all'installazione iniziale del sistema di comunicazione OpenScape Business X3/X5/X8. Per una descrizione, vedere Attività di chiusura.	Attività di chiusura Le attività di chiusura (compresa la concessione della licenza dei client UC) vengono eseguite insieme all'installazione iniziale del sistema di comunicazione OpenScape Business X3/X5/X8. Per una descrizione, vedere Attività di chiusura. Per le funzionalità speciali delle attività di chiusura, vedere Attività di chiusura

Installazione iniziale del server di OpenScape Business UC Booster

Il server di OpenScape Business UC Booster è integrato con il sistema di comunicazione OpenScape Business X3/X5/X8 nella LAN del cliente.

Il software di comunicazione OpenScape Business per OpenScape Business UC Booster, che fornisce la funzionalità OpenScape Business UC Booster, viene installato sul sistema operativo Linux SLES 12 SP5 a 64 bit o SLES 15 SP6 a 64 bit. Il software di comunicazione può essere utilizzato direttamente su un server Linux o in un ambiente virtuale con VMware vSphere. L'installazione del sistema operativo Linux è descritta nella *Guida all'installazione di OpenScape Business, Installazione del server Linux*.

UC Booster Server OpenScape Business dispone di un proprio WBM. Questo WBM viene utilizzato per gli aggiornamenti software, il backup dei dati di configurazione e la diagnostica del server di OpenScape Business UC Booster. L'installazione iniziale del server di OpenScape Business UC Booster viene eseguita tramite il WBM del sistema di comunicazione.

I passaggi di installazione specifici necessari per l'installazione differiscono a seconda che UC Booster Server venga messo in funzione per la prima volta con il sistema di comunicazione OpenScape Business X3/X5/X8 o che venga connesso in seguito a un sistema di comunicazione OpenScape Business X3/X5/X8 esistente e già configurato.

Panoramica delle fasi di installazione per entrambe le opzioni:

Integrazione in un nuovo sistema di comunicazione	Integrazione in un sistema di comunicazione esistente
	Backup dei dati di configurazione del sistema di comunicazione

Integrazione in un nuovo sistema di comunicazione	Integrazione in un sistema di comunicazione esistente
Installazione del server Linux L'installazione del server Linux è descritta nella Guida all'installazione del server Linux di OpenScape Business.	Installazione del server Linux L'installazione del server Linux è descritta nella Guida all'installazione del server Linux di OpenScape Business.
Installazione del software di comunicazione	Installazione del software di comunicazione
Configurazione di UC Booster Server La configurazione di UC Booster Server viene eseguita insieme all'installazione iniziale del sistema di comunicazione OpenScape Business X3/X5/X8. Per una descrizione, vedere Integrazione nella LAN del cliente.	Configurazione di UC Booster Server La configurazione di UC Booster Server viene eseguita in seguito su un sistema di comunicazione OpenScape Business X3/X5/X8 già configurato. Per una descrizione, vedere Integrazione nella LAN del cliente. Per le specifiche della configurazione, vedere Configurazione di UC Booster Server
Configurazione di base La configurazione di base viene eseguita insieme all'installazione iniziale del sistema di comunicazione OpenScape Business X3/X5/X8. Per una descrizione, vedere Configurazione di base.	Configurazione di base La configurazione di base viene eseguita in seguito su un sistema di comunicazione OpenScape Business X3/X5/X8 già configurato. Per una descrizione, vedere Configurazione di base. Per le funzionalità speciali della configurazione di base, vedere Configurazione di base
Attività di chiusura Le attività di chiusura (compresa la concessione della licenza dei client UC) vengono eseguite insieme all'installazione iniziale del sistema di comunicazione OpenScape Business X3/X5/X8. Per una descrizione, vedere Attività di chiusura.	Attività di chiusura Le attività di chiusura (compresa la concessione della licenza dei client UC) vengono eseguite insieme all'installazione iniziale del sistema di comunicazione OpenScape Business X3/X5/X8. Per una descrizione, vedere Attività di chiusura. Per le funzionalità speciali delle attività di chiusura, vedere Attività di chiusura

7.1 Requisiti richiesti per la configurazione iniziale

Soddisfare i prerequisiti per la configurazione iniziale assicura il corretto funzionamento di OpenScape Business UC Booster.

Generale

A seconda dell'hardware utilizzato (telefoni, ...) e dell'infrastruttura esistente, si applicano le seguenti condizioni generali:

- Il sistema di comunicazione OpenScape Business X3/X5/X8 è configurato e pronto all'uso.
- L'infrastruttura LAN (router Internet, switch, ecc.) è presente e utilizzabile.
- I telefoni IP sono connessi alla LAN del cliente.

- Si raccomanda una connessione a Internet a banda larga per gli aggiornamenti software e l'accesso remoto.
- Tutte le licenze necessarie per OpenScape Business UC Booster sono presenti (ad esempio, client UC, servizi di directory, ecc.). Se si effettua l'integrazione in un sistema di comunicazione già dotato di licenza, non vi è nessun periodo di attivazione.
- Uno schema di indirizzi IP esiste già ed è noto.
- Un piano di composizione (chiamato anche piano di numerazione) è presente e noto.

Per la scheda UC Booster

Per il funzionamento della scheda UC Booster è necessario rispettare i seguenti requisiti.

- Hardware per OpenScape Business:

  La scheda UC Booster è installata.
- Apparecchiature di rete:

  Per un corretto funzionamento, è obbligatorio disporre di un'apparecchiatura di rete abilitata per IPv6 tramite la quale la scheda UC Booster si collega al sistema di comunicazione. In questo modo la scheda UC Booster può ricevere automaticamente un indirizzo IP durante la configurazione iniziale e dopo ogni riavvio del sistema.

  Se l'apparecchiatura di rete non è abilitata per IPv6, il LED rosso del sistema di comunicazione lampeggia. In questo caso, la porta di amministrazione del sistema deve essere collegata alla seconda porta LAN della scheda UC Booster tramite un cavo Ethernet aggiuntivo. In questo modo, la scheda UC Booster riceve automaticamente un indirizzo IPv4 tramite il protocollo IPv6. Non appena la scheda UC Booster è raggiungibile tramite IP, il LED rosso del sistema di comunicazione si spegne. L'indirizzo IP desiderato per la scheda UC Booster può essere inserito durante la configurazione iniziale e dopo ogni riavvio del sistema. Adesso, la comunicazione tra il sistema e la scheda UC Booster avviene attraverso la connessione IPv4 dello switch.

  Nota: Il cavo Ethernet aggiuntivo deve essere lasciato collegato nel caso in cui sia necessario un riavvio o un ricaricamento.
- Kit ventola:

  La scheda UC Booster richiede una ventola aggiuntiva. Il kit ventola dipende dal sistema di comunicazione.
- Coperchio dell'alloggiamento:

  Per OpenScape Business X3W, è necessario un nuovo coperchio dell'alloggiamento per il kit ventola della scheda UC Booster.

  Se si sta effettuando la migrazione da sistemi HiPath 3000, per OpenScape Business X3W/X5W e X3R/X5R sono necessari nuovi coperchi per alloggiare il kit ventola della scheda UC Booster.
- Software di comunicazione:

  Il software del sistema di comunicazione deve essere aggiornato all'ultima versione rilasciata. A tale scopo, è necessario utilizzare l'immagine che include il software della scheda UC Booster.

- Browser Web:

  Per la configurazione iniziale della scheda UC Booster con OpenScape Business Assistant (WBM) viene utilizzato il PC amministratore. Il WBM è basato su browser e, quindi, dipende dal sistema operativo. È necessaria una risoluzione dello schermo di 1024 x 768 o superiore.

  Sono supportati i seguenti browser Web abilitati per HTML 5:

  – Microsoft Internet Explorer Versione 10 o successiva.
  – Microsoft Edge
  – Mozilla Firefox versione 17 o successiva
  – Google Chrome

  Se è installata una versione precedente del browser Web, è necessario installare una versione aggiornata prima di poter avviare la configurazione iniziale del sistema.

  Nota: È necessario un accesso di rete illimitato tra OSCC e OCAB.

Per UC Booster Server

Per il funzionamento di UC Booster Server è necessario rispettare i seguenti requisiti.

- Server Linux:

  Il server Linux necessario per OpenScape Business S è stato installato seguendo le istruzioni presenti nella *Guida all'installazione del server Linux per OpenScape Business*, è stato integrato nella LAN del cliente ed è pronto per l'uso.
- Software di comunicazione OpenScape Business:

  È disponibile il DVD di installazione con il software di comunicazione OpenScape Business. Dopo l'installazione del software, il software del sistema di comunicazione e il software di comunicazione di UC Booster Server devono essere aggiornati separatamente alla stessa versione software più recente.
- DVD o chiavetta USB con il sistema operativo Linux SLES 12 SP5 a 64 bit o SLES 15 SP6 a 64 bit.

  Il DVD Linux potrebbe essere necessario durante l'installazione del software di comunicazione OpenScape Business, poiché alcuni pacchetti software (RPM) necessari per il software di comunicazione potrebbero dover essere installati successivamente da questo DVD.
- Browser Web:

  Per la configurazione iniziale di UC Booster Server con OpenScape Business Assistant (WBM), è possibile utilizzare il server Linux o il PC amministratore. Il WBM è basato su browser e, quindi, dipende dal sistema

operativo. È necessaria una risoluzione dello schermo di 1024 x 768 o superiore.

Sono supportati i seguenti browser Web abilitati per HTML 5:

- Microsoft Internet Explorer versione 10 e successive (PC amministratore).
- Microsoft Edge
- Mozilla Firefox versione 17 o successiva (sever Linux/PC amministratore)
- Google Chrome

Se è installata una versione precedente del browser Web, è necessario installare una versione aggiornata prima di poter avviare la configurazione iniziale del sistema.

- Firewall:

  Se si è connessi a Internet, è necessario un firewall per il server Linux al fine di impedire l'accesso non autorizzato dall'esterno. Dopo l'installazione di Linux, il firewall di Linux è abilitato. L'installatore del software di comunicazione regola le impostazioni del firewall in modo che il software di comunicazione possa funzionare correttamente. Le porte per il software di comunicazione sono aperte e tutte le altre porte sono chiuse.

  Se viene utilizzato un firewall esterno nella rete, il firewall Linux deve essere disabilitato e gli indirizzi e le porte necessari per il software di comunicazione devono essere aperti (vedere Porte usate).

7.2 Backup dei dati di configurazione del sistema di comunicazione

Prima di installare OpenScape Business UC Booster, è assolutamente necessario eseguire un backup dei dati di configurazione esistenti del sistema di comunicazione OpenScape Business.

Il backup viene eseguito nel WBM del sistema di comunicazione OpenScape Business.

Per il backup è possibile utilizzare anche supporti di backup diversi (ad esempio, un supporto USB o un'unità di rete).

7.2.1 Come eseguire il backup dei dati

Prerequisiti

Si è connessi al WBM del sistema di comunicazione con il profilo **Advanced**.

Per effettuare un backup dei dati su un supporto USB è necessario che tale supporto sia collegato a un'interfaccia server USB del sistema di comunicazione.

Passo a passo

1) Nella barra di navigazione fare clic su **Backup dei dati**.
2) Nella struttura di navigazione fare clic su **Backup - immediato**.
3) Nell'area **Nome**, nel campo **Commento**, immettere un commento per il set di backup per facilitare l'identificazione in caso di ripristino dei dati. Non utilizzare dieresi e caratteri speciali.

4) Nell'area **Dispositivi**, selezionare l'unità di destinazione sulla quale si vuole salvare il set di backup.
5) Fare clic su **OK & Avanti**. Viene visualizzata una finestra che mostra l'avanzamento del backup.
6) Il backup ha esito positivo se viene visualizzato il messaggio **Backup completato**. Fare clic su **Chiudi**.
7) Se per il backup si utilizza un supporto USB, attendere fino a quando il LED di tale supporto non smette di lampeggiare. A questo punto il backup sulla chiave USB è stato eseguito. Rimuovere la chiave USB.
8) Il backup dei dati con il WBM è ora completata. Chiudere il WBM facendo clic in alto a destra sul collegamento **Disconnetti**, quindi chiudendo la finestra.

7.3 Messa in servizio della UC Booster Card

La messa in servizio della UC Booster Card comprende il montaggio nel sistema di comunicazione OpenScape Business e la configurazione iniziale per il funzionamento corretto.

Completata la configurazione, deve essere eseguito un aggiornamento del software.

7.3.1 Montaggio della UC Booster Card

La UC Booster Card viene integrata nel sistema di comunicazione OpenScape Business. Lo slot della UC Booster Card dipende dal sistema di comunicazione.

Il montaggio della UC Booster Card è descritto nel dettaglio nella documentazione di manutenzione, Montaggio dell'hardware, al capitolo "Descrizione dei moduli".

La UC Booster Card può essere integrata nei seguenti sistemi di comunicazione OpenScape Business:

- OpenScape Business X3R e X5R (OCCMR)

  UC Booster Card con kit ventola aggiuntivi.
- OpenScape Business X3W e X5W (OCCM)

  UC Booster Card con kit ventola aggiuntivi.

  Con OpenScape Business X3W, per il kit ventola è necessario un nuovo sportello dell'alloggiamento.
- OpenScape Business X8 (OCCL)

  UC Booster Card con kit ventola aggiuntivi.

7.3.2 Configurazione della UC Booster Card

Durante la configurazione vengono definite le impostazioni fondamentali per l'uso della UC Booster Card.

Viene eseguita la configurazione della UC Booster Card con la procedura guidata **Configurazione di base** del WBM del sistema di comunicazione. Per

la descrizione della configurazione, vedere il capitolo Installazione iniziale di OpenScape Business X3/X5/X8.

La procedura guidata **Configurazione di base** del WBM comprende la configurazione iniziale dell'intero sistema di comunicazione. Per l'uso della OpenScape Business UC Booster Card, sono necessarie le seguenti parti:

- Indirizzo IP della UC Booster Card

  La UC Booster Card richiede un indirizzo IP indipendente del segmento di rete del sistema di comunicazione.
- Scelta della soluzione UC

  È possibile scegliere se utilizzare la soluzione UC Smart o UC Suite.

La modifica dell'indirizzo IP della UC Booster Card o della soluzione UC determina il riavvio del sistema di comunicazione.

7.3.3 Aggiornamento software per la UC Booster Card

Per l'uso corretto della UC Booster Card, il software del sistema di comunicazione deve essere aggiornato. In questo modo vengono installati tutti i componenti software mancanti necessari per la UC Booster Card.

Se il software del sistema di comunicazione è già aggiornato, il sistema deve essere aggiornato con il software più recente per assicurare che vengano installati tutti i componenti necessari per la funzionalità UC.

L'aggiornamento del software può essere eseguito tramite Internet o tramite un file immagine disponibile sul Software Download Server. Quando si esegue un aggiornamento tramite un file immagine, occorre assicurarsi che venga utilizzato il file immagine contenente la parte UC Booster Card (osbiz..._ocab.tar).

7.3.3.1 Come eseguire l'aggiornamento del software

Prerequisiti

È disponibile un accesso a Internet.

Si è connessi a WBM con il profilo **Advanced**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione, fare clic su **Aggiornamento SW** > **Aggiornamento via Internet**. Viene visualizzata la versione software attualmente installata.
3) Fare clic su **OK & Avanti**.
4) Leggere il contratto di licenza (EULA) e attivare il pulsante di opzione **Accetto il contratto di licenza**.
5) Fare clic su **OK & Avanti**.
6) Selezionare il pulsante di opzione **Inizio dell'azione subito/subito dopo la trasmissione**.

7) Fare clic su **OK & Avanti**. L'aggiornamento software viene caricato in background nel sistema di comunicazione e attivato automaticamente dopo la trasmissione. Dopo due riavvii il software viene aggiornato.

   Nota: La finestra del browser può essere chiusa in qualsiasi momento.

8) Lo stato dell'aggiornamento può essere richiesto tramite il WBM selezionando **Centro assistenza** > **Aggiornamento del software** > **Stato**.

7.4 Messa in servizio dell'UC Booster Server

La messa in servizio dell'UC Booster Server comprende l'installazione del sistema di comunicazione OpenScape Business sul server Linux e la configurazione iniziale per il funzionamento corretto.

Completata la configurazione, deve essere eseguito un aggiornamento del software.

7.4.1 Installazione del software di comunicazione

Il software di comunicazione OpenScape Business è installato sul server Linux utilizzando il DVD di OpenScape Business.

Assicurarsi di modificare, ove necessario, gli indirizzi IP e le maschere di rete in base alla LAN del cliente.

Server DHCP

Un server DHCP assegna automaticamente agli utenti IP (telefoni IP, PC, ecc.) un indirizzo IP e fornisce i dati di rete, quali ad esempio l'indirizzo IP del gateway predefinito.

Come server DHCP è possibile utilizzare un server DHCP esterno (ad esempio, il server DHCP del router Internet o del sistema di comunicazione) o il server DHCP del server Linux. Se si utilizza il server Linux del server DHCP, è necessario disattivare il server DHCP esterno. La configurazione del server Linux DHCP può essere eseguita durante l'installazione del software di comunicazione OpenScape Business.

Ambiente virtuale

Il software di comunicazione può essere eseguito in un ambiente virtuale. A tal fine, viene innanzitutto installato e configurato il software di virtualizzazione sul PC server (sistema operativo host). Successivamente viene installato il sistema operativo Linux. Infine sul sistema operativo Linux viene installato il software di comunicazione (vedere *OpenScape Business, Server Linux, Istruzioni di installazione*).

Uso di istantanee su macchine virtuali (VM):

Le istantanee possono costituire un prezioso meccanismo di manutenzione, ad esempio per un rapido ripristino di uno stato operativo predefinito della macchina virtuale, prima dell'esito negativo di uno script di distribuzione di massa.

- Le istantanee non possono essere create durante il normale funzionamento. Mentre viene scattata un'istantanea, lo stato della macchina virtuale viene congelato. Pertanto, i terminali e le applicazioni correlate, ad esempio i telefoni IP o i client UC, possono perdere la connessione al server.
- Le istantanee possono determinare la mancata sincronizzazione dei processi server interni e non garantiscono un funzionamento stabile del sistema di comunicazione. Pertanto, in seguito a un'istantanea, è necessario pianificare un riavvio del server con la finestra di manutenzione.
- Le precedenti istantanee non devono restare nell'ambiente di produzione durante il normale funzionamento.
- Le istantanee possono essere catturate durante una finestra di manutenzione programmata o in fase di installazione.
- Le istantanee vengono utilizzate internamente da strumenti di backup quali VDP o VDR. Occorre assicurarsi che queste operazioni di backup siano programmate al di fuori degli orari di lavoro e che le istantanee generate da questi strumenti siano cancellate al termine dell'operazione.

Per ulteriori informazioni sulle istantanee consultare la Knowledge Base (KB) di WMware. Un buon punto di partenza è l'articolo della KB 1025279 - Best Practices for virtual machine snapshots in the VMware environment (`http://kb.vmware.com/kb/1025279`).

7.4.1.1 Come installare il software di comunicazione

Prerequisiti

- Il sistema operativo SLES 12 SP5 o SLES 15 SP6 è stato installato e avviato correttamente sul server Linux.
- DVD o file .ISO con software di comunicazione OpenScape Business.
- DVD, file .ISO o chiavetta USB con sistema operativo Linux SLES 12 SP5 a 64 bit o SLES 15 SP6 a 64 bit, per un'eventuale successiva installazione di pacchetti software (RPM), in caso di necessità.
- Sono disponibili i dati dell'accesso root (nome utente e password) per accedere al server Linux.

Importante: Durante l'installazione, il software di comunicazione OpenScape Business sovrascrive qualsiasi file di configurazione esistente (ad esempio, per DHCP, FTP, Postfix, ecc.).

Passo a passo

1) Accedere al server Linux con i privilegi root.

2) Inserire il DVD o il file .ISO di OpenScape Business nell'unità DVD.

3) Confermare il messaggio con **Esegui**. Viene visualizzata la finestra "Welcome".

4) Selezionare la lingua di configurazione desiderata (ad es, **Inglese**) e fare clic su **Avvia**. Qui viene descritto il resto dell'installazione per la lingua inglese.

5) Selezionare il prodotto desiderato dall'elenco e fare clic su **Seleziona**. Viene eseguito un controllo per determinare se l'hardware soddisfa tutti i requisiti per l'installazione. In caso di carenze di poca importanza nei

requisiti, viene visualizzato un avviso. Dopo la conferma, è possibile proseguire con l'installazione. In caso di carenze gravi, l'installazione viene annullata automaticamente.

6) Viene eseguito un controllo per determinare se devono essere installati altri pacchetti RPM. In tal caso, confermare con **Conferma**. A questo punto sarà necessario tornare a SLES 12 o SLES 15, su DVD o file .ISO, in un secondo momento.

7) Viene visualizzata una finestra con i termini della licenza (ossia il Contratto di licenza per l'utente finale o EULA). Leggere i termini della licenza e accettare il contratto di licenza con **Sì**.

8) Se è già presente un server DHCP nella LAN del cliente (ad esempio, il server DHCP del router Internet), interrompere qui la configurazione del server DHCP Linux con **No** e procedere on il passaggio 12 per continuare.

Nota: Per garantire che il software dei telefoni di sistema possa essere aggiornato automaticamente anche quando si utilizza un server DHCP esterno, si hanno due possibilità:

a) L'indirizzo IP del server Linux deve essere inserito come indirizzo DLS in ogni telefono di sistema.

b) I dati specifici della rete devono essere inseriti nel server DHCP esterno. I parametri si trovano in `/var/log/OPTI.txt`.

---

9) Se si desidera utilizzare il server DHCP Linux, fare clic su **Sì** per abilitare e configurare il server DHCP Linux.

10) Inserire i seguenti valori (preimpostati con valori predefiniti):

- **Instradamento predefinito**: l'indirizzo IP del gateway predefinito; come regola, l'indirizzo IP del router Internet, ad esempio `192.168.5.1`.
- **Dominio** (opzionale): il dominio specificato durante l'installazione di Linux, ad esempio `<cliente>.com`
- **Server DNS** (opzionale): l'indirizzo IP del server DNS specificato durante l'installazione di Linux. Se nella rete interna non è disponibile nessun server DNS, inserire qui l'indirizzo IP del router Internet (ad esempio, `192.168.5.1`).
- **Server SNTP**: indirizzo IP del server NTP interno o esterno.
- **Server DLS/DLI**: l'indirizzo IP del server DLS, ovvero l'indirizzo IP del server Linux (ad esempio, `192.168.5.10`).
- **Sottorete**: sottorete appropriata per l'intervallo di indirizzi IP, ad esempio: `192.168.5.0`.
- **Maschera di rete**: la maschera di sottorete del server Linux specificata durante l'installazione di Linux, ad esempio: `255.255.255.0`.
- **Inizio intervallo IP** e **Fine intervallo IP**: l'intervallo di indirizzi IP dal quale il server DHCP può assegnare gli indirizzi IP, ad esempio: da `192.168.5.100` a `192.168.5.254`.

11) Fare clic su **Continua**.

12) Dopo l'installazione, è necessario riavviare il sistema operativo Linux. Selezionare la casella di controllo **Riavvio PC** e confermare con **Continua**.

13) Se è necessario installare ulteriori pacchetti RPM, verrà chiesto di inserire il DVD SLES 12 o la chiavetta USB SLES 15. Inserire il DVD o la chiavetta USB e confermare con **Continua**. Dopo aver installato correttamente i

pacchetti RPM, reinserire il DVD o il file .ISO di OpenScape Business e confermare con **Continua**, seguito da **Esegui**.

14) Il software di comunicazione OpenScape Business viene installato. Il sistema operativo esegue automaticamente un riavvio.

15) Dopo il riavvio, accedere con l'account utente configurato in precedenza durante l'installazione di Linux.

16) Fare clic con il tasto destro del mouse sull'icona dell'unità DVD sul desktop e selezionare la voce di menu **Espelli**. Rimuovere il DVD di OpenScape Business dall'unità DVD.

Nota: Sono necessari alcuni minuti prima che tutti i componenti del software di comunicazione OpenScape Business siano attivi.

7.4.2 Configurazione dell'UC Booster Server

Durante la configurazione vengono definite le impostazioni fondamentali per l'uso dell'UC Booster Server.

La configurazione dell'UC Booster Server viene eseguita con la procedura guidata **Configurazione di base** del WBM del sistema di comunicazione. Per la descrizione della configurazione, vedere il capitolo Installazione iniziale di OpenScape Business X.

La procedura guidata **Configurazione di base** del WBM comprende la configurazione iniziale dell'intero sistema di comunicazione. Per l'uso dell'OpenScape Business UC Booster Server, sono necessarie le seguenti sezioni:

- Scelta della soluzione UC

  È possibile scegliere se utilizzare la soluzione UC Smart o UC Suite. A tal fine, è necessario inserire anche l'indirizzo IP del server Linux.

  La modifica della soluzione UC determina il riavvio del sistema di comunicazione.

Inoltre nel WBM dell'UC Booster Server occorre inserire l'indirizzo IP del sistema di comunicazione.

7.4.2.1 Comunicazione dell'indirizzo IP del sistema di comunicazione

Prerequisiti

L'UC Booster Server è integrato nella LAN del cliente ed è operativo.

Il sistema di comunicazione OpenScape Business è pronto all'uso.

Passo a passo

1) Sul PC Linux, avviare il browser Web e richiamare il WBM del server OpenScape Business al seguente indirizzo:

`https ://<indirizzo IP del server Linux>`, ad es. `https://192.168.1.10`

2) Se il browser Web segnala un problema con un certificato di sicurezza, installare il certificato (nell'esempio Internet Explorer V10).

a) Chiudere il browser Web.

b) Aprire il browser Web con i diritti di amministratore facendo clic con il pulsante destro del mouse sull'icona del browser, quindi nel menu di scelta rapida selezionare la voce **Esegui come amministratore**.

c) Consentire il controllo dell'ID utente.

d) Richiamare il WBM del server OpenScape Business al seguente indirizzo:

`https ://<indirizzo IP del server Linux>`, ad es. `https://192.168.1.10`

e) fare clic su **Continua caricamento del sito Web**.

f) Fare clic sul messaggio **Errore certificato** nella barra di navigazione del browser Web.

g) Fare clic su **Mostra certificati**.

h) Fare clic su **Installa certificato** (visibile solo con i privilegi di amministratore).

i) Selezionare l'opzione **Computer locale** e confermare con **Avanti**.

j) Selezionare l'opzione **Salva tutti i certificati nella seguente memoria**, fare clic su **Ricerca** e immettere le **Autorità di certificazione radice attendibili**.

k) Confermare con **OK** e successivamente con **Avanti** e **Fine**.

l) Confermare l'importazione del certificato con **OK** e chiudere la finestra del certificato con **OK**.

m) Chiudere il browser Web.

n) Avviare di nuovo il browser Web (senza i diritti di amministratore) e richiamare il WBM del server OpenScape Business al seguente indirizzo:

`https ://<indirizzo IP del server Linux>`, ad es. `https://192.168.1.10`

3) In alto a destra, fare clic sul codice della lingua e dal menu selezionare la lingua in cui deve essere visualizzata l'interfaccia del WBM. La pagina di registrazione viene visualizzata nella lingua desiderata.

4) Nel primo campo in **Accesso** immettere il nome utente predefinito `administrator@system` per accedere come amministratore.

Nota: Se si digita il termine `administrator` nel campo **Password**, il sistema completa automaticamente la stringa con `@system`.

---

5) Nel secondo campo in **Accesso** immettere la password predefinita, `administrator`, per l'accesso come amministratore.

6) Fare clic su **Accesso**.

7) I seguenti passaggi sono necessari solo una volta al primo accesso al WBM:

a) Nel campo **Password** immettere ancora la password predefinita, `administrator`.

b) Per proteggere il sistema dall'uso improprio, nei campi **Nuova password** e **Conferma nuova password** immettere la nuova password. Prestare attenzione alle lettere maiuscole e minuscole e allo

stato dei tasti `Num`e `CapsLock` (tasto bloc maiusc) La password viene visualizzata come una serie di asterischi (*).

Nota: Tale password deve essere di almeno 8 caratteri e contenere un numero. Annotarsi esattamente la nuova password.

c) Fare clic su **Accesso**.
d) Selezionare la data corrente e inserire l'ora corretta.
e) Fare clic su **OK & Avanti**. Si viene automaticamente disconnessi dal WBM.
f) Nel primo campo in **Accesso** immettere il nome utente predefinito `administrator@system` per accedere come amministratore.

Nota: Se si digita il termine `administrator` nel campo **Password**, il sistema completa automaticamente la stringa con `@system`.

g) Nel secondo campo in **Accesso** immettere la nuova password definita per l'accesso come amministratore.
h) Fare clic su **Accesso**. Viene visualizzata la pagina iniziale di WBM.
i) Nella barra di navigazione fare clic su **Amministratori**.
j) Nell'**Elenco amministratori**, selezionare la casella di controllo prima della voce di elenco **Amministratore**.
k) Fare clic su **Modifica**.
l) Nell'elenco a discesa **Funzione utente**, selezionare il profilo utente **Expert**.
m) Fare clic su **OK & Avanti**.
n) Disconnettersi dal WBM utilizzando il collegamento **Disconnetti**.
o) Accedere nuovamente al WBM con il nome utente predefinito `administrator@system` e la password precedentemente impostata.

8) Nella barra di navigazione fare clic su **Modalità esperti**.
9) Nella struttura di navigazione fare clic su **Manutenzione** > **Configurazione**.
10) Nella scheda **Modifica indirizzo IP gateway** , in **Indirizzo IP gateway**, inserire l'indirizzo IP del sistema di comunicazione, ad esempio `192.168.1.2`.
11) Fare clic su **Applica**.

7.4.3 Aggiornamento software per l'UC Booster Server

Per l'uso corretto dell'UC Booster Server, il software del sistema di comunicazione e il software di comunicazione dell'UC Booster Server devono essere aggiornati alla stessa versione software.

Se il software del sistema di comunicazione è già aggiornato, sarà necessario aggiornare solo il software dell'UC Booster Server.

L'aggiornamento del software può essere eseguito tramite Internet o tramite un file immagine disponibile sul Software Download Server. Quando si aggiorna l'UC Booster Server tramite un file immagine, occorre assicurarsi che venga utilizzato il file immagine che contiene la sezione UC Booster Server (osbiz..._pcx.tar).

7.5 Configurazione base

Durante la configurazione di base vengono definite le principali impostazioni per l'uso di OpenScape Business UC Booster.

Sia per la UC Booster Card che per l'UC Booster Server, la configurazione di base viene eseguita mediante la procedura guidata **Installazione di base** del WBM del sistema di comunicazione. Per la descrizione della configurazione di base, vedere il capitolo Installazione iniziale di OpenScape Business X.

La configurazione di base comprende la configurazione iniziale dell'intero sistema di comunicazione. Per l'uso di OpenScape Business UC Booster, sono necessarie le seguenti parti:

- Dati dell'utente

  I numeri speciali necessari per l'uso di OpenScape Business UC Booster possono essere modificati. Qui è necessario specificare ad esempio il numero di telefono indicato nella casella vocale della UC Suite (VoiceMail).
- Configurazione della UC Booster Card

  Se una UC Booster Card è integrata nel sistema di comunicazione, deve essere avviata la configurazione automatica della stessa.
- Impostazioni della conferenza Incontro

  Con OpenScape Business UC Booster è disponibile la funzione Conferenza Incontro. Il numero di telefono pre-assegnato e il numero di accesso pre-assegnato per la conferenza Incontro possono essere modificati.

7.6 Attività finali

Una volta conclusa l'installazione iniziale e l'installazione di base eseguita con il WBM, è necessario eseguire ancora alcune importanti impostazioni per l'uso di OpenScape Business UC Booster.

Sia per la UC Booster Card che per l'UC Booster Server, le ultime operazioni vengono eseguite mediante il WBM del sistema di comunicazione. La descrizione delle ultime operazioni è disponibile nella guida in linea o nella documentazione per l'amministratore di OpenScape Business, al capitolo Installazione iniziale di OpenScape Business X.

Per l'uso di OpenScape Business UC Booster è importante eseguire le seguenti operazioni finali:

- Attivazione e assegnazione licenze

  Se OpenScape Business UC Booster viene integrato in un sistema di comunicazione già in licenza, le licenze devono essere attivate immediatamente per utilizzare le sue funzionalità. Se OpenScape Business UC Booster viene integrato in un sistema di comunicazione non ancora concesso in licenza, le licenze devono essere attivate entro un periodo di 30 giorni. Dopo l'attivazione, le licenze devono essere assegnate agli utenti. In un sistema indipendente, le funzioni a livello di sistema sono già automaticamente abilitate all'attivazione.
- Preparare i client UC all'installazione

  I client UC sono componenti della UC Suite. I file di installazione per i client UC sono accessibili tramite il WBM e possono essere messi a disposizione degli utenti IP in modo automatico o manuale.

- Esecuzione del backup dei dati

  Le modifiche apportate a OpenScape Business devono essere salvate. Per il backup può essere memorizzato ad esempio su un supporto USB un set di backup.

  Con la UC Booster Card, è sufficiente eseguire un backup del sistema di comunicazione. Nell'UC Booster Server devono essere salvati separatamente i dati del sistema di comunicazione e i dati del software di comunicazione dell'UC Booster Server.

7.7 Disinstallazione del software di comunicazione

Per la disinstallazione del software di comunicazione viene utilizzata una console di tipo testuale.

7.7.1 Come disinstallare il software di comunicazione

Passo a passo

1) Aprire un terminale (ad esempio, terminale GNOME).
2) Inserire nell'interfaccia shell il comando `su` (a indicare superuser = utente root) e confermare con Invio.
3) Inserire nell'interfaccia shell la password per l'utente "root" e confermare con Invio.
4) Inserire nell'interfaccia shell il comando `oso_deinstall.sh` e confermare con Invio. Seguire le istruzioni fornite dal programma di disinstallazione.

7.8 Aggiornamento da UC Booster Card a UC Booster Server

Per eseguire l'aggiornamento da un sistema di comunicazione OpenScape Business con UC Booster Card integrata a un sistema di comunicazione collegato a un UC Booster Server, occorre attenersi alla seguente procedura.

Procedura di aggiornamento

Eseguire i seguenti passaggi nell'ordine indicato:

1) **Backup dei dati di configurazione**

   Eseguire un backup dei dati di configurazione del sistema di comunicazione.

   Per la descrizione della procedura di backup, vedere Backup dei dati di configurazione del sistema di comunicazione.
2) **Modifica dell'indirizzo IP della UC Booster Card**

   Nel WBM del sistema di comunicazione, modificare con la procedura guidata **Configurazione di base** l'indirizzo IP della UC Booster Card indicando un indirizzo IP non utilizzato. Il collegamento ai client UC viene interrotto.

   Per la descrizione dell'indirizzamento IP, vedere Impostazioni di sistema .

3) **Modifica della scelta dell'applicazione**

   Utilizzando UC Suite, nel WBM del sistema di comunicazione, modificare con la procedura guidata **Prima installazione**la selezione dell'applicazione da **Pacchetto con UC Suite** a **Pacchetto con UC Suite su OSBiz UC Booster Server**; se si utilizza UC Smart, modificare la selezione dell'applicazione da **Pacchetto con UC Smart** a **Pacchetto con UC Smart su OSBiz UC Booster Server**) e inserire l'indirizzo IP dell'UC Booster Card come indirizzo IP dell'UC Booster Server.

   Per la descrizione della scelta applicazione, vedere Soluzione UC.

4) **Installazione del server Linux**

   Sul server Linux deve essere installato il sistema operativo Linux approvato per l'UC Booster Server.

   Per la descrizione dell'installazione di Linux, vedere le istruzioni di installazione del server Linux di OpenScape Business.

5) **Modifica dell'indirizzo IP dell'UC Booster Server**

   Per l'indirizzo IP dell'UC Booster Server (= indirizzo IP del server Linux), è necessario indicare l'indirizzo IP originario della UC Booster Card. L'indirizzo IP del server Linux può essere inserito durante l'installazione del sistema operativo Linux o successivamente tramite YaST.

   Per la descrizione dell'assegnazione degli indirizzi IP durante l'installazione di Linux, vedere le istruzioni di installazione del server Linux.

6) **Installazione del software di comunicazione**

   Sul server Linux deve essere installato il software di comunicazione OpenScape Business.

   Per la descrizione dell'installazione del sistema di comunicazione, vedere Installazione del software di comunicazione.

7) **Configurazione dell'UC Booster Server**

   Nel WBM dell'UC Booster Server, inserire l'indirizzo IP del sistema di comunicazione.

   Per la descrizione dell'assegnazione degli indirizzi IP del sistema di comunicazione, vedere Configurazione dell'UC Booster Server.

8) **Riavvio del software di comunicazione**

   Nel WBM dell'UC Booster Server riavviare il software di comunicazione dell'UC Booster Server.

   Per la descrizione del riavvio, vedere Riavvio dell'applicazione UC .

9) **Aggiornamento del software**

   Il software del sistema di comunicazione e dell'UC Booster Server deve essere aggiornato all'ultima versione.

   Per la descrizione dell'aggiornamento del software, vedere Aggiornamenti.

10) **Ripristino dei dati di configurazione**

    Nel WBM del sistema di configurazione, importare il backup dei dati di configurazione del sistema di comunicazione. Successivamente, il sistema di comunicazione e il software di comunicazione si riavviano. Il collegamento ai client UC Suite viene ripristinato.

    Per la descrizione del ripristino dei dati, vedere Ripristino.

7.9 Porte usate

I componenti del sistema OpenScape Business utilizzano porte diverse, che potrebbero dover essere aperte nel firewall in base alle necessità. Per le porte dei client basati sul Web (ad esempio, myPortal to go), è necessario configurare l'inoltro delle porte nel router.

L'elenco completo di tutte le porte utilizzate da OpenScape Business è disponibile nel "Database di gestione delle interfacce" (IFMD), accessibile tramite il Portale partner di Unify (https://unify.com/en/partners/partner-portal.

Nota: Le porte identificate nell'elenco seguente con "O" sono opzionali, cioè non sono aperte in modo permanente nel firewall.

Descrizione	TCP	UDP	Numero di porta	OpenScape Business X	Scheda UC Booster	OpenScape Business S	Server UC Booster
Componenti del sistema							
Portale di amministrazione (https)	X		443	X	X	X	X
Verifiche CAR Alive	X		12062	X		X	
CLA	X		61740	A		A	A
CLA Auto Discovery		X	23232	X		X	X
CLS	X		7780, 7790 (fino alla versione V3R3) 7780, 7791 (dalla versione V3R3.1 in poi)	A		A	
Programma di installazione del client di comunicazione	X		8101	X	X	X	X
Csta Message Dispatcher (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	
Csta Service Provider (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	A		A	
FTP Passive	X		40000-40040	A		A	
HFA	X		4060	X		X	

Descrizione	TCP	UDP	Numero di porta	OpenScape Business X	Scheda UC Booster	OpenScape Business S	Server UC Booster
HFA Secure	X		4061	X		X	
Messaggistica istantanea (http)	X		8101	X	X	X	X
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS Cloud Service	X		8602	X			
Server LDAP	X		389		X	X	X
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
NAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
Openfire Admin (https)	X		9091		X	X	X
OpenScape Business Auto Update Service (http)	X		8101	X	X	X	X
OpenScape Business Multisite	X		8778		X	X	X
OpenScape Business myReports (http)	X		8101		X	X	X
Server stato OpenScape Business	X		8808	X		X	X
Portale utenti OpenScape Business	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (integrato)		X	29100-30530	X	X	X	X
RTP (server)		X	29100-30888	X	X	X	X
SIP (server)	X	X	5060	X		X	
SIP TLS SIPQ (server)	X		5061	X		X	
SIP TLS Subscriber (server)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (traps)		X	162	X		X	
VSL	X		8770-8780		X	X	X
Webadmin per client	X		8803	X	X	X	X
Client basati sul Web							
Client basati sul Web (http)	X		8801	X	X	X	X

Descrizione	TCP	UDP	Numero di porta	OpenScape Business X	Scheda UC Booster	OpenScape Business S	Server UC Booster
Client basati sul Web (https)	X		8802	X	X	X	X

Nota: Per motivi di sicurezza, si consiglia di utilizzare solo https per i client basati sul Web e di impostare l'inoltro delle porte da TCP/443 esterno a TCP/8802 interno.

Certificato CLS

A partire dalla V3R3.1, viene fornito un nuovo certificato CLS con un nome comune (CN) aggiornato tramite una porta di nuova introduzione. Ciò offre un algoritmo digest migliorato e più forte, nonché entità legali aggiornate. I sistemi con licenza online tramite la modalità CLS Connect richiedono i seguenti due prerequisiti:

- L'indirizzo IP 188.64.16.4 è abilitato per il traffico in uscita nel firewall.
- Le porte 7780 e 7791 sono abilitate per il traffico in uscita nel firewall.

La porta 7790 usata in precedenza può essere rimossa dalla configurazione del firewall dopo l'aggiornamento alla V3R3.1 per aumentare la sicurezza.

8 Concessione della licenza

Il concetto di flessibilità di licenza su cui è basato OpenScape Business offre ai clienti aziendali la possibilità di personalizzare l'ambito funzionale del software in base alle proprie esigenze tramite le licenze. Tutti i sistemi di comunicazione OpenScape Business X e OpenScape Business S sono soggetti a questo concetto di licenza. Telefoni, client UC, funzioni UC e servizi a livello di sistema possono essere attivati in funzione delle esigenze specifiche dei clienti. Per tutti i sistemi di comunicazione OpenScape Business vengono utilizzate licenze uniformi.

Se in un secondo momento occorre espandere OpenScape Business o dotarlo di altre funzionalità, ciò è possibile acquistando licenze aggiuntive.

Tutte le licenze sono sempre legate alla licenza di base del sistema di comunicazione e consentono l'uso delle funzionalità acquistate per la versione associata di OpenScape Business.

Al fine di testare o valutare funzioni particolari, il cliente può acquistare una licenza dimostrativa valevole per 90 giorni.

Nota: Si consiglia di non installare file di licenza o eseguire alcuna procedura guidata se il sistema è attivo, in quanto è possibile che le chiamate attive vengano interrotte.

Periodo di attivazione

L'attivazione della licenza deve avvenire entro il periodo di attivazione (30 giorni). Il periodo di attivazione decorre da quando si inserisce la data corrente nel WBM. In questo momento viene salvata la data di scadenza del periodo di attivazione.

Il prodotto è completamente funzionale durante il periodo di attivazione ed è disponibile il numero massimo di licenze consentito.

Se durante il periodo di attivazione si cancella la data corrente nel sistema (ad esempio a causa della batteria scarica sulla scheda madre), occorre aggiornare tempestivamente la data nel WBM, per poter utilizzare senza limitazioni il sistema durante il periodo di attivazione.

Se alla scadenza del periodo di attivazione non è stata attivata alcuna licenza, il sistema di comunicazione è utilizzabile solo in modo molto limitato. La comunicazione interna tra gli utenti continua a essere possibile, ma solo i primi due telefoni attivi possono effettuare chiamate esterne (ad esempio per chiamate di emergenza). L'accesso al sistema di comunicazione attraverso l'accesso remoto è ancora possibile. Il sistema rimane in questo stato limitato anche quando l'installazione iniziale è stata effettuata con Manager E, in quanto ciò non avvia il periodo di attivazione.

Struttura delle licenze

Le licenze per il sistema di comunicazione sono strutturate come segue:

- Una licenza di base attiva il software del sistema di comunicazione in modo permanente ed è requisito essenziale per l'attivazione di tutte le altre licenze.
- Licenze apparecchio per l'attivazione dei telefoni per la comunicazione voce con l'esterno.

- Licenze orientate all'utente per l'attivazione di funzioni specifiche per un utente.
- Licenze di sistema per attivare le funzioni generali a livello di sistema.

Migrazione

Per i clienti HiPath 3000 V9 esistenti la migrazione della licenza può avvenire mediante una licenza di upgrade. La migrazione della licenza assicura ai clienti una protezione dell'investimento per l'uso continuato di telefoni e funzioni vocali.

Nota: Per informazioni relative alle licenze e all'aggiornamento o alla migrazione dei sistemi in una rete, vedere la sezione **Rete - Licenze** al capitolo Aggiornamenti.

Concetti correlati

Utenti alla pagina 419

8.1 Procedura per la concessione della licenza

Per la concessione della licenza è disponibile una procedura centralizzata per la gestione licenza, OpenScape License Management, che consente di gestire e attivare le licenze. Ciò assicura che un cliente possa utilizzare la configurazione del sistema e i servizi per i quali ha acquistato le licenze (diritti d'uso).

Le licenze dei sistemi di comunicazione OpenScape Business sono legate al locking ID o all'Advanced Locking ID del sistema di comunicazione (vedere Locking ID e Advanced ID Locking).

Il cliente ordina le funzioni desiderate e riceve una chiave di attivazione della licenza (LAC). Dopo la prima installazione del sistema di comunicazione, il cliente attiva le licenze acquistate utilizzando un file di licenza. Il file di licenza fornisce al sistema un pool di licenze con tutte le licenze acquistate per la successiva assegnazione.

Il WBM offre funzionalità con procedura guidata per la registrazione di clienti, l'attivazione e l'assegnazione delle licenze per sistemi indipendenti e sistemi appartenenti a un sistema di reti OpenScape Business. Non è possibile gestire le licenze con Manager E.

Passaggi richiesti per la concessione delle licenze

1) Configurazione del sistema all'interno del periodo di attivazione
2) Registrazione dei dati cliente
3) Attivazione della licenza
4) Assegnazione della licenza

Registrazione clienti

Nel contesto della concessione delle licenze, è obbligatoria la registrazione dei clienti e l'inserimento dei dati dei clienti di ciascun sistema. I dati del cliente vengono utilizzati per informare rapidamente lo stesso in caso di problemi legati alla sicurezza e in particolare eventuali richiami dei prodotti. Inoltre, i clienti ricevono informazioni sulla protezione dall'uso improprio delle licenze da parte di terzi, ad esempio nuovi collegamenti alle informazioni di licenza.

Attivazione della licenza

Con l'attivazione delle licenze, utilizzando la sezione Gestione delle licenze del WBM, le licenze acquistate vengono associate al sistema di comunicazione. A tal fine sono disponibili 2 metodi:

- Attivazione online

  Durante l'attivazione online, dopo l'inserimento del LAC viene realizzata una connessione al server licenze centrale (Central License Server, CLS) tramite Internet e il file della licenza viene automaticamente integrato nell'agente licenze del sistema di comunicazione (Customer License Agent, CLA). Successivamente, le licenze vengono attivate automaticamente.
- Attivazione non in linea

  Durante l'attivazione offline non vi è alcuna connessione del sistema di comunicazione con il server licenze centrale (License Server Centrale, CLS). Il file di licenza viene generato da un partner autorizzato nel CLS durante l'attivazione delle licenze e deve essere trasferito manualmente all'agente delle licenze (Customer License Agent, CLA) integrato nel sistema di comunicazione.

Assegnazione della licenza

Tramite la gestione delle licenze del WBM, tutte le licenze acquistate sono assegnate all'utente in modo permanente.

Per poter assegnare le licenze agli utenti, è necessario prima configurare gli utenti con il WBM durante l'installazione iniziale. Ogni configurazione del sistema può essere configurata in modo indipendente dalle licenze esistenti. Tuttavia, la corrispondente funzione può essere utilizzata solo dopo l'assegnazione della licenza.

Esistono due tipi assegnazione delle licenze: la configurazione e l'assegnazione vera e propria. Per le licenze apparecchio e orientate all'utente, vengono configurate le richieste di licenza. Se per una richiesta di licenza è disponibile una licenza del pool, la funzione corrispondente viene attivata. Se nel pool di licenze non è disponibile alcuna licenza, la richiesta di licenza configurata viene mantenuta, ma la funzione corrispondente non viene attivata. Le licenze eventualmente mancanti devono essere acquistate.

Concessione della licenza nel sistema di reti

Per un sistema di reti OpenScape Business viene generato nel server delle licenze centrale (CLS) un file di licenza a livello di rete (file di licenza di rete) da un partner autorizzato. Questo file di licenza a livello di rete viene gestito dall'agente delle licenze centrale (CLA) del nodo master e mette a disposizione le licenze ai singoli nodi. L'assegnazione delle licenze viene eseguita tramite il WBM di ogni singolo nodo. All'interno di un sistema di reti, le licenze possono essere trasferite utilizzando il WBM.

Per la concessione della licenza di un sistema di reti, l'attivazione online non è possibile.

Pagamento a consumo

Oltre al tradizionale schema di licenza, OpenScape Business supporta il modello di licenza in abbonamento (Pay As You Go). "Pay As You Go" offre l'opportunità di fatturare solo le licenze utilizzate in ogni periodo di fatturazione e utilizzare licenze extra senza estendere il file di licenza. Non è necessario decidere in anticipo il numero delle licenze

È necessaria una connessione Internet permanente dal sistema OpenScape Business al server centrale delle licenze (CLS). Può essere attivato online con un codice di attivazione della licenza (LAC) o con caricamento di file. Dopo l'installazione, la configurazione della soluzione secondo le esigenze personalizzate e l'attivazione del "Pay As You Go" viene inviato un report periodico delle licenze utilizzate al server centrale delle licenze (CLS) e valutato. Una volta al mese, viene creato un report finale sul sito dei prodotti del server centrale delle licenze (CLS) e il contenuto delle licenze utilizzate di questo report finale viene utilizzato per la contabilità delle licenze.

Con la licenza in abbonamento viene introdotto un nuovo periodo di tempo: il periodo di qualificazione. Il periodo di qualificazione inizia con l'avvio del sistema o se viene attivato un file di licenza "Pay As You Go". Il periodo inizia consecutivamente e durante questo periodo una configurazione della licenza eseguita in WBM non porterà all'aggiornamento dell'utilizzo della licenza. La durata massima del periodo di qualificazione è di 2 ore.

Nota: Affinché il firewall abbia accesso al CLS sono necessarie le seguenti azioni:-

- Porta 7790 per il traffico IP in uscita rilasciata

- Indirizzo 188.64.16.4 per il traffico IP in uscita rilasciato

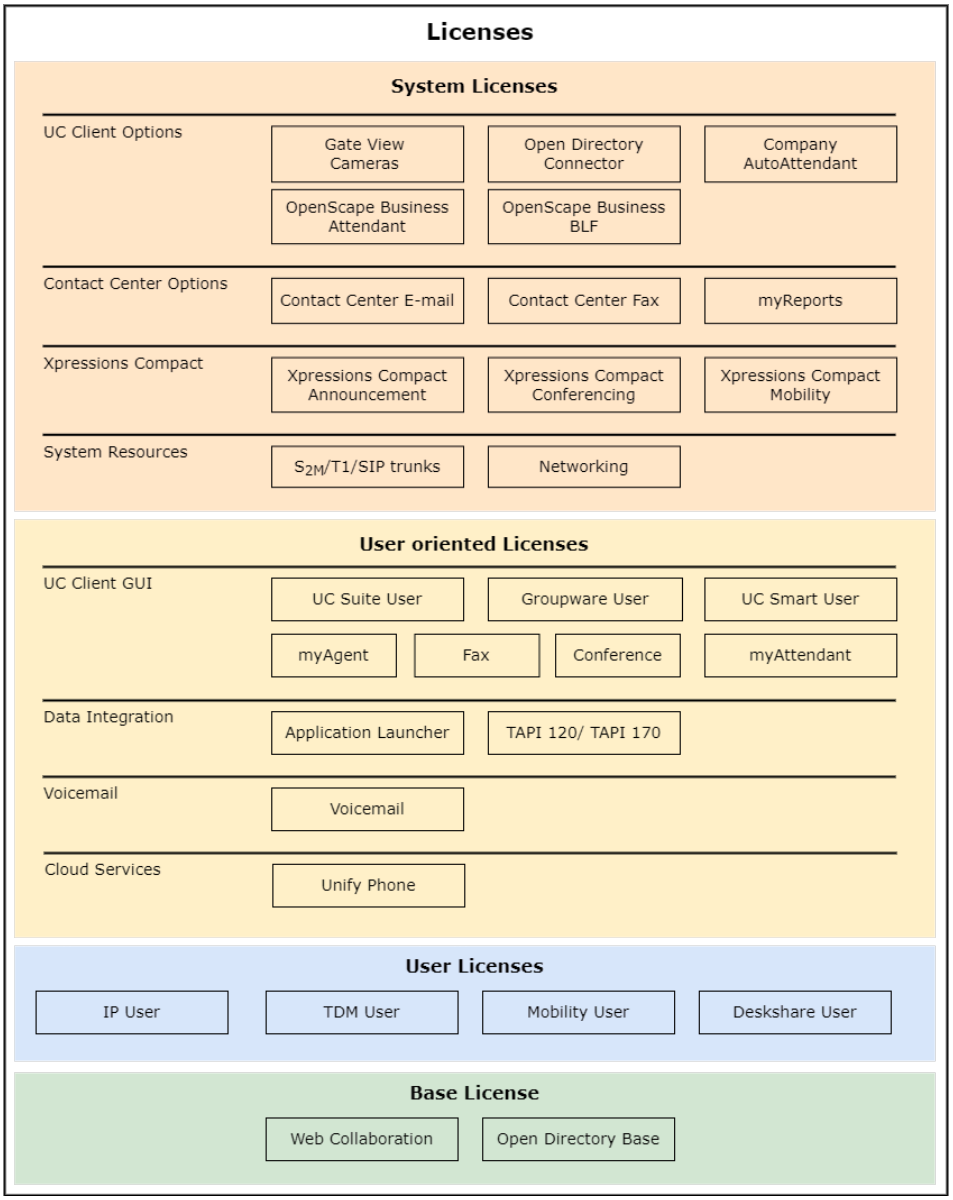
I sistemi software V3R3 più recenti utilizzano la porta 7791 per l'attivazione della licenza online.

8.2 Licenze

Per utilizzare le funzioni del sistema di comunicazione, occorre acquistare le licenze. Le licenze acquistate devono essere attivate entro un certo periodo di tempo (periodo di attivazione).

Le licenze sono raggruppate tematicamente per gruppi di licenze. Sono disponibili i seguenti gruppi di licenze:

- Licenze base
- Licenze apparecchio
- Licenze orientate all'utente
- Licenze di sistema



Le licenze sopra indicate possono essere usate per OpenScape Business X, OpenScape Business S e OpenScape Business UC Booster Server. L'UC Booster Server non dispone di una licenza base. Le licenze coprono tutte le funzioni e possono essere organizzate in base alle esigenze del cliente. Le possibili combinazioni di licenze sono descritte nella sezione Assegnazione delle licenze e dei profili licenza.

Le licenze apparecchio e le licenze orientate all'utente vengono assegnate permanentemente agli utenti.

8.2.1 Licenza di base

La licenza base consente l'uso generale del sistema di comunicazione ed è requisito essenziale per l'attivazione di tutte le altre licenze.

La telefonia Internet e il servizio d'emergenza possono essere utilizzati anche senza licenza di base.

Sono disponibili le seguenti licenze base:

- **OpenScape Business V2 X1 Base**

  Per sbloccare la funzionalità V2 di

  – OpenScape Business X1

  La licenza di base contiene anche le licenze OpenDirectory base per l'uso di Open Directory Service (ODS) e Web Collaboration per avviare una sessione di Web Collaboration. In questo modo, la soluzione di comunicazione unificata UC Smart posso essere collegata con un database esterno.
- **OpenScape Business V2 Base**

  Per sbloccare la funzionalità V2 di

  – OpenScape Business X3/X5/X8 con o senza UC Booster (UC Booster Card o UC Booster Server) o
  – OpenScape Business S

  La licenza di base contiene anche la licenza OpenDirectory base per l'uso di Open Directory Service (ODS) e Web Collaboration per avviare una sessione di Web Collaboration. In questo modo, le soluzioni UC UC Suite o UC Smart possono essere collegati con un database esterno.

8.2.2 Licenze utente

Ogni utente collegato al sistema di comunicazione necessità di una licenza utente per la telefonia esterna. Questa licenza viene assegnata in modo permanente al numero di telefono dell'utente tramite WBM.

Le licenze degli utenti includono tutte le funzionalità vocali di OpenScape Business. Per l'utilizzo delle soluzioni UC Smart o UC Suite sono necessarie ulteriori licenze (vedere Licenze orientate all'utente).

Sono disponibili le seguenti licenze apparecchio:

- **Utente IP**

  Per l'uso di telefoni di sistema IP (HFA) e di telefoni SIP.
- **Utente TDM**

  Per l'uso di telefoni di sistema UP0, telefoni analogici, fax analogico, telefoni ISDN, fax ISDN e telefoni DECT.
- **Utente Mobility**

  Per l'uso di telefoni GSM/cellulari, smartphone e PC tablet come interni del sistema di comunicazione. Per l'utilizzo di myPortal to go e Mobility Entry. L'assegnazione di un telefono da scrivania aggiuntivo non è necessaria. In combinazione con OpenScape Business, per utilizzare il client Unify Phone.
- **Utente DeskShare**

  Per l'uso della funzione DeskSharing. A questo utente viene assegnato solo un numero di telefono e nessun telefono fisico. L'utente può utilizzare telefoni IP di sistema specifici con il proprio numero di telefono e su questi telefono ha accesso alle proprie impostazioni telefoniche personali.
- **Utente fallback**

  Per l'utilizzo della telefonia di base in caso di guasto di un nodo del sistema. La licenza è supportata come licenza basata su consumo e tempo. Pertanto,

il tempo di utilizzo viene calcolato in base ai giorni in cui il sistema ospita utenti da altri nodi. Le licenze sono effettive esclusivamente durante questo tempo di hosting. In una modalità di funzionamento normale, gli utenti secondari sono considerati utenti senza licenza.

Attivazione delle licenze utente flessibile

Grazie alla flessibilità del sistema di assegnazione delle licenze agli utenti, gli utenti TDM, Mobility e DeskShare possono utilizzare anche licenze Utente IP. Se agli utenti sono già state assegnate tutte le licenze utente TDM, DeskShare e Mobility e sussiste la necessità di altri utenti TDM, DeskShare e Mobility, è possibile utilizzare licenze Utente IP per coprire questa necessità.

Per l'attivazione flessibile delle licenze utente è necessaria la versione software V1R3.3 e un file di licenza generato di nuovo dal CLS che deve essere importato e attivato in OpenScape Business.

Attivazione delle licenze utente flessibile per UC Suite

Grazie alla flessibilità del sistema di assegnazione delle licenze agli utenti UC Suite, gli utenti myPortal for Desktop possono utilizzare anche licenze utente myPortal for Outlook. Se sono già state assegnate tutte le licenze utente myPortal for Desktop e sussiste la necessità di altri utenti, è possibile utilizzare licenze utente myPortal for Outlook per coprire questa necessità.

Per l'attivazione flessibile delle licenze utente è necessaria la versione software V2 e un file di licenza generato di nuovo dal CLS che deve essere installato e attivato in OpenScape Business.

8.2.3 Licenze orientate all'utente

Le licenze orientate all'utente sono basate sugli apparecchi e autorizzate all'uso delle funzioni di comunicazione unificata e di applicazioni per l'integrazione dei dati. Una licenza orientata all'utente richiede sempre una licenza apparecchio ed è assegnata in modo permanente al numero dell'utente.

Sono disponibili le seguenti licenze orientate all'utente:

Casella vocale

- **Casella vocale**

  Per l'uso di una casella vocale personale tramite telefono (TUI) e tramite l'interfaccia della soluzione UC UC Smart o UC Suite.

  Nota: Se la soluzione UC UC Smart viene ampliata in UC Suite, vengono mantenute le licenze per casella vocale e l'assegnazione agli utenti.

  Nota: Quando si assegna una licenza Casella vocale a un interno, viene creato un utente UC Suite e tutti gli inoltri di chiamata attivi vengono reimpostati.

Servizi cloud

- **Unify Phone**

  Per l'utilizzo del client Unify Phone in combinazione con OpenScape Business.

Interfaccia utente client UC

- **Utente UC Smart**

  Per l'utilizzo delle funzioni UC Smart dei client di comunicazione myPortal @work, myPortal to go e altri client Web Service.
- **Utente UC Suite**

  Per l'utilizzo delle funzioni UC Suite dei client di comunicazione myPortal @work, myPortal for Desktop, myPortal to go e altri client Web Service.
- **Utente Groupware**

  Per l'utilizzo delle funzioni UC Smart dei client di comunicazione myPortal @work, myPortal for Outlook, myPortal to go e altri client Web Service.
- **Fax**

  Per l'uso di una casella fax nella UC Suite. È richiesta inoltre una licenza Utente UC o Utente Groupware.
- **Conferenza**

  Per l'uso della gestione conferenze all'interno della UC Suite, quali ad esempio la gestione e l'avvio di conferenze permanenti e ricorrenti. È richiesta inoltre una licenza Utente UC o una licenza Utente Groupware.

  Per la partecipazione alle conferenze non è richiesta alcuna licenza.
- **myAttendant**

  Per l'utilizzo delle funzioni posto operatore della UC Suite.
- **myAgent**

  Per l'uso delle funzioni del Contact Center, quali ad esempio informazioni sulle code, finestre popup con informazioni sui clienti all'arrivo di chiamate, accesso alla cronologia chiamate.

Nota: Per il client mobile myPortal to go, oltre alla licenza Utente Mobility, è richiesta inoltre una licenza Utente UC o una licenza Utente Groupware per la soluzione UC UC Smart o per la soluzione UC UC Suite.

Integrazione dei dati

- **Application Launcher**

  Per il controllo delle applicazioni di un PC client mediante una chiamata, ad esempio con l'apertura di un'applicazione o la visualizzazione delle informazioni sul chiamante all'arrivo o all'effettuazione di una chiamata. Application Launcher può essere utilizzato con UC Smart, UC Suite o myAgent e richiede una licenza UC Suite/Utente Groupware o una licenza myAgent. Come opzione può utilizzare Open Directory Service.

- **OpenScape Business TAPI**

  Per l'uso di applicazioni TAPI compatibili e telefonia supportata da PC con programmi dei clienti di diverse case software. È richiesto UC Booster (UC Booster Card o UC Booster Server).

8.2.4 Licenze di sistema

Le licenze di sistema non sono basate sugli apparecchi e attivano le funzioni a livello di sistema. Queste funzioni possono essere utilizzate da tutti gli apparecchi del sistema di comunicazione.

Panoramica dei requisiti delle licenze di sistema

Tipo di linea	Licenza SSP	Licenze/canale della linea	Licenza per il collegamento in rete
ITSP	sì	sì	no
Linea SIP nativo	sì	no	sì
Skype for Business	sì	sì	no
Unify Phone	sì	no	no
Interconnessione SIPQ	no	no	sì

Sono disponibili le seguenti licenze di sistema.

Risorse di sistema

- **Linee S_{2M}/T1/SIP**

  Per l'uso di canali S_{2M}/T1 e ITSP. I canali S_0 non richiedono alcuna licenza. In quanto considerano anche interfacciamenti al Fax-Server S_0 in modalità PP. Per le connessioni multiplex primarie S_{2M} o T1, i singoli canali voce richiedono una licenza. Con le connessioni ITSP, la licenza è basata sul numero di connessioni contemporanee a uno o più provider ITSP (provider SIP). Il numero di connessioni simultanee consentite dipende dalla larghezza di banda delle porte.
- **Collegamento in rete**

  Per i collegamenti in rete IP tramite SIP-Q/SIP nativo e/o i collegamenti in rete TDM tramite CorNet-NQ o QSIG. Per i collegamenti in rete delle applicazioni della UC Suite. È necessaria una licenza per nodo.

  Nota: La licenza per il collegamento in rete di un nodo attiva le linee per i collegamenti voce e per il collegamento in rete della UC Suite. Per i collegamenti in rete non sono necessarie licenze per linee S_{2M}/T1/SIP.

Tabella 3: Descrizione delle licenze per le risorse di sistema (S_{2M}/ITSP)

Protocollo	Licenze			
	Nessuna licenza	Collegamento in rete di OpenScape Business (1x per sistema)	OpenScape Business S_{2M}/ITSP (1x per canale)	Utente TDM
Interno S_0				
Fax-Server (DSS1/QSIG)	X			
Bus EURO				Per utente S_0
Linee urbane S_0				
Linea urbana Euro PP	X			
Linea urbana Euro PMP	X			
Linee urbane S_{2M}				
Linea urbana Euro PP			X	
Provider ITSP				
Da 1 fino 8 ITSP			X	
Collegamento in rete S_0				
QSIG		X		
CorNet-NQ		X		
Collegamento in rete S_{2M}				
QSIG		X		
CorNet-NQ		X		
Collegamento in rete SIP				
SIP-Q		X		
SIP nativo		X		

Opzioni Contact Center

- **Posta Contact Center**

  per la configurazione di una o più caselle di posta elettronica per la ricezione e l'invio di e-mail per gli agenti del Contact Center. È richiesta una licenza apparecchio e una licenza myAgent. È necessaria una licenza per nodo.
- **Contact Center Fax**

  per la configurazione di una o più caselle fax per la ricezione e l'invio di fax per gli agenti del Contact Center. È richiesta una licenza apparecchio e una licenza myAgent. È necessaria una licenza per nodo.
- **myReports**

  Per la creazione di statistiche sull'utilizzo delle risorse del Contact Center in base a vari criteri. Con Gestione pianificazione è possibile creare oltre 100 modelli di rapporti predefiniti per rapporti su telefonate, e-mail, fax e contatti. La gestione dei modelli di rapporti viene eseguita tramite Gestione rapporti

con la possibilità di raggruppamento, aggiunta ed eliminazione dei modelli di rapporti creati.

Opzioni client UC

- **Open Directory Connector**

  Per la connessione a Open Directory Service (ODS), per poter accedere a un database esterno o a una directory esterna. È possibile collegare fino a quattro database per nodo.
- **AutoAttendant aziendale**

  Per l'uso di un AutoAttendant centrale basato su UC Smart o UC Suite per il trasferimento automatico delle chiamate. È necessaria una licenza per nodo.

  Gli annunci del tipo "musica su attesa" (continua) vengono riprodotti solo con questa licenza.
- **OpenScape Business Attendant**

  Per l'utilizzo di un PC posto operatore OpenScape Business Attendant. È possibile assegnare licenze a un massimo di 8 OpenScape Business Attendant per nodo.

  Se OpenScape Business Attendant deve poter accedere alle informazioni sullo stato presenza, è necessaria un'ulteriore licenza Utente UC.
- **OpenScape Business BLF**

  per l'utilizzo di altri display dello stato occupato OpenScape Business BLF. È richiesta una licenza BLF e una licenza Utente UC per ogni utente. È possibile assegnare licenze a un massimo di 50 OpenScape Business BLF per nodo.

8.2.5 Licenze dimostrative

Con una licenza dimostrativa è possibile testare gratuitamente funzioni specifiche entro un dato arco di tempo (periodo di valutazione), con funzionalità complete. Se durante il periodo di valutazione vengono attivate licenze regolari per la funzione, la licenza dimostrativa viene disattivata.

Sono disponibili le seguenti licenze dimostrative:

- **Valutazione OpenScape Business V3 Service**

  Questa licenza di valutazione è destinata a partner che hanno preconfigurato il sistema di comunicazione nella propria azienda e successivamente desiderano metterlo in servizio presso i clienti. Durante la preconfigurazione parte il periodo di attivazione di 30 giorni. Per consentire il riavvio del periodo di attivazione di 30 giorni dopo la messa in servizio del sistema, occorre attivare questa licenza di valutazione dopo la messa in servizio presso il cliente.

  L'attivazione è consentita una volta per sistema e solo durante il periodo di attivazione. Se il periodo di attivazione è scaduto al sistema deve essere assegnata una licenza permanente.

  Nota: Quando la valutazione del servizio è attivata, CLS connect non può essere attivato.

- **Valutazione OpenScape Business V3 UC Smart**

  Questa licenza dimostrativa è intesa per clienti che desiderano testare le funzioni UC di UC Smart. Questa licenza dimostrativa consente di utilizzare tutti i servizi di UC Smart.

  Nota: Questa licenza di valutazione non può essere utilizzata se il sistema di comunicazione fa parte di un sistema di reti e se è attiva la licenza "Rete". Se le licenze Voicemail sono già disponibili, queste vengono utilizzate in combinazione con le nuove licenze di valutazione UC.

- **Valutazione di OpenScape Business V3 UC Suite**

  Questa licenza dimostrativa è intesa per clienti che desiderano testare le funzioni UC di UC Suite. Questa licenza dimostrativa consente di utilizzare tutte le funzioni di UC Suite.

  Nota: Questa licenza di valutazione non può essere utilizzata se il sistema di comunicazione fa parte di un sistema di reti e se è attiva la licenza "Rete". Se le licenze Voicemail sono già disponibili, queste vengono utilizzate in combinazione con le nuove licenze di valutazione UC.

- **Valutazione OpenScape Business V3 UC Suite Contact Center**

  Questa licenza dimostrativa è intesa per clienti che desiderano testare il Contact Center multimediale. Questa licenza dimostrativa consente di utilizzare tutti i servizi del Contact Center multimediale.

  Nota: Se la licenza di Contact Center multimediale non viene attivata entro di periodo di valutazione, l'amministratore deve annullare le impostazioni del Contact Center prima della scadenza della licenza dimostrativa (ad es. cancellare le pianificazioni e le code d'attesa, disattivare gli agenti ecc.), poiché altrimenti possono verificarsi malfunzionamenti di OpenScape Business.)

- **Valutazione OpenScape Business V3 CRM**

  Questa licenza dimostrativa è intesa per clienti che desiderano provare Application Launcher, Open Directory Service e TAPI.

- **Valutazione OpenScape Business V3 Attendant**

  Questa licenza dimostrativa è intesa per clienti che desiderano testare l'applicazione OpenScape Business Attendant.

- **Valutazione OpenScape Business V3 BLF**

  Questa licenza dimostrativa è intesa per clienti che desiderano testare l'applicazione OpenScape Business BLF, ad esempio per la visualizzazione dei BLF e delle informazioni sulla presenza.

Regole

- L'attivazione di una licenza dimostrativa avviene sul Customer License Server (CLS) ed è possibile una sola volta.

- Il periodo di valutazione è di 90 giorni. Dopo 60 giorni, sul display dei telefoni di sistema viene visualizzato un conto alla rovescia del tempo rimanente, espresso in giorni.
- Alla scadenza del periodo di valutazione le funzioni vengono disattivate automaticamente.
- Più licenze di valutazione possono essere attive contemporaneamente nel sistema, ma possono scadere in momenti diversi.
- Se è attiva una licenza a tempo perpetua, la licenza di valutazione non viene avviata o se già esistente, arrestata.

8.2.6 Licenze di upgrade

Le licenze di upgrade sono necessarie per aggiornare i sistemi da HiPath 3000 V9, OpenScape Office V3 e OpenScape Business V1 ai sistemi OpenScape Business V2.

Per la migrazione della licenza di sistemi HiPath 3000 è richiesto un sistema HiPath 3000 V9 in esecuzione e con licenza. I passaggi per la migrazione hardware della licenza devono essere rispettati alla lettera (vedere Migrazione). I sistemi TDM HiPath 3000 puri senza licenze devono prima essere aggiornati alla versione 9 e successivamente possono essere aggiornati a OpenScape Business con una licenza di aggiornamento.

Sono disponibili le seguenti licenze di upgrade:

- **Upgrade da HiPath 3000 V9 a OpenScape Business V2**

  Per la migrazione da HiPath 3000 V9 a OpenScape Business V2 X3/X5/X8.
- **Upgrade da HiPath 3000 V8 a OpenScape Business V2**

  Per la migrazione da HiPath 3000 V8 a HiPath 3000 V9 e successivamente a OpenScape Business V2 X3/X5/X8.
- **Upgrade da HiPath 3000 V7 a OpenScape Business V2**

  Per la migrazione da HiPath 3000 V7 a HiPath 3000 V9 e successivamente a OpenScape Business V2 X3/X5/X8.
- **Upgrade di OpenScape Office V3 MX/LX a OpenScape Business V2**

  per la migrazione da OpenScape Office V3 MX/LX a OpenScape Business V2.

8.2.7 Suggerimenti per combinazioni di licenze

Le licenze possono essere combinate in base alle proprie necessità. Di seguito sono elencati alcuni suggerimenti su come combinare in modo pratico le licenze e su come poter utilizzare le funzioni desiderate.

Occorre notare che alcune funzioni richiedono più licenze.

Telefonia

- Richiesto: licenza apparecchio Utente IP, Utente TDM o Utente DeskShare

---

Nota: Senza una licenza valida, il telefono può essere usato solo per le connessioni interne.

Telefonia con UC Smart

- Telefonia con casella vocale (UC Smart)
  - Richiesto: licenza apparecchio Utente IP, Utente TDM o Utente DeskShare
  - Richiesto: licenza orientata all'utente per casella vocale
- Telefonia con Mobility Entry (Mobility basata su DISA)
  - Richiesto: licenza apparecchio Utente Mobility
- Telefonia con myPortal to go
  - Richiesto: licenza apparecchio Utente Mobility

    Nella modalità **Telefono scrivania** (Controllo del telefono dell'ufficio) non è necessaria una licenza Utente Mobility.
  - Richiesto: licenza orientata all'utente Utente UC
  - Opzionale: licenza orientata all'utente per casella vocale
- Telefonia con myPortal @work
  - Richiesto: Utente IP
  - Richiesto: licenza orientata all'utente Utente UC
  - Opzionale: licenza orientata all'utente per casella vocale
  - Opzionale: licenza orientata all'utente per conferenze
- Telefonia con VoIP myPortal @work VoIP
  - Richiesto: Utente IP
  - Richiesto: licenza orientata all'utente Utente UC
  - Opzionale: licenza orientata all'utente per casella vocale
  - Opzionale: licenza orientata all'utente per conferenze
- Telefonia con optiClient Attendant
  - Richiesto: licenza apparecchio Utente IP, Utente TDM o Utente DeskShare
  - Richiesto: licenza di sistema per OpenScape Business Attendant
  - Opzionale: licenza orientata all'utente per casella vocale
  - Opzionale: licenza orientata all'utente per Utente UC (per visualizzazione stato presenza)

Telefonia con UC Suite

- Telefonia con casella vocale (UC Suite)
  - Richiesto: licenza apparecchio Utente IP, Utente TDM o Utente DeskShare
  - Richiesto: licenza orientata all'utente per casella vocale
- Telefonia con myPortal for Desktop
  - Richiesto: licenza apparecchio Utente IP, Utente TDM o Utente DeskShare
  - Richiesto: licenza orientata all'utente Utente UC
  - Opzionale: licenza orientata all'utente per casella vocale
  - Opzionale: licenza orientata all'utente per fax
  - Opzionale: licenza orientata all'utente per conferenze

- Telefonia con myPortal for Outlook
  - Richiesto: licenza apparecchio Utente IP, Utente TDM o Utente DeskShare
  - Richiesto: licenza orientata all'utente per Utente Groupware
  - Opzionale: licenza orientata all'utente per casella vocale
  - Opzionale: licenza orientata all'utente per fax
  - Opzionale: licenza orientata all'utente per conferenze
- Telefonia con myPortal to go
  - Richiesto: licenza apparecchio Utente Mobility

    Nella modalità **Telefono scrivania** (Controllo del telefono dell'ufficio) non è necessaria una licenza Utente Mobility.
  - Richiesto: licenza orientata all'utente per Utente Groupware o licenza per Utente UC
  - Opzionale: licenza orientata all'utente per casella vocale
- Telefonia con myPortal @work
  - Richiesto: Utente IP
  - Richiesto: licenza orientata all'utente per Utente Groupware o licenza per Utente UC
  - Opzionale: licenza orientata all'utente per casella vocale
  - Opzionale: licenza orientata all'utente per conferenze
- Telefonia con VoIP myPortal @work VoIP
  - Richiesto: Utente IP
  - Richiesto: licenza orientata all'utente per Utente Groupware o licenza per Utente UC
  - Opzionale: licenza orientata all'utente per casella vocale
  - Opzionale: licenza orientata all'utente per conferenze
- Telefonia con myAttendant
  - Richiesto: licenza apparecchio Utente IP, Utente TDM o Utente DeskShare
  - Richiesto: licenza orientata all'utente myAttendant
  - Opzionale: licenza orientata all'utente per casella vocale

Telephony with Unify Phone

- Richiesto: Utente IP
- Required: user-oriented Unify Phone license
- Optional: user-oriented VoiceMail license and additional IP User license for the team configuration

Uso del Contact Center

- Richiesto: licenza apparecchio Utente IP, Utente TDM o Utente DeskShare oppure Utente Mobility
- Richiesto: licenza orientata all'utente myAgent

  At least one myAgent license must be active for the system to route and address Contact Center calls.
- Opzionale: licenza di sistema per Contact Center E-mail
- Opzionale: licenza di sistema per Contact Center Fax

- Opzionale: licenza di sistema per myReports

Utilizzo di Company AutoAttendant

- Richiesto: licenza di sistema per Company AutoAttendant

  The Company AutoAttendant system license must be active for the system to route and address Auto Attendant calls.

8.3 Concessione della licenza di un sistema di comunicazione (indipendente)

La concessione della licenza di un sistema indipendente deve essere eseguita in un ordine preciso. Questa sequenza è illustrata nell'esempio di uno dei sistemi di comunicazione OpenScape Business X.

Il seguente paragrafo descrive come eseguire i passaggi 3 e 4 utilizzando il WBM.

1) **Codice di autorizzazione per la licenza (LAC)**

   All'acquisto di licenze, il cliente riceve un codice di autorizzazione licenza (LAC). I dati delle licenze acquisite vengono salvati nel database del server centrale delle licenze (CLS).
2) **Installazione e configurazione**

   Il cliente o il tecnico possono installare e configurare il sistema di comunicazione utilizzando la procedura guidata WBM (compresi gli utenti e le linee). Al primo avvio del WBM, occorre inserire la data corrente. Da questo momento parte il periodo di attivazione (periodo di 30 giorni durante il quale occorre definire l'attivazione della licenza del sistema di comunicazione).
3) **Attivazione licenza**

   Il cliente o il tecnico potranno attivare le licenze con il WBM sia online, utilizzando il codice di autorizzazione della licenza (attivazione della licenza online) che offline, direttamente con il file della licenza (attivazione della licenza offline).
4) **Assegnazione della licenza**

   Il cliente o il tecnico assegnano con il WBM gli utenti e le linee alle licenze acquistate. Completata l'assegnazione, vengono attivate le funzioni coperte da licenza.

8.3.1 CLS Connect

CLS Connect consente di effettuare procedure di rehost illimitate dei sistemi OpenScape Business. A tale scopo, deve essere attivato il flag **CLS Connect**.

Nota: Dopo l'attivazione, questo flag non può essere disattivato.

Se il sistema perde la connessione a CLS, inizia il periodo di failover. Se la connessione non viene ripristinata dopo 30 giorni, il sistema entra in modalità di emergenza e viene considerato non autorizzato.

Nota: Quando un sistema OpenScape Business con connessione CLS attiva deve essere riprogrammato, non è possibile creare un file di backup. È necessario eseguire un ricaricamento con lo stesso ID MAC e ID SIEL. CLS Connect non può essere attivato senza una licenza base attiva. Il file di licenza esistente da CLS può essere caricato manualmente nel sistema tramite WBM.

8.3.1.1 Come attivare CLS Connect

CLS Connect consente di effettuare procedure di rehost illimitate dei sistemi OpenScape Business.

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**

Per la connessione a CLS è necessario l'accesso a Internet

Sono disponibili le seguenti impostazioni del firewall:

a) La porta 7790 viene rilasciata per il traffico IP in uscita

I sistemi software V3R3 più recenti utilizzano la porta 7791 per l'attivazione della licenza online.

b) L'IP 188.64.16.4 viene rilasciato per il traffico IP in uscita

Nota: Per rendere più sicure le regole firewall si raccomanda di consentire solo la comunicazione in uscita.

La connessione a CLS è possibile; vedere Come verificare la connessione al Central License Server (CLS)

Nota: Quando si attiva CLS Connect, non è possibile disattivarlo.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Attiva CLS Connect**.
3) Selezionare la casella di controllo per attivare **CLS Connect**.
4) Fare clic su **Attiva**.

Nota: Nell'area delle notifiche della pagina principale se è attivato il controllo della licenza online viene visualizzato il messaggio seguente:

'Modalità della licenza: "CLS Connect".'

8.3.1.2 Passaggio da CLS connect

Passaggio da CLS connect a una licenza Permanente o PAYGO.

Se attualmente si utilizza uno schema di licenza "CLS Connect" e si desidera passare a una licenza permanente o PAYGO, occorre seguire alcuni passaggi per garantire una transizione senza problemi:

Passo a passo

1) Attivare la funzione CLS Connect Stop per il file di licenza del sistema. Questa operazione può essere eseguita inviando un ticket di supporto CLS.
2) Attivare un nuovo file di licenza per OSBiz per reimpostare il bit sicuro. Dopodiché, è possibile abilitare PAYGO o la licenza locale permanente per il sistema su CLS. Si riceverà quindi un nuovo file da attivare sul sistema.

Nota: Se si dispone di un ambiente OSBiz in rete concesso in licenza in CLS Connect, anche i nodi slave avranno il set di bit sicuro. Se a un certo punto si prevede di utilizzare un nodo slave come sistema autonomo separato con una licenza non CLS Connect, inviare un ticket di supporto per i passaggi richiesti.

8.3.2 Attivazione licenza (sistema indipendente)

Una volta acquistato un prodotto o un servizio, è necessario attivare la licenza fornita con il prodotto/servizio. Dopo l'attivazione vengono assegnate le licenze.

Per attivare le licenze sono disponibili due possibilità:

- **Attivazione della licenza online** (tramite codice di autorizzazione licenza)

  Il cliente o il tecnico trasferiscono, con l'aiuto di WBM, il codice di autorizzazione licenza tramite Internet al server licenze centrale(CLS). Per l'attivazione della licenza, insieme al LAC, viene utilizzato il Locking ID del sistema di comunicazione. Il CLS creati un file di licenza dai dati e lo invia al sistema, che attiva le licenze acquistate.

  Per l'accesso al CLS è necessaria una connessione a Internet. L'indirizzo IP del CLS viene salvato nel WBM in **Gestione delle licenze** > **Impostazioni** e può essere cambiato in caso di necessità da un amministratore con il profilo **Expert**.

Nota: Per l'attivazione della licenza online viene normalmente utilizzata la porta 7790. Questa porta deve essere attivata nel firewall della rete del cliente.

I sistemi software V3R3 più recenti utilizzano la porta 7791 per l'attivazione della licenza online.

Nota: Prima della concessione online della licenza, i dati della registrazione devono essere inseriti correttamente.

- **Attivazione licenza offline** (direttamente dal file di licenza)

  Il cliente o il tecnico accedono al server licenze centrale (CLS) e immettono il codice di autorizzazione licenza unitamente al Locking ID del sistema di comunicazione. Il CLS crea un file di licenza dai dati. Il cliente o il tecnico dell'assistenza scaricano il file di licenza e lo copiano nel WBM. Successivamente il sistema attiva le licenze acquistate.

  L'indirizzo IP del CLS viene salvato nel WBM in **Gestione delle licenze** > **Impostazioni** e può essere cambiato in caso di necessità da un amministratore con il profilo **Expert**.

Se occorre ampliare il sistema di comunicazione, è possibile acquistare ulteriori licenze. Con l'acquisto di licenze aggiuntive, viene fornito un nuovo codice di autorizzazione licenza (LAC) con il quale è possibile attivarle.

Nota: Le ulteriori licenze acquistate possono essere attivate anche in remoto.

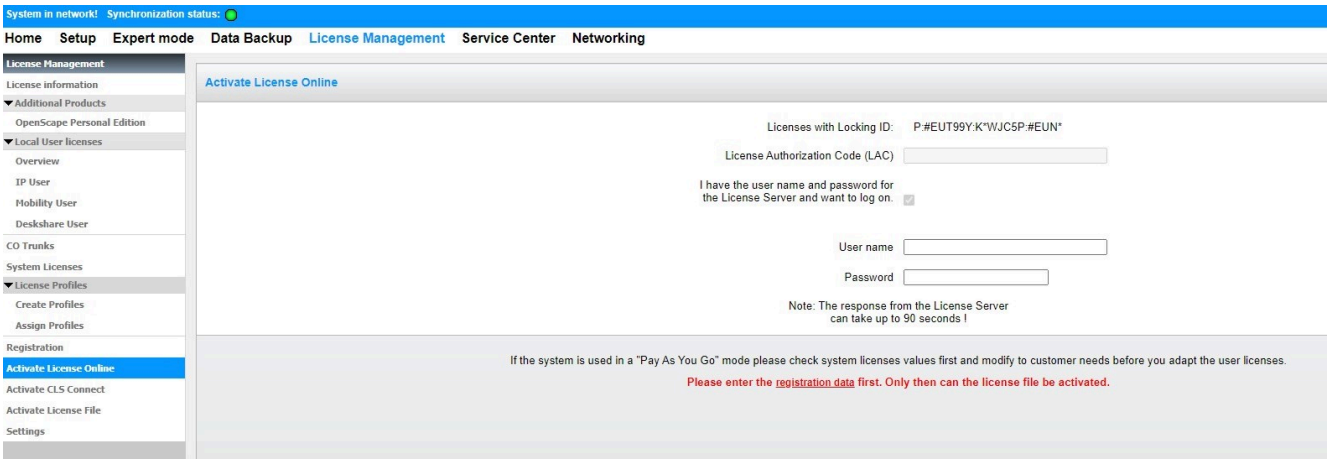
8.3.2.1 Come attivare le licenze online (indipendente)

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Il codice di autorizzazione licenza (LAC) per il rilascio della licenza è noto.

Per la connessione al server delle licenze, il sistema di comunicazione dispone di una connessione a Internet.



Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Registrazione**.
3) Inserire i dati e fare clic su **OK**.
4) Nella struttura di navigazione fare clic su **Attiva licenza in linea**.
5) Nel campo **Codice autorizzazione licenza (LAC)** immettere il LAC.
6) Selezionare la casella di controllo **Dispongo del nome utente e della password per il server delle licenze e desidero accedere**.

7) In **Nome utente** e **Password**, inserire i rispettivi dati per l'accesso al server delle licenze.
8) Fare clic su **Attiva**. Viene stabilita la connessione al server delle licenze e le licenze vengono trasferiti nel sistema di comunicazione. Una volta concluso il rilascio, la connessione si interrompe automaticamente.

8.3.2.2 Come attivare le licenze offline (indipendente)

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Il file di licenza viene creato e memorizzato sul server licenze centralizzato. La posizione di memorizzazione del file di licenza deve essere nota.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Attiva file della licenza**.
3) In **File di licenza** fare clic su **Sfoglia** quindi selezionare la posizione di memorizzazione del file di licenza.
4) Fare clic su **Attiva**.

8.3.3 Assegnazione della licenza (indipendente)

Dopo l'attivazione della licenza, le licenze acquistate devono essere assegnate agli utenti e alle linee. In un sistema indipendente, le funzioni a livello di sistema sono già automaticamente abilitate all'attivazione.

Assegnazione di licenze utente e licenze orientate all'utente

Agli utenti possono essere assegnate licenze utente e licenze orientate all'utente.

Ai seguenti tipi di utenti possono essere assegnate licenze utente:

Icona	Licenza utente	Descrizione
	Utente IP	Per l'uso di telefoni di sistema IP (HFA o SIP) e di telefoni SIP
	Utente TDM	Per l'uso di telefoni di sistema UP0, telefoni ISDN, telefoni analogici e telefoni DECT
	Utente Mobility	Per l'utilizzo di myPortal to go, Mobility Entry e DISA (servizio One Number)
	Utente Deskshare	Per l'uso della funzione desk sharing per gli utenti IP

Le licenze utente vengono assegnate in modo fisso ai numeri di telefono degli utenti. Se viene eliminato un utente o un numero di telefono viene assegnato a un altro tipo di utente, la licenza utente associata viene rilasciata.

Alcune licenze sono contrassegnate da un asterisco rosso. L'asterisco rosso indica che queste licenze possono anche essere coperte assegnando un'altra licenza.

Grazie alla flessibilità del sistema di assegnazione delle licenze agli utenti, gli utenti TDM, Mobility e DeskShare possono utilizzare anche licenze Utente IP. Se agli utenti sono già state assegnate tutte le licenze utente TDM, DeskShare e Mobility e sussiste la necessità di altri utenti TDM, DeskShare e Mobility, è possibile utilizzare licenze Utente IP per coprire questa necessità.

Una volta assegnata all'utente una licenza utente, è possibile assegnare allo stesso utente anche licenze orientate all'utente.

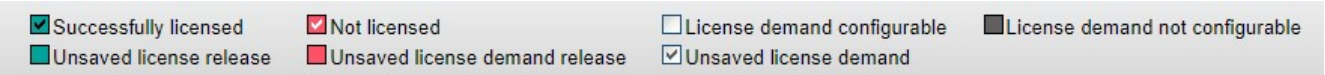
Agli utenti possono essere assegnate le seguenti licenze orientate all'utente:

Icona	Licenza orientata all'utente	Descrizione
	Casella vocale	Per l'uso della casella vocale.
	Utente Groupware	Per l'utilizzo delle funzioni UC Suite tramite myPortal for Outlook.
	Utente UC	Per l'utilizzo delle funzioni UC Suite tramite myPortal for Desktop.
	Fax	Per l'uso di una casella fax nella UC Suite. È richiesta una licenza utente UC o una licenza groupware.
	Conferenza	Per l'uso delle funzioni conferenza della UC Suite. È richiesta una licenza utente UC o una licenza groupware.
	myAttendant	Per l'utilizzo delle funzioni posto operatore della UC Suite.
	myAgent	Per l'uso delle funzioni del Contact Center.
	Application Launcher	Per il controllo delle applicazioni di un PC client mediante una chiamata, ad esempio con l'apertura di un'applicazione o la visualizzazione delle informazioni sul chiamante all'arrivo o all'effettuazione di una chiamata.
	Unify Phone	Per l'utilizzo del client Unify Phone in combinazione con OpenScape Business.
	TAPI	Per l'uso di applicazioni TAPI compatibili e telefonia supportata da PC con programmi dei clienti di diverse case software.

È possibile visualizzare una panoramica di tutte le licenze utente e le licenze orientate all'utente (selezionando **Licenze di utente locali** > **Panoramica)**.

In questa panoramica viene visualizzato per ogni utente lo stato delle relative licenze.

Per le licenze esistono i seguenti tipi di stati:



Assegnazione di licenze di sistema

Le licenze di sistema includono le licenze per le linee e per le funzioni a livello di sistema.

Alle seguenti linee è possibile assegnare licenze:

- Linee S_{2M}/T1: numero di canali B
- Linee ITSP: numero di chiamate simultanee eseguibili tramite un ITSP

In un sistema indipendente, le licenze per le funzioni a livello di sistema verranno rilasciate per impostazione predefinita durante l'attivazione delle licenze. Non sono necessarie altre assegnazioni.

Procedura di assegnazione delle licenze

Prerequisito: Il file di licenza è stato attivato e gli utenti sono stati configurati.

- Concessione delle licenze agli utenti
  1) Assegnare una licenza utente a un utente. Mediante questa assegnazione viene generata una richiesta di licenza per l'utente e contemporaneamente vengono assegnate le licenze orientate all'utente rilasciate.
  2) Assegnare le licenze orientate all'utente a un utente. Con queste assegnazioni vengono generate ulteriori richieste di licenza per l'utente. Occorre notare che alcune licenze richiedono altre licenze (vedere Suggerimenti per combinazioni di licenze).
  3) Verifica e rilascio delle richieste di licenza.
  4) Se le licenze disponibili non sono sufficienti per il rilascio, viene segnalata un'errata assegnazione mediante gli stati licenza (rossi). Correggere le assegnazioni delle licenza, quindi verificare nuovamente e rilasciare le licenze.

  Nota: Per una migliore visione d'insieme, è possibile stampare una panoramica di tutte le assegnazioni di licenze per tutti gli utenti (tramite **Licenze di utente locali** > **Panoramica** > **Stampa**). Nello stampato, tutte le assegnazioni non valide vengono elencate in una tabella separata.

- Attivazione delle licenze per le linee

  Le licenze per le linee devono essere distribuite alle linee S_{2M}/T1 e alle linee ITSP necessarie.

8.3.3.1 Come concedere licenze agli utenti (indipendente)

Distribuire le licenze apparecchio e le licenze orientate all'utente disponibili agli apparecchi. Terminata l'assegnazione, gli utenti dispongono delle licenze necessarie.

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

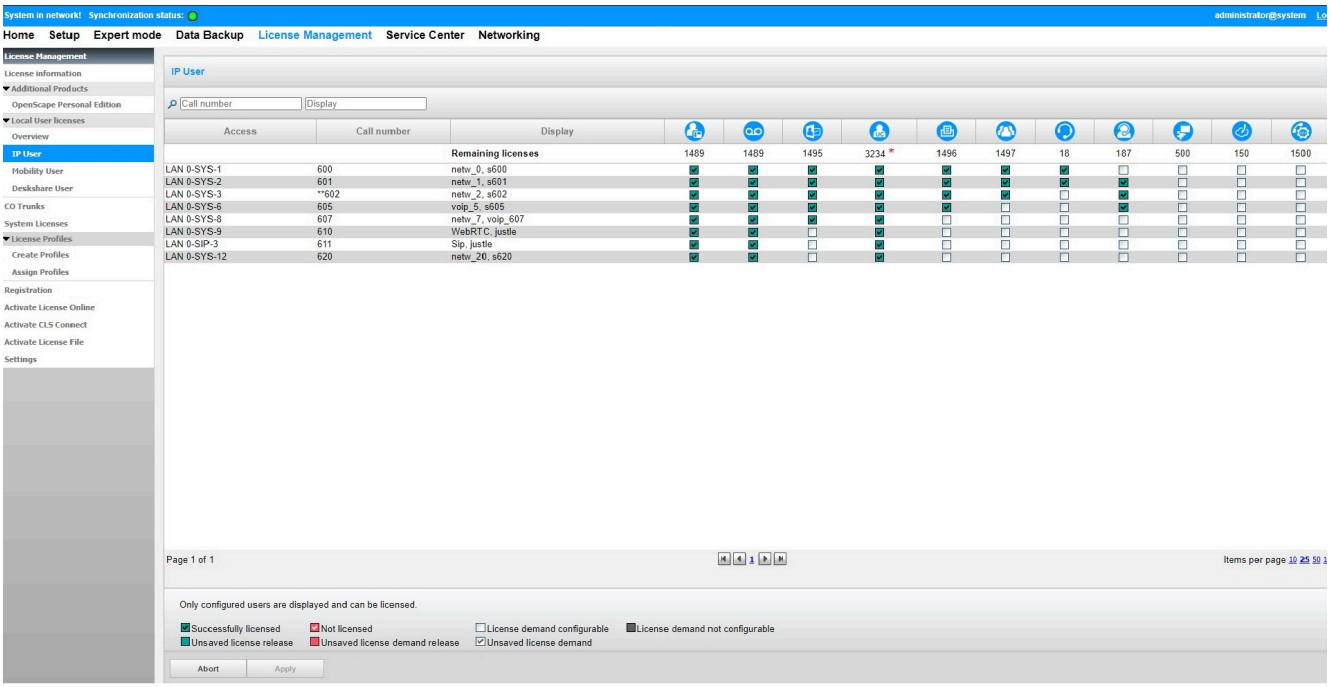
Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione, selezionare **Licenze di utenti locali** > **...** fino al tipo di utente desiderato. Viene visualizzato un elenco di tutti gli utenti del tipo selezionato.

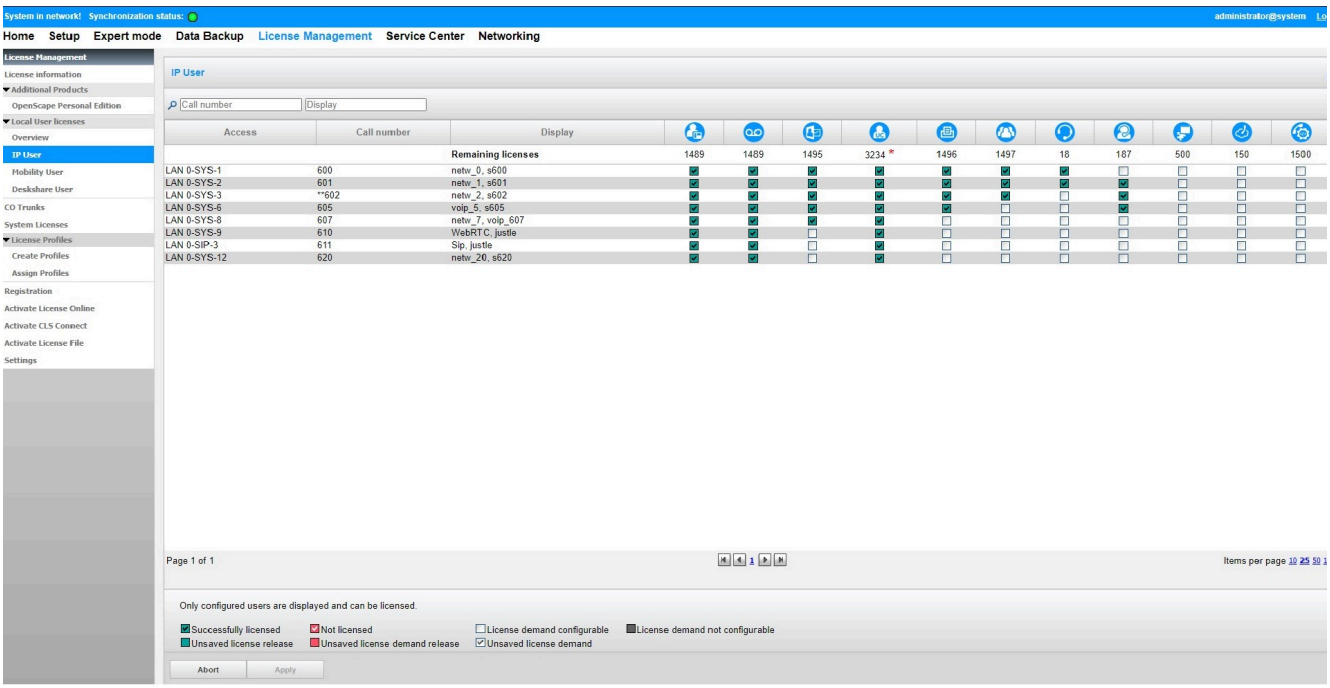
   In **licenze restanti** è possibile visualizzare quante licenze possono ancora essere assegnate agli utenti. Con gli utenti TDM, Mobility e DeskShare, la visualizzazione comprende anche tutte le licenze utente IP rimanenti, poiché tali licenze possono essere utilizzate anche per gli utenti TDM, Mobility e DeskShare (assegnazione flessibile delle licenze).

   Se il tipo di utente selezionato è Utente Mobility, sarà visualizzato anche il numero totale di licenze Unify Phone disponibili e la relativa data di scadenza.
3) Nella riga dell'utente desiderato, attivare la licenza apparecchio selezionando la casella di controllo con sfondo chiaro (prima colonna con caselle di controllo). Le caselle di controllo nelle altre colonne sono attivate.

Nota: È inoltre possibile visualizzare un utente selezionato inserendo nel campo di ricerca **Numero di telefono** o **Nome** il termine da cercare e quindi premendo il tasto Invio o facendo clic sull'icona a forma di lente d'ingrandimento. Se si lasciano vuoti tutti i campi di ricerca e quindi si fa clic sul tasto Invio o sull'icona della lente di ingrandimento, vengono visualizzati tutti gli utenti.



4) Nella riga dell'utente desiderato, attivare le licenze orientate all'utente selezionando le caselle di controllo desiderate.



Nota: Le licenze orientate all'utente possono essere assegnate a un apparecchio solo se è stata in precedenza assegnata una licenza all'apparecchio (punto 3).

Nota: Quando si assegna una licenza Casella vocale a un interno, viene creato un utente UC Suite e tutti gli inoltri di chiamata attivi vengono reimpostati.

Nota: Nel caso del pagamento a consumo, la licenza della casella vocale viene selezionata/deselezionata automaticamente, ogni volta che si attiva/disattiva una licenza utente vocale. Tuttavia è sempre possibile deselezionare la licenza della casella vocale.

Le funzionalità delle licenze Groupware, UC User, Fax, myAttendant e myAgent non sono configurabili in modalità UC Smart.

Le licenze Groupware e UC User si escludono l'un l'altra in modalità UC Suite.

---

5) Fare clic su **OK & Avanti**. Il sistema verifica che per la propria assegnazione siano disponibili licenze sufficienti.

   Se le licenze disponibili sono sufficienti, la concessione delle licenze dell'utente è ora completata.

   Nota: Nel caso del pagamento a consumo viene visualizzata una finestra popup. Fare clic su **OK** per confermare la propria scelta.

6) In caso di mancanza di licenze, viene segnalato l'errore con una casella di controllo rossa ombreggiata. Correggere l'errore e ripetere il passaggio 5.

   Nota: Se si desidera rimuovere una licenza apparecchio, è necessario confermare il messaggio di avvertimento. Viene quindi visualizzata una nuova casella di controllo **Avvisi attivati**. Se si deseleziona questa casella di controllo, è possibile rimuovere le licenze apparecchio aggiuntive senza preavviso.

8.3.3.2 Come concedere licenze alle linee (indipendente)

Distribuire le licenze acquistate per le linee alle linee SIP e S_{2M}/T1.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Linee urbane**. Nell'area **Linee urbane** viene visualizzato il numero delle licenze disponibili per le linee urbane SIP e S_{2M}/T1.
3) Per le linee SIP: nell'area **Linee SIP**, in **Richiesta licenze per numero di chiamante simultanee via Internet in questo nodo**, inserire il numero di chiamate Internet che possono essere eseguite contemporaneamente tramite un ITSP.
4) Per le linee S_{2M}: nell'area **PRI (S2M/T1)**, nella riga degli slot S_{2M} desiderati nell'elenco a discesa della colonna **Demands**, selezionare il numero di canali B desiderato.
5) Per le linee digitali T1 (solo per USA): nell'area **PRI (S2M/T1)**, nella riga degli slot T1 desiderati nell'elenco a discesa della colonna **Demands**, selezionare il numero di canali B desiderato.
6) Per linee T1 analogiche (solo USA): attivare la linea analogica T1 selezionando nel campo **PRI (S2M/T1)** nella riga della linea analogica T1 nell'elenco a discesa della colonna **Demands** la voce **1** (**0** significa che la linea è disattivata).

7) Fare clic su **OK & Avanti**.

Nota: Il numero di linee SIP con licenza e il numero di linee S_{2M}/TI con licenza non può superare il numero di licenze disponibili per le linee.

8.4 Concessione della licenza in più sistemi di comunicazione (sistema di reti)

La concessione della licenza in più sistemi di comunicazione deve essere eseguita in un ordine preciso. Questa sequenza è illustrata nell'esempio di un sistema di reti composto da un OpenScape Business S (master) e due OpenScape Business X3 (slave).

Se più OpenScape Business (nodi) sono riuniti in un sistema di reti, la concessione della licenza avviene in modo centralizzato tramite un file di licenza di rete che viene attivato presso il nodo master. Inoltre, ogni nodo slave di un sistema di reti richiede una propria licenza di sistema di rete. Il nodo con la maggiore larghezza di banda dovrebbe essere il nodo master.

Con la procedura guidata Rete del WBM, i nodi sono configurati nel sistema di reti come nodi master e slave. Il nodo master contiene l'agente delle licenze centrale (CLA centrale, central Customer License Agent). Tutti i nodi slave nel sistema di reti utilizzano questo CLA per la concessione della licenza. A tale scopo l'indirizzo IP del nodo master viene reso noto al nodo slave con l'ausilio del WBM.

Esiste un solo file di licenza di rete per l'intero sistema di reti. Questo è collegato al nodo master tramite il suo Locking ID. Se OpenScape Business S (soft switch) è il nodo master e se il soft switch è utilizzato in un ambiente virtuale, il file di licenza di rete viene collegato al nodo master tramite il Locking ID del server Linux del soft switch o tramite l'Advanced Locking ID del soft switch. Il file di licenza di rete è salvato nel CLA centrale e contiene tutti i dati delle licenze nel sistema di reti. Può essere attivato solo sul nodo master tramite il WBM. Solo il nodo master ha accesso al CLS, su tutti gli altri nodi l'accesso è disattivato.

Nel sistema di reti, non deve essere eseguita un'assegnazione delle licenze specifica per un nodo. Se per ogni nodo è già disponibile un proprio file di rete, è possibile riunirli nel CLS per creare un singolo file di licenza di rete.

Comportamento in caso di problemi di rete (failover)

Se cade la connessione al nodo master, e quindi al CLA centrale, sul display dei telefoni di sistema viene visualizzato "Failover Period". Entro questo periodo di failover (max. 30 giorni), tutti i nodi e i relativi servizi sono ancora funzionanti. Una volta risolti i problemi di rete e ripristinata la connessione al CLA centrale, tutti i nodi passano nuovamente allo stato di licenza regolare.

Se i problemi di rete non vengono risolti entro il periodo di failover, i nodi passano servizio d'emergenza. Al termine è necessario ottenere nuovamente la licenza per il sistema di reti.

Procedura di concessione della licenza nel sistema di reti secondo l'esempio sopra riportato

OpenScape Business S (master) ed entrambi gli OpenScape Business X3 (slave) sono già installati, configurati e connessi a un sistema di reti.

1) **Codice di autorizzazione per la licenza (LAC)**

   All'acquisto di licenze, il cliente riceve un codice di autorizzazione licenza (LAC). I dati delle licenze acquisite vengono salvati nel database del server centrale delle licenze (CLS).

2) **OpenScape Business S come nodo master**

   Il cliente o il tecnico accedono al WBM di OpenScape Business S e installano, utilizzando la procedura guidata Rete, OpenScape Business S come nodo master.

   Il sistema è già stato installato e configurato, funziona nel periodo di attivazione (periodo di 30 giorni durante il quale occorre definire il processo di licensing).

3) **Locking ID del nodo master**

   Il cliente o il tecnico prendono nota del Locking ID o dell'Advanced Locking ID di OpenScape Business S.

   Per la descrizione vedere Come controllare il Locking ID del sistema di comunicazione

4) **OpenScape Business X3 come nodo slave**

   Il cliente o il tecnico accedono al WBM di OpenScape Business S e installano, utilizzando la procedura Il cliente o il tecnico accedono prima al WBM del primo OpenScape Business X3 e installano, utilizzando la procedura guidata Rete, il primo OpenScape Business X3 come nodo slave, quindi ripetono questa procedura presso il WBM del secondo OpenScape Business X3.

   I sistemi sono già stati installati e configurati e si trovano nel periodo di attivazione.

5) **Locking ID di OpenScape Business X3**

   Il cliente o il tecnico prendono nota dei Locking ID di entrambi gli OpenScape Business X3.

   Per la descrizione vedere Come controllare il Locking ID del sistema di comunicazione

6) **Attivazione licenza**

   Il cliente o il tecnico accedono al CLS per generare il file di licenza di rete, unitamente al codice di autorizzazione della licenza e al Locking ID. Successivamente caricano il file nel nodo master utilizzando il WBM.

   Per la descrizione vedere Come attivare le licenze offline (sistema di reti)

   Successivamente il sistema attiva le licenze acquistate.

7) **Assegnazione della licenza**

   Il cliente o il tecnico distribuiscono le licenze ai nodi. A tal fine, l'utente accede al WBM di ogni nodo e assegna al nodo il numero desiderato di licenze. È importante che a ogni nodo venga assegnata una licenza sistema di rete, in caso contrario non verrà integrato nel sistema di reti.

   Per la descrizione vedere Come assegnare le licenze di sistema a un nodo

8.4.1 Attivazione licenza (sistema di reti)

Una volta acquistato un prodotto o un servizio, è necessario attivare la licenza fornita con il prodotto/servizio. A tal fine sono necessari i file di licenza. Dopo l'attivazione vengono assegnate le licenze.

Per attivare le licenze sono disponibili le seguenti possibilità:

- **Attivazione licenza offline** (direttamente dal file di licenza)

  Il cliente o il tecnico accedono al server licenze centrale (CLS) e immettono il codice di autorizzazione licenza unitamente ai Locking ID dei sistemi di comunicazione. Il CLS crea un file di licenza dai dati. Il cliente o il tecnico dell'assistenza scaricano il file di licenza e lo copiano nel WBM del nodo master.

  Il nodo master verifica se gli Advanced Locking ID salvati nel file di licenza corrispondono con quelli dei sistemi. Se la verifica ha esito positivo, le licenze vengono attivate e i sistemi passano allo stato di licenza regolare. In caso contrario i sistemi continuano a funzionare in periodo di tolleranza e al termine di tale periodo solo in servizio d'emergenza.

  L'indirizzo IP del CLS è memorizzato nel WBM selezionando **Gestione delle licenze** > **Impostazioni**

I file di licenza possono essere combinati come segue:

- **Come unire più file di licenza in un file di licenza di rete**

  Se uno o più nodi sono già dotati di licenza e devono essere riuniti in un sistema di reti, l'amministratore dovrà unire tramite il CLS i singoli file di licenza in un file di licenza di rete e caricare quest'ultimo nel CLA centrale. Su tutti gli altri nodi deve essere specificato l'indirizzo IP del nodo master con l'agente delle licenze centrale tramite la procedura guidata Configurazione di rete di WBM.

8.4.1.1 Come attivare le licenze offline (sistema di reti)

Questo esempio descrive la generazione e l'attivazione del file di licenza di rete comune di un OpenScape Business S come nodo master (nodo 1) e due OpenScape Business X3 (nodo 2 e nodo 3).

Prerequisiti

È disponibile un accesso al CLS.

Tutti i nodi sono installati e collegati in rete tra loro, vedere Collegamento in rete di Open Scape Business X e OpenScape Business S (gateway multiplo).

Passo a passo

1) Accedere al CLS con il nome utente e la password.
2) Nel campo **Licenze**, selezionare la voce **Generazione e download chiave di licenza**.
3) Nel campo **LAC** specificare il codice di autorizzazione per la licenza (LAC), quindi fare clic su **Trova**.
4) Aprire il prodotto OpenScape Business S e selezionare i servizi da assegnare al nodo 1.

5) Fare clic su **Crea chiave di licenza**.
6) Nel campo **Indirizzo MAC** specificare l'indirizzo MAC o l'Advanced Locking ID di OpenScape Business S (nodo 1) e nel campo **Indirizzo MAC del CLA di rete** specificare di nuovo l'indirizzo MAC o l'Advanced Locking ID di OpenScape Business S (nodo master).

Nota: L'indirizzo MAC di OpenScape Business S è l'indirizzo MAC della scheda di rete del server Linux di OpenScape Business S, utilizzato al momento dell'installazione del sistema operativo Linux. Se OpenScape Business S viene utilizzato in un ambiente virtualizzato, l'Advanced Locking ID di OpenScape Business S sostituisce l'indirizzo MAC.

---

7) Immettere il numero desiderato per i servizi, quindi fare clic su **Avanti**.
8) Verificare i dati dei clienti e fare clic su **Avanti**.
9) Leggere l'informativa legale, quindi fare clic su **Accetto le condizioni della licenza**.
10) Fare clic su **Termina** per creare la chiave di licenza.
11) Per il nodo 2, nel campo **Licenze** selezionare la voce **Generazione e download chiave di licenza**.
12) Nel campo **LAC** specificare nuovamente il codice di autorizzazione per la licenza (LAC), quindi fare clic su **Trova**.
13) Aprire il prodotto OpenScape Business X3 e selezionare i servizi da assegnare al nodo 2.
14) Fare clic su **Crea chiave di licenza**.
15) Nel campo **Indirizzo MAC** specificare l'indirizzo MAC del nodo 2 e nel campo **Indirizzo MAC del CLA di rete** specificare l'indirizzo MAC del nodo 1 (nodo master).
16) Immettere il numero desiderato per i servizi, quindi fare clic su **Avanti**.
17) Fare clic su **Avanti**.
18) Confermare l'informativa legale selezionando la casella di controllo **Accetto il contratto di licenza**.
19) Fare clic su **Termina** per creare la chiave di licenza.
20) Ripetere i passi 11 -19 per il nodo 3.
21) Fare clic su **Chiave di licenza**, quindi su **Download** per scaricare il file di licenza di rete.
22) Salvare il file di licenza di rete.
23) Accedere a WBM del nodo master richiamando nel browser Web la pagina `https://<indirizzo IP del nodo master>` e specificando il nome utente e la password.
24) Nella barra di navigazione fare clic su **Gestione delle licenze**.
25) Nella struttura di navigazione fare clic su **Attiva file della licenza**.
26) In **File di licenza** fare clic su **Sfoglia** quindi selezionare la posizione di memorizzazione del file di licenza di rete.
27) Fare clic su **Attiva**.

8.4.1.2 Come unire più file di licenza in un file di licenza di rete

Se in un sistema di reti vengono integrati più nodi non precedentemente collegati in rete, i file di licenza dei singoli nodi devono essere uniti con l'ausilio del CLS in un file di licenza di rete comune.

Prerequisiti

È disponibile un accesso al CLS e si possiedono i diritti di accesso per i pacchetti licenze del singolo nodo.

Tutti i nodi sono installati e collegati in rete tra loro, vedere Collegamento in rete di Open Scape Business X e OpenScape Business S (gateway multiplo).

Passo a passo

1) Accedere al CLS con il nome utente e la password.
2) Nel campo **Concessione licenze di rete**, selezionare la voce **Aggiungere/rimuovere sistema**.
3) Selezionare l'indirizzo MAC del nodo da integrare nel sistema di reti.
4) Fare clic su **Rehost**.
5) Nel campo **Indirizzo MAC** specificare l'indirizzo MAC del nodo.
6) Nel campo **Indirizzo MAC del CLA di rete** specificare l'indirizzo MAC di un nodo master. Normalmente OpenScape Business S è il nodo master.

   Nota: L'indirizzo MAC di OpenScape Business S è l'indirizzo MAC della scheda di rete del server Linux di OpenScape Business S, utilizzato al momento dell'installazione del sistema operativo Linux.

7) Fare clic su **Avanti**.
8) Verificare i dati dei clienti e fare clic su **Avanti**.
9) Leggere l'informativa legale, quindi fare clic su **Accetto le condizioni della licenza**.
10) Fare clic su **Termina** per creare la chiave di licenza.
11) Ripetere i passi 2 – 10 per i vari nodi.
12) Fare clic su **Chiave di licenza**, quindi su **Download** per scaricare il file di licenza di rete.
13) Salvare il file di licenza di rete.
14) Accedere a WBM del nodo master richiamando nel browser Web la pagina `https://<indirizzo IP del nodo master>` e specificando il nome utente e la password.
15) Nella barra di navigazione fare clic su **Gestione delle licenze**.
16) Nella struttura di navigazione fare clic su **Attiva file della licenza**.
17) In **File di licenza** fare clic su **Sfoglia** quindi selezionare la posizione di memorizzazione del file di licenza di rete.
18) Fare clic su **Attiva**.

8.4.2 Assegnazione della licenza (sistema di reti)

Dopo l'attivazione della licenza, le licenze acquistate devono essere assegnate agli utenti e alle linee. L'assegnazione viene eseguita separatamente in ogni nodo.

Assegnazione di licenze utente e licenze orientate all'utente

Agli utenti possono essere assegnate licenze utente e licenze orientate all'utente.

Ai seguenti tipi di utenti possono essere assegnate licenze utente:

Icona	Licenza utente	Descrizione
	Utente IP	Per l'uso di telefoni di sistema IP (HFA o SIP) e di telefoni SIP
	Utenti TDM	Per l'uso di telefoni di sistema UP0, telefoni ISDN, telefoni analogici e telefoni DECT
	Utenti mobili	Per l'utilizzo di myPortal to go, Mobility Entry e DISA (servizio One Number)
	Utente Desk sharing	Per l'uso della funzione desk sharing per gli utenti IP
	Utente secondario	Per l'utilizzo della telefonia di base in caso di guasto.

Le licenze utente vengono assegnate in modo fisso ai numeri di telefono degli utenti. Se viene eliminato un utente o un numero di telefono viene assegnato a un altro tipo di utente, la licenza utente associata viene rilasciata.

Grazie alla flessibilità del sistema di assegnazione delle licenze agli utenti, gli utenti TDM, Mobility e DeskShare possono utilizzare anche licenze Utente IP. Se agli utenti sono già state assegnate tutte le licenze utente TDM, DeskShare e Mobility e sussiste la necessità di altri utenti TDM, DeskShare e Mobility, è possibile utilizzare licenze Utente IP per coprire questa necessità.

Una volta assegnata all'utente una licenza utente, è possibile assegnare allo stesso utente anche licenze orientate all'utente.

Agli utenti possono essere assegnate le seguenti licenze orientate all'utente:

Icona	Licenza orientata all'utente	Descrizione
	Casella vocale	Per l'uso della casella vocale.
	Utente Groupware	Per l'utilizzo delle funzioni UC Suite tramite myPortal for Outlook.
	UC Suite	Per l'utilizzo delle funzioni UC Suite tramite myPortal for Desktop.
	Fax	Per l'uso di una casella fax nella UC Suite. È richiesta una licenza utente UC o una licenza groupware.

Icona	Licenza orientata all'utente	Descrizione
	Conferenza	Per l'uso delle funzioni conferenza della UC Suite. È richiesta una licenza utente UC o una licenza groupware.
	myAttendant	Per l'utilizzo delle funzioni posto operatore della UC Suite.
	myAgent	Per l'uso delle funzioni del Contact Center.
	Application Launcher	Per il controllo delle applicazioni di un PC client mediante una chiamata, ad esempio con l'apertura di un'applicazione o la visualizzazione delle informazioni sul chiamante all'arrivo o all'effettuazione di una chiamata.
	Unify Phone	Per l'utilizzo del client Unify Phone in combinazione con OpenScape Business.
	TAPI 120 / 170	Per l'uso di applicazioni TAPI compatibili e telefonia supportata da PC con programmi dei clienti di diverse case software.

È possibile visualizzare una panoramica di tutte le licenze utente e le licenze orientate all'utente (selezionando **Licenze di utente locali** > **Panoramica)**.

In questa panoramica viene visualizzato per ogni utente lo stato delle relative licenze.

Per le licenze esistono i seguenti tipi di stati:



Assegnazione di licenze di sistema

Le licenze di sistema includono le licenze per le linee e per le funzioni a livello di sistema.

Alle seguenti linee è possibile assegnare licenze:

- Linee S_{2M}/T1: numero di canali B
- Linee ITSP: numero di chiamate simultanee eseguibili tramite un ITSP

Le licenze a livello di sistema vengono assegnate a ogni sistema (nodo) nel sistema di reti. Questa configurazione deve essere eseguita in sequenza su ciascun nodo. Il numero totale di licenze a livello di sistema memorizzati nel file di licenza di rete sul nodo master viene ridotto del numero configurato sul nodo.

Procedura di assegnazione delle licenze

Prerequisito: Il file di licenza è stato attivato e gli utenti sono stati configurati.

- Concessione delle licenze agli utenti

  1) Assegnare una licenza utente a un utente. Mediante questa assegnazione viene generata una richiesta di licenza per l'utente e

contemporaneamente vengono assegnate le licenze orientate all'utente rilasciate.

2) Assegnare le licenze orientate all'utente a un utente. Con queste assegnazioni vengono generate ulteriori richieste di licenza per l'utente. Occorre notare che alcune licenze richiedono altre licenze (vedere Suggerimenti per combinazioni di licenze).
3) Verifica e rilascio delle richieste di licenza.
4) Se le licenze disponibili non sono sufficienti per il rilascio, viene segnalata un'errata assegnazione mediante gli stati licenza (rossi). Correggere le assegnazioni delle licenza, quindi verificare nuovamente e rilasciare le licenze.

Nota: Per una migliore visione d'insieme, è possibile stampare una panoramica di tutte le assegnazioni di licenze per tutti gli utenti (tramite **Licenze di utente locali** > **Panoramica** > **Stampa**). Nello stampato, tutte le assegnazioni non valide vengono elencate in una tabella separata.

- Attivazione delle licenze per le linee

  Le licenze per le linee devono essere distribuite alle linee S_{2M}/T1 e alle linee ITSP necessarie.

8.4.2.1 Come concedere licenze agli utenti (sistema di reti)

Distribuire le licenze apparecchio e le licenze orientate all'utente disponibili agli apparecchi. Terminata l'assegnazione, gli utenti dispongono delle licenze necessarie.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

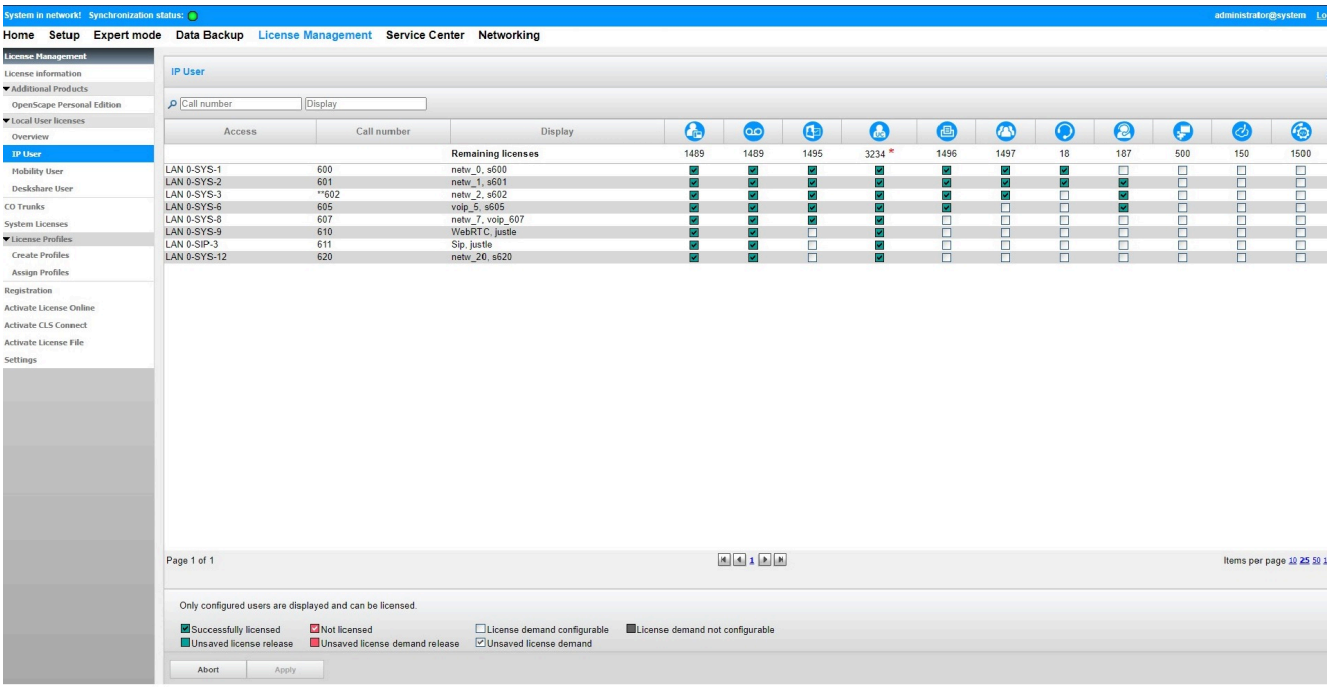
1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione, selezionare **Licenze di utenti locali** > **...** fino al tipo di utente desiderato. Viene visualizzato un elenco di tutti gli utenti del tipo selezionato.

   In **licenze restanti** è possibile visualizzare quante licenze possono ancora essere assegnate agli utenti. Con gli utenti TDM, Mobility e DeskShare, la visualizzazione comprende anche tutte le licenze utente IP rimanenti, poiché tali licenze possono essere utilizzate anche per gli utenti TDM, Mobility e DeskShare (assegnazione flessibile delle licenze).

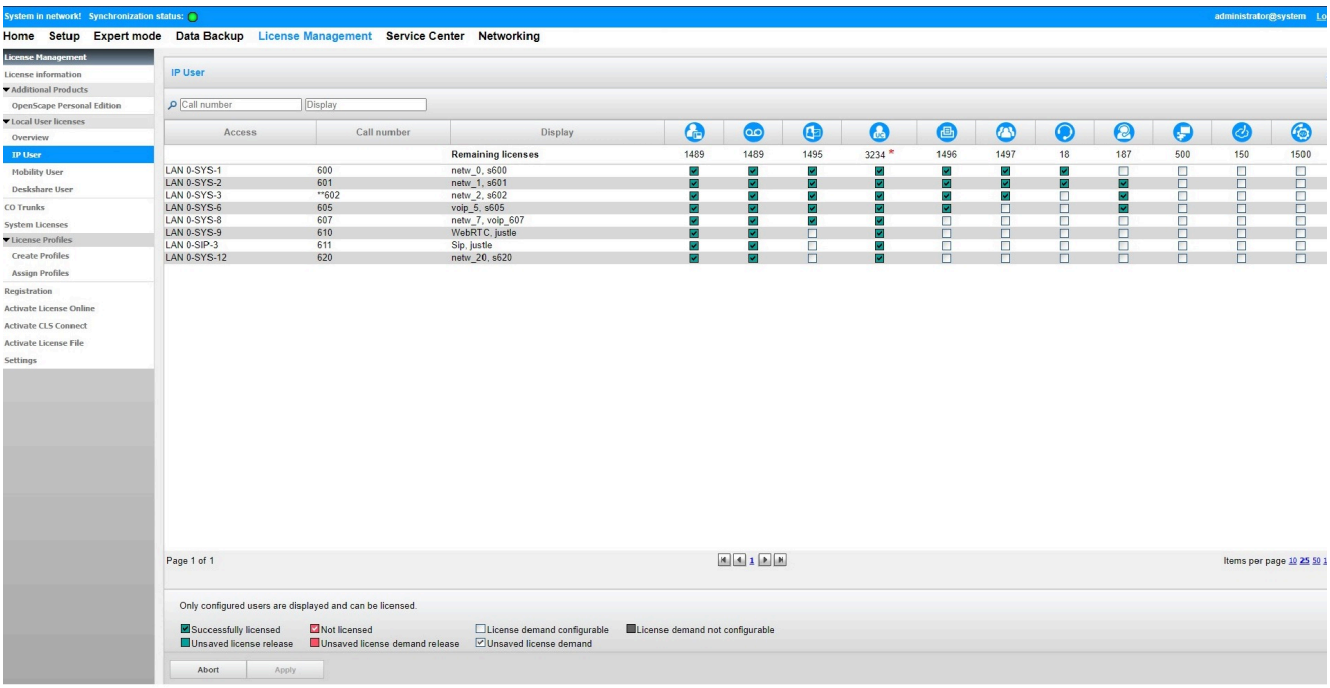
   Se il tipo di utente selezionato è Utente Mobility, sarà visualizzato anche il numero totale di licenze Unify Phone disponibili e la relativa data di scadenza.

3) Nella riga dell'utente desiderato, attivare la licenza apparecchio selezionando la casella di controllo con sfondo chiaro (prima colonna con caselle di controllo). Le caselle di controllo nelle altre colonne sono abilitate.

Nota: È inoltre possibile visualizzare un utente selezionato inserendo nel campo di ricerca **Numero di telefono** o **Nome** il termine da cercare e quindi premendo il tasto Invio o facendo clic sull'icona a forma di lente d'ingrandimento. Se si lasciano vuoti tutti i campi di ricerca e quindi si fa clic sul tasto Invio o sull'icona della lente di ingrandimento, vengono visualizzati tutti gli utenti.



4) Nella riga dell'utente desiderato, attivare le licenze orientate all'utente selezionando le caselle di controllo desiderate.



Nota: Le licenze orientate all'utente possono essere assegnate a un apparecchio solo se è stata in precedenza assegnata una licenza all'apparecchio (punto 3).

Nota: "Pay As You Go" non è disponibile in caso di file di licenza di rete.

Nel caso di una rete di sistemi OpenScape Business, qualsiasi sistema può utilizzare Pay As You Go tramite Central License Agent (CLA) locale.

5) Fare clic su **OK & Avanti**. Il sistema verifica che per la propria assegnazione siano disponibili licenze sufficienti.

   Se le licenze disponibili sono sufficienti, la concessione delle licenze dell'utente è ora completata.

6) In caso di mancanza di licenze, viene segnalato l'errore con una casella di controllo rossa ombreggiata. Correggere l'errore e ripetere il passaggio 5.

Nota: Se si desidera rimuovere una licenza apparecchio, è necessario confermare il messaggio di avvertimento. Viene quindi visualizzata una nuova casella di controllo **Avvisi attivati**. Se si deseleziona questa casella di controllo, è possibile rimuovere le licenze apparecchio aggiuntive senza preavviso.

8.4.2.2 Come concedere licenze alle linee (sistema di reti)

Distribuire le licenze acquistate per le linee alle linee SIP e S_{2M}/T1.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Linee urbane**. Nell'area Linee urbane viene visualizzato il numero delle licenze disponibili per le linee urbane SIP e S**2M**/T1.
3) Per le linee SIP: nell'area **Linee SIP**, in **Richiesta licenze per numero di chiamante simultanee via Internet in questo nodo**, inserire il numero di chiamate Internet che possono essere eseguite contemporaneamente tramite un ITSP.
4) Per le linee S_{2M}: nell'area **S2M**, nella riga degli slot desiderati nell'elenco a discesa della colonna **Demands**, selezionare il numero di canali B desiderato.
5) Per le linee T1 (solo per USA): nell'area **T1**, nella riga degli slot desiderati nell'elenco a discesa della colonna **Demands**, selezionare il numero di canali B desiderato.
6) Fare clic su **OK & Avanti**.

Nota: Il numero di linee SIP con licenza e il numero di linee S_{2M}/TI con licenza non può superare il numero di licenze disponibili per le linee.

8.4.2.3 Come assegnare le licenze di sistema a un nodo

Prerequisiti

Si è connessi al WBM del nodo desiderato.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Licenze di sistema**. Vengono visualizzate tutte le licenze di sistema disponibili.
3) Nella colonna **Licenze utilizzate**, nelle licenze di sistema desiderate, selezionare il numero di licenze di sistema che devono essere assegnate al nodo.

   Nella colonna **disponibile per la distribuzione** viene visualizzato il numero di licenze disponibili per l'intero sistema di reti.

   Nota: Assicurarsi che ai nodi venga assegnata la licenza di sistema "Networking", in caso contrario il nodo non verrà integrato nel sistema di reti.

   ---

4) Fare clic su **Salva**.

8.4.2.4 Come assegnare la licenza di sistema "Rete" a un nodo

Prerequisiti

Si è connessi al WBM del nodo desiderato.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Licenze di sistema**. Vengono visualizzate tutte le licenze di sistema disponibili.
3) Nella licenza di sistema **Rete**, nella colonna **Licenze utilizzate**, selezionare dall'elenco a discesa la voce **1**.

   Nella colonna **disponibile per la distribuzione** viene visualizzato il numero di licenze disponibili per l'intero sistema di reti.
4) Fare clic su **Salva**.

8.5 Informazioni licenza

Le informazioni relative a licenze disponibili e assegnate nonché su prodotti e servizi da esse coperti, vengono visualizzate con WBM. Nel sistema di reti è possibile richiamare le informazioni sulle licenze di tutti i nodi disponibili sulla rete.

È possibile visualizzare le seguenti informazioni:

- **Indirizzo MAC**: indirizzo MAC della piattaforma hardware o del server Linux soft switch a cui sono collegate le licenze.

  Nota: Se il sistema di comunicazione si trova nel periodo di attivazione, qui può venire visualizzato un indirizzo MAC non corretto. L'indirizzo MAC corretto può essere verificato nel **Centro assistenza** in **Inventario** (Inventario).
- **Advanced Locking ID**: Advanced Locking ID del softswitch in un ambiente virtualizzato, a cui le licenze sono collegate.
- **Locking ID:**: locking ID del server applicazioni a cui sono collegate le licenze.
- **Nodo**: nome del sistema di comunicazione, al quale sono legate le licenze.
- **Nome del prodotto**: nome del prodotto a cui viene assegnata la licenza.
- **Servizio**: servizio a cui viene assegnata la licenza.
- **Licenze utilizzate**: visualizza il numero di licenze utilizzate e disponibili.
- **Disponibili per la distribuzione**: visualizza le licenze ancora disponibili sul sistema di reti.
- **Stato**: lo stato della licenza.

Per assegnare la licenza al prodotto OpenScape Personal Edition viene utilizzato un proprio file di licenza. Le informazioni sulla licenza vengono visualizzate in **Prodotti aggiuntivi**.

8.5.1 Informazioni sulle licenze in assenza di un sistema di reti (configurazione indipendente)

Possono essere visualizzate tutte le licenze assegnate al sistema di comunicazione e le relative informazioni.

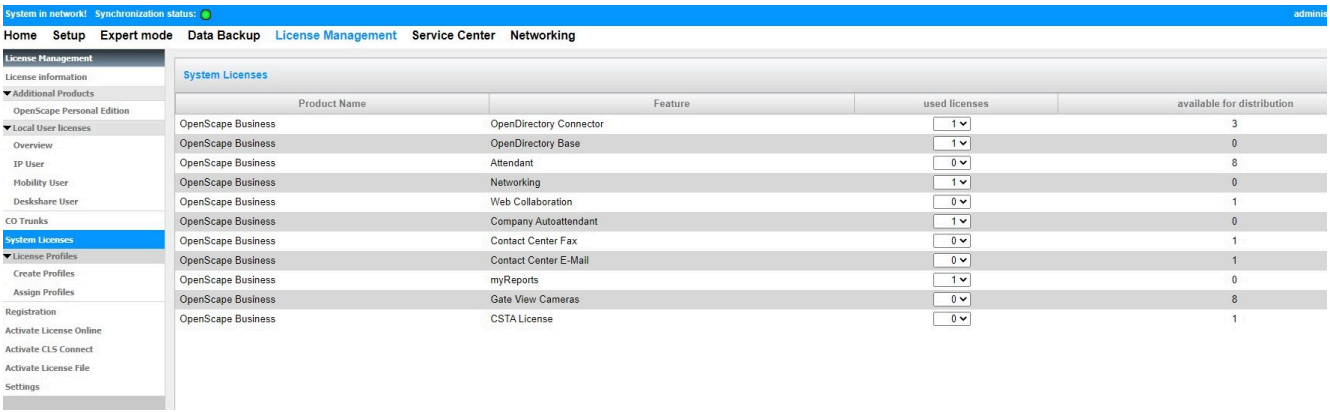
8.5.1.1 Come visualizzare le informazioni sulla licenza

Prerequisiti

Si è connessi al WBM.

Passo a passo

Nella barra di navigazione fare clic su **Gestione delle licenze**. Vengono visualizzate le informazioni sulla licenze per il proprio sistema di comunicazione.



Nota: In caso di "Pay As You Go" le licenze utilizzate sono configurabili ad eccezione di Contact Center Fax, Contact Center E-mail e myReports in modalità UC Smart.

8.5.2 Informazioni sulle licenze nel sistema di reti

In un sistema di reti possono essere visualizzate tutte le licenze e le relative informazioni. Queste informazioni vengono lette dal file di licenza di rete.

Le licenze in un sistema di reti, ad eccezione delle licenze base sono di tipo "flottante" e sono gestite in un pool di licenze. Se una licenza non è più richiesta da un nodo (sistema di comunicazione), viene rilasciata e può quindi essere utilizzata per un altro nodo.

In un sistema di reti possono essere visualizzate tutte le licenze del sistema di reti, tutte le licenze usate (floating) e tutte quelle legate in modo speciale a un nodo.

Inoltre, le licenze apparecchio e le licenze orientate all'utente possono essere ordinate in base al nodo e visualizzate in una panoramica.

8.5.2.1 Come visualizzare tutte le licenze del sistema di reti

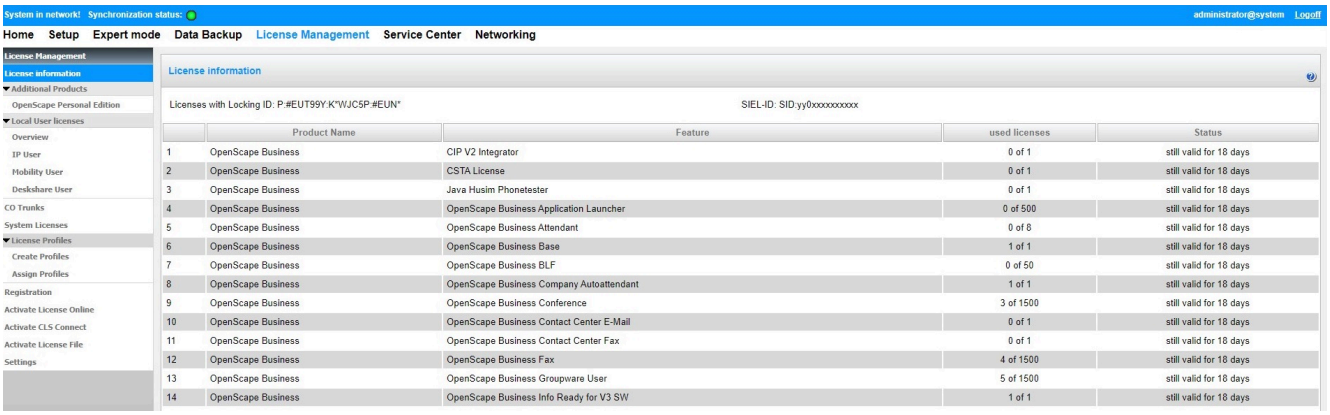
Prerequisiti

Il sistema di comunicazione si trova in un sistema di reti.

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Informazioni licenza**. Vengono visualizzate tutte le licenze del sistema di reti.



	Product Name	Feature	used licenses	Status
1	OpenScape Business	CIP V2 Integrator	0 of 1	still valid for 18 days
2	OpenScape Business	CSTA License	0 of 1	still valid for 18 days
3	OpenScape Business	Java Husim Phonetester	0 of 1	still valid for 18 days
4	OpenScape Business	OpenScape Business Application Launcher	0 of 500	still valid for 18 days
5	OpenScape Business	OpenScape Business Attendant	0 of 8	still valid for 18 days
6	OpenScape Business	OpenScape Business Base	1 of 1	still valid for 18 days
7	OpenScape Business	OpenScape Business BLF	0 of 50	still valid for 18 days
8	OpenScape Business	OpenScape Business Company Autoattendant	1 of 1	still valid for 18 days
9	OpenScape Business	OpenScape Business Conference	3 of 1500	still valid for 18 days
10	OpenScape Business	OpenScape Business Contact Center E-Mail	0 of 1	still valid for 18 days
11	OpenScape Business	OpenScape Business Contact Center Fax	0 of 1	still valid for 18 days
12	OpenScape Business	OpenScape Business Fax	4 of 1500	still valid for 18 days
13	OpenScape Business	OpenScape Business Groupware User	5 of 1500	still valid for 18 days
14	OpenScape Business	OpenScape Business Info Ready for V3 SW	1 of 1	still valid for 18 days

8.5.2.2 Come visualizzare le licenze collegate a un nodo

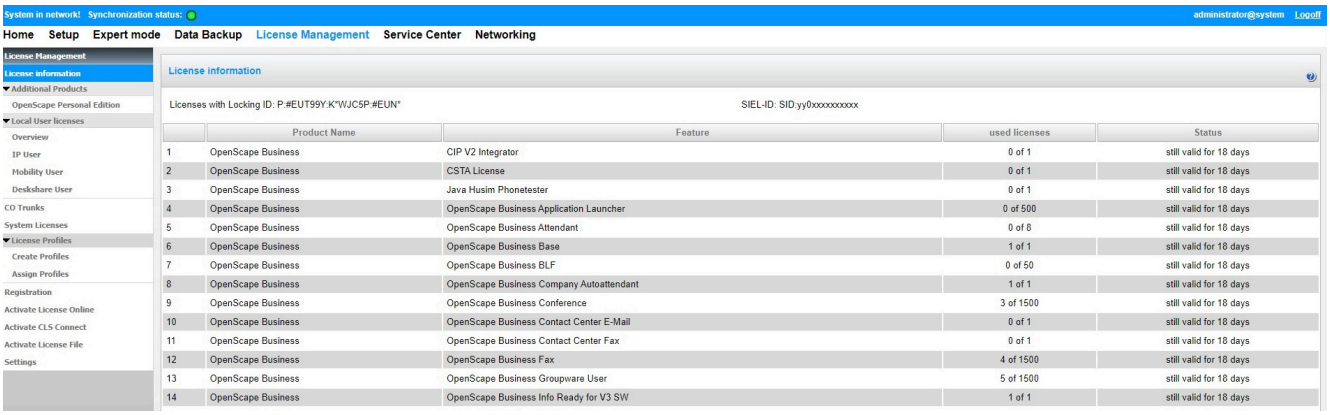
Prerequisiti

Il sistema di comunicazione si trova in un sistema di reti.

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Informazioni licenza**.
3) Nella struttura di navigazione fare clic sul nome del sistema o sul Locking ID del nodo desiderato. Vengono visualizzate le licenze legate specificatamente a questo nodo, ad esempio la licenza di base.



	Product Name	Feature	used licenses	Status
1	OpenScape Business	CIP V2 Integrator	0 of 1	still valid for 18 days
2	OpenScape Business	CSTA License	0 of 1	still valid for 18 days
3	OpenScape Business	Java Husim Phonetester	0 of 1	still valid for 18 days
4	OpenScape Business	OpenScape Business Application Launcher	0 of 500	still valid for 18 days
5	OpenScape Business	OpenScape Business Attendant	0 of 8	still valid for 18 days
6	OpenScape Business	OpenScape Business Base	1 of 1	still valid for 18 days
7	OpenScape Business	OpenScape Business BLF	0 of 50	still valid for 18 days
8	OpenScape Business	OpenScape Business Company Autoattendant	1 of 1	still valid for 18 days
9	OpenScape Business	OpenScape Business Conference	3 of 1500	still valid for 18 days
10	OpenScape Business	OpenScape Business Contact Center E-Mail	0 of 1	still valid for 18 days
11	OpenScape Business	OpenScape Business Contact Center Fax	0 of 1	still valid for 18 days
12	OpenScape Business	OpenScape Business Fax	4 of 1500	still valid for 18 days
13	OpenScape Business	OpenScape Business Groupware User	5 of 1500	still valid for 18 days
14	OpenScape Business	OpenScape Business Info Ready for V3 SW	1 of 1	still valid for 18 days

8.5.2.3 Come visualizzare tutte le licenze condivise nel sistema di reti

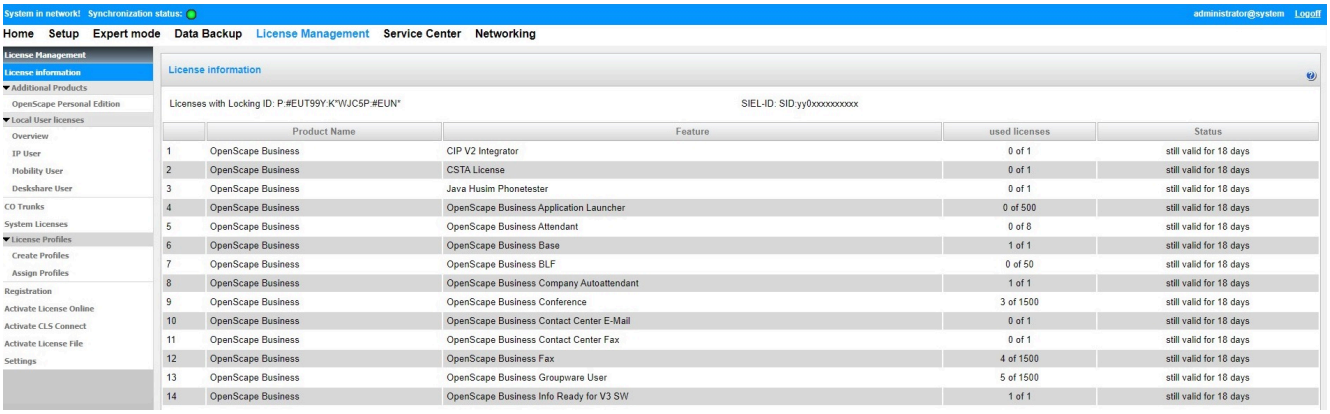
Prerequisiti

Il sistema di comunicazione si trova in un sistema di reti.

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Informazioni licenza**.
3) Nella struttura di navigazione fare clic su **Floating**. Vengono visualizzate tutte le licenze condivise nel sistema di reti.



	Product Name	Feature	used licenses	Status
1	OpenScape Business	CIP V2 Integrator	0 of 1	still valid for 18 days
2	OpenScape Business	CSTA License	0 of 1	still valid for 18 days
3	OpenScape Business	Java Husim Phonetester	0 of 1	still valid for 18 days
4	OpenScape Business	OpenScape Business Application Launcher	0 of 500	still valid for 18 days
5	OpenScape Business	OpenScape Business Attendant	0 of 8	still valid for 18 days
6	OpenScape Business	OpenScape Business Base	1 of 1	still valid for 18 days
7	OpenScape Business	OpenScape Business BLF	0 of 50	still valid for 18 days
8	OpenScape Business	OpenScape Business Company Autoattendant	1 of 1	still valid for 18 days
9	OpenScape Business	OpenScape Business Conference	3 of 1500	still valid for 18 days
10	OpenScape Business	OpenScape Business Contact Center E-Mail	0 of 1	still valid for 18 days
11	OpenScape Business	OpenScape Business Contact Center Fax	0 of 1	still valid for 18 days
12	OpenScape Business	OpenScape Business Fax	4 of 1500	still valid for 18 days
13	OpenScape Business	OpenScape Business Groupware User	5 of 1500	still valid for 18 days
14	OpenScape Business	OpenScape Business Info Ready for V3 SW	1 of 1	still valid for 18 days

8.5.2.4 Come visualizzare in base ai nodi le licenze apparecchio e orientate all'utente

Prerequisiti

Il sistema di comunicazione si trova in un sistema di reti.

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Panoramica licenze a livello rete**. Vengono visualizzate tutte le licenze apparecchio e le licenze orientate all'utente nel sistema di reti, ordinate per nodo.

8.6 Assegnazione del profilo licenza

I profili licenza contengono assegnazioni licenza predefinite e possono essere assegnati a uno o più utenti. I profili licenza sono utili quando più utenti devono ottenere la stessa licenza.

È possibile utilizzare profili licenza predefiniti o creare nuovi profili licenza.

Un profilo licenza vale per un tipo di utente e può essere assegnato solo a tale tipo di utente. È possibile creare e assegnare un nome a più profili licenza per un tipo di utente.

Per i seguenti tipi di utente possono essere creati profili licenza:

- Utente IP (telefoni di sistema IP, telefoni SIP)
- Utente TDM (telefoni UP0, telefoni ISDN, telefoni analogici, telefoni DECT)
- Utente Desk sharing
- Utenti mobili

In un profilo licenza, è possibile assegnare a un tipo utente licenze orientate all'utente, in base alle proprie esigenze.

Se l'assegnazione delle licenze a un utente di un profilo licenza viene modificata separatamente, l'assegnazione dell'utente al relativo profilo licenza viene automaticamente annullata.

8.6.1 Come aggiungere un profilo licenza

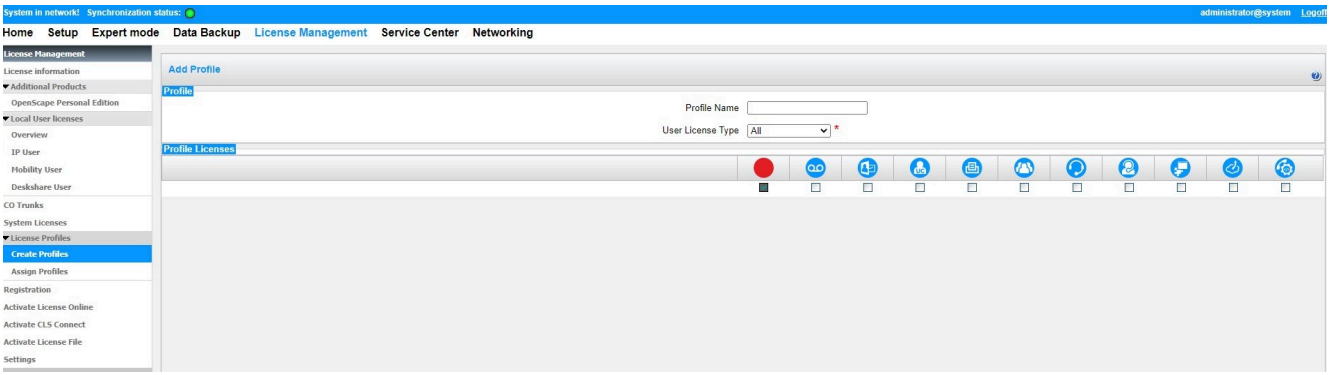
Creare un nuovo profilo licenza.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione, fare clic su **Profili licenza** > **Crea profili**. Vengono visualizzati tutti i profili licenza disponibili.
3) Fare clic su **Aggiungi**.



4) Nel campo **Nome del profilo** inserire un nome a scelta per il nuovo profilo.
5) Dall'elenco a discesa **Tipo licenza utente**, selezionare il tipo di utente a cui deve essere applicato il profilo.
6) Scegliere le licenze orientate all'utente selezionando le caselle di controllo desiderate.
7) Fare clic su **OK & Avanti**. Viene verificata la correttezza delle assegnazioni.

   Se tutte le licenze sono assegnate correttamente, la concessione delle licenze agli apparecchi è completata.
8) In caso di assegnazione errata viene visualizzato l'errore con una casella di controllo rossa ombreggiata. Correggere l'errore e ripetere il passaggio 7.

8.6.2 Come modificare un profilo licenza

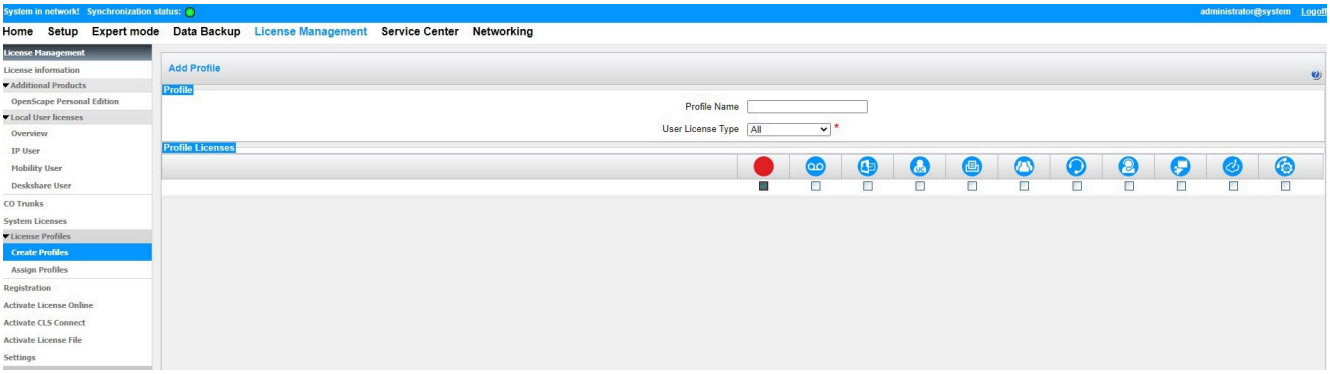
Modificare un profilo licenza esistente.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione, fare clic su **Profili licenza** > **Crea profili**. Vengono visualizzati tutti i profili licenza disponibili.



3) Attivare il pulsante di opzione di fianco al profilo licenza desiderato, quindi premere **Modifica**.
4) Modificare il profilo licenza in base alle proprie esigenze.
5) Fare clic su **OK & Avanti**. Viene verificata la correttezza delle assegnazioni.

   Se tutte le licenze sono assegnate correttamente, la modifica dei profili licenza è completata.
6) In caso di assegnazione errata viene visualizzato l'errore con una casella di controllo rossa ombreggiata. Correggere l'errore e ripetere il passaggio 5.

8.6.3 Come assegnare un profilo licenza a un utente

Assegnare un profilo licenza agli utenti disponibili.

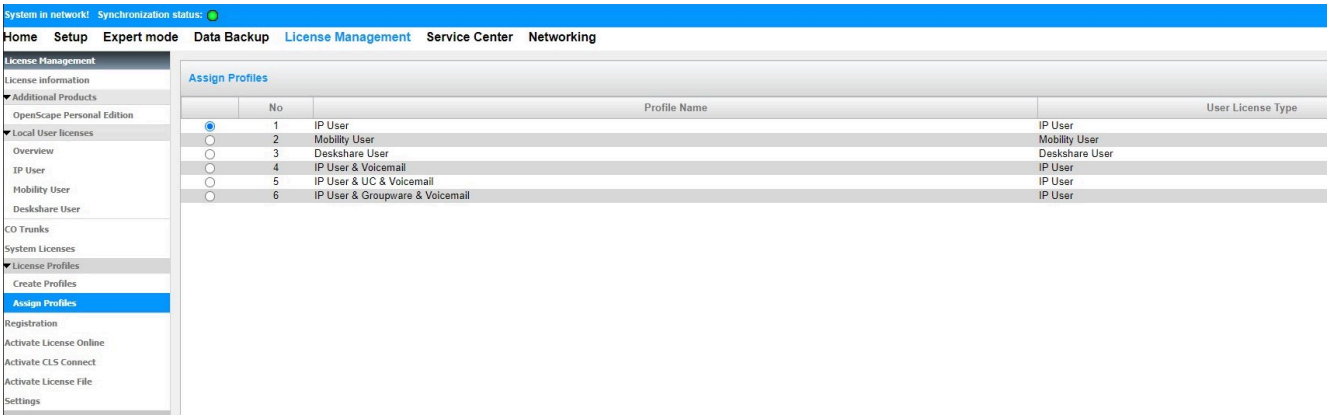
Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.

2) Nella struttura di navigazione, fare clic su **Profili licenza** > **Assegna profili**. Vengono visualizzati tutti i profili licenza disponibili.



3) Attivare il pulsante di opzione di fianco al profilo licenza desiderato, quindi premere **OK&Avanti**.
4) Nel campo a sinistra **Selezione** selezionare tutti gli utenti a cui occorre assegnare un profilo licenza.
5) Fare clic su **Aggiungi**. Gli utenti selezionati vengono visualizzati nella finestra a destra **Membri**.
6) Fare clic su **OK & Avanti**. Le licenze selezionate nel profilo licenza vengono assegnate agli utenti.

Nota: Nel caso del pagamento a consumo viene visualizzata una finestra popup. Fare clic su **OK** per confermare la propria scelta.

Nota: Gli utenti possono anche essere rimossi da un profilo utente o aggiunti ad esso successivamente.

8.6.4 Come eliminare un profilo licenza

Eliminare il profilo licenza esistente.

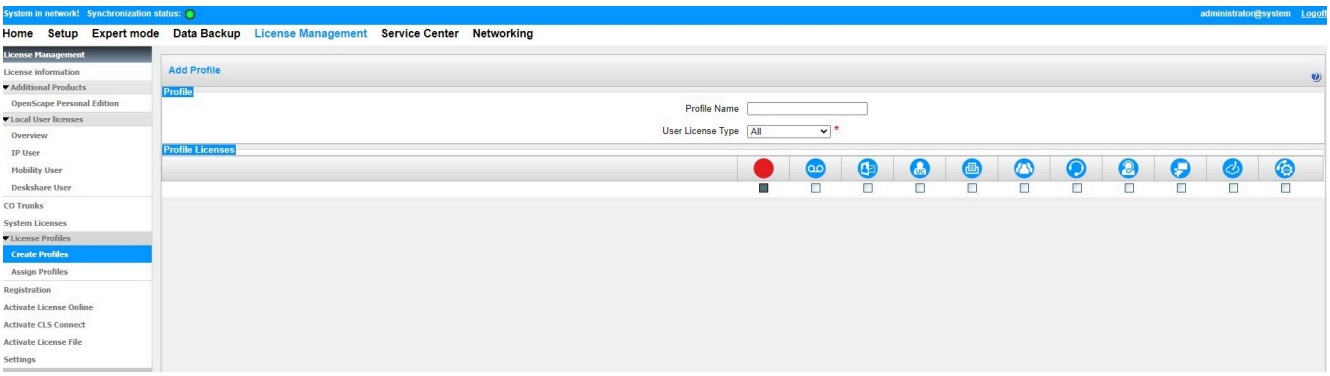
Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.

2) Nella struttura di navigazione, fare clic su **Profili licenza** > **Crea profili**. Vengono visualizzati tutti i profili licenza disponibili.



3) Attivare il pulsante di opzione di fianco al profilo licenza desiderato, quindi premere **Elimina**.
4) Confermare con **OK**. Il profilo licenza viene eliminato.

8.7 Rehost dopo sostituzione dell'hardware

È necessario aggiornare le licenze ogni volta che, nel sistema di comunicazione, si sostituiscono la scheda madre della piattaforma hardware o la scheda di rete del server Linux. Per il rehost sono necessari l'indirizzo MAC del vecchio hardware, quello del nuovo hardware e i dati di accesso per il server licenze centrale (CLS).

Dopo la sostituzione dell'hardware, i dati di configurazione devono essere ripristinati utilizzando il set di backup più recente (vedere Ripristino).

Essendo le licenze collegate all'indirizzo MAC assegnato all'hardware, alla sostituzione dell'hardware, sia l'indirizzo MAC che le licenze non saranno più validi. Dopo la sostituzione dell'hardware, il sistema di comunicazione si trova nuovamente nel cosiddetto "periodi di attivazione". Dopo aver inserito nel CLS il vecchio e il nuovo indirizzo MAC, può essere generato il nuovo file di licenza. Tale file viene caricato nel sistema di comunicazione in seguito all'aggiornamento offline; successivamente tutte le licenze disponibili vengono automaticamente attivate.

Per il soft switch viene utilizzato l'indirizzo MAC della scheda di rete del server Linux selezionato al momento dell'installazione del sistema operativo Linux (visibile sopra YaST). L'indirizzo MAC può essere letto anche usato il WBM.

Nota: Ogni procedura di rehost viene registrata nel CLS. Una licenza può essere utilizzata massimo tre volte per un rehost.

Nota: L'indirizzo IP del CLS può essere controllato e se necessario modificato tramite il WBM in **Gestione delle licenze** > **Impostazioni**.

8.7.1 Come eseguire un rehost dopo una sostituzione dell'hardware

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

L'hardware è stato sostituito ed è stata eseguita una procedura di rehost sul CLS.

I dati di configurazione sono stati ripristinati utilizzando il set di backup.

Il codice di autorizzazione licenza (LAC) per il rilascio della licenza è noto.

Per la connessione al server delle licenze, il sistema di comunicazione dispone di una connessione a Internet.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Attiva licenza in linea**.
3) Nel campo **Codice autorizzazione licenza (LAC)** immettere il LAC.
4) Non selezionare la casella di controllo per l'accesso al server delle licenze tramite nome utente e password. L'accesso al server delle licenze avviene automaticamente. (l'immissione di nome utente e password è necessaria solo per i rivenditori).
5) Fare clic su **Attiva**. Viene stabilita la connessione al server delle licenze e le licenze vengono aggiornate. Una volta concluso l'aggiornamento, la connessione si interrompe automaticamente.
6) Riavviare il sistema di comunicazione.

Passaggi successivi

Salvare i dati di configurazione in un nuovo set di backup (vedere Salvataggio immediato).

8.8 Server delle licenze (Central License Server, CLS)

Il server licenze (CLS) crea e gestisce i file di licenza.

Un file di licenza viene generato quando il cliente invia il codice di autorizzazione licenza al CLS tramite il WBM. La trasmissione del file di licenza al sistema di comunicazione avviene automaticamente tramite Internet. Se non è possibile la trasmissione automatica, è possibile caricare il file di licenza anche manualmente nel sistema di comunicazione.

8.8.1 Come interrogare o modificare l'indirizzo IP del server licenze

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Se è stato modificato l'indirizzo IP del server licenze centrale, è necessario conoscere l'indirizzo IP corrente.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Impostazioni**. Nel campo **Indirizzo IP server licenze centrale** viene visualizzato l'indirizzo IP del server licenze centrale (CLS). L'indirizzo IP attualmente valido è `188.64.16.4`.
3) Se è necessario modificare l'indirizzo IP del server licenze centrale, nel campo **Indirizzo IP server licenze centrale**, inserire il nuovo indirizzo IP del server licenze centrale, nel formato `123.124.125.126`.
4) Fare clic su **Attiva**.

8.8.2 Come verificare la connessione al Central License Server (CLS)

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Impostazioni**.
3) Nell'area **Server licenze centrale**, fare clic su **Verifica connessione CLS**.

Se è attiva una connessione Internet, viene visualizzato il messaggio **Connesso correttamente a CLS!**.

Se non è disponibile alcuna connessione Internet, viene visualizzato il messaggio **Nessuna connessione a CLS!**.

8.9 Agente licenze (Customer License Agent, CLA)

L'agente delle licenze (CLA) è parte integrante del software di comunicazione OpenScape Business e viene eseguito automaticamente in background. Gestisce il file di licenza e le licenze ivi contenute. Il CLA controlla i requisiti di licenza e se sono disponibili licenze sufficienti, attiva le licenze. È presente un solo CLA (CLA locale) per sistema di comunicazione. Se in un sistema di reti sono presenti più sistemi di comunicazione (nodi), è necessario usare solo un CLA (CLA centrale) sul nodo master.

Sono possibili le seguenti configurazioni:

- **Come configurare la connessione all'agente delle licenze locale**

  Se un nodo viene eliminato dal sistema di reti, viene eliminato anche il collegamento nel CLA centrale. Viene automaticamente utilizzato il CLA locale installato sul nodo. Se questo automatismo non funziona, è possibile realizzare manualmente la connessione al CLA locale.
- **Come modificare la connessione all'agente delle licenze centrale**

  Ogni nodo del sistema di reti richiede la connessione al CLA centrale sul nodo master. Questa connessione viene creata automaticamente con la procedura guidata **Rete** del WBM. Se viene modificato l'indirizzo IP del nodo master, occorre riconfigurare il collegamento al CLA centrale su tutti i nodi slave.

8.9.1 Come configurare la connessione all'agente delle licenze locale

Prerequisiti

Si è connessi al WBM del nodo desiderato.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Impostazioni**.
3) Selezionare il pulsante di opzione **Agente delle licenze locale (CLA)**.
4) Fare clic su **Attiva**.

8.9.2 Come modificare la connessione all'agente delle licenze centrale

Prerequisiti

Il sistema di comunicazione si trova in un sistema di reti.

Si è connessi al WBM del nodo desiderato.

Passo a passo

1) Nella barra di navigazione fare clic su **Gestione delle licenze**.
2) Nella struttura di navigazione fare clic su **Impostazioni**.
3) Selezionare il pulsante di opzione **Agente delle licenze centrale** e nel campo **Indirizzo IP agente delle licenze centralizzato** inserire l'indirizzo IP del nodo master (nodo 1) nel formato `123.124.125.126`.
4) Fare clic su **Attiva**.

8.10 Locking ID e Advanced Locking ID

A ogni sistema di comunicazione è assegnato un Locking ID o un Advanced Locking ID. Per garantire l'assegnazione univoca delle licenze, queste vengono collegate ai Locking ID.

ID del blocco

Con le piattaforme hardware, il Locking ID è l'indirizzo MAC del sistema di comunicazione.

Con i soft switch, il Locking ID è l'indirizzo MAC della scheda di rete del server Linux. Se il server Linux comprende più schede di rete, occorre selezionare la scheda di rete che alla prima messa in servizio verrà utilizzata dal server Linux.

Se il sistema di comunicazione si trova nel periodo di attivazione, nelle informazioni sulla licenza può venire visualizzato un indirizzo MAC non corretto. L'indirizzo MAC corretto può essere verificato nel **Centro assistenza** in **Inventario**.

Advanced Locking ID

Se un soft switch si trova in un ambiente virtuale, al posto del Locking ID, viene utilizzato l'Advanced Locking ID. Nel CLS viene generato l'Advanced Locking ID mediante l'ALI Calculator.

Devono essere configurati i seguenti parametri di sistema e di rete, in quanto sono utilizzati per la generazione dell'Advanced Locking ID a 24 caratteri:

- Indirizzo IP del gateway predefinito (server Linux)
- Nome host del server Linux
- Indirizzo IP del server Linux
- Indirizzo IP del server DNS (configurato nel server Linux)
- Fuso orario (server Linux)

Se uno o più di questi parametri di rete e di sistema non sono configurati, non è possibile generare l'Advanced Locking ID.

L'Advanced Locking ID viene visualizzato nel WBM. In alcuni casi, è possibile che l'ALI, generato nel CLS per il file di licenza sia diverso dall'ALI visualizzato nel WBM durante il periodo di attivazione. Il file di licenza con l'ALI diverso viene comunque accettato dal sistema.

Se viene modificato uno dei parametri di sistema e di rete sopra indicati, il soft switch ritorna allo stato senza licenza e viene generato un nuovo Advanced Locking ID. Per poter utilizzare il file di licenza acquistato, è necessario eseguire un rehost dal vecchio al nuovo Advanced Locking ID presso il server licenze centrale (CLS).

Se il sistema rileva una variazione dell'ALI, viene visualizzato un messaggio nella Home page di WBM, area Concessione della licenza, per informare l'utente della variazione dell'ALI. L'utente deve fare clic su Conferma per confermare di essere informato della modifica. Quindi il messaggio viene rimosso dalla Home page WBM, finché non si rileva una nuova istanza di variazione dell'ALI. Se l'utente non fa clic su Conferma, il messaggio rimane sempre visibile nella Home page.

Importante: In caso di modifica dei parametri Locking ID (indirizzo IP, indirizzo gateway, indirizzo DNS, nome hostname per i sistemi S, indirizzo MAC per i sistemi X), la licenza del sistema non è più valida. È necessario contattare un partner autorizzato presso il server licenze centrale per generare un nuovo file di licenza, che deve essere installato nel sistema.

Importante: Se un utente preme il pulsante di conferma, non viene inviata alcuna e-mail. L'e-mail viene inviata solo se l'utente non ha confermato le modifiche tramite la Home page. Il meccanismo dell'e-mail viene attivato ogni giorno, a intervalli di 24 ore, a partire dall'ultimo riavvio del sistema.

8.10.1 Come controllare il Locking ID del sistema di comunicazione

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Inventario**. Viene visualizzata una panoramica dei componenti appartenenti al sistema di comunicazione.

3) Fare clic su **OK & Avanti**. Vengono visualizzate informazioni su hardware e software. In **ID MAC per licenza** è riportato il Locking ID del sistema di comunicazione.

8.10.2 Come ottenere il Locking ID del soft switch

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Inventario**. Vengono visualizzate informazioni sul software del soft switch, sullo spazio di memoria libero e occupato del disco rigido e sullo stato delle applicazioni. In **ID MAC per licenza** è riportato il Locking ID del soft switch.

8.10.3 Come ottenere l'Advanced Locking ID dello soft switch

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

Nella barra di navigazione fare clic su **Gestione delle licenze**. Vengono visualizzate tutte le licenze disponibili. In **Locking ID** sono riportati gli Advanced Locking ID degli soft switch, se questi sono usati in un ambiente virtualizzato.

8.11 Come migrare dalla scheda madre V2 alla scheda madre V3 (sistema indipendente)

Prerequisiti

- Aggiornare all'ultima versione del sistema.
- Disinserire le schede IVM, pulire gli slot scheda e rimuovere la configurazione IVM dal sistema.
- Verificare che le porte nell'intervallo 511-532 non siano configurate. Queste porte verranno riservate da SmartVM sulla scheda madre V3. Questo è necessario solo per i sistemi che funzionano in modalità UC Smart.

  Per risolvere i problemi con la funzionalità UC Fax durante la migrazione al sistema con scheda madre V3, si consiglia di configurare la modalità operativa del sistema prima della migrazione. Se il sistema funziona in modalità UC Smart, l'amministratore deve eliminare la configurazione dalle porte 511-532 prima che abbia luogo la migrazione. Se il sistema funziona in modalità UC Smart, le porte SmartVM aggiuntive non saranno create e la configurazione fax non sarà interessata. Ad esempio, se il set di backup proviene da un sistema UC Suite, la modalità operativa del sistema della

scheda madre V3 deve essere impostata sulla modalità UC Suite prima di eseguire la migrazione del set di backup.

Nota: Quando si aggiorna un sistema OpenScape Business PAYGO, aggiornare prima il sistema OpenScape Business al software V3 e successivamente utilizzare la funzione di **ricreazione della chiave di licenza** su CLS per ricevere un file di licenza valido per V3 che disponga della licenza "OpenScape Business Info Ready for V3 SW F31505-K158-D129". Fatto ciò, il file di licenza ricreato deve essere attivato manualmente all'interno di OpenScape Business System WBM, alla voce **Gestione delle licenze**.

Nota: Quando si aggiorna un sistema OpenScape Business PAYGO, aggiornare prima il sistema OpenScape Business al software V3 e successivamente utilizzare la funzione di **ricreazione della chiave di licenza** su CLS per ricevere un file di licenza valido per V3 che disponga della licenza "OpenScape Business Info Ready for V3 SW F31505-K158-D129". Fatto ciò, il file di licenza ricreato deve essere attivato manualmente all'interno di OpenScape Business System WBM, alla voce **Gestione delle licenze**.

Passo a passo

1) Passare alla modalità operativa del sistema appropriata.

Il backup del sistema eseguito in una modalità operativa non può essere utilizzato in un'altra. Se, ad esempio, si esegue il backup del sistema nella modalità UC Suite, occorrerà far passare il sistema aggiornato alla modalità UC Suite prima di ripristinare il backup; non è possibile ripristinare un backup nella modalità UC Smart.

Il sistema con scheda madre V3 funziona in modalità UC Smart:

Le porte Smart VM aggiuntive verranno create come oggi, l'amministratore deve eliminare la configurazione dal suddetto intervallo di porte sul sistema OCC prima che avvenga la migrazione.

Il sistema con scheda madre V3 funziona in modalità UC Suite:

Le porte SmartVM aggiuntive non verranno create, quindi la configurazione del fax non sarà interessata.

2) Attivare la licenza del sistema.

CLS Connect	Azione
Attivata	Ricreare la licenza sull'indirizzo MAC V3 di CLS.
Non attivata	Importare la nuova licenza e attivarla sul sistema OpenScape Business V2. Si attiva la richiesta di autenticazione del codice di conferma, che viene visualizzato nella pagina iniziale di WBM.

3) Eseguire il backup del sistema V2, inclusa la configurazione del sistema.
   Se l'OCC è connessa a un Booster Server, occorre scaricare e salvare un backup completo impostato da Booster Server.
4) Cambiare la scheda madre.
5) Importare la nuova licenza

CLS Connect	Azione
Attivata	Importare il file di licenza V3 da CLS in OpenScape Business; **CLS Connect** verrà attivato sulla scheda madre V3.
Non attivata	Creare una nuova licenza V3 utilizzando il codice di conferma su CLS con l'indirizzo MAC della scheda madre V3 e importare il nuovo file di licenza V3 in OpenScape Business.

6) Ripristinare il backup di V2 nella scheda madre V3.
7) Modificare la configurazione degli indirizzi IP dei client UC.
   Alla prima connessione dei client UC (dopo la migrazione), utilizzare il nuovo indirizzo IP della scheda madre V3.

Solo la modalità Full-duplex è supportata con la scheda madre V3.

La scheda madre V3 non supporta più i dispositivi OptiPoint 4xx/5xx.

8.12 Come migrare il nodo master di un sistema connesso in rete dalla scheda madre V2 alla scheda madre V3

Prerequisiti

Il sistema dispone di una licenza per il collegamento in rete.

Passo a passo

1) Aggiornare tutti i nodi slave di OpenScape Business a V3.

Scenario	Procedura da seguire
Eseguire l'aggiornamento con CLS Connect	Aggiornamento da V2 a V3 con CLS Connect alla pagina 342
Eseguire l'aggiornamento senza CLS Connect	Aggiornamento da V2 a V3 senza CLS Connect alla pagina 343

2) Migrare il nodo master del sistema.
   Seguire le istruzioni su Come migrare dalla scheda madre V2 alla scheda madre V3 (sistema indipendente) alla pagina 339

Fino alla migrazione del nodo master, i nodi slave saranno in modalità failover. Dopo la migrazione del nodo master, funzioneranno di nuovo appieno.

8.13 Come migrare il nodo slave di un sistema connesso in rete dalla scheda madre V2 alla scheda madre V3

Prerequisiti

Il sistema dispone di una licenza per il collegamento in rete.

Nota: Se CLS Connect non è attivato, rimuovere prima il sistema slave dalla rete su CLS.

Passo a passo

1) Migrare il sistema slave.
   Seguire le istruzioni su Come migrare dalla scheda madre V2 alla scheda madre V3 (sistema indipendente) alla pagina 339
2) Aggiornare o migrare il nodo master.

Scenario	Procedura da seguire
Migrazione dalla scheda madre V2 alla scheda madre V3	Come migrare dalla scheda madre V2 alla scheda madre V3 (sistema indipendente) alla pagina 339
Eseguire l'aggiornamento software con CLS Connect	Aggiornamento da V2 a V3 con CLS Connect alla pagina 342
Eseguire l'aggiornamento software senza CLS Connect	Aggiornamento da V2 a V3 senza CLS Connect alla pagina 343

8.14 Migrazione dei sistemi HiPath 3000 al software OSBiz V3 con scheda madre V3

La migrazione del software viene eseguita tramite il normale processo di migrazione da HiPath 3000 a OSBiz utilizzando lo strumento Manager E. Le licenze HiPath 3000 ComScendo e S2m esistenti vengono aggiornate all'indirizzo MAC della scheda madre OCCe. Le licenze TDM e l'indicatore software V3 vengono generati dal CLS, in base alle informazioni del file XML create da ManagerE durante questa procedura.

Nel caso di una scheda madre OCC riutilizzata da una precedente migrazione di OSBiz a OCCe, non è possibile alcuna migrazione della licenza. Tutte le licenze devono essere acquistate.

In caso di un OCC da stock di parti di ricambio o appena acquistato (l'indirizzo MAC non è bloccato in CLS), è possibile aggiornare HiPath 3000 a quell'indirizzo MAC e viene generato un nuovo file di licenza (come con la migrazione a OSBiz V2).

8.15 Aggiornamento da V2 a V3 con CLS Connect

Occorre aggiornare la V2R7 più recente e **CLS Connect** è attivo. Le licenze OpenScape Business V2 collegate all'indirizzo MAC della scheda madre OCC sono valide anche per V3.

Aggiornato il software, all'avvio, il software OpenScape Business V3 indica su CLS che le licenze funzionano in combinazione con il software V3. Le informazioni V3 vengono aggiunte nel file di licenza e ritrasferite automaticamente nel sistema tramite CLS Connect durante l'avvio. Non sono necessarie azioni manuali.

Non sono necessarie azioni nel caso in cui si aggiorni il software senza migrare i sistemi slave con una licenza per il collegamento in rete. In questo caso, i sistemi slave possono essere aggiornati e la relativa licenza verrà aggiornata automaticamente dopo l'aggiornamento/la migrazione del sistema master.

8.16 Aggiornamento da V2 a V3 senza CLS Connect

Prerequisiti

- CLS Connect non è attivo
- OpenScape Business S necessita dell'accesso a Internet
- Se si aggiorna un nodo slave in un sistema connesso in rete, rimuovere prima lo slave da CLS.

Passo a passo

1) Attivare la licenza di upgrade software su CLS come una normale licenza per il sistema OpenScape Business. L'attivazione sulla licenza di upgrade software su CLS crea un nuovo file di licenza contenente:

- La nuova licenza V3
- Il nuovo ID (progressivo) del file di licenza
- Se il sistema è OSBiz S, al certificato viene aggiunto CLS Connect Start.

2) Importare questo nuovo file di licenza e attivarlo su OpenScape Business V2.

3) Eseguire l'aggiornamento software da V2 a V3.

Durante l'avvio, eseguito l'aggiornamento software a V3, il sistema OpenScape Business controlla il file di licenza e consente la funzionalità di concessione della licenza solo se il componente licenza V3 è disponibile nel file di licenza.

9 Integration nella rete dati interna (LAN)

L'integrazione del sistema di comunicazione nella rete interna esistente (LAN) consente l'utilizzo di soluzioni UC e la gestione del sistema di comunicazione sul PC della rete interna.

Occorre configurare nel WBM i seguenti parametri di rete:

- Piattaforma hardware OpenScape Business X: indirizzo IP e maschera di rete della scheda madre e della UC Booster Card (se presente). Queste impostazioni vengono eseguite durante l'installazione iniziale, tuttavia possono essere modificate anche in seguito.

  Softswitch OpenScape Business S: l'indirizzo IP e la maschera di rete del server Linux su cui viene eseguito il software di comunicazione. Queste impostazioni vengono eseguite durante l'installazione di Linux, tuttavia possono essere modificate anche in seguito.
- Il sistema di comunicazione può in via opzionale essere configurato come server DHCP (provvisto di parametri di rete specifici, tra cui maschera di sottorete, gateway predefinito, server DNS) o come agente di inoltro DHCP. La configurazione come server DHCP avviene durante l'installazione iniziale ma può essere in seguito modificata. Per la configurazione come agente di inoltro DHCP è richiesta la Modalità esperti.
- Indirizzo IP del router predefinito e del server DNS (esterno) per l'accesso ad altre reti IP (ad esempio, Internet). Queste impostazioni vengono eseguite durante l'installazione iniziale, tuttavia possono essere modificate anche in seguito.

9.1 Interfaccia LAN

Per collegare il sistema di comunicazione all'infrastruttura LAN, occorre adeguare l'indirizzo IP e l'intervallo di indirizzi IP interni del sistema di comunicazione allo schema di indirizzi IP della rete interna (LAN).

9.1.1 Indirizzo IP e maschera di rete dell'interfaccia LAN

L'indirizzo IP e la maschera di rete del sistema di comunicazione sono definiti alla prima installazione, tuttavia possono essere successivamente modificati. Se necessario, l'indirizzo IP e/o la maschera di rete devono essere adattati all'intervallo di indirizzi IP della LAN.

Piattaforma hardware

Per impostazione predefinita, alla piattaforma hardware viene assegnato un indirizzo IP e una maschera di sottorete. La UC Booster Card richiede anche un indirizzo IP. Indipendentemente dal fatto che La UC Booster Card sia collegata o meno, è necessario configurare il relativo indirizzo IP.

Per l'integrazione nella LAN, la piattaforma hardware utilizza l'interfaccia "LAN" della scheda madre. Se viene inserita la UC Booster Card, è necessario connettere l'interfaccia "LAN" della UC Booster Card alla LAN. La piattaforma hardware e la UC Booster Card devono trovarsi nella stessa sottorete.

Per rendere effettive le modifiche dell'intervallo di indirizzi IP o della maschera di rete, è necessario riavviare la piattaforma hardware.

In seguito a un aggiornamento del software, le modifiche apportate all'indirizzo IP e alla maschera di sottorete vengono mantenute, ma in caso di ricarica della piattaforma hardware, verranno ripristinate le impostazioni predefinite. Queste modifiche non possono essere salvate in un set di backup.

Soft switch

Con il softswitch, il server Linux su cui è installato il software di comunicazione viene integrato nella LAN tramite la sua scheda di rete.

Le modifiche dell'indirizzo IP o della maschera di sotto rete diventano effettive dopo il riavvio dell'applicazione (vedere Riavvia, Ricarica, Arresta).

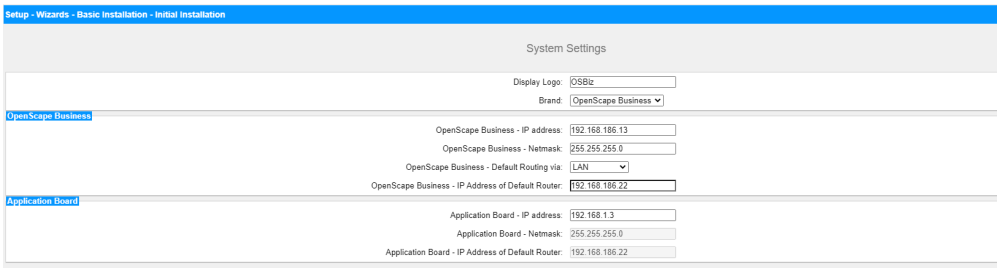
9.1.1.1 Come modificare l'indirizzo IP e la maschera di rete della piattaforma hardware

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Fare clic su **Modifica**, per avviare la procedura guidata **Prima installazione**.



3) In **OpenScape Business - Indirizzo IP**, modificare l'indirizzo IP della piattaforma hardware. L'indirizzo IP deve essere conforme allo schema di indirizzi IP e non può essere già assegnato ad alcun client della rete esistente, in quanto ciò produrrebbe un conflitto tra indirizzi IP. Per impostazione predefinita, l'indirizzo IP preimpostato è `192.168.1.2`.
4) In **OpenScape Business - Maschera di rete**, modificare la maschera di rete della piattaforma hardware. La maschera di rete deve corrispondere allo schema degli indirizzi IP della rete interna. Per impostazione predefinita, la maschera di sub-rete preimpostata è `255.255.255.0`.
5) Fare clic su **OK & Avanti**.
6) Fare clic su **OK & Avanti** finché non viene visualizzato il messaggio che segnala la configurazione riuscita del servizio.
7) Fare clic su **Fine**. La piattaforma hardware si riavvia automaticamente.

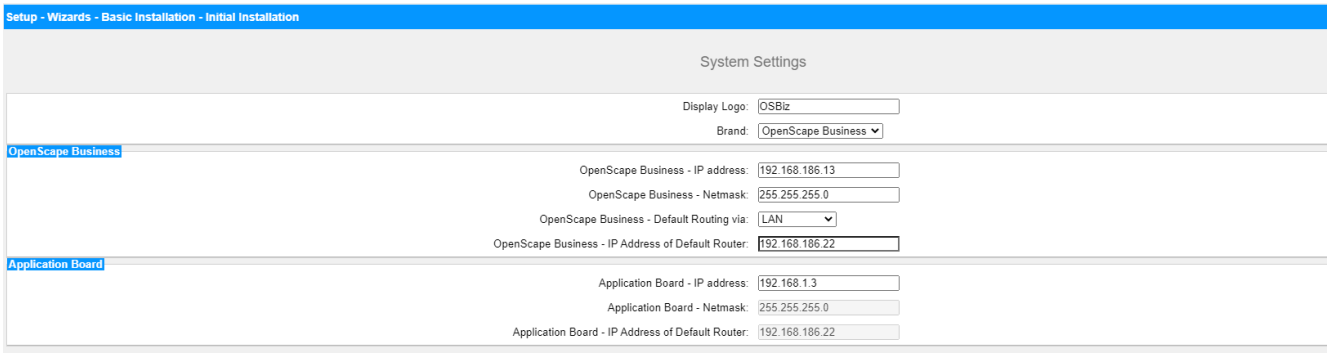
9.1.1.2 Come modificare l'indirizzo IP della UC Booster Card

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Fare clic su **Modifica**, per avviare la procedura guidata **Prima installazione**.



3) In **UC Booster Card - Indirizzo IP**, modificare l'indirizzo IP della UC Booster Card. L'indirizzo IP deve essere conforme allo schema di indirizzi IP e non può essere già assegnato ad alcun client della rete esistente, in quanto ciò produrrebbe un conflitto tra indirizzi IP. Per impostazione predefinita, l'indirizzo IP preimpostato è `192.168.1.3`.
4) Fare clic su **OK & Avanti**.
5) Fare clic su **OK & Avanti** finché non viene visualizzato il messaggio che segnala la configurazione riuscita del servizio.
6) Fare clic su **Fine**. La piattaforma hardware si riavvia automaticamente.

9.1.1.3 Come modificare l'indirizzo IP e la maschera del soft switch

Passo a passo

1) Nella barra delle applicazioni, fare clic su **Computer**.
2) Nella struttura dei menu fare clic su **Sistema** > **YaST**.
3) Immettere la password dell'utente root e fare clic su **Continue** (Continua). Si apre YaST Control Center.
4) Nella struttura dei menu, fare clic su **Network Devices** (Periferiche di rete).
5) Nell'area **Periferiche di rete**, fare clic su **Impostazioni di rete**.
6) Nella finestra **Overview** (Panoramica) selezionare la scheda di rete desiderata e fare clic su **Edit** (Modifica).
7) Selezionare il pulsante di opzione **Statically assigned IP Address** (Indirizzo IP assegnato staticamente).
8) In **Indirizzo IP**, modificare l'indirizzo IP del server Linux su cui viene eseguito il software del soft switch. L'indirizzo IP deve essere conforme allo schema di indirizzi IP e non può essere già assegnato ad alcun client della rete esistente, in quanto ciò produrrebbe un conflitto tra indirizzi IP.
9) In **Maschera di sub-rete** modificare la maschera di sub-rete del server Linux. La maschera di sub-rete deve corrispondere allo schema degli indirizzi IP della rete interna.
10) Fare clic su **Avanti**, quindi su **OK**.
11) Chiudere il **YaST Control Center**.

9.1.2 Intervallo di indirizzi IP interno dell'interfaccia LAN

All'occorrenza, è possibile modificare l'intervallo di indirizzi IP interni dell'interfaccia LAN utilizzato dalla piattaforma hardware per la comunicazione interna dei suoi moduli.

Per impostazione predefinita, la piattaforma hardware utilizza l'intervallo di indirizzi IP interno 192.168.3.xxx. Questo può essere modificato anche con l'intervallo di indirizzi IP desiderato. La maschera di sub-rete interna è 255.255.255.0 e non può essere modificata.

Per rendere effettive le modifiche dell'intervallo di indirizzi IP interno, è necessario riavviare la piattaforma hardware.

In seguito a un aggiornamento del software, le modifiche apportate all'intervallo di indirizzi IP interni vengono mantenute, ma in caso di ricarica del sistema, verranno ripristinate le impostazioni predefinite. Queste modifiche non possono essere salvate in un set di backup.

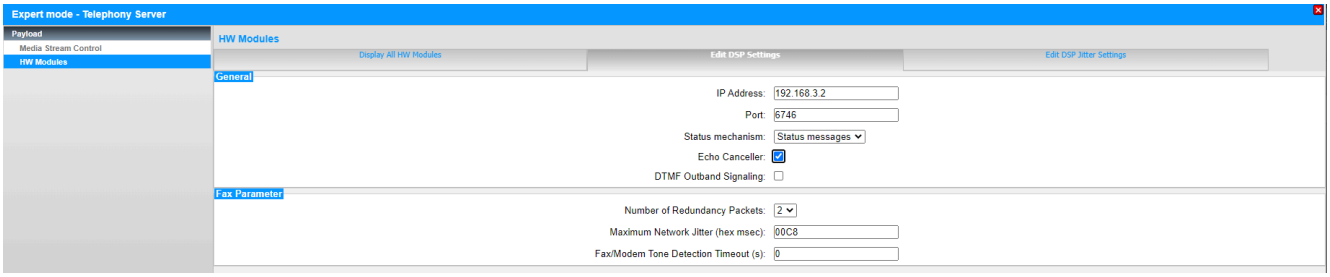
9.1.2.1 Come modificare l'intervallo di indirizzi IP interni della piattaforma hardware

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Payload**.
3) Nella struttura dei menu fare clic su **Moduli hardware**.
4) Fare clic sulla scheda **Modifica le impostazioni DSP**.



5) Nell'area **Generale** in **Indirizzo IP**, inserire un indirizzo IP per il sistema di comunicazione compreso nel nuovo intervallo interno desiderato, ad esempio `192.168.40.2`. L'intero intervallo di indirizzi IP (nell'esempio `192.168.40.xxx`) è ora inaccessibile ad altri client della LAN.
6) Fare clic su **Applica** e confermare con **OK**.

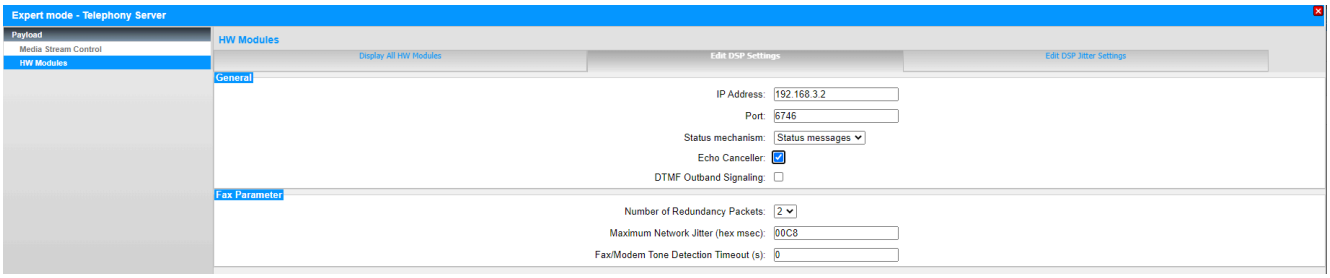
9.1.2.2 Come reimpostare l'intervallo di indirizzi IP interni della piattaforma hardware

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Payload**.
3) Nella struttura dei menu fare clic su **Moduli hardware**.
4) Fare clic sulla scheda **Modifica le impostazioni DSP**.



5) Nell'area **Generale** in **Indirizzo IP**, inserire l'indirizzo IP `192.168.3.2`. L'intero intervallo IP (`192.168.3.xxx`) è ora inaccessibile ad altri client della LAN.
6) Fare clic su **Applica** e confermare con **OK**.

9.2 DHCP

Il Dynamic Host Configuration Protocol (DHCP) consente, grazie server DHCP, l'assegnazione dinamica di dati specifici della rete agli utenti IP di una rete (ad esempio, una rete LAN).

Mediante DHCP è possibile l'integrazione automatica di un utente IP (ad esempio un telefono IP o un PC) in una LAN esistente. L'utente IP deve essere configurato per ricevere automaticamente i dati specifici della rete ed è quindi un client DHCP. Su richiesta, il server DHCP fornisce a utenti IP dati specifici della rete.

9.2.1 Agente di inoltro DHCP

Quando si utilizza il server DHCP interno della piattaforma hardware, il server DHCP interno e quello dei client DHCP devono trovarsi sullo stesso segmento di rete. In caso contrario, la piattaforma hardware deve essere configurata come agente di inoltro DHCP. Le interrogazioni DHCP degli utenti IP vengono in seguito inoltrate dalla piattaforma hardware al server DHCP effettivo.

9.2.1.1 Come configurare la piattaforma hardware come agente relè DHCP

Se la piattaforma hardware è configurata come agente relè DHCP, inoltra le richieste DHCP al server DHCP esterno.

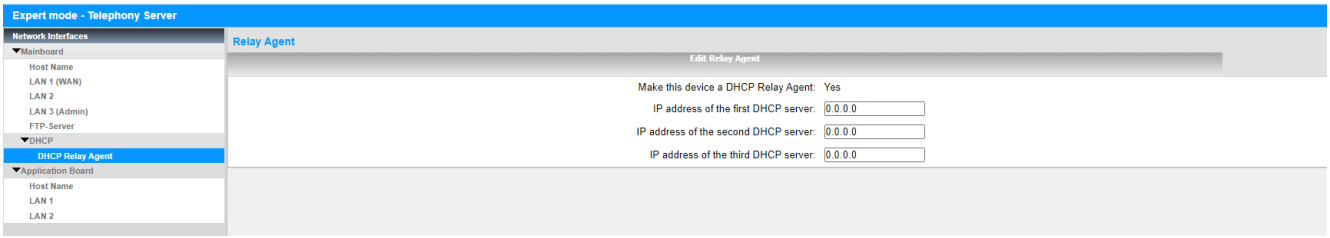
Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Interfacce di rete**.
3) Nella struttura dei menu, fare clic su **Scheda madre** > **DHCP**.
4) Abilitare il pulsante di opzione **Agente relè DHCP**.
5) Fare clic su **Applica** e confermare con **OK**.
6) Nella struttura dei menu, fare clic su **Agente relè DHCP**.



7) Inserire qui l'**Indirizzo IP del primo server DHCP**.
8) Inserire qui l'**Indirizzo IP del secondo server DHCP**.
9) Inserire qui l'**Indirizzo IP del terzo server DHCP**.

Suggerimento: È possibile inserire fino a tre server DHCP. L'inserimento del primo server DHCP è obbligatorio.

10) Fare clic su **Applica**, quindi su **OK**.

9.2.2 Server DHCP

Il server DHCP assegna dinamicamente agli utenti IP (telefoni IP, telefoni SIP, PC, access point WLAN ecc.) dati di rete specifici, quali l'indirizzo IP da utilizzare, la maschera di rete dell'utente IP, l'indirizzo IP del gateway predefinito, l'indirizzo IP del server SNTP ecc.

Come server DHCP può essere usato il server DHCP interno del sistema di comunicazione o un server DHCP esterno (ad esempio il server DHCP-del router Internet).

Nella piattaforma hardware, per impostazione predefinita viene attivato il server DHCP integrato. Se viene utilizzato il server DHCP esterno, occorre disattivare il server DHCP interno. In caso contrario, si verificano conflitti con il server DHCP esterno.

Con il soft switch è possibile configurare il server Linux come server DHCP interno.

In occasione della prima messa in servizio si deve decidere se verrà utilizzato il server DHCP interno del sistema di comunicazione o un server DHCP esterno. Il server DHCP interno può essere attivato o disattivato anche successivamente. Successivamente è possibile configurare anche i dati specifici della rete.

Server DHCP interno

Se viene utilizzato il server DHCP interno, gli utenti IP ricevono automaticamente i seguenti dati specifici della rete:

- Indirizzo IP e maschera di rete dell'utente IP
- Indirizzo IP del sistema di comunicazione (gateway predefinito)

- Indirizzo IP del server SNTP (per l'indicazione con data e ora)
- Indirizzo IP del server DNS (per la risoluzione del nome)
- Indirizzo IP del server SIP (destinato all'autenticazione degli utenti SIP)
- Indirizzo IP del server DLI interno o del server DLS esterno (per l'aggiornamento del software dei telefoni di sistema IP)
- Regole di routing

Server DHCP esterno

Se viene utilizzato un server DHCP esterno, questo deve disporre di uno spazio riservato a opzioni specifiche del fornitore che consenta di definire parametri specifici del produttore. Nel server DHCP esterno è necessario inserire i seguenti dati specifici di rete:

- Indirizzo IP e maschera di rete dell'utente IP
- Indirizzo IP del router predefinito = Opzione 3
- Indirizzo IP del sistema di comunicazione (gateway predefinito) = Opzione 33
- Indirizzo IP del server DNS (per la risoluzione del nome) = Opzione 6
- Indirizzo IP del server DLI interno o del server DLS esterno (per l'aggiornamento del software dei telefoni di sistema IP) = Opzione 43
- Consentiti solo per telefoni SIP: indirizzo IP del server SIP (destinato all'autenticazione degli utenti SIP) = Opzione 120
- Consentiti solo per telefoni SIP: indirizzo IP del server SNTP (per l'indicazione di data e ora nei telefoni SIP) = Opzione 42

Nota: Per ulteriori informazioni sul server DHCP in un ambiente Windows, vedere: http://wiki.unify.com/wiki/DHCP_Server_in_a_Windows_environment.

Se non è possibile inserire tali dati nel server DHCP esterno, dovranno essere immessi direttamente nei telefoni IP di sistema. Solo a questo punto, è possibile fornire ai telefoni IP di sistema, ad esempio, la data e l'ora corrente e il software più aggiornato.

Per ulteriori informazioni, consultare la seguente pagina di Unify Experts Wiki in: http://wiki.unify.com/wiki/DHCP

Pool di indirizzi di DHCP (intervallo di indirizzi IP)

Quando un utente IP accede al server DHCP, gli viene assegnato tra l'altro un indirizzo IP dinamico. L'amministratore può definire un intervallo di indirizzi IP entro il quale il server DHCP può assegnare gli indirizzi IP agli utenti IP. Ad es. non è ammesso assegnare qualsiasi indirizzo IP previsto dalla banda 192.168.1.x, bensì solo da 192.168.1.50 a 192.168.1.254, poiché gli indirizzi IP più bassi fino a 192.168.1.49 sono riservati agli utenti IP con indirizzi IP statici.

È anche possibile configurare più intervalli IP per il server interno DHCP in Modalità esperti, selezionando **Interfacce di rete**.

9.2.2.1 Come abilitare e configurare il server DHCP della piattaforma hardware

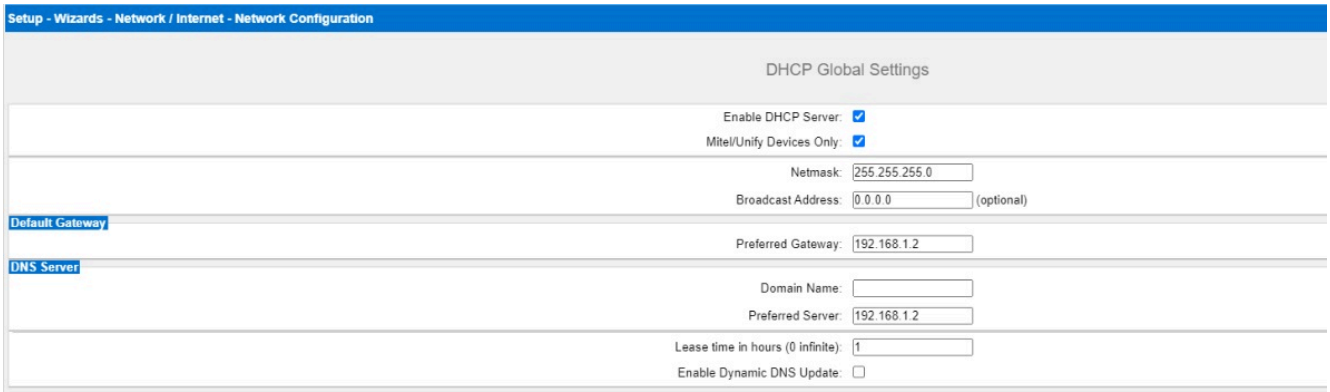
È possibile usare la procedura guidata **Configurazione di rete** per abilitare e configurare il server DHCP della piattaforma hardware.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Rete/ Internet**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Rete Internet**.



4) Selezionare la casella di controllo **Abilita server DHCP**.
5) Se necessario, abilitare la casella di controllo **Solo dispositivi Mitel/Unify**.

Nota: Questa opzione è disponibile solo per le schede madri V3.

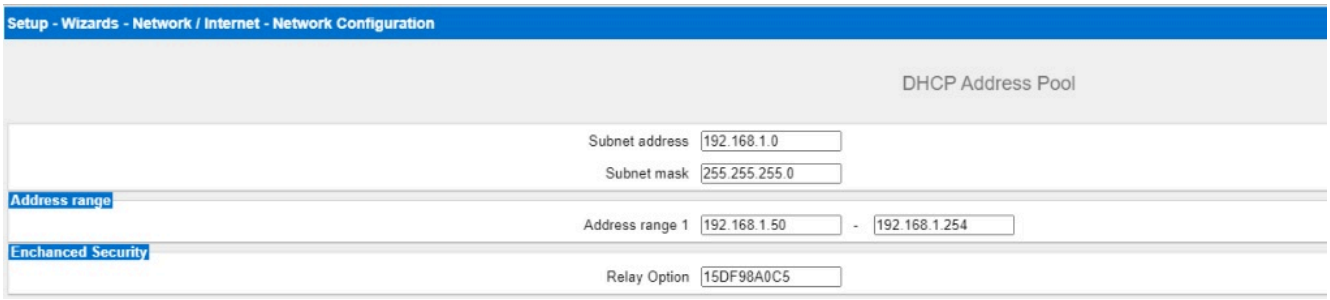
---

6) Inserire la maschera di sottorete della propria rete nel campo **Maschera di sottorete** (ad es. `255.255.255.0`).
7) Nel campo **Indirizzo di trasmissione**, inserire l'indirizzo di broadcast (l'ultimo indirizzo IP della rete o sottorete, valore predefinito: `0.0.0.0`) se necessario.
8) Nel campo **Gateway preferito**, inserire l'indirizzo IP del gateway predefinito. Di regola, l'indirizzo IP del router di Internet è `192.168.1.1`.
9) Se è necessario un nome di dominio completamente qualificato per il server DHCP, inserirlo in **Nome dominio** (massimo 80 caratteri).
10) Nel campo **Server preferito**, inserire l'indirizzo IP di un server DNS disponibile, ad esempio, l'indirizzo IP del router Internet, `192.168.1.1`.
11) Se necessario, inserire il periodo massimo di validità in ore (valore predefinito): 1 h, 0 = periodo di validità infinito, nel campo **Periodo di validità in ore (0 infinito)**.
12) Se si desidera consentire gli aggiornamenti dinamici del server DNS, abilitare l'opzione **Abilita aggiornamento DNS dinamico** (valore predefinito: disabilitato).

Nota: Se l'opzione Aggiornamento DNS dinamico è abilitata, è obbligatorio configurare il **Nome di dominio** nel campo Nome di dominio del pool di indirizzi IP.

---

13) Fare clic su **OK & Avanti**. Vengono visualizzate le impostazioni del pool di indirizzi DHCP.



14) Nel campo **Indirizzo sottorete**, inserire l'indirizzo IP più basso della sottorete in cui si trova l'intervallo di indirizzi IP desiderato (nel nostro esempio, `192.168.1.0`).
15) Inserire la maschera di sottorete dell'intervallo di indirizzi IP desiderato nel campo **Maschera di sottorete** (ad es. `255.255.255.0`).
16) Inserire la soglia superiore e inferiore per l'intervallo di indirizzi IP desiderato nel campo **Intervallo indirizzi 1** (ad es. da `192.168.1.50` a `192.168.1.254`).
17) Se necessario, specificare il valore del campo **Opzione relè**.

Nota: Questa opzione è disponibile solo per le schede madri V3.

---

18) Fare clic su **OK & Avanti**. Viene visualizzata la finestra **Impostazioni degli instradamenti**.
19) Nel campo **Indirizzo IP del server DNS**, inserire l'indirizzo IP di un server DNS disponibile, ad esempio, l'indirizzo IP del router Internet, `192.168.1.1`.
20) Dall'elenco a discesa **Instradamento predefinito tramite**, scegliere la voce **LAN**.
21) Se l'accesso a Internet avviene tramite un router Internet, inserire l'indirizzo IP del router Internet (ad es. `192.168.1.1`) nel campo **Indirizzo IP del router predefinito**.
22) Fare clic su **OK & Avanti**, quindi su **Fine**.

9.2.2.2 Come disabilitare il server DHCP della piattaforma hardware

È possibile usare la procedura guidata **Configurazione di rete** per disattivare il server DHCP della piattaforma hardware.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Rete/ Internet**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Rete Internet**.

4) Deselezionare la casella di controllo **Abilita server DHCP**.
5) Continuare a fare clic su **OK & Avanti** finché non si riceve un messaggio che indica che la funzione è stata installata.
6) Fare clic su **Fine**.

9.2.2.3 Come attivare e configurare il server DHCP del soft switch

Passo a passo

1) Nella barra delle applicazioni, fare clic su **Computer**.
2) Nella struttura dei menu fare clic su **Sistema** > **YaST**.
3) Immettere la password dell'utente root e fare clic su **Continue** (Continua). Si apre YaST Control Center.
4) Nella struttura dei menu, fare clic su **Servizi di rete**.
5) Nell'area **Servizi di rete**, fare clic su **Server DHCP**.
6) Selezionare la scheda di rete desiderata e premere **Seleziona**.
7) Selezionare la casella di controllo **Open Firewall for Selected Interfaces** (apri firewall per interfacce selezionate).
8) Fare clic su **Avanti**.
9) Se per il server DHCP è necessario un nome di dominio completo, inserirlo nel campo **Nome dominio** (max. 80 caratteri).
10) Nel campo **Primary Name Server IP** (IP server dei nomi principale), inserire l'indirizzo IP di un server DNS disponibile, ad esempio l'indirizzo del router Internet, `192.168.1.1`.
11) Nel campo **Gateway preferito**, immettere l'indirizzo IP del gateway predefinito. Normalmente si tratta dell'indirizzo IP del router Internet, ad esempio `192.168.1.1`.
12) Nel campo **NTP Time Server** (Server di riferimento ora NTP), inserire il server SNTP definito alla prima messa in servizio.
13) Fare clic su **Avanti**.
14) Nel campo **First IP Address** inserire il limite inferiore e nel campo **Last IP Address** il limite superiore dell'intervallo di indirizzi IP desiderato (ad esempio, da `192.168.1.50` fino a `192.168.1.254`).
15) Selezionare la casella di controllo **Allow Dynamic BOOTP**.
16) Fare clic su **Avanti**.
17) Selezionare il pulsante di opzione **When Booting** (All'avvio).
18) Fare clic su **Fine**.
19) Chiudere il **YaST Control Center**.

9.2.2.4 Come disattivare il server DHCP del soft switch

Passo a passo

1) Nella barra delle applicazioni, fare clic su **Computer**.
2) Nella struttura dei menu fare clic su **Sistema** > **YaST**.
3) Immettere la password dell'utente root e fare clic su **Continue** (Continua). Si apre YaST Control Center.
4) Nella struttura dei menu, fare clic su **Servizi di rete**.

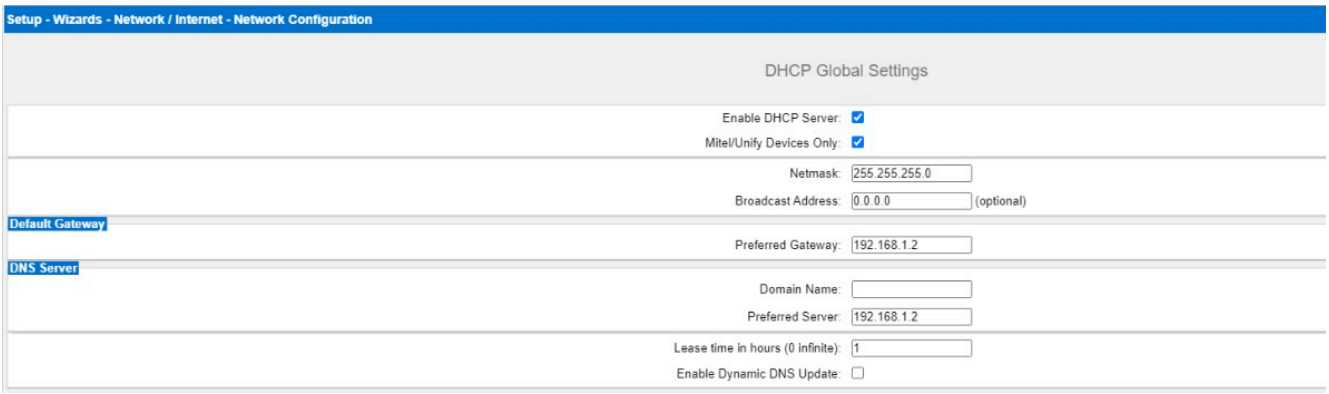
5) Nell'area **Servizi di rete**, fare clic su **Server DHCP**.
6) Deselezionare la casella di controllo **Avvio server DHCP**.
7) Fare clic su **Fine**.
8) Chiudere il **YaST Control Center**.

9.2.2.5 Come abilitare il DHCP solo per i dispositivi Mitel/Unify

Questa opzione consente all'amministratore di sistema di attivare il servizio DHCP di OpenScape Business esclusivamente per i dispositivi Mitel e Unify.

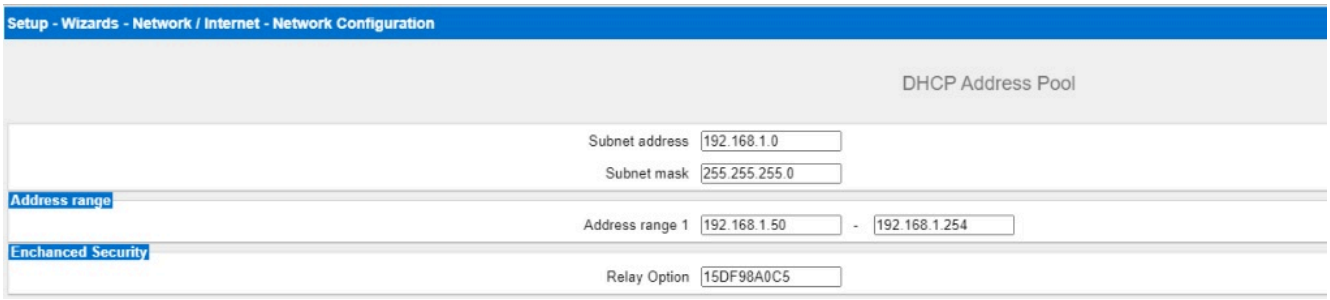
Prerequisiti

Si è nella finestra **Impostazioni DHCP globali**.



Passo a passo

1) Lasciare la casella di controllo **Abilita server DHCP** abilitata.
2) Fare clic per abilitare la casella di controllo **Solo dispositivi Mitel/Unify**. Per ulteriori informazioni su questa opzione, vedere la sezione Server DHCP > Parametri globali.
3) Andare su **Netmask** e regolare la maschera di sottorete in base all'intervallo di indirizzi IP (ad esempio `255.255.255.0`).
4) Nel campo **Gateway preferito**, inserire l'indirizzo IP del router Internet (ad esempio `192.168.1.1`).
5) Nel campo **Server preferito**, inserire l'indirizzo IP del server DNS (ad esempio, l'indirizzo IP del router Internet, `192.168.1.1`.
6) Fare clic su **OK & Avanti**. Si apre la finestra **Pool di indirizzi DHCP**.



7) Specificare i valori per **Indirizzo di sottorete**, **Maschera di sottorete** e **Intervallo indirizzi 1** per definire l'intervallo di indirizzi IP da gestire dal server DHCP interno.

   Se la rete interna utilizza indirizzi IP statici (ad esempio, per un server di stampa), l'intervallo di indirizzi IP (pool di indirizzi DHCP) deve essere selezionato in modo che gli indirizzi IP fissi non siano inclusi in questo intervallo.

   Esempio:

   Router Internet: `192.168.1.1`

   OpenScape Business: `192.168.1.2`

   UC Booster Card: `192.168.1.3`

   Indirizzo di sottorete: `192.168.1.0`

   Maschera di sottorete: `255.255.255.0`

   Server stampante: `192.168.1.10`

   Pool di indirizzi DHCP: da `192.168.1.50` a `192.168.1.254`
8) Specificare il valore del campo **Opzione relè**.
9) Fare clic su **OK & Avanti**.

Passaggi successivi

Configurare le impostazioni del paese e dell'ora.

9.3 DNS - Risoluzione dei nomi

Il Domain Name Service (DNS) si occupa della conversione di nomi in indirizzi numerici. In questo modo, i nomi dei computer o i nomi di dominio possono essere convertiti in indirizzi IP e viceversa.

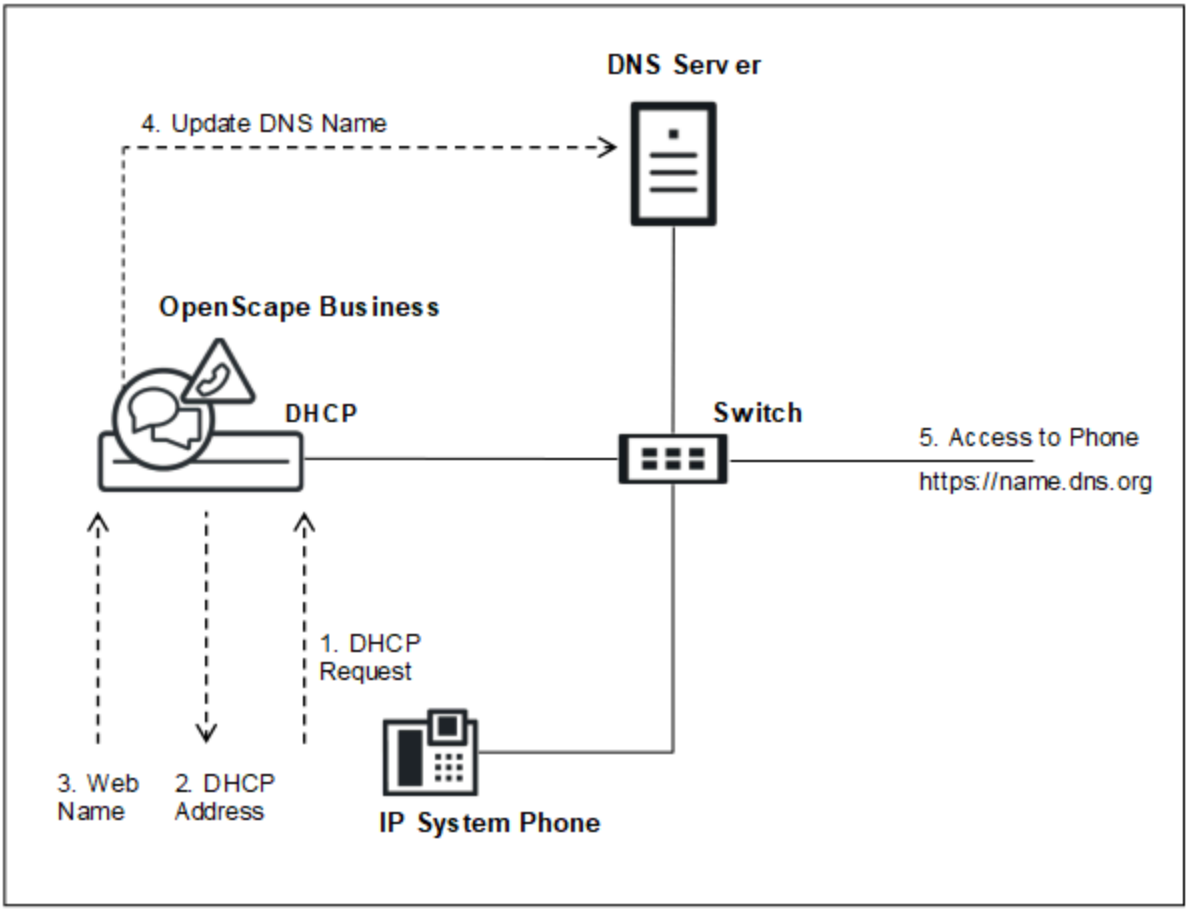
Il DNS usa un database mondiale ripartito su server, che gestisce lo spazio dei nomi di Internet. Questo spazio dei nomi è suddiviso in cosiddette zone (domini). Per le esigenze locali, all'interno di una rete aziendale, vengono di norma utilizzati server DNS propri, indipendenti da Internet.

Risoluzione dei nomi per i telefoni di sistema IP

Devono essere soddisfatti i seguenti requisiti:

- Server DNS Windows 2008 (con stato delle patch aggiornato e l'impostazione "Consenti aggiornamenti non sicuri" attivata)
- Il server DHCP interno è attivato
- La funzionalità "Aggiornamento DNS dinamico" è attivata nel server DHCP interno (vedere Server DHCP).
- Nel telefono di sistema IP è inserito il nome Web.

Il telefono IP di sistema invia una richiesta DHCP (1) e riceve dal server DHCP interno un indirizzo IP valido e altri dati specifici della rete (2). Dopo aver ricevuto questi dati, il telefono di sistema IP invia i nomi Web impostati al server DHCP interno (3), che automaticamente inoltra i nomi al server DNS configurato (4). Il server DNS conosce ora i nomi appartenenti all'indirizzo IP del telefono IP di sistema. Il telefono IP di sistema è ora raggiungibile tramite il WBM con il proprio nome Web (5).



Server DNS

Il server DNS, chiamato anche name server, è un programma che risponde alle domande sui nomi di dominio o nomi host. Anche il PC su cui viene eseguito questo programma può essere impostato come server DNS.

Alle interrogazioni relative a nomi di domino o nomi host, il server DNS risponde con l'indirizzo IP corrispondente.

Esempio: per `www.wikipedia.org`, i server DNS in Internet restituiscono l'indirizzo `IP 91.198.174.2`.

Se il server DNS preferito non risponde all'interrogazione, questa viene inoltrata a un altro server DNS.

Con il soft switch, il server Linux su cui è installato il software di comunicazione può essere configurato come server DNS. La piattaforma hardware non può essere utilizzata come server DNS. È possibile specificare un server DNS esterno sia per il soft switch che per la piattaforma hardware.

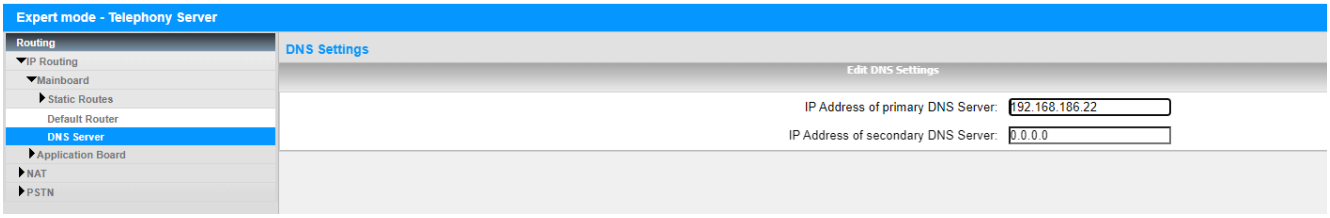
9.3.1 Come impostare il server DNS esterno

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Routing**.
3) Nella struttura dei menu selezionare **Routing IP** > **Scheda madre** > **Server DNS**. Viene visualizzata la finestra **Modifica impostazioni DNS**.



4) Nel campo **Indirizzo IP del server DNS** immettere l'indirizzo IP del server DNS esterno desiderato.
5) Fare clic su **Applica**, quindi su **OK**.

Nota: In un sistema OpenScape Business S è necessario il riavvio per applicare le modifiche.

9.4 Routing IP

Nella tecnologia dei dati, il routing IP indica la definizione dei percorsi (rotte) dei flussi di dati all'interno delle reti. Il routing IP è necessario se mittente e destinatario si trovano in reti diverse.

Router predefinito

Per garantire che gli utenti IP raggiungano anche destinazioni che si trovano all'esterno della propria rete non esplicitamente inserite in una tabella delle rotte, è necessario indicare un gateway per l'inoltro di tali pacchetti (router predefinito). Il router predefinito invia quindi i dati alla rete di livello superiore.

È possibile attivare o disattivare il routing IP tramite un router predefinito sia per la scheda madre che per la scheda applicazioni.

Route statiche

Le route statiche vengono utilizzate per assegnare i pacchetti di dati a una rete che non è possibile raggiungere tramite il router predefinito.

È possibile creare percorsi statici per la scheda madre e per la scheda applicazioni.

9.4.1 Come attivare o disattivare il router predefinito

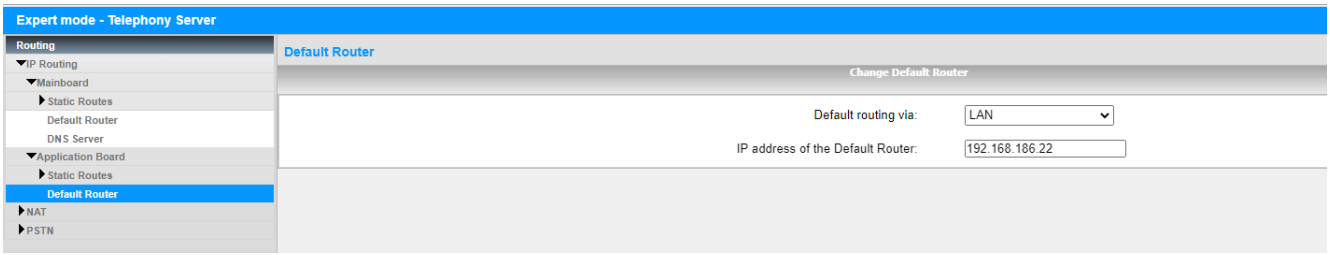
Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Routing**.
3) Nella struttura dei menu selezionare **Routing IP** > **Scheda madre / Scheda applicazioni** > **Router predefinito**. Viene visualizzata la finestra **Modifica router predefinito**.



4) Se si desidera attivare il routing IP tramite un router predefinito, nell'elenco a discesa **Routing predefinito tramite**, selezionare la voce **LAN**, quindi in Indirizzo `IP del router predefinito` inserire l'indirizzo IP del router predefinito, ad esempio l'indirizzo IP del router Internet: **192.168.1.1**.
5) Se si desidera disattivare il routing IP tramite un router predefinito, nell'elenco a discesa **Routing predefinito tramite**, selezionare la voce **Nessuna interfaccia**.
6) Fare clic su **Applica**, quindi su **OK**.

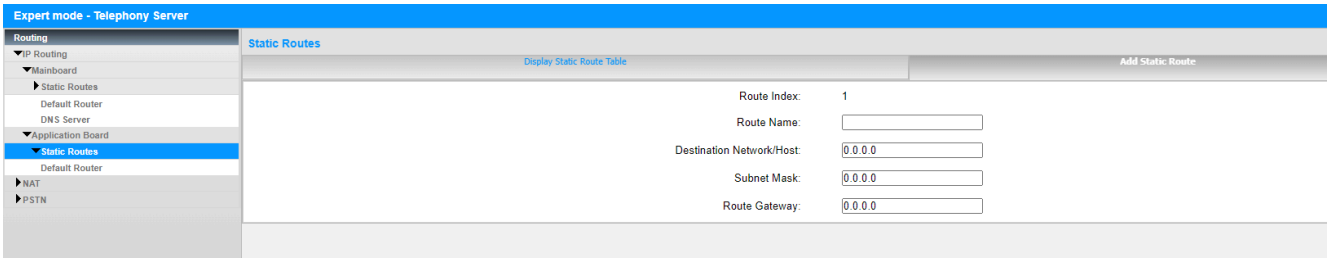
9.4.2 Come aggiungere la route statica

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Routing**.
3) Nella struttura dei menu selezionare **Routing IP** > **Scheda madre / Scheda applicazioni** > **Route statiche**. Viene visualizzata la finestra **Route statiche**.
4) Fare clic sulla scheda **Aggiungi route statica**. **Indice di route** visualizza quale route è stata aggiunta.



5) Nel campo **Nome delle route** immettere i nomi desiderati per questa route.
6) Immettere l'indirizzo IP della **Rete di destinazione/Host**.
7) Immettere l'indirizzo IP della **Maschera di rete di destinazione**.
8) Nel campo **Gateway della route**, immettere l'indirizzo IP del router da utilizzare per raggiungere la rete di destinazione desiderata.

9) Se sono state create uno o più rotte (percorsi) statiche per la scheda madre, è possibile copiare tutte le rotte statiche della scheda madre con il pulsante **Copia su OCAB** nella scheda applicazioni.

10) Fare clic su **Applica**, quindi su **OK**.

9.4.3 Come cancellare route statiche

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Telefonia** > **Routing**.

3) Nella struttura dei menu, selezionare **Routing IP** > **Scheda madre / Scheda applicazioni** > **Route statiche**.

4) Selezionare la route da cancellare.

5) Passare alla scheda **Cancella route statica**.

6) Fare clic su **Cancella**.

7) Confermare il messaggio informativo e fare clic su **OK**.

9.5 Servizio di distribuzione (DLI e DLS)

Utilizzando il DLI e il DLS, è possibile gestire centralmente i componenti IP e implementare il relativo software. Il DLI è integrato nel sistema di comunicazione. Il DLS è un'applicazione indipendente che deve essere installata su un PC server esterno.

DLI (Deployment Server Integrated)

Il DLI è un componente integrato nel sistema di comunicazione che fornisce funzionalità DLS limitate. Con il DLI interno, tutti i telefoni IP di sistema collegati al sistema di comunicazione possono essere configurati centralmente e automaticamente aggiornati alla versione più recente del software per i telefoni. Per DeskPhone CP 400/600/600E/700/700X/710, quando DLI è attivato, i seguenti parametri del server UC vengono configurati automaticamente: Protocollo UC, indirizzo del server UC, porta del server UC.

Il DLI interno funziona anche con il server FTP integrato sui cui è memorizzato il software dei telefoni più aggiornato.

Se l'indirizzo IP del DLI nel server DHCP è noto, il server DHCP invia tali dati al telefono di sistema IP (HFA, SIP) non appena il telefono accede alla rete interna. In questo modo, il telefono può prelevare il software più aggiornato dal server FTP del sistema di comunicazione. Per impostazione predefinita, nel server DHCP interno è configurato il DLI. Se al suo posto deve essere usato un server DLS esterno, è necessario configurare il suo indirizzo IP nel server DHCP interno.

DLS (Deployment Service)

Il DLS è una applicazione client/server per la gestione centralizzata dei componenti IP. Il server DLS non è integrato nel sistema di comunicazione

e deve essere installato separatamente su un PC server. Il client DLS viene eseguito sui componenti IP. Per l'amministrazione viene utilizzato un browser Web.

I componenti IP sono telefoni IP di sistema, telefoni SIP, client SIP e gateway IP.

Nota: Le caratteristiche e le funzioni del DLS sono riportate nella descrizione del DLS ed esulano dalla presente trattazione.

DLI o DLS con server DHCP esterno

Anche quando si utilizza un server DHCP esterno, il software dei telefoni di sistema IP (HFA, SIP) può essere aggiornato automaticamente e si hanno a disposizione le seguenti alternative:

- Configurazione dell'indirizzo IP del DLI o DLS nel server DHCP esterno

  Quando si utilizza un server DHCP esterno, è necessario inserire i dati di rete e l'indirizzo IP del server di distribuzione utilizzato (DLI o un server esterno DLS). Inoltre, il software di sistema aggiornato deve essere salvato sul server DLS esterno.
- Configurazione di tutti i telefoni IP di sistema

  Per ogni telefono di sistema IP, deve essere inserito l'indirizzo IP del server di distribuzione utilizzato come indirizzo DLS (indirizzo IP del sistema di comunicazione per il DLI interno o indirizzo IP del server DLS esterno).

Funzioni e limitazioni

Funzione	DLI	DLS
Configurazione centralizzata dei parametri dei componenti IP I parametri dei componenti IP sono configurabili tramite modelli XML personalizzabili.	sì	sì
Messa in servizio plug-and-play dei componenti IP Tramite un server DHCP, i componenti IP possono accedere automaticamente al sistema, ad esempio dopo essere stati connessi al sistema per la prima volta o dopo la sostituzione di componenti IP.	Sì	Sì
Aggiornamento software centralizzato e automatico dei componenti IP Quando è disponibile una nuova versione del software, i componenti IP vengono forniti automaticamente con la versione software più recente al primo accesso. Nei componenti IP, è necessario configurare l'indirizzo IP del DLI/DLS.	Sì	Sì Sul server DLS deve essere salvato il software del telefono alla versione più aggiornata.
Gestione inventario centrale dei componenti IP I dati sulle configurazioni hardware dei componenti IP sono accessibili centralmente.	no	Sì

Funzione	DLI	DLS
Supporto per IP Mobility (desk sharing) I dati di telefonia di un utente vengono salvati centralmente e possono quindi essere recuperati da altri telefoni (ad esempio, programmazioni dei tasti, voci della rubrica, diario).	Sì non per telefoni SIP, non possibile nel sistema di reti.	Sì non per telefoni SIP, in reti omogenee (solo sistemi OpenScape Business) solo con numerazione chiusa, in reti non omogenee (con OpenScape 4000 o OpenScape Voice).
Supporto di SPE sulle reti	È possibile utilizzare SPE nelle reti. Occorre utilizzare DLS (senza DLI).	Sì Le chiavi e i certificati da distribuire devono essere disponibili sul DLS.
Alimentazione centrale di più piattaforme diverse	no	Sì
Attivazione della 2° interfaccia LAN dei telefoni di sistema IP (modalità Ethernet PC). Vedere Impostazioni di base > Implementazione parametri telefoni	Sì	Sì

Client di distribuzione e licenze (DLSC)

Per utilizzare funzioni DLS, quali ad esempio Element Manager, il sistema di comunicazione deve concedere al DLS esterno l'accesso ai dati di configurazione. Il sistema di comunicazione viene quindi utilizzato come client di distribuzione e licenze.

9.5.1 Come configurare un server DLS esterno nel server DHCP interno

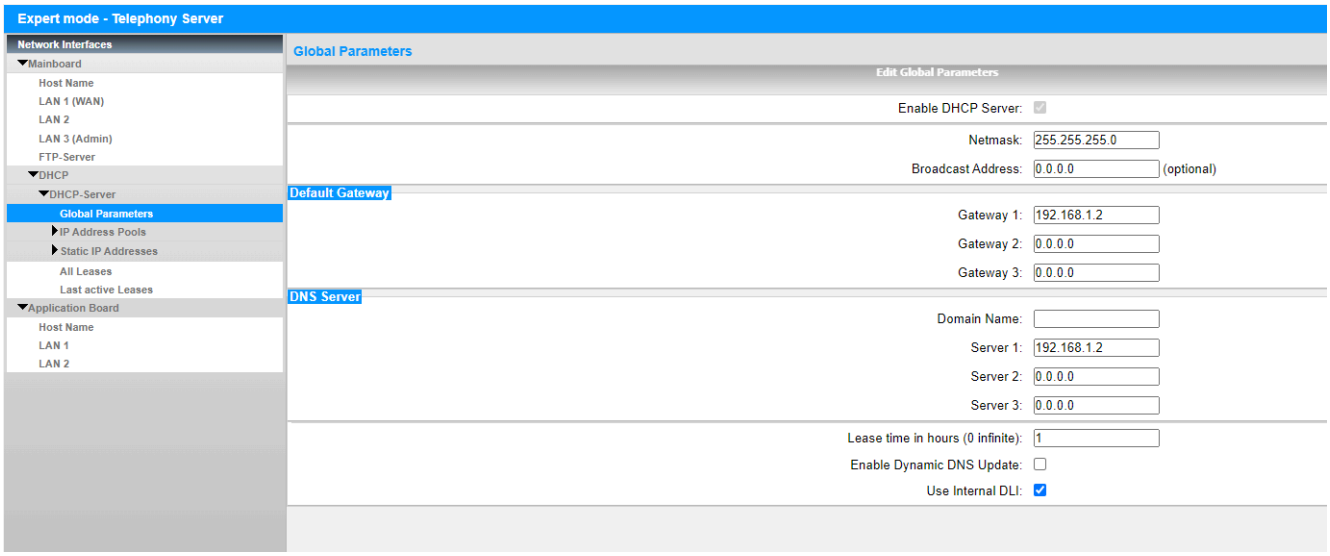
Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server di telefonia** > **Interfacce di rete**.

3) Nella struttura dei menu selezionare **Scheda madre** > **DHCP** > **Server DHCP** > **Impostazioni globali**. Viene visualizzata la finestra **Modifica parametri globali**.



4) Deselezionare la casella di controllo **Usa DLI interno**.
5) Nel campo **Indirizzo IP** immettere l'indirizzo IP al quale il server DLS esterno è raggiungibile.
6) Nel campo **Porta**, inserire la porta utilizzata dal server DLS. Questa porta deve essere abilitata nel firewall.
7) Fare clic su **Applica**, quindi su **OK**.

9.5.2 Come attivare il DLI interno

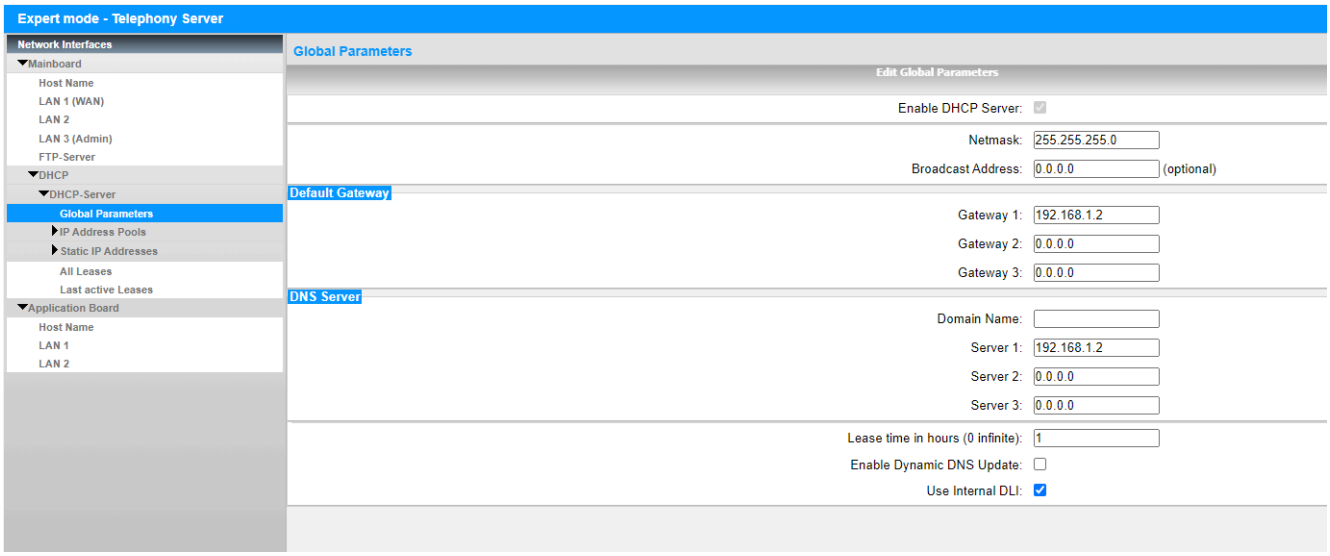
Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server di telefonia** > **Interfacce di rete**.

3) Nella struttura dei menu selezionare **Scheda madre** > **DHCP** > **Server DHCP** > **Impostazioni globali**. Viene visualizzata la finestra **Modifica parametri globali**.



4) Selezionare la casella di controllo **Usa DLI interno**. La casella di controllo è selezionata per impostazione predefinita.
5) Fare clic su **Applica**, quindi su **OK**.

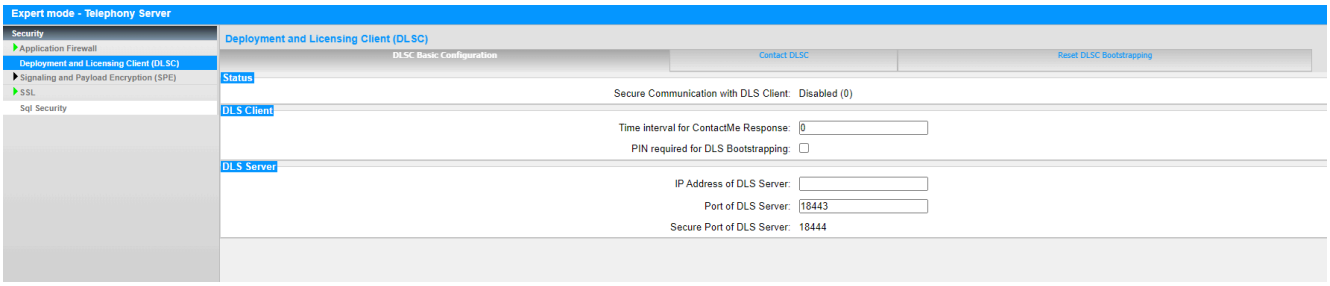
9.5.3 Come configurare il client del sistema di comunicazione come client di distribuzione e licenze

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Sicurezza**.
3) Nella struttura dei menu, fare clic su **Distribuzione e licenze client (DLSC)**.



4) Nella scheda **Configurazione base DLSC**, nell'area **Server DLS** nel campo **Indirizzo IP del server DLS** inserire l'indirizzo IP al qual il server DLS esterno sarà raggiungibile.
5) In **Porta del server DLS**, modificare se necessario la porta utilizzata dal server DLS. Le due porte visualizzate devono essere abilitate nel firewall.
6) Fare clic su **Applica**, quindi su **OK**.

10 Connessione al provider di servizi

Il sistema di comunicazione supporta il collegamento a reti di comunicazione pubbliche. Il collegamento alla rete IP consente l'accesso a Internet e alla telefonia Internet, la linea esterna offre accesso alla rete ISDN e alla rete analogica.

Per l'accesso a Internet viene utilizzato un modem Internet o un router Internet.

Con le piattaforme hardware, l'accesso alla linea ISDN esterna avviene tramite la scheda madre o altri moduli rimovibili. Con il soft switch non è possibile utilizzare una linea esterna ISDN.

La linea esterna analogica richiede che le piattaforme siano dotate di un ulteriore modulo estraibile. Con il softswitch non è possibile utilizzare una linea esterna analogica.

10.1 Accesso a Internet

Per l'accesso a Internet è necessaria una connessione a banda larga (linea DSL o connessione via cavo). In questo modo è possibile una rapida trasmissione dei dati con la larghezza di banda disponibile.

Accesso a Internet tramite linea DSL

La connessione a Internet a banda larga via DSL (Digital Subscriber Line) avviene tramite la linea telefonica esistente. L'accesso a Internet può essere utilizzato in parallelo al telefono. Fax, telefoni analogici o ISDN rimangono disponibili anche durante la connessione DSL. In questo modo si ottiene un accesso a Internet sempre disponibile (Flat).

Per l'accesso a Internet tramite DSL sono necessari un collegamento telefonico (analogico o ISDN) e un ISP. L'ISP mette a disposizione uno splitter e un modem Internet (modem DSL) o un router Internet con modem Internet integrato. Lo splitter suddivide il segnale fra DSL e telefonia e inoltra il segnale DSL al modem Internet.

Il sistema di comunicazione può essere collegato direttamente al modem Internet o a un router Internet con modem Internet integrato. Nel primo caso, i dati di accesso dell'ISP devono essere inseriti nel sistema di comunicazione, mentre nel secondo caso occorre comunicare al sistema di comunicazione il router Internet. I dati di accesso dell'ISP sono memorizzati nel router Internet.

Per poter utilizzare la telefonia Internet è necessario un ITSP (Internet Telephony Service Provider, provider SIP).

Accesso a Internet via cavo

La connessione a Internet a banda larga via cavo avviene tramite il cavo TV che può quindi essere utilizzato per la trasmissione del segnale TV, per l'accesso a Internet e per la telefonia. È possibile navigare in Internet e telefonare senza linea telefonica.

Per l'accesso a Internet via cavo è necessario un gestore di rete che offra questo servizio. Questo gestore funge contemporaneamente anche da ISP. Mette a disposizione un collegamento via cavo con un canale di ritorno e un modem via cavo che trasmette i dati tramite il canale TV. Il collegamento via

cavo e il sistema di comunicazione vengono collegati al modem via Ethernet. Il filtro dei dati Internet viene effettuato dallo stesso modem via cavo.

Il sistema di comunicazione può essere collegato direttamente al modem via cavo o a un router Internet, a sua volta connesso al modem via cavo. In entrambi i casi, il sistema di comunicazione deve riconoscere il modem via cavo o il router Internet.

Per poter utilizzare la telefonia Internet è necessario un ITSP (Internet Telephony Service Provider, provider SIP).

Configurazione dell'accesso a Internet

La configurazione dell'accesso a Internet nel WBM varia a seconda che tale accesso sia già impostato in un router esterno o che venga eseguito tramite un modem Internet e quindi configurato nel WBM.

- **Accesso a Internet tramite un modem Internet** (**DSL direttamente sulla porta WAN**)

  Si desidera utilizzare il sistema di comunicazione direttamente collegato al modem Internet (DSL, cavo, UMTS, …). OpenScape Business dispone di un router Internet integrato. Inserire i dati di accesso del provider di servizi Internet (ISP) direttamente nel sistema di comunicazione e utilizzare la porta WAN del sistema di comunicazione. Questo non è possibile nel soft switch.

  Sono disponibili le seguenti opzioni:

  – Accesso a Internet tramite ISP preconfigurato
  – Accesso a Internet tramite un ISP PPPoE predefinito
  – Accesso a Internet tramite un ISP PPTP predefinito

  Se il proprio ISP non è compreso tra quelli preconfigurati, usare l'ISP predefinito PPPoE o PPTP.

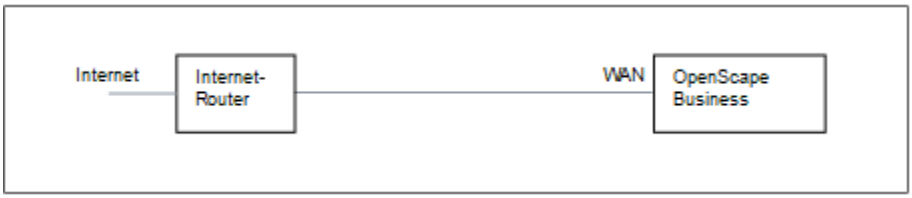
- **Accesso ad Internet tramite un router Internet esterno**

  Si desidera utilizzare il sistema di comunicazione direttamente collegato a un router Internet. Il provider di servizi Internet è già configurato nel router Internet.

  Sono disponibili le seguenti opzioni:

  – **Accesso a Internet tramite router Internet esterno nella porta WAN**

    (**TCP/IP alla porta WAN tramite router esterno**)

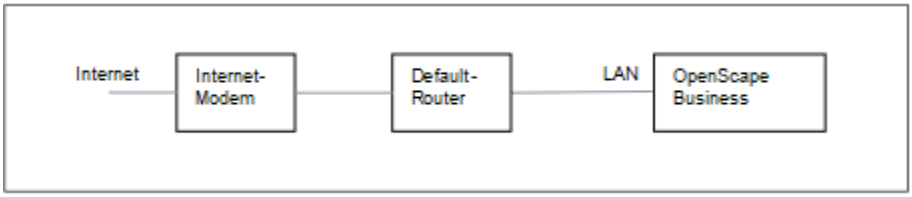
    

    A tal fine, utilizzare la porta WAN del sistema di comunicazione. OpenScape Business riconosce il router Internet o funge da client DHCP.

Questa opzione può essere utilizzata se il router Internet si trova in un altro segmento di rete e dispone di un proprio server DHCP.

– **Accesso a Internet tramite router Internet esterno nella porta LAN**

(**TCP/IP alla porta LAN tramite router esterno**)



A tal fine utilizzare la porta LAN del sistema di comunicazione. OpenScape Business riconosce solo il router predefinito e non l'infrastruttura sottostante. Per attivare la connessione al router Internet, occorre comunicare al sistema di comunicazione l'indirizzo IP del router predefinito e del server DNS.

- **Disattivazione dell'accesso a Internet** (impostazione predefinita)

  Non si desidera utilizzare Internet. Lasciare l'accesso a Internet disattivato.

10.1.1 Accesso a Internet tramite router esterno

La procedura guidata **Configurazione Internet** consente di configurare l'accesso a Internet tramite un router aggiuntivo.

Per la configurazione dell'accesso a Internet sono disponibili le seguenti opzioni:

- **Accesso a Internet tramite router Internet esterno nella porta LAN**

  A tal fine utilizzare la porta LAN del sistema di comunicazione. Per attivare la connessione al router Internet, occorre comunicare al sistema di comunicazione l'indirizzo IP del router predefinito e del server DNS.
- **Accesso a Internet tramite router Internet esterno nella porta WAN**

  A tal fine, utilizzare la porta WAN del sistema di comunicazione. Questa opzione può essere utilizzata se il router Internet si trova in un altro segmento di rete e dispone di un proprio server DHCP.

10.1.1.1 Come configurare l'accesso a Internet tramite un router Internet esterno mediante una connessione LAN

Le procedura guidata **Configurazione Internet** consente di configurare l'accesso a Internet quando si desidera gestire il sistema di comunicazione su un router aggiuntivo. Il sistema di comunicazione e il router devono trovarsi nello stesso segmento LAN. Occorre definire l'indirizzo IP del router e quello del server DNS.

Prerequisiti

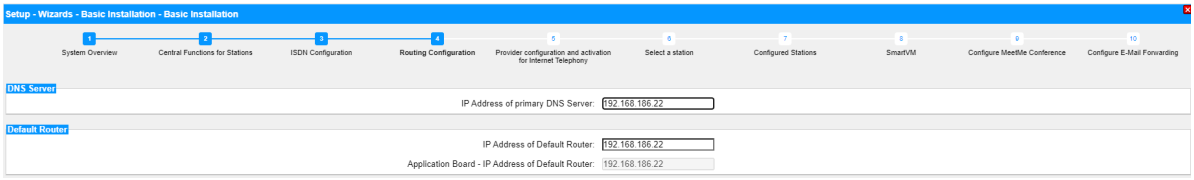
Si è connessi a WBM con il profilo **Avanzate**.

Per OpenScape Business X: il sistema di comunicazione è collegato tramite l'interfaccia "LAN" alla rete del cliente. La connessione non può avvenire tramite l'interfaccia "WAN".

Per OpenScape Business S: il server Linux è collegato tramite l'interfaccia LAN della scheda di rete con la rete del cliente.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Rete / Internet**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Configurazione Internet**.
4) Deselezionare la casella di controllo **Nessun accesso ad Internet**.
5) Selezionare **TCP/IP alla porta LAN tramite router esterno** quindi fare clic su **OK & Avanti**.



6) Nel campo **Indirizzo IP dei server DNS** immettere l'indirizzo IP del server DNS locale (ad esempio il router Internet) o del server DNS Internet (ad esempio per telefonia Internet).
7) Nel campo **Indirizzo IP del router predefinito** immettere l'indirizzo IP del router Internet esterno.
8) Fare clic su **OK & Avanti**, quindi su **Fine**.

10.1.1.2 Come configurare l'accesso a Internet con un router Internet esterno mediante una connessione WAN

Le procedura guidata **Configurazione Internet** consente di configurare l'accesso a Internet quando si desidera gestire il sistema di comunicazione su un router aggiuntivo. Il sistema di comunicazione e il router Internet non devono trovarsi nello stesso segmento LAN.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

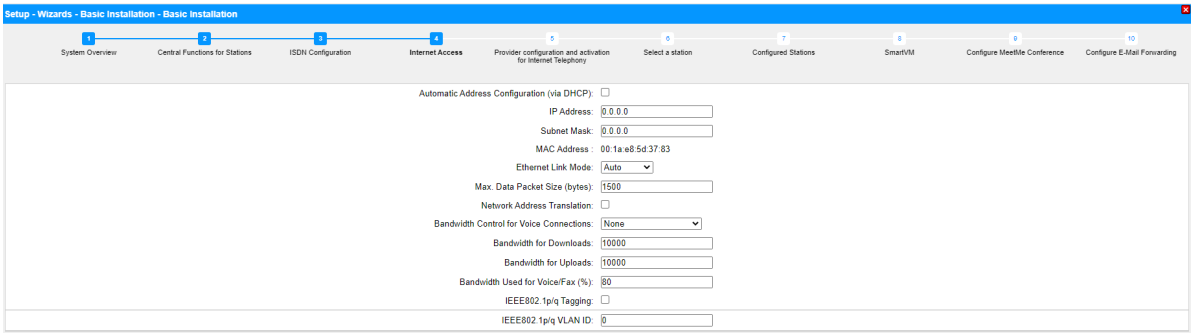
Il sistema di comunicazione deve essere collegato tramite l'interfaccia "WAN" al segmento LAN della rete del cliente in cui si trova il router Internet.

Si è nella finestra **Configurazione accesso a Internet**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Rete / Internet**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Configurazione Internet**.

4) Deselezionare la casella di controllo **Nessun accesso ad Internet**.
5) Selezionare **TCP/IP alla porta WAN tramite router esterno** quindi fare clic su **OK & Avanti**.



6) Se da un server DHCP già attivo devono essere ottenuti i dati specifici della rete per l'interfaccia WAN:
   a) Selezionare la casella di controllo **Configurazione automatica indirizzo (via DHCP)**.
   b) Selezionare la casella di controllo **Accetta indirizzo IP del router predefinito**.
   c) Se necessario, attivare la casella di controllo **Accetta indirizzo IP dei server DNS**.
   d) Se necessario, attivare la casella di controllo **Accetta indirizzo IP dei server SNTP**.
7) Se all'interfaccia WAN deve essere assegnato un indirizzo IP fisso:
   a) Deselezionare la casella di controllo **Configurazione automatica indirizzo (via DHCP)**.
   b) Inserire l'**Indirizzo IP** e la **Maschera di rete** desiderati per l'interfaccia WAN.
8) Selezionare la casella di controllo **Network Address Translation (NAT)**.
9) Se si desidera utilizzare anche la telefonia Internet, nell'elenco a discesa **Controllo della larghezza di banda per connessioni voce** selezionare **Solo upload** o **Upload e download**, come necessario. In caso di una larghezza di banda elevata per il download e più limitata per il caricamento, la regolazione della larghezza di banda deve essere attivata solo per il caricamento, affinché non venga inutilmente riservata molta larghezza di banda di download per la trasmissione voce.
10) Nei campi **Larghezza di banda per download** e **Larghezza di banda per upload** immettere la larghezza di banda per download e upload espressa in kbit/sec. messa a disposizione dal proprio provider di servizi Internet.
11) Fare clic su **OK & Avanti**, quindi su **Fine**.

10.1.1.3 Come configurare l'accesso a Internet tramite un router Internet esterno sulla LAN con porta WAN dedicata all'ITSP

Prerequisiti

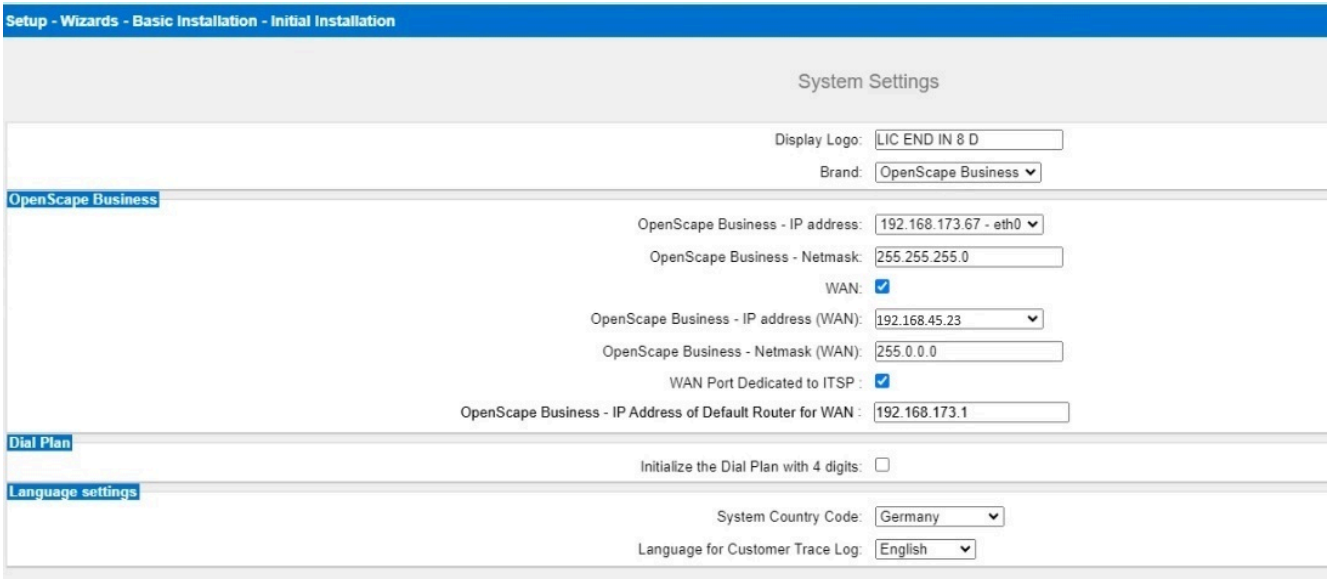
È stata creata una nuova interfaccia di rete in SLES.

Si è nella finestra **Impostazioni di sistema** della procedura guidata **Installazione iniziale**.

Tenere presente che questa funzione è valida solo per gli ITSP che non richiedono l'uso di STUN nelle impostazioni del provider.

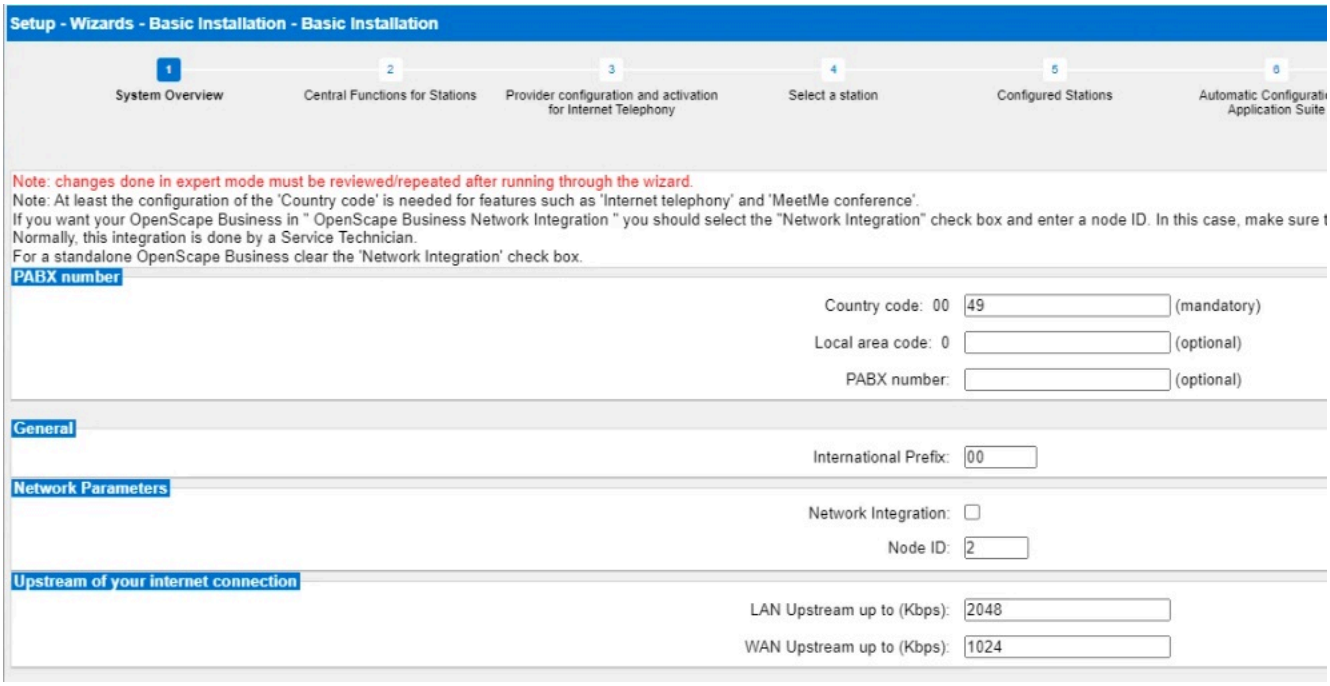
Passo a passo

1) Attivare la casella di controllo **WAN** e selezionare l'interfaccia di rete appropriata.
   L'opzione **Interfaccia WAN dedicata all'ITSP** diventerà disponibile.
2) Fare clic per abilitare la casella di controllo **Interfaccia WAN dedicata all'ITSP**.



3) Fare clic su **OK & Avanti**.
4) Spostarsi su **Configurazione > Installazione di base** e lanciare la procedura guidata **Installazione di base**.

5) Configurare i valori massimi di upstream nei campi **LAN upstream fino a (Kbps)** e **WAN upstream fino a (Kbps)** corrispondenti.



6) Fare clic su **OK & Avanti**.

7) Dopo aver applicato la configurazione, è necessario riavviare il sistema.

10.1.2 Accesso a Internet tramite modem Internet

La procedura guidata **Configurazione Internet** consente di configurare l'accesso a Internet tramite un modem Internet. In questo modo la connessione WAN del sistema di comunicazione si collega direttamente al modem Internet. Nel sistema di comunicazione è possibile utilizzare un ISP pre-configurato o di tipo standard (da richiedere all'ISP).

Per la configurazione dell'accesso a Internet sono disponibili le seguenti opzioni:

- **Configurazione dell'accesso a Internet tramite ISP pre-configurato**

  In un sistema di comunicazione viene utilizzato un ISP pre-configurato. È possibile selezionare tale ISP dall'elenco degli ISP pre-configurati dell'utente.
- **Configurazione dell'accesso a Internet tramite un ISP standard PPPoE**

  Si utilizza il tipo ISP **Provider PPPoE**. Richiedere le impostazioni necessarie al proprio ISP.
- **Configurazione dell'accesso a Internet tramite un ISP standard PPTP**

  Si utilizza il tipo ISP **Provider PPPTP**. Richiedere le impostazioni necessarie al proprio ISP.

Interruzione della connessione in base al modello tariffario

In base al modello tariffario è possibile definire se mantenere o meno la connessione all'ISP in caso di inattività.

- Con una tariffa Flat non occorre interrompere la connessione Internet in caso di inattività. Molti ISP offrono ogni 24 ore un'interruzione forzata. Il momento in cui deve essere interrotta la connessione è definibile.
- Con una tariffa a tempo è necessario interrompere la connessione a Internet in caso di inattività. La durata dell'inattività superata la quale viene interrotta la connessione (ad es. 60 secondi) è definibile. Alla successiva richiesta Internet, la connessione viene ripristinata automaticamente. Se è configurata una VPN, la connessione non può essere interrotta in caso di inattività. A tal fine è necessario selezionare il modello tariffario Flatrate.

Nota: I programmi o servizi in rete possono stabilire automaticamente una connessione a Internet e originare costi aggiuntivi in caso di tariffazione a tempo.

Larghezza di banda

L'ISP mette a disposizione diverse larghezze di banda per il download e il caricamento di dati. La larghezza di banda viene espressa in kbit/s. Se si utilizza la telefonia Internet la larghezza di banda viene ripartita fra trasmissione voce e trasmissione dati. Pertanto, allo scopo di ottenere una buona qualità voce, è importante destinare una larghezza di banda sufficientemente ampia a tale servizio. Tuttavia in caso di intensa trasmissione voce viene penalizzata la trasmissione dati (ad es. download più lento).

È possibile scegliere se la regolazione della larghezza di banda per la connessione voce deve essere attiva solo per il caricamento o anche per il download. In caso di una larghezza di banda elevata per il download e più limitata per il caricamento, la regolazione della larghezza di banda deve essere attivata solo per il caricamento, affinché non venga inutilmente riservata molta larghezza di banda di download per la trasmissione voce.

Nota: Per una conversazione Internet vengono riservati circa 128 kbit/s di larghezza di banda.

10.1.2.1 Come configurare l'accesso a Internet tramite ISP preimpostato

La procedura guidata **Configurazione Internet** consente di configurare l'accesso a Internet tramite un Internet Service Provider (ISP) pre-configurato nel sistema di comunicazione.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

I dati di accesso Internet del proprio ISP sono disponibili (ad es. ID utente, password, ecc).

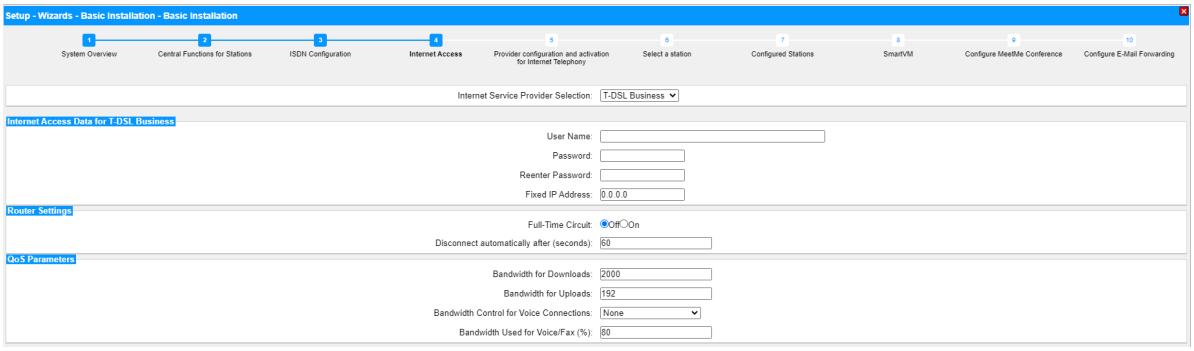
Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.

2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Rete / Internet**.

3) Fare clic su **Modifica**, per avviare la procedura guidata **Configurazione Internet**.

4) Deselezionare la casella di controllo **Nessun accesso ad Internet**.
5) Selezionare il campo opzione **DSL direttamente su porta WAN** quindi fare clic su **OK & Avanti**.



6) Nell'elenco a discesa **Scelta del provider di servizi Internet**, selezionare il proprio ISP.
7) Nell'area **Dati di accesso ad Internet per** immettere i dati di accesso forniti dal provider. Le opzioni presenti in quest'area dipendono dal provider di servizi. Nell'immettere i dati rispettare maiuscole e minuscole.
8) In **Impostazioni router**, **Connessione permanente**, selezionare una delle seguenti opzioni in base al proprio modello tariffario:
   - In caso di tariffa Flatrate, selezionare **On**. Nel campo **Interruzione alle (hh:mm)**, immettere l'orario in cui interrompere la connessione a Internet (ad es. 04:59).
   - Se il modello tariffario è a tempo, selezionare **Off**. Nel campo **Disconnetti automaticamente dopo (secondi)**, immettere la durata dell'inattività trascorsa la quale viene interrotta la connessione Internet (ad es. 60 secondi).
9) Nell'area **Parametri QoS** immettere i seguenti valori:
   a) Nei campi **Larghezza di banda per download** e **Larghezza di banda per upload** immettere la larghezza di banda per download e upload espressa in kbit/sec. messa a disposizione dall'ISP.
   b) Se si desidera utilizzare anche la telefonia Internet, nell'elenco a discesa **Controllo della larghezza di banda per connessioni voce** selezionare **Solo upload** o **Upload e download**, come necessario. Nel campo **Larghezza di banda per connessioni voce/fax (%)** immettere la percentuale di larghezza di banda da riservare alle connessioni voce e fax (predefinito: 80%).
10) Fare clic su **OK & Avanti**. Si aprirà la finestra **Configura account DynDNS**.
11) Se si desidera utilizzare una VPN o la funzione di accesso remoto e non si dispone di un indirizzo IP statico, è necessario disporre di un account DynDNS (ad esempio, presso dyndns.org) e configurarlo.
   a) Se il provider DynDNS desiderato è disponibile nel menu a discesa **Nome del dominio**, selezionarlo dall'elenco (ad esempio dyndns.org).
   b) Se il provider del DynDNS desiderato non è compreso nell'elenco a discesa **Nome del dominio**, selezionare la casella di controllo **Dominio definito dall'utente**. Nel campo **Nome del dominio** immettere il provider del DynDNS desiderato e nel campo **URL aggiornamento** l'URL aggiornato del provider DynDNS. La struttura di tale URL dipende

dal provider DynDNS. Inoltre, completare con i parametri specifici per il cliente (nell'esempio contrassegnati in *corsivo*).

```
http://www.anydns.info/update.php?
user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>
```

c) Inserire il **Nome utente** e la **Password** del proprio account DynDNS.
d) Nel campo **Nome dell'host**, immettere il nome host indicato al fornitore DynDNS, senza nome di dominio, ad es. myhost. Il nome di dominio completo risulta myhost.dyndns.org.
e) Testare l'account DynDNS utilizzando **Test connessione**.
f) Se il test ha avuto esito positivo, fare clic su a **OK**.
g) Fare clic su **OK & Avanti**.

12) Se si dispone di un indirizzo IP statico pubblico o non si desidera utilizzare la VPN o l'accesso remoto, fare clic su **Nessun DynDNS**.

13) Fare clic su **Fine**. Il sistema di comunicazione si riavvia.

10.1.2.2 Come configurare l'accesso a Internet tramite un ISP standard PPPoE

La procedura guidata **Configurazione Internet** consente di configurare l'accesso a Internet tramite l'Internet Service Provider standard PPPoE.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

L'ISP deve mettere a disposizione i seguenti dati per l'accesso a Internet:

Campo	Descrizione	Valore da ISP
Parametri IP (solo per indirizzi IP fissi)		
Indirizzo IP partner della connessione PPP	Indirizzo IP del server dell'ISP.	
Indirizzo IP locale della connessione PPP	Indirizzo IP comunicato dall'ISP per l'accesso a Internet.	
Autenticazione (tramite PAP o CHAP). PAP viene difficilmente utilizzata poiché l'autenticazione non è crittografata.		
Nome d'utente PPP	Nome utente per la connessione PPP, comunicato dall'ISP.	
Modalità di autenticazione PAP	Modalità di autenticazione per la connessione PPP su PAP: **Client PAP**, **Host PAP** o **Non utilizzato**.	
Password PAP	Password per l'autenticazione PAP, comunicata dall'ISP.	
Modalità di autenticazione CHAP	Modalità di autenticazione per la connessione PPP tramite CHAP: **Client CHAP**, **Host CHAP**, **Client e host CHAP** o **Non utilizzato**.	
Password CHAP	Password per l'autenticazione tramite CHAP, comunicata dall'ISP.	
Parametri QoS dell'interfaccia		

Campo	Descrizione	Valore da ISP
Larghezza di banda per download	Valore della larghezza di banda complessiva in kbit/sec. per il download dall'ISP.	
Larghezza di banda per upload	Valore della larghezza di banda complessiva in kbps per il caricamento fornito dall'ISP.	

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Rete / Internet**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Configurazione Internet**.
4) Deselezionare la casella di controllo **Nessun accesso ad Internet**.
5) Selezionare il pulsante di opzione **DSL direttamente su porta WAN**, quindi fare clic su **OK & Avanti**.
6) Nell'elenco a discesa **Scelta del provider di servizi Internet**, selezionare il tipo ISP standard **Provider PPPoE**.
7) Nell'area **Parametri IP**, selezionare la casella di controllo **Parametri IP** solo se l'ISP ha richiesto una modifica dei parametri. In questo caso, nei campi **Indirizzo IP partner della connessione PPP**, **Indirizzo IP locale della connessione PPP** e **Lunghezza max. pacchetto dati (byte)** immettere i valori comunicati dall'ISP. Nell'elenco a discesa **Negoziazione dell'indirizzo IP** selezionare la voce **Utilizza indirizzo IP configurato**.
8) In **Impostazioni router**, **Connessione permanente**, selezionare una delle seguenti opzioni in base al proprio modello tariffario:
   - In caso di tariffa Flatrate, selezionare **On**. Nel campo **Interruzione alle (hh:mm)**, immettere l'orario in cui interrompere la connessione a Internet (ad es. 04:59).
   - Se il modello tariffario è a tempo, selezionare **Off**. Nel campo **Disconnetti automaticamente dopo (secondi)**, immettere la durata dell'inattività trascorsa la quale viene interrotta la connessione Internet (ad es. 60 secondi).
9) Le impostazioni nell'area **Autenticazione** dipendono dal fatto che l'ISP metta a disposizione o meno un'autenticazione tramite PPP.
   - Se l'autenticazione viene fornita dall'ISP: Assicurarsi di selezionare la casella di controllo **Autenticazione PPP**. Come Nome utente PPP utilizzare il nome fornito dall'ISP per l'accesso a Internet. Lo standard utilizzato per la modalità di autenticazione è **CHAP-Client**.
   - Se l'autenticazione non viene fornita dall'ISP: Assicurarsi di deselezionare la casella di controllo Autenticazione PPP.
10) Se si desidera utilizzare NAT, nell'area **Conversione indirizzi**, selezionare la casella di controllo **NAT** (per impostazione predefinita è già selezionata).

11) Nell'area **Parametri QoS dell'interfaccia** immettere i seguenti valori:
    a) Nei campi **Larghezza di banda per download** e **Larghezza di banda per upload** immettere la larghezza di banda per download e upload espressa in kbit/sec. messa a disposizione dall'ISP.
    b) Se si desidera utilizzare anche la telefonia Internet, nell'elenco a discesa **Controllo della larghezza di banda per connessioni voce** selezionare **Solo upload** o **Upload e download**, come necessario. Nel campo **Larghezza di banda per connessioni voce/fax (%)** immettere la percentuale di larghezza di banda da riservare alle connessioni voce e fax (predefinito: 80%).
12) Fare clic su **OK & Avanti**. Si aprirà la finestra **Configura account DynDNS**.
13) Se si desidera utilizzare una VPN o la funzione di accesso remoto e non si dispone di un indirizzo IP statico, è necessario disporre di un account DynDNS (ad esempio, presso dyndns.org) e configurarlo.
    a) Se il provider DynDNS desiderato è disponibile nel menu a discesa **Nome del dominio**, selezionarlo dall'elenco (ad esempio dyndns.org).
    b) Se il provider del DynDNS desiderato non è compreso nell'elenco a discesa **Nome del dominio**, selezionare la casella di controllo **Dominio definito dall'utente**. Nel campo **Nome del dominio** immettere il provider del DynDNS desiderato e nel campo **URL aggiornamento** l'URL aggiornato del provider DynDNS. La struttura di tale URL dipende dal provider DynDNS. Inoltre, completare con i parametri specifici per il cliente (nell'esempio contrassegnati in *corsivo*).

       `http://www.anydns.info/update.php?user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`
    c) Inserire il **Nome utente** e la **Password** del proprio account DynDNS.
    d) Nel campo **Nome dell'host** immettere il nome host indicato dal fornitore DynDNS, senza nome di dominio, ad es. myhost. Il nome di dominio completo risulta myhost.dyndns.org.
    e) Testare l'account DynDNS utilizzando **Test connessione**.
    f) Se il test ha avuto esito positivo, fare clic su **OK**.
    g) Fare clic su **OK & Avanti**.
14) Se si dispone di un indirizzo IP statico pubblico o non si desidera utilizzare la VPN o l'accesso remoto, fare clic su **Nessun DynDNS**.
15) Fare clic su **Fine**.

10.1.2.3 Come configurare l'accesso a Internet tramite un ISP standard PPTP

La procedura guidata **Configurazione Internet** consente di configurare l'accesso a Internet tramite l'Internet Service Provider standard PPTP.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

L'ISP deve mettere a disposizione i seguenti dati per l'accesso a Internet:

Campo	Descrizione	Valore da ISP
Parametri IP (solo per indirizzi IP fissi)		

Campo	Descrizione	Valore da ISP
Indirizzo IP partner della connessione PPP	Indirizzo IP del server dell'ISP.	
Indirizzo IP locale della connessione PPP	Indirizzo IP comunicato dall'ISP per l'accesso a Internet.	
Parametri PPTP		
Indirizzo IP locale della connessione di controllo	Indirizzo IP comunicato dall'ISP per la connessione PPTP. Il valore predefinito è 10.0.0.140.	
Indirizzo IP partner della connessione di controllo	Indirizzo IP del server ISP destinato alla connessione PPTP. Il valore predefinito è 10.0.0.138.	
Maschera di rete partner della connessione di controllo	Maschera di rete comunicata dall'ISP per la connessione PPTP. Il valore predefinito è 255.255.255.248.	
Autenticazione (tramite PAP o CHAP). PAP viene difficilmente utilizzata poiché l'autenticazione non è crittografata.		
Nome utente PPP	Nome utente per la connessione PPP, comunicato dall'ISP.	
Modalità di autenticazione PAP	Modalità di autenticazione per la connessione PPP via PAP: **Client PAP**, **Host PAP** o **non utilizzata**.	
Password PAP	Password per l'autenticazione PAP, comunicata dall'ISP.	
Modalità di autenticazione CHAP	Modalità di autenticazione per la connessione PPP via CHAP: **Client CHAP**, **Host CHAP**, **Client e Host CHAP** o **non utilizzata**.	
Password CHAP	Password per l'autenticazione tramite CHAP, comunicata dall'ISP.	
Parametri QoS dell'interfaccia		
Larghezza di banda per download	Valore della larghezza di banda complessiva in kbit/sec. per il download dall'ISP.	
Larghezza di banda per upload	Valore della larghezza di banda complessiva in kbit/sec. fornito dall'ISP.	

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Rete / Internet**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Configurazione Internet**.
4) Deselezionare la casella di controllo **Nessun accesso ad Internet**.

5) Selezionare il campo opzione **DSL direttamente su porta WAN** quindi fare clic su **OK & Avanti**.

6) Nell'elenco a discesa **Scelta del provider di servizi Internet**, selezionare il tipo ISP standard **Provider PPTP**.

7) Nell'area **Parametri IP**, selezionare la casella di controllo **Parametri IP** solo se l'ISP ha richiesto una modifica dei parametri. In questo caso, nei campi **Indirizzo IP partner della connessione PPP**, **Indirizzo IP locale della connessione PPP** e **Lunghezza max. pacchetto dati (byte)** immettere i valori comunicati dall'ISP. Nell'elenco a discesa **Negoziazione dell'indirizzo IP** selezionare la voce **Utilizza indirizzo IP configurato**.

8) Nell'area **Parametri PPTP** immettere i valori indicati dall'ISP.

9) Se si utilizza una tariffazione a tempo, selezionare la casella di controllo **Modalità Short Hold**. Nel campo **Tempo Short Hold (s)**, immettere la durata dell'inattività trascorsa la quale viene interrotta la connessione Internet (ad es. 60 secondi).

10) Le impostazioni nell'area **Autenticazione** dipendono dal fatto che l'ISP metta a disposizione o meno un'autenticazione tramite PPP.

- Se l'autenticazione viene fornita dall'ISP: assicurarsi di selezionare la casella di controllo **Autenticazione PPP**. Come Nome utente PPP utilizzare il nome fornito dall'ISP per l'accesso a Internet. Immettere le impostazioni PAP e CHAP, come indicato dall'ISP.
- Se l'autenticazione non viene fornita dall'ISP: assicurarsi di deselezionare la casella di controllo Autenticazione PPP.

11) Se si desidera utilizzare NAT, nell'area **Conversione indirizzi**, selezionare la casella di controllo **NAT** (per impostazione predefinita è già selezionata).

12) Nell'area **Parametri QoS dell'interfaccia** immettere i seguenti valori:

a) Nei campi **Larghezza di banda per download** e **Larghezza di banda per upload** immettere la larghezza di banda per download e upload espressa in kbit/sec. messa a disposizione dall'ISP.

b) Se si desidera utilizzare anche la telefonia Internet, nell'elenco a discesa **Controllo della larghezza di banda per connessioni voce** selezionare **Solo upload** o **Upload e download**, come necessario. Nel campo **Larghezza di banda per connessioni voce/fax (%)** immettere la percentuale di larghezza di banda da riservare alle connessioni voce e fax (predefinito: 80%).

13) Fare clic su **OK & Avanti**. Si aprirà la finestra **Configura account DynDNS**.

14) Se si desidera utilizzare una VPN o la funzione di accesso remoto e non si dispone di un indirizzo IP statico, è necessario disporre di un account DynDNS (ad esempio, presso dyndns.org) e configurarlo.

a) Se il provider DynDNS desiderato è disponibile nel menu a discesa **Nome del dominio**, selezionarlo dall'elenco (ad esempio dyndns.org).

b) Se il provider del DynDNS desiderato non è compreso nell'elenco a discesa **Nome del dominio**, selezionare la casella di controllo **Dominio definito dall'utente**. Nel campo **Nome del dominio** immettere il provider del DynDNS desiderato e nel campo **URL aggiornamento** l'URL aggiornato del provider DynDNS. La struttura di tale URL dipende dal provider DynDNS. Inoltre, completare con i parametri specifici per il cliente (nell'esempio contrassegnati in *corsivo*).

```
http://www.anydns.info/update.php?
user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>
```

c) Inserire il **Nome utente** e la **Password** del proprio account DynDNS.
d) Nel campo **Nome dell'host** immettere il nome host indicato dal fornitore DynDNS, senza nome di dominio, ad es. myhost. Il nome di dominio completo risulta myhost.dyndns.org.
e) Testare l'account DynDNS utilizzando **Test connessione**.
f) Se il test ha avuto esito positivo, fare clic su **OK**.
g) Fare clic su **OK & Avanti**.

15) Se si dispone di un indirizzo IP statico pubblico o non si desidera utilizzare la VPN o l'accesso remoto, fare clic su **Nessun DynDNS**.

16) Fare clic su **Fine**. Il sistema di comunicazione si riavvia.

10.1.3 Interfaccia WAN

Le WAN (**W**ide **A**rea **N**etwork) vengono utilizzate per riunire diverse LAN (**L**ocal **A**rea **N**etwork), e singoli PC. All'interfaccia WAN è possibile collegare un modem Internet per l'accesso a Internet.

L'interfaccia WAN non può essere utilizzato per la connessione dei nodi di rete e per il collegamento di utenti IP o di client IP.

10.1.4 DynDNS

DynDNS (Dynamic Domain Name Service) è un servizio Internet che assegna a un indirizzo IP che cambia dinamicamente un nome DNS fisso.

OpenScape Business X mette a disposizione il servizio DynDNS se è collegato un modem Internet alla relativa porta WAN e il sistema di comunicazione è utilizzato come router Internet. In caso contrario, il servizio DynDNS nel router Internet esterno viene configurato nell'infrastruttura del cliente.

Nome DNS

Grazie a DynDNS un client connesso a Internet con indirizzo IP dinamico può essere sempre associato allo stesso nome DNS. A tale scopo è necessario un account DynDNS presso un fornitore DynDNS. Se al sistema di comunicazione viene assegnato un nuovo indirizzo IP (ad es. dall'ISP), questo indirizzo viene inviato automaticamente al fornitore DynDNS che lo memorizza nell'account Dyn DNS. L'intervallo di tempo per questo aggiornamento è definibile. Se viene indicato un nome DNS, viene risolto nell'indirizzo IP valido al momento tramite una richiesta al fornitore DynDNS. Il nome DNS completo (definito anche nome di dominio) comprende il nome host selezionabile (ad es. myhost) e il fornitore DynDNS scelto (ad es. dyndns.org), ovvero myhost.dyndns.org. Per informazioni più dettagliate, visitare l'indirizzo Internet:

`http://www.dyndns.org/services/dyndns`

DynDNS consente inoltre di creare una rete privata virtuale (VPN) tramite un Internet Service Provider (ISP) che fornisce indirizzi IP dinamici. In questo modo gli operatori in remoto possono accedere alla rete interna aziendale tramite Internet. Per ulteriori informazioni consultare Virtual Private Network, VPN .

Mail Exchanger

La voce Mail Exchange (MX Record) indica, nell'ambito del DNS (Domain Name Service), a quale indirizzo IP inviare le e-mail per i nomi di dominio configurati (ad es. myhost.dyndns.org). L'indirizzo IP deve corrispondere a un server di posta (Mail Exchanger). Un indirizzo e-mail per questo dominio potrebbe essere: mymail@myhost.dyndns.org.

Con la funzione Backup MX, le e-mail che non possono essere inoltrate al Mail Exchanger indicato (ad es. per temporanea indisponibilità) vengono salvate e inviate una volta che Mail Exchanger torna disponibile.

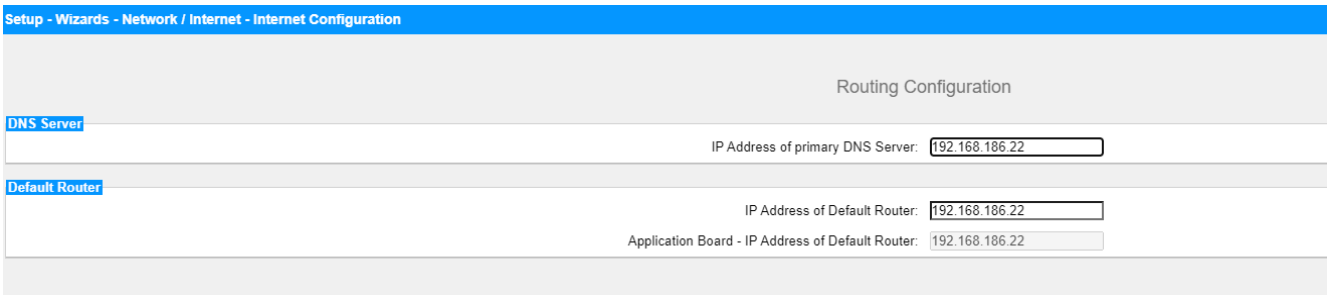
10.1.4.1 Come configurare il servizio DynDNS

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

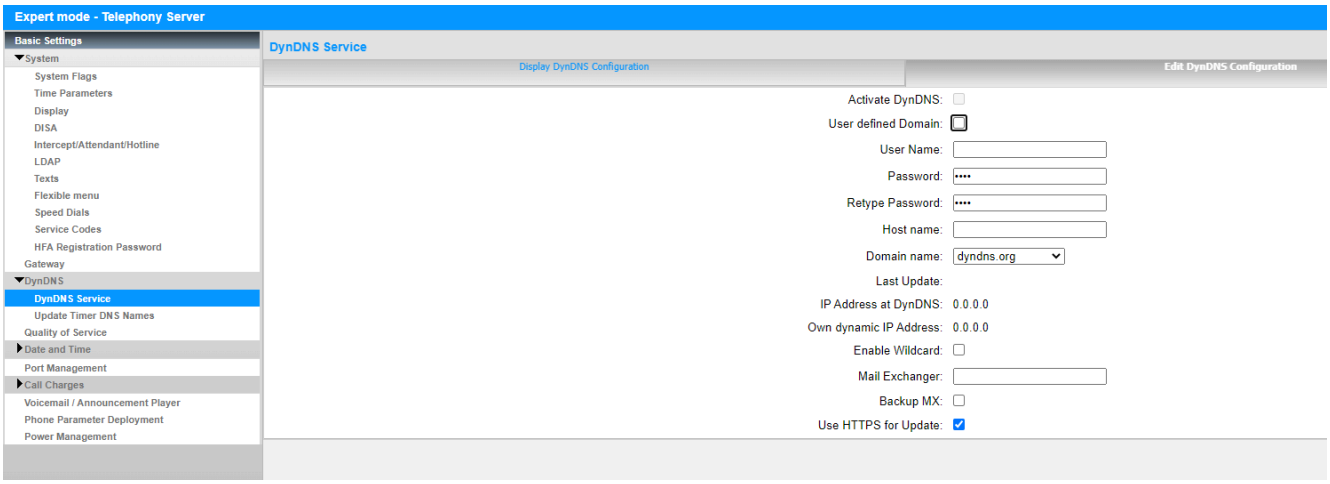
1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **DynDNS**.
4) Fare clic su **Ora aggiornamento nomi DNS**.



5) Selezionare il pulsante di opzione **Aggiorna nome DNS**.
6) Questo valore del timer vale solo per la VPN: inserire nel campo **Valore del timer per l'aggiornamento del nome DNS**, il tempo in secondi trascorso il quale il componente della VPN verifica se il Nome DNS eventualmente utilizzato nella configurazione della VPN viene risolto nei nuovi indirizzi IP (VPN con indirizzi IP dinamici). In questo caso, la VPN viene riconfigurata con i nuovi indirizzi IP.

   Il campo è pre-compilato con `180`, che corrisponde a un intervallo di aggiornamento di 3 minuti.
7) Nella struttura dei menu fare clic su **Servizio DynDNS**.

8) Fare clic sulla scheda **Modifica configurazione DynDNS**.



9) Selezionare la casella di controllo **Attiva DynDNS**.

10) Se il provider DynDNS desiderato è disponibile nel menu a discesa **Nome del dominio**, selezionarlo dall'elenco (ad esempio dyndns.org).

11) Se il provider del DynDNS desiderato non è compreso nell'elenco a discesa **Nome del dominio**, selezionare la casella di controllo **Dominio definito dall'utente**. Nel campo **Nome del dominio** immettere il provider del DynDNS desiderato e nel campo **URL aggiornamento** l'URL aggiornato del provider DynDNS. La struttura di tale URL dipende dal provider DynDNS. Inoltre, completare con i parametri specifici per il cliente (nell'esempio contrassegnati in *corsivo*).

`http://www.anydns.info/update.php?`
`user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

Esempio di un URL aggiornamento con autenticazione crittografata Base64:

`https://<b64><`*`username`*`>:<`*`pass`*`></`
`b64>@members.dyndns.org/nic/update?`
`hostname=<`*`domain`*`>&myip=<`*`ipaddr`*`>&wildcard=NOCHG&mx=NOCHG&backmx=NOC`

<b64>...</b64> per il parametro crittografato Base64

12) Nel campo **Nome utente** immettere il nome utente dell'account DynDNS attivo presso il fornitore DynDNS.

13) Nei campi **Password** e **Ripeti password** immettere la password dell'account DynDNS attivo presso il fornitore DynDNS.

14) Nel campo **Nome dell'host** immettere il nome host indicato dal fornitore DynDNS, senza nome di dominio, ad es. myhost. Il nome di dominio completo risulta myhost.dyndns.org.

15) Visibile solo per i provider DynDNS inclusi nell'elenco a discesa **Nome del dominio**: Attivare il pulsante di opzione **Attiva Wildcard** se si desidera che vengano accettate anche le query a un nome di dominio subordinato come any.myhost.dyndns.org.

16) Visibile solo per i provider DynDNS inclusi nell'elenco a discesa **Nome del dominio**: Attivare il pulsante di opzione **Esegui aggiornamento con HTTPS** se si desidera utilizzare una connessione sicura al provider DynDNS per aggiornare l'indirizzo IP.

17) Fare clic su **Applica**, quindi su **OK**.

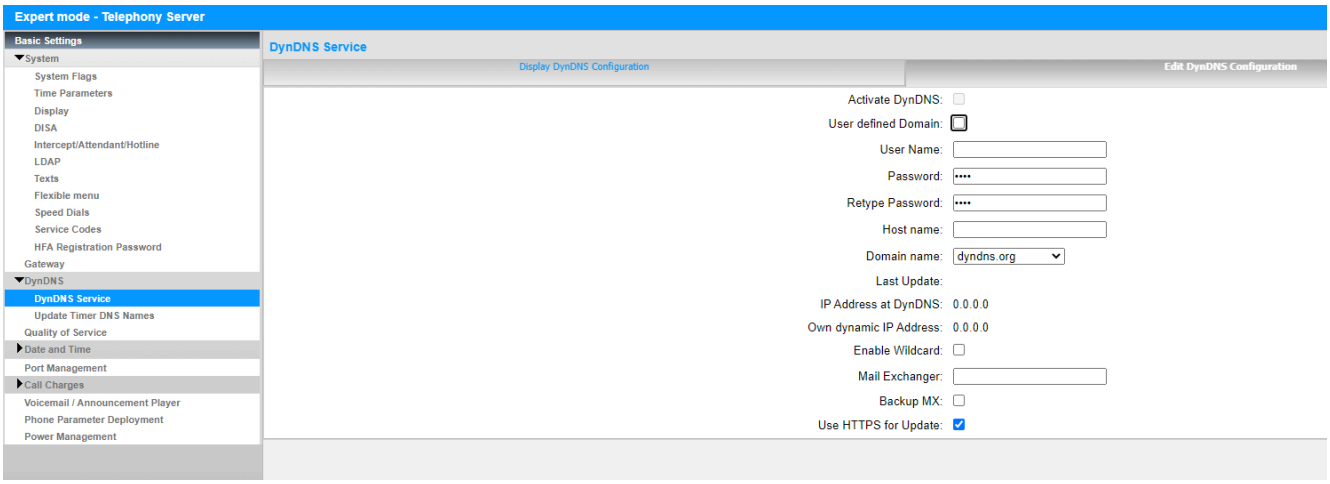
10.1.4.2 Come definire Mail Exchanger

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **DynDNS**.
4) Fare clic su **Servizio DynDNS**.
5) Fare clic sulla scheda **Modifica la configurazione di DynDNS**.



6) Nel campo **Mail Exchanger** immettere l'indirizzo IP del server di posta (voce Mail Exchange o Record MX).
7) Selezionare l'opzione **Backup MX**.
8) Fare clic su **Applica**, quindi su **OK**.

10.2 Linea esterna tramite ITSP

Per poter telefonare tramite Internet è necessario un accesso tramite ITSP (Internet Telephony Service Provider, provider SIP). A tale scopo occorre richiedere una connessione per telefonia Internet presso l'ITSP e configurare un account utente.

Connessione all'ITSP

Il sistema di comunicazione utilizza le opzioni descritte nel capitolo "Accesso a Internet" per raggiungere l'ITSP (OpenScape Business X: tramite LAN o WAN/ OpenScape Business S: solo tramite LAN).

L'accesso ITSP è basato su SIP (Session Initiation Protocol) per la segnalazione e su RTP (Realtime Transport Protocol) per le connessioni voce e dati.

I provider di servizi di telefonia Internet non offrono tutti la stessa gamma di servizi SIP. Pertanto, dovrebbero essere utilizzati solo ITSP certificati per il

sistema di comunicazione. Un elenco di ITSP certificati, nonché il processo di certificazione, è riportato al seguente collegamento:

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

Nota: I numeri di telefono speciali e i numeri di emergenza non supportati dall'ITSP devono essere composti tramite il collegamento di rete fissa.

In caso di guasto/mancata disponibilità dell'ITSP, è possibile attivare una soluzione secondaria mediante istradamento su rete fissa utilizzando il Least Cost Routing (LCR).

Account utente ITSP

L'account utente ITSP (SIP User Account) viene fornito dall'ITSP. A tale scopo l'ITSP mette a disposizione un server Registrar SIP al quale il sistema di comunicazione deve prima accedere (a seconda del provider).

Nota: La registrazione non è necessaria se l'ITSP utilizza l'autenticazione IP statica o tunnel VPN.

Numero interno mobile (MEX)

Questa funzionalità è offerta da alcuni operatori di telefonia mobile unitamente al servizio MDA (Mobile Direct Access). In questo modo, i cellulari/smartphone possono essere integrati in un sistema di comunicazione come utenti interni.

Questa funzione può essere utilizzata soltanto mediante accesso alla telefonia Internet in selezione passante. A tal fine per la configurazione dell'ITSP occorre inserire il numero MEX fornito dall'ITSP stesso. Presso l'ITSP il numero del cellulare è associato al numero MEX. Inoltre, il cellulare/smartphone deve essere configurato nel sistema di comunicazione come utente Mobility (vedere Configurazione di myPortal to go e Mobility Entry).

Descrizione breve:

- L'operatore mobile offre tariffe flat per il telefono cellulare.
- Servizio One Number: il telefono cellulare è raggiungibile tramite un singolo numero di rete fissa che viene trasmesso anche al proprio interlocutore.
- Lo stato presenza e lo stato della connessione di telefoni cellulari è visibile come per gli utenti interni.
- Ogni telefonata da/per un telefono cellulare viene eseguita esclusivamente tramite OpenScape Business in combinazione con un ITSP certificato.
- Il numero di cellulare non è noto esternamente, ciò significa che il telefono non può essere chiamato direttamente. Allo stesso modo non è possibile effettuare chiamate dirette in uscita. Tutte le chiamate passano attraverso OpenScape Business.
- Il telefono cellulare può essere integrato in team interni al sistema.
- Le applicazioni UC quali myPortal for Desktop e myPortal for Outlook possono essere utilizzate come utenti interni.
- myPortal to go è utile durante i viaggi.
- I telefoni cellulari integrati si identificano con il proprio nome quando si chiama un utente interno.

- L'analisi della selezione e l'instradamento delle chiamate nel sistema o sulla rete avviene come per gli altri utenti interni (ad esempio numeri di telefono permessi e vietati, regole LCR)
- L'ITSP utilizza una speciale segnalazione di chiamata da/per OpenScape Business che deve essere gestita di conseguenza.
- Ogni cellulare integrato richiede una licenza utente Mobility.
- Per utilizzare le applicazioni UC, è inoltre necessaria una licenza client UC.

10.2.1 Configurazione di un ITSP

È possibile configurare provider di servizi di telefonia Internet (ITSP) nuovi o predefiniti. Per ogni ITSP è possibile configurare uno o più account. È possibile attivare contemporaneamente fino a 8 ITSP.

Per ulteriori informazioni sugli ITSP e sui relativi servizi, consultare:

`http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#Overview`

Nota: Gli esempi di configurazione sono disponibili su Internet alla pagina **Unify Experts Wiki** in *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"* (disponibile solo in inglese e tedesco).

Assegnazione dei numeri di telefono ITSP

- Con una **connessione analogica di telefonia Internet** l'ITSP mette a disposizione singoli numeri di telefono, ad esempio 70005555, 70005556, ... Questi numeri vengono poi assegnati manualmente ai numeri interni degli utenti.
- Con una **connessione punto-punto di telefonia Internet** l'ITSP mette a disposizione una fascia di numeri (intervallo di numeri), ad esempio da (+39) 02 7007-100 a (+39) 02 7007-147. I numeri di telefono di questa fascia vengono successivamente assegnati manualmente ai numeri interni degli utenti.

I due tipi di connessione possono essere combinati.

In alternativa, per entrambi i tipi di collegamenti, i numeri di telefono dell'ITSP possono essere inseriti nella configurazione degli utenti come selezione passante dell'utente.

Numero di telefono interno	Nome	DID
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

In questo modo, i numeri di telefono degli ITSP sono costituiti dal numero di sistema configurato (ad esempio il codice paese 49) e dal numero di selezione

passante inserito in formato esteso. Ciò rappresenta un vantaggio nell'analisi del numero da comporre e nella gestione delle chiamate, anche in una rete. Quindi la connessione dell'ITSP è ad esempio estensibile anche a un altro nodo.

Eventuali ulteriori attacchi linea urbana via ISDN sono possibili solo con limitazioni.

Gestione multisito

Gli utenti del sistema di comunicazione possono essere assegnati a siti differenti (ad esempio, con un diverso prefisso di area). A ciascuna località è assegnato un fascio e a ogni fascio è assegnata una registrazione ITSP. È possibile gestire un massimo di 8 registrazioni ITSP. È possibile eseguire una registrazione per ogni ITSP oppure più registrazioni a un ITSP. A ciascuna registrazione ITSP può essere assegnato un prefisso di area, al quale possono essere assegnati più utenti. La connessione degli utenti nei diversi siti al sistema di comunicazione avviene tramite connessione VPN. Tutti i siti devono trovarsi all'interno di un unico paese e utilizzare lo stesso codice di accesso alla linea urbana (vedere anche *Collegamento in rete di OpenScape Business nell'ambiente host*, Scenario 1b).

Utilizzo dei modelli ITSP

Per impostazione predefinita viene usato un modello di ITSP preconfigurato. A tal fine, nel modello vengono inseriti i propri dati e i numeri di telefono e questo viene successivamente attivato.

In Modalità esperti, è anche possibile modificare un modello di ITSP preconfigurato e salvarlo come un nuovo modello.

Aggiornamento dei modelli ITSP

I modelli ITSP preconfigurati vengono aggiornati automaticamente dopo un aggiornamento del software di sistema, se in tale aggiornamento sono presenti nuovi modelli ITSP preconfigurati o nuovi valori predefiniti per i modelli preconfigurati esistenti.

Se per l'ITSP è già stato attivato un modello, l'aggiornamento non viene eseguito automaticamente, poiché aggiornando i valori predefiniti possono venire sovrascritte modifiche importanti. Pertanto, l'aggiornamento deve essere eseguito manualmente, tramite la Modalità esperti. Successivamente, i valori predefiniti devono essere nuovamente modificati con i propri criteri.

Modalità di direzione linea

Le singole linee di una linea ITSP possono bloccate per il traffico in entrata e/o in uscita. Sono disponibili le modalità di direzione linea seguenti:

- solo in uscita
- solo in entrata
- in uscita e in entrata (predefinito)

La direzione della linea viene valutata quando il sistema di comunicazione deve riservare una linea ITSP per una chiamata in entrata o in uscita.

10.2.1.1 Come configurare un ITSP predefinito

La procedura guidata **Telefonia Internet** può essere utilizzata per configurare e attivare un provider di servizi di telefonia Internet (ITSP) preferito. È possibile configurare uno o più account per ogni ITSP.

Prerequisiti

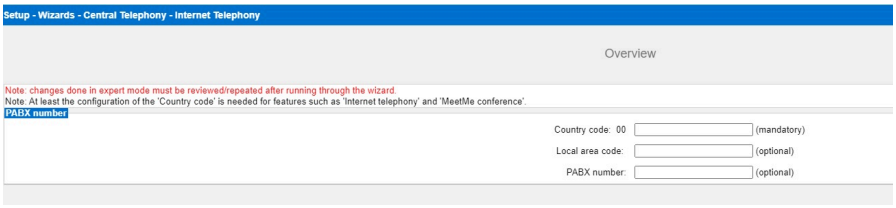
La connessione a Internet deve essere operativa.

I dati di accesso per la telefonia Internet del proprio ITSP sono disponibili (ad es. account utente, password, numero per telefonia Internet).

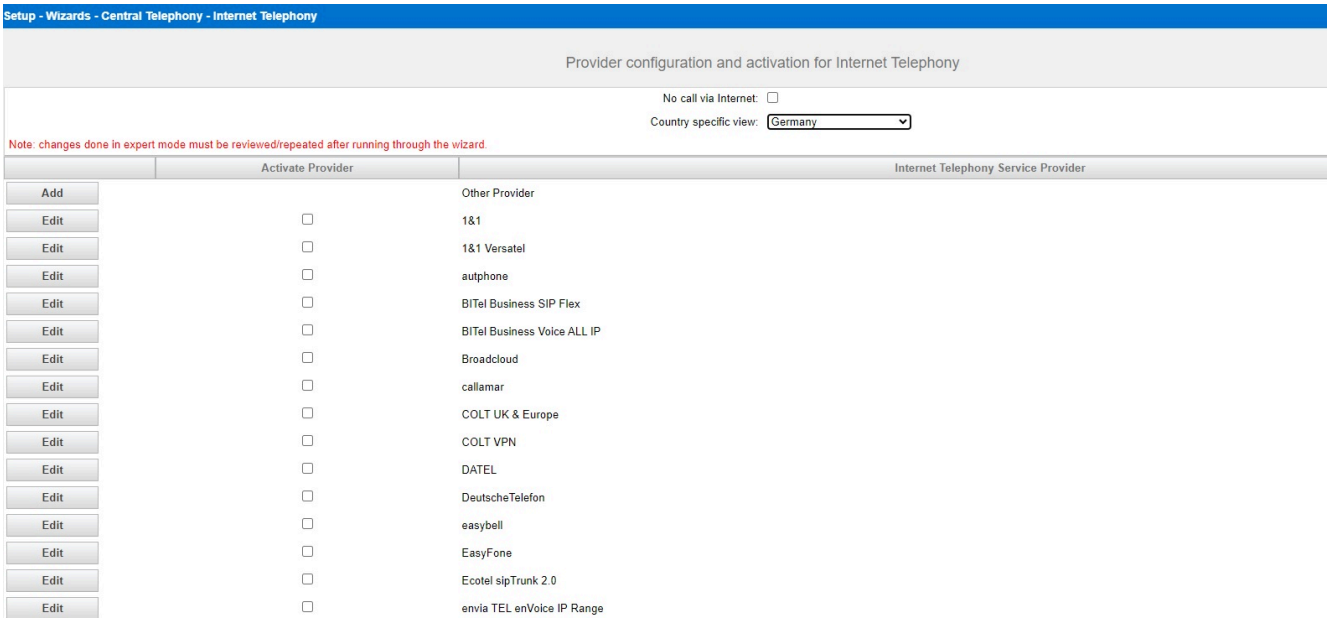
Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Telefonia Internet**.

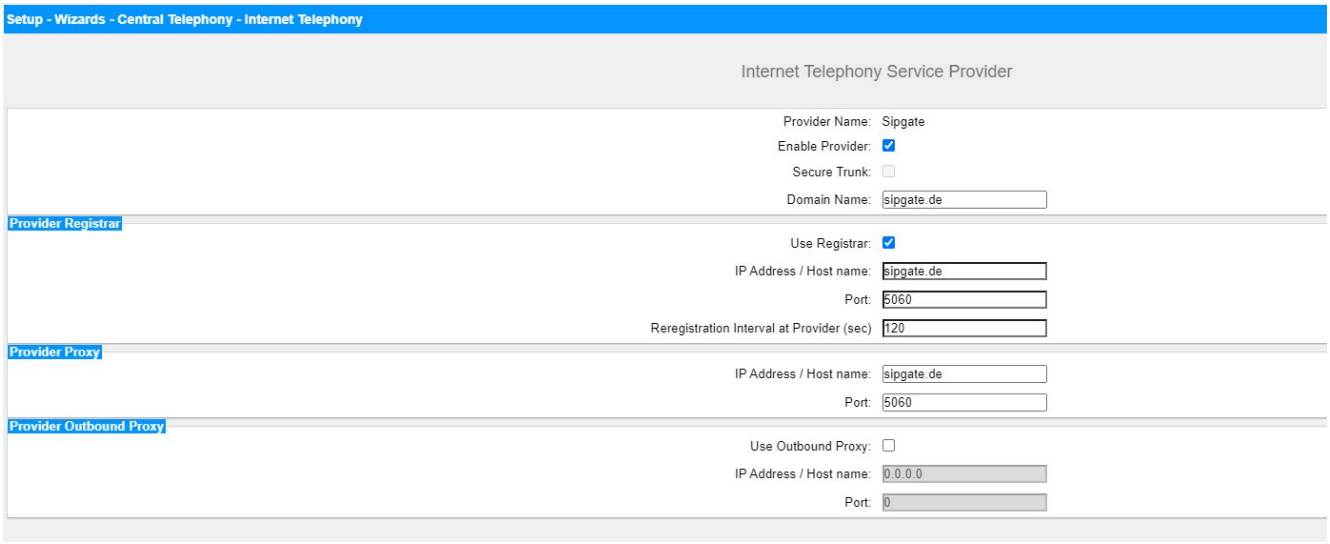


4) Deselezionare la casella di controllo **No telefonia tramite Internet**. Viene visualizzata una lista degli ITSP possibili, in base al Paese. L'elenco contiene gli ITSP predefiniti per il paese selezionato e gli ITSP creati.

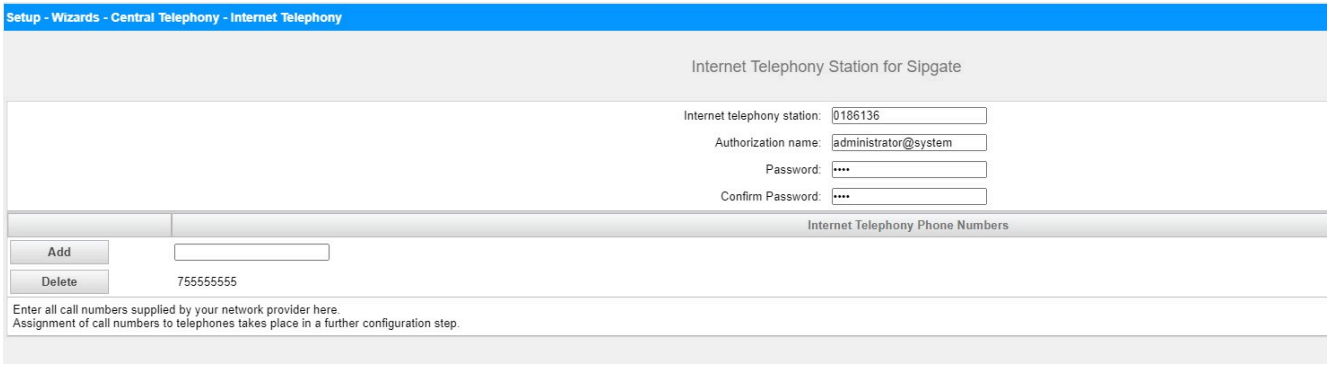


5) Se si desidera modificare il Paese preimpostato, dall'elenco a discesa **Panoramica specifica del paese** selezionare il Paese desiderato. Verranno visualizzati gli ITSP disponibili per il Paese scelto.

6) Se necessario, fare clic su **Mostra stato**, per visualizzare quali sono gli ITSP già attivi e quali utenti di telefonia Internet sono configurati per i singoli ITSP. Si possono attivare fino a 8 ITSP. Fare quindi clic su **OK**.
7) Per configurare l'ITSP predefinito, fare clic su **Modifica** nella riga associata all'ITSP corrispondente.
8) Selezionare la casella di controllo **Attiva provider**.
9) Se il provider supporta la connessione sicura, è possibile attivare la casella di controllo **Trunk sicuro**.
10) I valori per "**Provider Registrar**", "**Proxy del provider**", "**Proxy in uscita del provider**" e "**Funzione del provider**" se abilitato) sono predefiniti in base alle esigenze della maggior parte degli ITSP. Per alcuni ITSP vengono utilizzati indirizzi di server specifici per il cliente. In questo caso, i campi non disattivati devono essere compilati in base alla documentazione ricevuta dall'ITSP.
11) Se il provider supporta la deflessione di chiamata, viene visualizzata la sezione Funzioni del provider e si può attivare la funzione di deflessione delle chiamate. Quando la deflessione delle chiamate è attivata, la deviazione delle chiamate viene effettuata nella rete del provider e la gestione delle chiamate nel sistema non è efficace.



12) Fare clic su **OK & Avanti**.
13) Fare clic su **Aggiungi** per configurare il proprio account ITSP con i relativi numeri di telefonica Internet. I campi visualizzati dipendono dal provider.



14) Nel campo **Utente di telefonia Internet** immettere i dati di accesso del proprio account. I dati sono stati forniti dall'ITSP. In base all'ITSP, possono venire utilizzati termini diversi, ad esempio: Utente SIP, ID SIP, ecc.

    Ulteriori dettagli sono disponibili sul sito http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers

15) Nel campo **Nome autorizzazione** immettere il valore corrispondente. I dati sono stati forniti dall'ITSP. Se non si è ricevuto alcun nome autorizzazione, inserire gli stessi dati già indicati in **Utente di telefonia Internet**.

    Nota: Se non viene utilizzata alcuna registrazione, il campo **Nome autorizzazione** è in grigio e non può essere configurato.

    ---

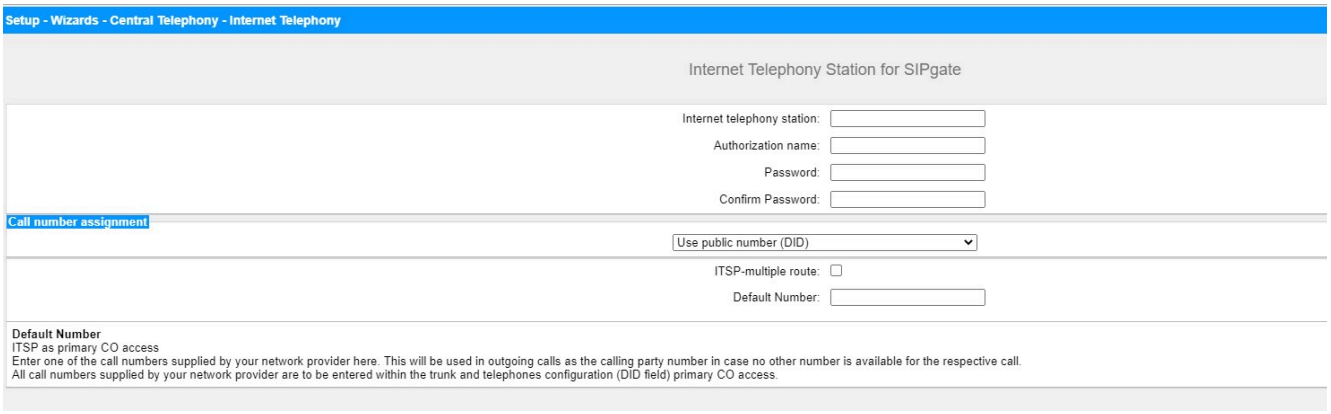
16) Nei campi **Nuova password** e **Ripeti password** immettere la password ricevuta dall'ITSP. In base all'ITSP, possono venire utilizzati termini diversi, ad esempio: Password, Password SIP, ecc.

    Nota: Se non viene utilizzata alcuna registrazione, il campo **Password** è in grigio e non può essere configurato.

    ---

17) Assegnazione dei numeri di telefonia Internet - Opzione 1:

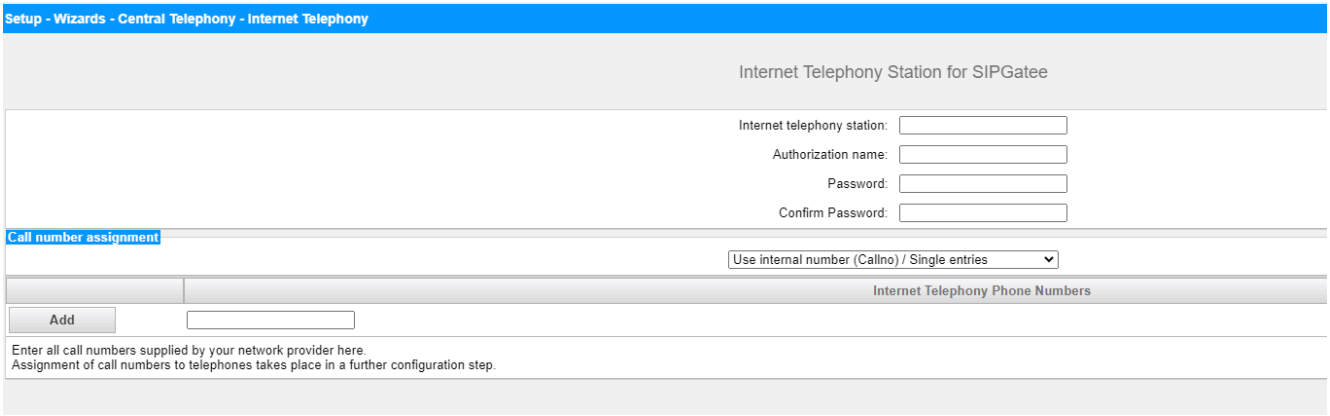
    Usa numero pubblico (DID): i numeri telefonici di telefonia Internet (DID) della propria connessione di telefonia Internet vengono configurati durante la configurazione delle stazioni (nei campi **DID**). Non è necessaria alcuna configurazione di mappatura durante la configurazione dell'ITSP.



    a) Nell'area **Assegnazione numero di telefono**, selezionare il pulsante di opzione **Usa numero pubblico (DID)**.
    b) In **Numero predefinito**, inserire il numero di telefono da utilizzare per le chiamate in uscita quando non è disponibile un numero DID del chiamante.
    c) Se il proprio ITSP supporta la funzione "Mobile Extension (MEX)", in **Numero MEX** inserire il numero MEX messo a disposizione dall'ITSP (8 cifre, solo numeri). Se l'ITSP non supporta la funzione "Mobile Extension (MEX)", il campo **Numero MEX** non viene visualizzato.
    d) Se è necessario configurare più percorsi, attivare la casella di controllo **Percorso ITSP multiplo**.
    e) Inserire i **Prefissi del percorso ITSP** assegnati al percorso e fare clic su **Aggiungi**.

18) Assegnazione dei numeri di telefonia Internet - Opzione 2:

Usa numero interno (N° tel.) / singole voci: Si dispone di un ITSP che ha bisogno di una registrazione SIP per ogni numero di chiamata (ad esempio 70005555, 70005556,...). Per ogni numero di chiamata deve essere creata una stazione di telefonia Internet e deve essere assegnato un singolo numero di chiamata. Se l'ITSP consente di utilizzare più numeri di chiamata con un'unica registrazione, si deve utilizzare l'opzione 1.



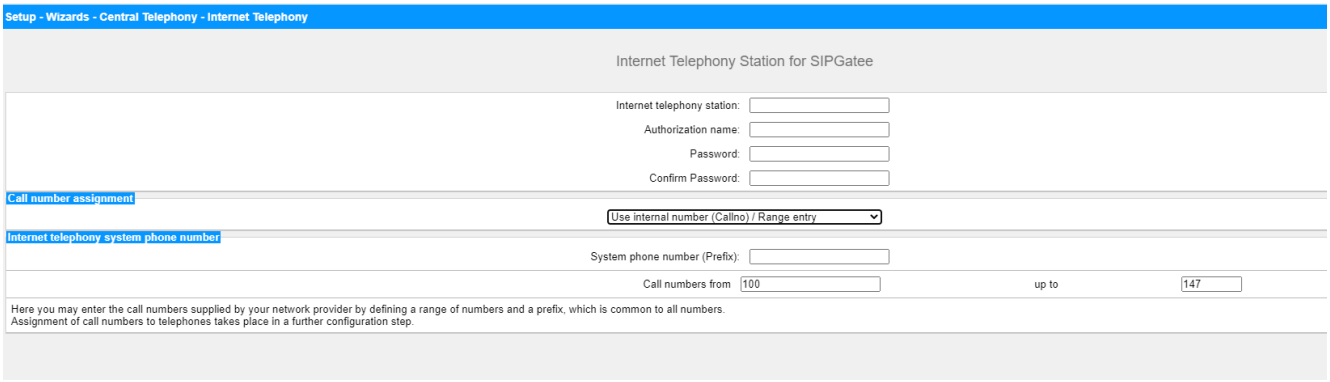
a) Nell'area **Assegnazione numero di telefono**, selezionare il pulsante di opzione **Usa numero interno (N° tel.) / singole registrazioni**.
b) Nell'area **Numeri telefonia Internet**, nel campo accanto al pulsante **Aggiungi** inserire uno dei numeri per telefonia Internet ricevuto dall'ITSP e fare clic su **Aggiungi**.
c) Se si desidera assegnare all'account altri numeri di telefonia Internet, ripetere il passo b).

19) Assegnazione dei numeri di telefonia Internet - Opzione 3:

Usa numero interno (N tel.) / registrazione area:: l'uso di questa opzione è deprecato, per la configurazione di DID si deve usare l'opzione 1.

Si dispone di una connessione punto-punto di telefonia Internet e si è ricevuto un intervallo di numeri di telefono per la telefonia Internet, ad esempio da (+39) 02 7007-100 a (+39) 02 7007-147. I numeri di chiamata

provenienti dall'intervallo di numeri di telefono vengono assegnati come numeri di chiamata interni degli utenti.



a) Nell'area **Assegnazione numero di telefono**, selezionare il pulsante di opzione **Usa numero interno (N° tel.) / registrazione area**.

b) In **Numero del sistema (prefisso)**, immettere il numero del sistema.

c) Nei campi **Fascia numeri interni diretti da** e **a**, immettere l'intervallo di numeri interni desiderato per l'utente di telefonia Internet. Di norma da 100 a 147.

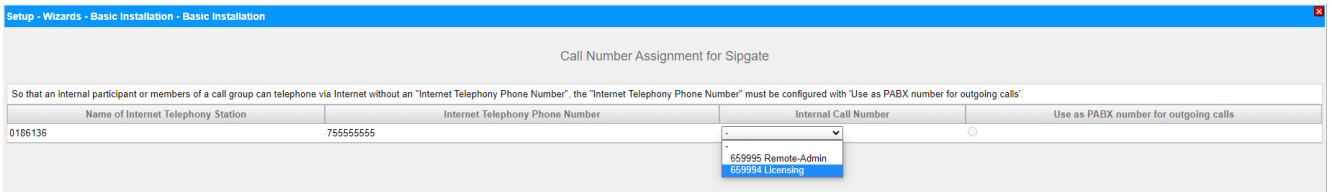
20) Fare clic su **OK & Avanti**.

21) Se si desidera configurare account aggiuntivi, ripetere i passi da 13 a 20.

22) Fare clic su **OK & Avanti**. Viene visualizzata una panoramica che riporta i numeri di telefono di telefonia Internet e gli account a cui sono assegnati.

23) Assegnare sempre tutti i numeri per telefonia Internet a un numero interno di un utente.

Questo passaggio non si applica se è stata selezionata l'opzione 1 per l'assegnazione dei numeri di telefono di telefonia Internet. In questo caso, l'assegnazione si effettua con la configurazione dell'utente nel campo **DID**. Anche in questo caso la schermata è visibile ma non modificabile.



a) Nella riga corrispondente dell'elenco a tendina **Numero interno** selezionare un numero di telefono interno.

b) Se un utente non dotato di numero di telefono per la telefonia Internet o membri di un gruppo di chiamata deve eseguire telefonate tramite Internet, è necessario selezionare il pulsante di opzione **Voce predefinita**. Il pulsante di opzione può essere selezionato solo per un singolo numero di telefonia Internet.

24) Fare clic su **OK & Avanti**. Anche in questo caso è presente una panoramica dei possibili ITSP. Gli ITSP attivati sono contrassegnati con un segno di spunta nella colonna **Attiva provider**. Con Mostra stato è possibile controllare lo stato della connessione. Con **Riavvia ITSP** presente in questa pagina è possibile registrarsi nuovamente presso l'ITSP attivo in caso di problemi di connessione.

25) Fare clic su **OK & Avanti**.

26) Nel campo **Larghezza di banda della connessione (Kbit/s)** immettere il valore della velocità in upload della propria connessione Internet. Da non confondere con la velocità di download!

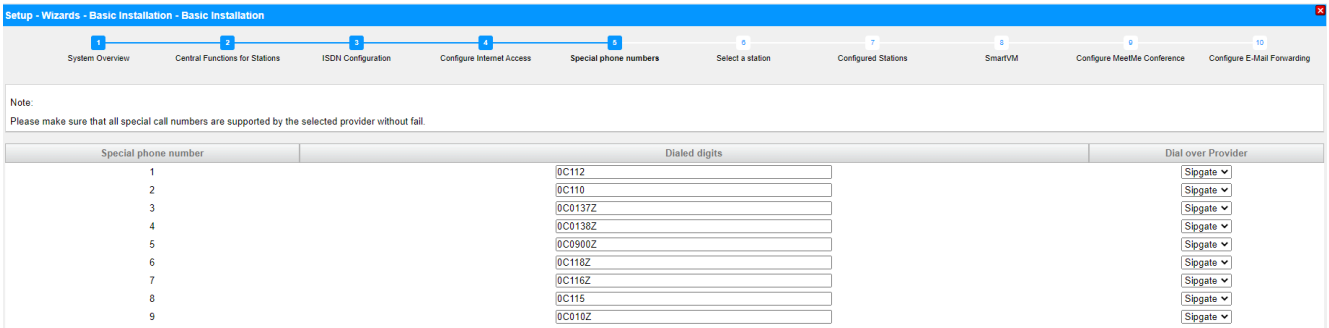
Nota: Nel campo **Numero conversazioni Internet simultanee** viene visualizzato il numero di conversazioni telefoniche Internet conducibili contemporaneamente. Se la qualità della conversazione peggiora a causa del sovraccarico della rete, è necessario ridurre il numero indicato.

Per ulteriori informazioni sul numero di chiamate Internet simultanee, fare riferimento a Limitazione del numero di chiamate simultanee tramite ITSP alla pagina 820.

---

27) Fare clic su **OK & Avanti**.

28) Nella colonna **Cifre selezionate** indicare i numeri di telefono speciali desiderati.



Sono valide le seguenti voci relative ai numeri di telefono:

- 0 - 9: cifre consentite
- -: Separatore di campi
- X: Cifra a piacere fra 0 e 9
- N: Cifra a piacere fra 2 e 9
- Z: seguono una o più cifre fino alla fine della selezione
- C: Tono di selezione simulato (può essere specificato fino a tre volte)

29) Nella colonna **Chiama tramite provider**, selezionare se i numeri di telefono speciali devono essere selezionati via ISDN o tramite un ITSP. Vengono visualizzati solo gli ITSP attivi.

Nota: Assicurarsi che i numeri di emergenza possano sempre essere selezionati. Se i numeri di emergenza devono essere selezionati tramite un Internet Telephony Service Provider, l'ITSP deve supportare questo servizio.

---

30) Fare clic su **OK & Avanti**. Viene visualizzato lo stato degli ITSP.

31) Fare clic su **Avanti**, quindi su **Fine**. Dopo questa fase, eseguire la procedura guidata **Trunk CO ISDN/Analogico/ITSP** per impostare la priorità per l'impegno della linea urbana (ad esempio: Impegno della linea urbana prima su ITSP e poi su ISDN).

10.2.1.2 Come aggiungere un nuovo ITSP

La procedura guidata **Telefonia Internet** può essere utilizzata per configurare e attivare un nuovo fornitore di servizi di telefonia Internet (ITSP). È possibile configurare uno o più account per ogni ITSP.

Prerequisiti

La connessione a Internet deve essere operativa.

Si è connessi a WBM con il profilo **Avanzato**.

L'ITSP deve mettere a disposizione i seguenti dati per l'accesso a Internet:

Campo	Descrizione	Valore da ISP
Nome del dominio del gateway	Nome di dominio del gateway dell'ITSP, di solito identico al nome dell'host (ad esempio, sip-voice.de)	
Provider Registrar		
Usa Registrar	Predefinito dall'ITSP e generalmente sempre configurato (non richiesto per gli ITSP che utilizzano l'autenticazione IP statica).	
Indirizzo IP/Nome host	Nome host o indirizzo IP del server Registrar (ad esempio, sip-voice.de).	
Porta	Numero di porta del server Registrar (ad esempio, 5060).	
Intervallo di registrazione presso il provider (sec.)	Intervallo (in secondi) con cui viene ripetuta la registrazione ITSP. Il valore dell'intervallo non deve essere 0 e non deve essere impostato troppo alto perché, ripetendo la registrazione presso l'ITSP, può venire rilevata anche una caduta della connessione e, se necessario, può essere selezionato un percorso alternativo (via ISDN o un provider alternativo). Valore predefinito: 120 secondi.	
Proxy del provider		
Indirizzo IP/Nome host	Nome host o indirizzo IP del server proxy (ad esempio, sip-voice.de). Di solito è identico alla voce Provider Registrar.	
Porta	Numero di porta del server proxy (ad esempio, 5060). Di solito è identico al numero di porta del Provider Registrar.	
Funzione del provider		

Campo	Descrizione	Valore da ISP
Deflessione di chiamata	Visibile solo se il modello base selezionato supporta la deflessione di chiamata	
Proxy in uscita del provider		
Usa proxy in uscita	Da impostare solo se l'ITSP utilizza un proxy in uscita.	
Indirizzo IP/Nome host	Nome host o indirizzo IP del proxy in uscita	
Porta	Numero della porta del proxy in uscita	
Proxy in entrata del provider		
Usa proxy in entrata	Da impostare solo se l'ITSP utilizza un secondo proxy.	
Indirizzo IP/Nome host	Nome host o indirizzo IP del proxy in entrata	
Porta	Numero di porta del secondo proxy	
STUN provider		
Usa STUN	Da usare solo se è richiesta la funzionalità STUN. Abilita anche la modalità STUN globale.	
Indirizzo IP/Nome host	Indirizzo IP STUN se l'ITSP utilizza un server STUN.	
Porta	Numero di porta STUN se l'ITSP utilizza un server STUN.	

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonai centrale**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Telefonia Internet**.
4) Deselezionare la casella di controllo **No telefonia tramite Internet**. Viene visualizzata una lista degli ITSP possibili, in base al Paese. L'elenco contiene gli ITSP predefiniti per il paese selezionato ed eventuali ITSP già creati.
5) Se necessario, fare clic su **Mostra stato**, per visualizzare quali sono gli ITSP già attivi e quali utenti di telefonia Internet sono configurati per i singoli ITSP. Si possono attivare fino a 8 ITSP. Fare quindi clic su **OK**.
6) Fare clic su **Aggiungi** per configurare un nuovo ITSP. Viene visualizzata la finestra di configurazione del nuovo ITSP.
7) Selezionare un **Modello base** dall'elenco a discesa. Questa opzione consente di avere lo stesso ITSP configurato in diversi percorsi.

8) Assegnare un nome di propria scelta per l'ITSP nel campo **Nome provider**.

Nota: Il limite massimo di caratteri è 10.

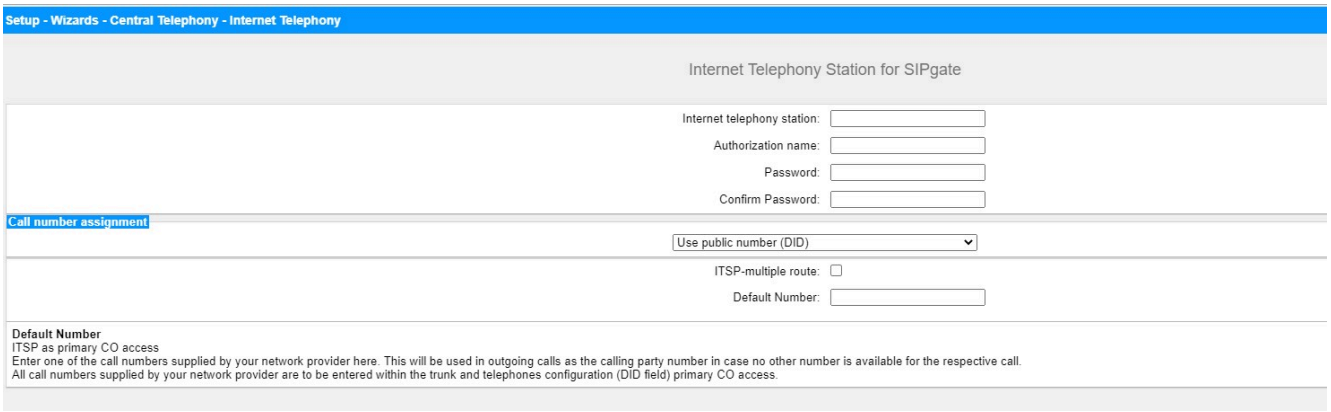
9) Selezionare la casella di controllo **Attiva provider**.

10) Inserire i valori forniti dal proprio ITSP nelle aree rimanenti (vedere la tabella subito dopo i prerequisiti).

Nota: I valori di "Dati provider SIP estesi" possono essere modificati solo da personale di assistenza autorizzato, in collaborazione con il reparto di sviluppo!

11) Fare clic su **OK & Avanti**.

12) Fare clic su **Aggiungi** per configurare il proprio account ITSP con i relativi numeri di telefonica Internet. I campi visualizzati dipendono dal provider.



13) Nel campo **Utente di telefonia Internet** immettere i dati di accesso del proprio account. I dati sono stati forniti dall'ITSP. In base all'ITSP, possono venire utilizzati termini diversi, ad esempio: Utente SIP, ID SIP, ecc.

Ulteriori dettagli sono disponibili sul sito http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers

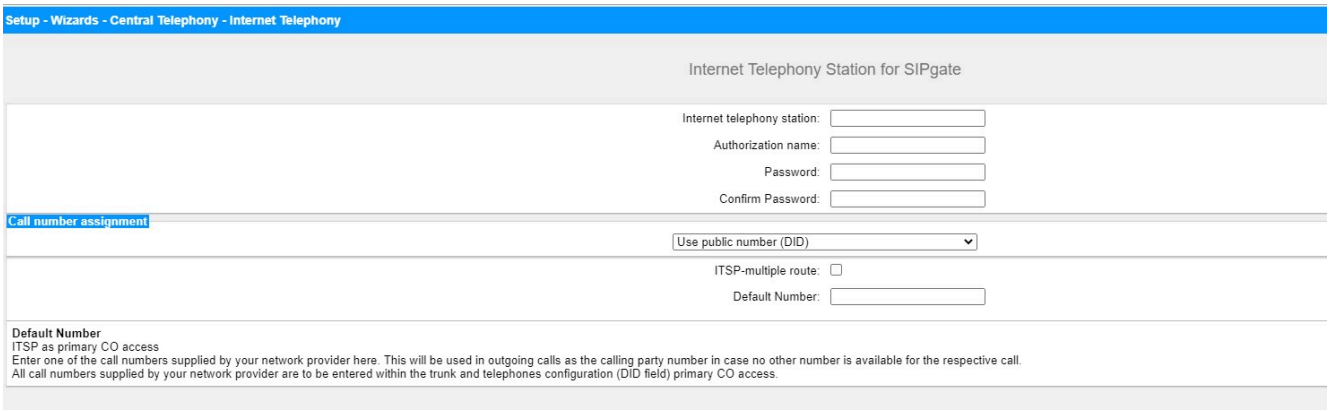
14) Nel campo **Nome autorizzazione** immettere il valore corrispondente. I dati sono stati forniti dall'ITSP. Se non si è ricevuto alcun nome autorizzazione, inserire gli stessi dati già indicati in **Utente di telefonia Internet**.

15) Nei campi **Nuova password** e **Ripeti password** immettere la password ricevuta dall'ITSP. In base all'ITSP, possono venire utilizzati termini diversi, ad esempio: Password, Password SIP, ecc.

16) Assegnazione dei numeri di telefonia Internet - Opzione 1:

Usa numero pubblico (DID): i numeri telefonici di telefonia Internet (DID) della propria connessione di telefonia Internet vengono configurati durante

la configurazione delle stazioni (nei campi **DID**). Non è necessaria alcuna configurazione di mappatura durante la configurazione dell'ITSP.



a) Nell'area **Assegnazione numero di telefono**, selezionare il pulsante di opzione **Usa numero pubblico (DID)**.
b) In **Numero predefinito**, inserire il numero di telefono da utilizzare per le chiamate in uscita quando non è disponibile un numero DID del chiamante.
c) Se il proprio ITSP supporta la funzione "Mobile Extension (MEX)", in **Numero MEX** inserire il numero MEX messo a disposizione dall'ITSP (8 cifre, solo numeri).
d) Attivare la casella di controllo **Percorso ITSP multiplo**.
e) Inserire i **Prefissi del percorso ITSP** assegnati al percorso e fare clic su **Aggiungi**.

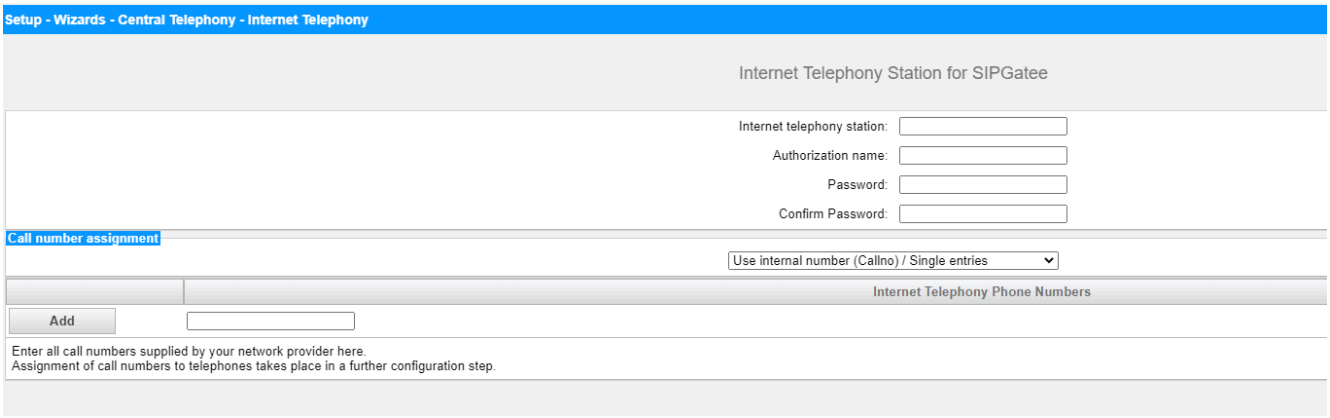
Nota: Per configurare più percorsi è necessario ripetere i passaggi precedenti. Ulteriori informazioni sono disponibili nel wiki di Unify all'indirizzo: http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#General_Configuration_guides

---

17) Assegnazione dei numeri di telefonia Internet - Opzione 2:

Usa numero interno (N° tel.) / singole voci: Si dispone di un ITSP che ha bisogno di una registrazione SIP per ogni numero di chiamata (ad esempio 70005555, 70005556,...). Per ogni numero di chiamata deve essere creata una stazione di telefonia Internet e deve essere assegnato

un singolo numero di chiamata. Se l'ITSP consente di utilizzare più numeri di chiamata con un'unica registrazione, si deve utilizzare l'opzione 1.

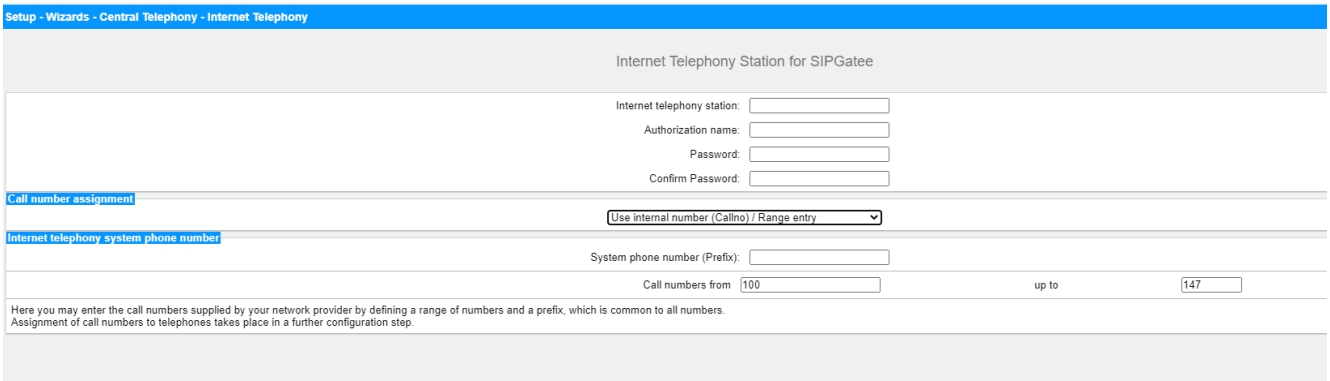


a) Nell'area **Assegnazione numero di telefono**, selezionare il pulsante di opzione **Usa numero interno (N° tel.) / singole registrazioni**.
b) Nell'area **Numeri telefonia Internet**, nel campo accanto al pulsante **Aggiungi** inserire uno dei numeri per telefonia Internet ricevuto dall'ITSP e fare clic su **Aggiungi**.
c) Se si desidera assegnare all'account altri numeri di telefonia Internet, ripetere il passo b).

18) Assegnazione dei numeri di telefonia Internet - Opzione 3:

Usa numero interno (N tel.) / registrazione area:: l'uso di questa opzione è deprecato, per la configurazione di DID si deve usare l'opzione 1.

Si dispone di una connessione punto-punto di telefonia Internet e si è ricevuto un intervallo di numeri di telefono per la telefonia Internet, ad esempio da (+39) 02 7007-100 a (+39) 02 7007-147. I numeri di chiamata provenienti dall'intervallo di numeri di telefono vengono assegnati come numeri di chiamata interni degli utenti.



a) Nell'area **Assegnazione numero di telefono**, selezionare il pulsante di opzione **Usa numero interno (N° tel.) / registrazione area**.
b) In **Numero del sistema (prefisso)**, immettere il numero del sistema.
c) Nei campi **Fascia numeri interni diretti da** e **a**, immettere l'intervallo di numeri interni desiderato per l'utente di telefonia Internet. Di norma da 100 a 147.

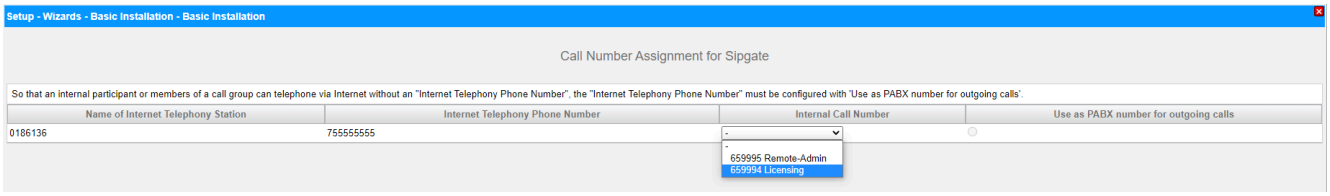
19) Fare clic su **OK & Avanti**.

20) Se si desidera configurare account aggiuntivi, ripetere i passi da 12 a 19.

21) Fare clic su **OK & Avanti**. Viene visualizzata una panoramica che riporta i numeri di telefono di telefonia Internet e gli account a cui sono assegnati.

22) Assegnare sempre tutti i numeri per telefonia Internet a un numero interno di un utente.

Questo passaggio non si applica se è stata selezionata l'opzione 1 per l'assegnazione dei numeri di telefono di telefonia Internet. In questo caso, l'assegnazione si effettua con la configurazione dell'utente nel campo **DID**. Anche in questo caso la schermata è visibile ma non modificabile.



a) Nella riga corrispondente dell'elenco a tendina **Numero interno** selezionare un numero di telefono interno.

b) Se un utente non dotato di numero di telefono per la telefonia Internet o membri di un gruppo di chiamata deve eseguire telefonate tramite Internet, è necessario selezionare il pulsante di opzione **Voce predefinita**. Il pulsante di opzione può essere selezionato solo per un singolo numero di telefonia Internet.

23) Fare clic su **OK & Avanti**. Anche in questo caso è presente una panoramica dei possibili ITSP. Gli ITSP attivati sono contrassegnati con un segno di spunta nella colonna **Attiva provider**. Con Mostra stato è possibile controllare lo stato della connessione. Con **Riavvia ITSP** presente in questa pagina è possibile registrarsi nuovamente presso l'ITSP attivo in caso di problemi di connessione.

24) Fare clic su **OK & Avanti**.

25) Nel campo **Larghezza di banda della connessione (Kbit/s)** immettere il valore della velocità in upload della propria connessione Internet. Da non confondere con la velocità di download!

Nota: Nel campo **Numero conversazioni Internet simultanee** viene visualizzato il numero di conversazioni telefoniche Internet conducibili contemporaneamente. Se la qualità della conversazione peggiora a causa del sovraccarico della rete, è necessario ridurre il numero indicato.

Per ulteriori informazioni sul numero di chiamate Internet simultanee, fare riferimento a Limitazione del numero di chiamate simultanee tramite ITSP alla pagina 820.

---

26) Fare clic su **OK & Avanti**.

27) Nella colonna **Cifre selezionate** indicare i numeri di telefono speciali desiderati.

    Sono valide le seguenti voci relative ai numeri di telefono:

    - 0 - 9: cifre consentite
    - -: Separatore di campi
    - X: Cifra a piacere fra 0 e 9
    - N: Cifra a piacere fra 2 e 9
    - Z: seguono una o più cifre fino alla fine della selezione
    - C: Tono di selezione simulato (può essere specificato fino a tre volte)

28) Nella colonna **Chiama tramite provider**, selezionare se i numeri di telefono speciali devono essere selezionati via ISDN o tramite un ITSP. Vengono visualizzati solo gli ITSP attivi.

    Nota: Assicurarsi che i numeri di emergenza possano sempre essere selezionati. Se i numeri di emergenza devono essere selezionati tramite un Internet Telephony Service Provider, l'ITSP deve supportare questo servizio.

29) Fare clic su **OK & Avanti**. Viene visualizzato lo stato degli ITSP.

30) Fare clic su **Avanti**, quindi su **Fine**. Dopo questa fase, eseguire la procedura guidata **Trunk CO ISDN/Analogico/ITSP** per impostare la priorità per l'impegno della linea urbana (ad esempio: Impegno della linea urbana prima su ITSP e poi su ISDN).

10.2.1.3 Come configurare un multisito tramite ITSP

Con la procedura guidata **Gestione multisito**, è possibile definire fino a 8 località per il sistema di comunicazione, a ciascuna delle quali si può assegnare una registrazione ITSP e più utenti.

Prerequisiti

Il numero delle registrazioni create presso uno o più ITSP corrisponde alle località che possono essere configurate.

Tutte le località si trovano all'interno di un paese.

Si è connessi a WBM con il profilo **Advanced**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su > **Procedure guidate**Telefonia centrale.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Gestione multisito**.
4) In **Codice località** indicare per ogni località un codice (inclusi gli zeri non significativi, ad esempio `02` per Milano e `06` per Roma). È possibile inserire codici località diversi o uguali.
5) In **Località**, inserire per ogni località un nome (ad esempio le città corrispondenti ai codici località `Milano` e `Roma` o se il codice località è lo stesso, le descrizioni dei reparti `Assistenza` e `Vendite`).

6) Nell'elenco a discesa **Percorso dedicato** assegnare a ogni località un fascio. Per ogni registrazione ITSP è automaticamente riservato un fascio (fino a 8).
7) Per eliminare una o più località, selezionare le località nella colonna **Eliminare** quindi fare clic su **Salva.**
8) Fare clic su **OK & Avanti**.
9) Assegnare alle località gli utenti e i gruppi:
   a) Evidenziare gli utenti e i gruppi desiderati.

   Nota:

   È anche possibile cercare utenti e gruppi inserendo nei campi di ricerca **N. chiamata**, **DID** o **Nome** il termine da cercare e quindi facendo clic sull'icona a forma di lente di ingrandimento. Se si lasciano vuoti tutti i campi di ricerca e quindi si fa clic sull'icona della lente di ingrandimento, vengono visualizzati tutti gli utenti e i gruppi.

   L'opzione **Tipo** consente di visualizzare tutti i tipi di utenti (ad esempio, **Client SIP** o **Client di sistema**).

   Gli utenti e i gruppi trovati possono essere selezionati singolarmente nella colonna **Selezione** o tutti assieme utilizzando la casella di controllo **Seleziona tutto**.

   b) In **Per intervallo** selezionare la località desiderata.
   c) Fare clic su **Salva**.
   d) Per altre località, ripetere i passaggi precedenti.
10) Se necessario, è possibile anche assegnare gli utenti e i gruppi di una località a un'altra località:
   a) In **Sposta la selezione dall'intervallo** selezionare la località i cui utenti e gruppi devono essere assegnati a un'altra località. Vengono visualizzati tutti gli utenti e i gruppi della località.
   b) Selezionare gli utenti desiderati singolarmente nella colonna **Selezione** o utilizzando la caselle di controllo **Seleziona tutto**.
   c) In **per intervallo** selezionare la nuova località desiderata.
   d) Fare clic su **Salva**.
   e) Per altre località, ripetere i passaggi precedenti.
11) Fare clic su **OK & Avanti**.

10.2.1.4 Come salvare un modello ITSP preconfigurato come un nuovo modello

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **Gateway**.
3) Nella struttura del menu, fare clic su **Provider di servizi di telefonia Internet**.

4) Fare clic sulla scheda **Aggiungi provider di servizi di telefonia Internet**.
5) Selezionare il modello ITSP desiderato dall'elenco **Modello base**.
6) Nel campo **Nome provider** indicare il nome desiderato per il nuovo modello ITSP.
7) Modificare i valori del modello secondo le proprie esigenze. La spiegazione dei valori è disponibile nella sezione Gateway voce>Provider di servizi di telefonia Internet.
8) Fare clic su **Applica**, quindi su **OK**.

10.2.1.5 Come modificare il modello ITSP preconfigurato

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Gateway voce**.
3) Nella struttura dei menu fare clic su **Provider di servizi di telefonia Internet**.
4) Nella struttura dei menu fare clic sul modello di ITSP desiderato.
5) Fare clic sulla scheda **Modifica provider di servizi telefonia Internet**.
6) Modificare il valore del modello secondo i propri criteri. Per informazioni sui valori, consultare Gateway voce>Provider di servizi di telefonia Internet.

Nota: Il pulsante **Reimposta valori predefiniti** consente di riportare le modifiche ai valori predefiniti. Se l'ITSP del modello è già attivato, tutti gli account dell'ITSP vengono immediatamente disconnessi e quindi registrati di nuovo con i valori predefiniti.

Nota: Con il pulsante **Aggiorna** è possibile aggiornare i valori predefiniti a condizione che sia stato effettuato un aggiornamento del software e che in tale aggiornamento siano presenti nuovi valori predefiniti aggiornati per questo modello.

---

7) Fare clic su **Applica**, quindi su **OK**.

10.2.1.6 Come aggiornare manualmente il modello ITSP preconfigurato

Prerequisiti

L'ITSP di questo modello è attivato.

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Gateway voce**.

3) Nella struttura dei menu fare clic su **Provider di servizi di telefonia Internet**.
4) Nella struttura dei menu fare clic sul modello di ITSP desiderato.
5) Fare clic sulla scheda **Modifica provider di servizi telefonia Internet**.
6) Annotare i valori del modello modificati rispetto ai valori predefiniti (ad esempio con l'aiuto di una schermata).
7) Fare clic su **Aggiornamento**. I valori predefiniti del modello vengono aggiornati a condizione che sia stato eseguito un aggiornamento del software e che in tale aggiornamento siano presenti valori predefiniti più recenti per questo modello.
8) Modificare di nuovo il valore del modello secondo i propri criteri. Per informazioni sui valori, consultare Gateway voce>Provider di servizi di telefonia Internet.

Nota: Il pulsante **Reimposta valori predefiniti** consente di riportare le modifiche ai valori predefiniti. Tutti gli account dell'ITSP vengono immediatamente disconnessi e quindi registrati di nuovo con i valori predefiniti.

---

9) Fare clic su **Applica**, quindi su **OK**.

10.2.2 STUN (Simple Traversal of UDP through NAT)

Quando si utilizza il sistema di comunicazione dietro a un router NAT, STUN determina la propria porta/indirizzo IP pubblico, richiesti da alcuni ITSP. La funzionalità viene messa a disposizione su Internet da server STUN, i cui indirizzi devono essere immessi nella configurazione del sistema di comunicazione.

La modalità STUN richiesta dipende dall'infrastruttura ITSP e dal router Internet utilizzato. STUN non è richiesto con gli ITSP che risolvono NAT trasversalmente utilizzando i componenti dell'infrastruttura nella rete del provider, quali Session Border Controller (SBC).

È possibile configurare nel sistema di comunicazione le seguenti modalità STUN:

- **Automatico (opzione predefinita)**

  Se nessun ITSP è attivo, in questa modalità STUN è completamente disattivato. Se è attivo un ITSP, STUN determina il tipo di firewall utilizzato (tipo NAT) all'avvio del sistema e può rilevare le modifiche agli indirizzi IP durante l'uso. A seconda del tipo NAT rilevato, STUN modifica parametri specifici nei messaggi SIP.

  Nota: NAT simmetrico non è supportato.

- **Sempre**

  STUN è sempre attivo. A seconda del tipo NAT definito, alcuni parametri dei messaggi SIP vengono modificati.

- **Usa IP statico**

  Il modem DSL o il router Internet utilizzano un indirizzo IP statico (indirizzo IP pubblico) e l'ITSP richiede una autenticazione IP statica. Devono inoltre essere indicati gli indirizzi IP statici e le porte usate dal router o dal modem.
- **Router di protezione porte**

  L'indirizzo IP pubblico viene determinato utilizzando STUN. Nei messaggi SIP, la porta viene inserita senza modifiche.

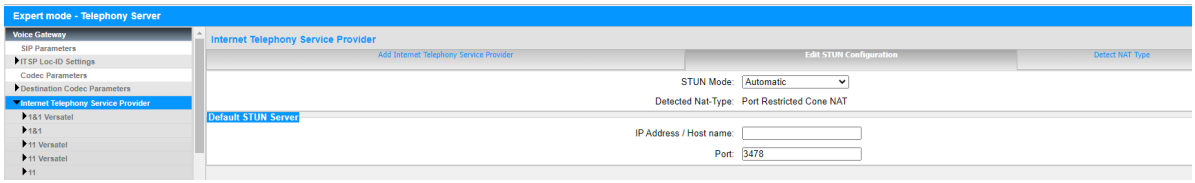
10.2.2.1 Come definire la modalità STUN

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Gateway voce**.
3) Nella struttura dei menu fare clic su **Provider di servizi di telefonia Internet**.
4) Fare clic sulla scheda **Modifica configurazione STUN**.



5) Nell'elenco a discesa **Modalità STUN**, selezionare la modalità STUN desiderata.
6) Se è stata selezionata la modalità STUN **Usa IP statico**, specificare in **Indirizzo IP pubblico** e in **Porta SIP pubblica** l'indirizzo IP statico e la porta del modem DSL o il router Internet.
7) Fare clic su **Applica**, quindi su **OK**.

10.3 Accesso alla linea urbana tramite linee analogiche e digitali

L'accesso alla linea urbana tramite ISDN o linee analogiche collega le piattaforme hardware con la rete pubblica (PSTN).

Le procedure guidate semplificano la configurazione di un accesso ISDN o analogico alla linea esterna.

10.3.1 Linee

Le linee collegano le piattaforme hardware con la rete pubblica (PSTN). A ogni linea deve essere assegnato un fascio attraverso il quale è possibile assegnare alla linea diverse proprietà.

Per impostazione predefinita, a tutte le linee è assegnato un codice di linea e un fascio. Le assegnazioni possono essere modificate dall'amministratore.

In caso di attacco di linea urbana ISDN, le linee vengono definite anche canali B.

Codice della linea

Sulla base del codice della linea, il sistema di comunicazione impegna la linea assegnata a tale codice. L'identificazione della linea viene utilizzata anche per la programmazione di un tasto di linea o per il controllo di una linea.

Assegnazione numero MSN

Il provider di servizi assegna a ogni connessione ISDN punto - multipunto (PMP, Point-to-Multipoint) uno o più numeri MSN (Multiple Subscriber Number). Questi possono essere assegnati direttamente a una linea.

Numeri di telefono completi

I numeri di telefono completi includono il prefisso internazionale, il prefisso urbano e il numero del sistema (PABX) o uno o più numeri MSN.

Protocollo ISDN

Il protocollo ISDN utilizzato dipende prefisso internazionale. Può essere modificato solo se il collegamento ad un PSTN richiede esplicitamente un protocollo diverso. Sono disponibili numerosi modelli di protocollo che possono essere adattati alle proprie esigenze. Le informazioni necessarie sono disponibili presso il proprio provider di servizi.

Modalità di impegno del canale B

I singoli canali B di una linea ISDN possono essere bloccati per il traffico in entrata e/o in uscita.

Sono possibili le seguenti modalità di impegno del canale B:

- solo in uscita
- solo in entrata
- in uscita e in entrata (predefinito)

La modalità di impegno del canale B viene analizzata solo quando il sistema di comunicazione deve suggerire un canale B. Ciò si verifica nelle seguenti situazioni.

S_2 in uscita:	Il sistema di comunicazione deve offrire un canale B.
S_2 in entrata:	Il terminale sul lato opposto è obbligato a offrire un canale B. Questo canale B viene accettato dal sistema di comunicazione senza una verifica dell'impostazione. L'impostazione non ha quindi alcuna influenza.
S_0 in uscita:	Siccome nel sistema di comunicazione non sono predefiniti canali B (any channel), l'impostazione non ha alcuna influenza.
S_0 in entrata:	Quando il terminale remoto effettua una chiamata senza specificare un canale B, il sistema di comunicazione offre un canale B, prendendo in considerazione la modalità di impegno del canale B impostata.

Tipo di selezione per linee urbane analogiche (HKZ)

Il tipo di selezione viene automaticamente riconosciuto dal sistema di comunicazione a ogni impegno della linea. In casi speciali, è possibile impostare anche direttamente il metodo di selezione su segnalazione multifrequenza a due toni (DTMF) o impulsi di selezione (DP).

10.3.1.1 Come configurare la linea esterna ISDN

La procedura guidata **Linea ISDN / analogica / ITSP** consente di configurare la linea esterna ISDN. In base alla porta disponibile nel sistema di comunicazione per la linea urbana (ISDN o analogica) la procedura guidata presenterà passaggi diversi.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Il sistema di comunicazione è collegato ad una linea ISDN.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Linea esterna ISDN / analogica / ITSP**. La procedura guidata visualizza una panoramica di box, slot e porte S_0.
4) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. `39` per l'Italia o `1` per gli USA.
5) Nel campo **Prefisso interurbano**, immettere l'indicativo località, ad es. 051 per Bologna.
6) Con un collegamento punto-punto, nel campo **Numero del sistema**, immettere il numero del sistema della linea urbana (ad esempio 7007, il proprio numero di connessione).
7) Modificare il campo **Prefisso internazionale** solo quando necessario. Per la Germania si utilizza `00`, per gli Stati Uniti `011`).

   Per le chiamate all'estero, il numero di telefono è preceduto dal prefisso internazionale e dal prefisso nazionale, ad esempio per telefonare dalla Germania agli USA `00-1` e dagli USA alla Germania `011-49`.
8) Fare clic su **OK & Avanti**.
9) Selezionare uno dei seguenti tipi di connessione per l'attacco in questione (box, slot e porta S_0):

   - Per configurare una connessione punto - punto, fare clic sul pulsante di opzione **Connessione punto - punto**.
   - Per configurare una Connessione punto - multipunto, fare clic sul pulsante di opzione **Connessione punto - multipunto**.
10) Fare clic su **OK & Avanti**.
11) Se il sistema è realizzato mediante un collegamento punto - multipunto indicare il numero MSN per la connessione in questione (box, slot e porta S_0), quindi fare clic su **OK & Avanti**.

12) Mantenere l'impostazione della casella di controllo **No telefonia tramite Internet** quindi premere **Ignora**.
13) Nel menu a tendina **Prima tramite** selezionare la linea urbana preferita, quindi fare clic su **OK & Avanti**.
14) Fare clic su **OK & Avanti**, quindi su **Fine**.

10.3.1.2 Come configurare la linea esterna analogica

La procedura guidata **Linea ISDN / analogica / ITSP** consente di configurare la linea esterna analogica.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Il sistema di comunicazione è collegato a una linea urbana analogica.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Linea esterna ISDN / analogica / ITSP**. La procedura guidata visualizza una panoramica di box, slot e porte analogiche.
4) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. `39` per l'Italia o `1` per gli USA.
5) Nel campo **Prefisso interurbano**, immettere l'indicativo località, ad es. 051 per Bologna.
6) Con un collegamento punto-punto, nel campo **Numero del sistema**, immettere il numero del sistema della linea urbana (ad esempio 7007, il proprio numero di connessione).
7) Modificare il campo **Prefisso internazionale** solo quando necessario. Per la Germania si utilizza `00`, per gli Stati Uniti `011`).

   Per le chiamate all'estero, il numero di telefono è preceduto dal prefisso internazionale e dal prefisso nazionale, ad esempio per telefonare dalla Germania agli USA `00-1` e dagli USA alla Germania `011-49`.
8) Fare clic su **OK & Avanti**.
9) Fare clic su **Salta ISDN**.
10) Mantenere l'impostazione della casella di controllo **No telefonia tramite Internet** quindi premere **Ignora**.
11) Nell'elenco a discesa **Protocollo** selezionare il protocollo per la visualizzazione del numero di telefono (diverso a seconda del provider di servizi):
    - Se si desidera utilizzare la funzione Frequency Shift Keying, selezionare **FSK**.
    - Se si desidera utilizzare la funzione DTMF, selezionare **DTMF**.
    - Se non si intende utilizzare la funzione Visualizzazione del chiamante, selezionare **nessuno**.
12) Fare clic su **OK & Avanti**.

13) Fare clic su **Modifica**, per configurare le proprietà della linea in questione. Se necessario, modificare **Tipo di selezione**, **Identificazione chiamata**, **Flash**, **Lunghezza linea** e **Flags** e fare clic su **OK**.
14) Fare clic su **OK & Avanti**.
15) Fare clic su **Ignora**, quindi su **OK & Avanti**.
16) Nel menu a tendina **Prima tramite** selezionare la linea urbana preferita, quindi fare clic su **OK & Avanti**.
17) Fare clic su **OK & Avanti**, quindi su **Fine**.

10.3.1.3 Come mostrare tutte le linee

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee/Routing** > **Linee**. In base alla configurazione del sistema di comunicazione, verranno visualizzate tutte le possibili linee, con il codice di identificazione della linea e il fascio.

10.3.1.4 Come visualizzare una singola linea

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Navigare nella struttura dei menu in **Linee/Rete** > **Linee** > **…** fino alla linea desiderata. Viene visualizzata la linea collegata al sistema di comunicazione, ivi compreso il codice di identificazione della linea e il fascio.
4) Fare clic su **OK**.

10.3.1.5 Come modificare il codice della linea

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Navigare nella struttura dei menu in **Linee/Rete** > **Linee** > **…** fino alla linea desiderata.
4) Fare clic sulla scheda **Modifica linea**.

5) Immettere il valore desiderato nel campo **Codice**.

Nota: Se come codice non viene inserito alcun valore, la linea non avrà alcun codice di identificazione.

6) Fare clic su **Applica**, quindi su **OK**.

10.3.1.6 Come assegnare un MSN ad una linea

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee / Rete** > **Assegna numero MSN**.
4) Nella struttura dei menu fare clic sulla voce che si desidera modificare in **Assegna numero MSN**
5) Immettere il **Numero MSN**.
6) Nell'elenco a discesa selezionare la **Fascio** che si desidera assegnare.
7) Fare clic su **Applica**, quindi su **OK**.

10.3.1.7 Come modificare il protocollo ISDN

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu, seguire il percorso **Linee/Rete** > **Linee** > **...** fino alla porta desiderata.
4) Fare clic sulla scheda **Cambia flag ISDN**.
5) Nell'area **Protocollo: descrizione** selezionare il protocollo desiderato dall'elenco a discesa.
6) Fare clic su **Applica**, quindi su **OK**.

10.3.1.8 Come modificare la modalità di impegno del canale B

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.

3) Nella struttura dei menu, seguire il percorso **Linee/Rete** > **Linee** > **...** fino alla porta desiderata.
4) Fare clic sulla scheda **Cambia canale B**.
5) Per ciascun canale, deselezionare la casella di controllo nelle colonne: **in uscita** e **in entrata** in base alle proprie esigenze.
6) Fare clic su **Applica**, quindi su **OK**.

10.3.1.9 Come modificare il tipo di selezione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu, seguire il percorso **Linee/Rete** > **Linee** > **...** fino alla porta desiderata.
4) Fare clic sulla scheda **Cambia flag linea analogica**.
5) Impostare la selezione a toni (Dual Tone Multiple Frequency, DTMF) o a impulsi (DP).
6) Fare clic su **Applica**, quindi su **OK**.

10.3.2 Fasci

Con i fasci è possibile raggruppare le linee (canali B). Per ogni fascio di linee, è possibile configurare un proprio parametro.

A ogni linea può essere assegnato un fascio specifico. Per impostazione predefinita, tutte le linee sono assegnate al fascio 1.

Per ogni fascio è possibile assegnare un nome e un codice.

Suggerimento: I codici del fascio sono utilizzabili per gli impegni delle linee in uscita solo se LCR non è attivo.

Allocazione dei canali B

Per allocazione dei canali B, si intende l'allocazione di tali canali ai diversi fasci di linee. Per le connessioni linee ISDN con molti canali B, quali ad esempio le connessioni S_{2M}, può essere utile assegnare una parte di canali B ai diversi fasci di linee.

Per le chiamate in uscita vengono selezionati solo i canali B contenuti nel fascio (ad esempio tramite il codice del fascio selezionato, il fascio di overflow o il fascio selezionato mediante LCR).

Le chiamate in arrivo vengono accettate sempre, indipendentemente dal fascio. Solitamente viene impegnato il canale B offerto dal partner. Pertanto, la ripartizione dei canali B configurata nel sistema deve essere supportata anche dal lato partner (sistema o rete pubblica). In caso contrario, non è possibile garantire l'assegnazione corretta delle chiamate ai fasci corrispondenti.

Tasto di fascio

Un utente può programmare un tasto di fascio tramite telefono. Un tasto di fascio è riservato alle chiamate in uscita. Le chiamate eseguite tramite questi tasti sono sottoposte ai livelli e alle regole del controllo della selezione sulla base della classe di servizio (Class of Service).

Dopo che l'utente ha premuto un tasto di fascio (o ha selezionato un codice fascio), il sistema di comunicazione impegna una linea disponibile associata al fascio adeguato per eseguire la chiamata. Il telefono visualizza il numero della linea sul display. Se tutte le linee del fascio sono impegnate, il LED relativo si accende anche nel caso in cui l'overflow sia stato eseguito con successo.

Fascio di overflow con LCR disattivato

Per ogni fascio l'amministratore può definire un fascio di overflow dove viene continuata la ricerca qualora le linee di un fascio siano tutte occupate. Se anche in questo fascio di overflow sono occupate tutte le linee, non ha luogo nessun overflow.

Fascio di overflow con LCR attivo

Per la configurazione LCR, l'amministratore può configurare fino a 16 voci per tabella delle rotte che vengono successivamente elaborate in sequenza, nel contesto di un overflow.

Tipo di impegno

Per l'impegno del fascio in uscita, il sistema di comunicazione ricerca una linea disponibile nel fascio richiesto in base ai seguenti criteri definiti dall'amministratore:

- ciclico

  Dopo l'ultima linea impegnata in uscita - la ricerca inizia con il successivo numero di linea più alto, in riferimento all'ultima linea in uscita impegnata in questo fascio. In questo modo, tutte le linee vengono utilizzate con circa la stessa frequenza.
- lineare:

  sempre la prima linea libera - la ricerca inizia con il successivo numero di linea più basso assegnato a quel fascio.

Numero di telefono del sistema in entrata e in uscita

L'amministratore può definire i numeri di sistema per le chiamate in entrata e in uscita, separatamente. In questo modo, il proprio numero per le chiamate in uscita può essere rappresentato in modo diverso da quanto necessario per assicurare l'accessibilità per le chiamate in arrivo. In questo caso, le porzioni per il prefisso nazionale, il prefisso urbano e il numero di sistema devono quindi essere inserite separatamente. Diverse voci nel numero di telefono di sistema (PABX) in entrata e in uscita richiedono la disponibilità del servizio "CLIP no screening" sulla linea urbana. In caso non sia configurato nessun numero di sistema in uscita, il sistema di comunicazione utilizzerà sempre i dati del numero del sistema in entrata.

In caso di impegno in entrata su una linea ISDN, il sistema di comunicazione nasconde dal numero di telefono ricevuto la porzione relativa al numero di sistema (a sinistra) secondo il tipo di numero di telefono ricevuto (type of number = TON, vedere la tabella alla voce relativa alla trasmissione del numero di telefono) e interpreta la porzione restante come un interno. In caso

le informazioni sul numero di telefono vengano inviate al PSTN, il sistema di comunicazione inserisce automaticamente la porzione in uscita del numero di sistema come parte iniziale del numero di telefono secondo il tipo di numero configurato. In Germania, la porzione del numero del sistema deve essere trasmessa alla linea esterna senza prefisso di linea urbana e senza codice di rinvio (0).

Trasmissione del numero

Il numero di telefono inviato al PSTN e al destinatario può essere composto come segue:

Type Of Number (TON), in uscita	al numero di telefono trasmesso tramite PSTN
Sconosciuto Tono=Sconosciuto	solo numero interno (impostazione predefinita)
Numero del sistema Tono=Utente	Numero del sistema + MSN (interno)
Prefisso interurbano Tono=Nazionale	Prefisso interurbano + numero del sistema + MSN (Interno)
Prefisso internazionale Tono=Internazionale	Prefisso internazionale + prefisso interurbano + numero del sistema + MSN (Interno)
Interno Tono=Interno	solo per sistemi connessi in rete: in presenza di piani di numerazione chiusi non è consentito aggiungere alcun prefisso. Qui vengono soppressi i prefissi dei numeri di telefono.

È anche possibile specificare quali informazioni del numero di telefono dell'utente chiamante devono essere trasmesse alla destinazione.

Tipo di numero di telefono	al numero di telefono trasmesso tramite PSTN
Interno	Qui viene inviata solo un'informazione relativa al numero interno. Se la destinazione è un utente esterno non viene inviato alcun numero o viene inviato il numero del posto operatore. In caso di destinazioni interne, è possibile visualizzare il numero di telefono interno.
Selezione passante	Qui viene inviata solo un'informazione relativa al numero DISA. Con le destinazioni interne su un altro nodo manca il numero di telefono interno per la visualizzazione. Le informazioni sul numero di telefono sono sufficienti per le destinazioni esterne.

Tipo di numero di telefono	al numero di telefono trasmesso tramite PSTN
Interno / Sel.pass.	In una rete è utile scegliere questa impostazione. All'utente di destinazione vengono inviati sia i numeri interni che i numeri DISA. Se in una connessione di rete viene chiamato un utente, a tale utente può essere mostrato il numero interno del chiamante. Se la destinazione interna ha attivato l'inoltro chiamata ad esempio a una destinazione esterna, è possibile inviare in questo caso anche un numero DISA.

Inoltre, è possibile configurare il trattamento desiderato per il prefisso del fascio:

- Chiamata in entrata

  Durante la trasmissione al bus S0, il numero del chiamante viene aggiunto al codice del fascio (-> formato selezionabile per la richiamata automatica) o trasmesso in modo trasparente. Impostazione predefinita: funzione attivata.
- Chiamata in uscita

  Nel telefono di sistema, è possibile visualizzare o nascondere il prefisso del fascio. Impostazione predefinita: funzione attivata.

Secondo prefisso per linea esterna

Un secondo prefisso per linea esterna viene definito se il sistema di comunicazione è un sottosistema di un altro sistema di comunicazione o è collegato in rete con più sistemi di comunicazione. È rilevante per il fascio della connessione di rete (tipo fascio = PABX). In questo caso viene utilizzato il secondo codice di linea urbana come codice di impegno per il sistema principale. All'interno di una connessione di rete, i codici per l'impegno della linea, del fascio e il secondo codice di linea devono essere configurati in modo uniforme. Predefinito per Germania 0.

10.3.2.1 Come modificare l'assegnazione del fascio

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Navigare nella struttura dei menu in **Linee/Rete** > **Linee** > **…** fino alla linea desiderata.
4) Fare clic sulla scheda **Modifica linea**.
5) Nell'elenco a discesa **Fascio** selezionare il fascio che si desidera assegnare alla linea.
6) Fare clic su **Applica**, quindi su **OK**.

10.3.2.2 Come modificare i nomi dei fasci

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee/Rete** > **Fascio**.
4) Nella struttura dei menu fare clic sulla voce che si desidera modificare in **Fascio**.
5) Immettere il valore desiderato nel campo **Nome del fascio**.
6) Fare clic su **Applica**, quindi su **OK**.

10.3.2.3 Come modificare i codici del fascio

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Nota: I codici del fascio sono operativi solo se LCR è inattivo.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee/Rete** > **Fascio**.
4) Nella struttura dei menu fare clic sulla voce che si desidera modificare in **Fascio**.
5) Immettere il valore desiderato nel campo **Codici del fascio**.
6) Fare clic su **Applica**, quindi su **OK**.

10.3.2.4 Come configurare un fascio di overflow con la funzione LCR disattivata

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee / Rete** > **Fascio**.
4) Nella struttura dei menu fare clic sulla voce che si desidera modificare in **Fascio**.
5) Nell'elenco a discesa **Fascio di overflow** selezionare la voce desiderata.
6) Fare clic su **Applica**, quindi su **OK**.

10.3.2.5 Come configurare un fascio di overflow con la funzione LCR attivata

Se è attivato il servizio LCR, viene effettuato il trattamento di overflow tramite elaborazioni successive delle singole voci di una tabella LCR nell'ambito della configurazione LCR (vedere LCR (Least Cost Routing, Instradamento a minor costo)).

10.3.2.6 Come configurare il tipo di impegno

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee/Rete** > **Fascio**.
4) Nella struttura dei menu fare clic sul fascio che si desidera modificare in **Fascio**.
5) Fare clic sulla scheda **Cambia parametri del gruppo di linee**.
6) Nell'elenco a discesa **Tipo di impegno**, selezionare **Ciclico** o **Lineare**.
7) Fare clic su **Applica**, quindi su **OK**.

10.3.2.7 Come inserire il numero di telefono del sistema in entrata e in uscita

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee / Rete** > **Fascio**.
4) Nella struttura dei menu fare clic sulla voce che si desidera modificare in **Fascio**.
5) Nell'area **Numero del sistema in entrata** immettere i valori corrispondenti senza lo zero iniziale nei campi **Prefisso internazionale**, **Prefisso interurbano** e **Numero del sistema**.
6) Nell'area **Numero del sistema in uscita** immettere i valori corrispondenti senza lo zero iniziale nei campi **Prefisso internazionale**, **Prefisso interurbano** e **Numero del sistema**.
7) Selezionare una delle seguenti opzioni:
   - Per sopprimere il numero di telefono dell'utente, spuntare la casella di controllo **Sopprimi num. tel. utente**.
   - Se non si desidera sopprimere il numero di telefono dell'utente, deselezionare la casella di controllo **Sopprimi num. tel. utente**.
8) Fare clic su **Applica**, quindi su **OK**.

10.3.2.8 Come configurare il formato del numero di telefono trasmesso

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee/Rete** > **Fascio**.
4) Nella struttura dei menu fare clic sul fascio che si desidera modificare in **Fascio**.
5) Fare clic sulla scheda **Cambia parametri del gruppo di linee**.
6) Nell'elenco a discesa **Tipo nr., in uscita** selezionare il formato desiderato del numero di telefono da trasmettere.
7) Fare clic su **Applica**, quindi su **OK**.

10.3.2.9 Come configurare il tipo di numero di telefono trasmesso

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee/Rete** > **Fascio**.
4) Nella struttura dei menu fare clic sul fascio che si desidera modificare in **Fascio**.
5) Fare clic sulla scheda **Cambia parametri del gruppo di linee**.
6) Nell'elenco a discesa **Tipo di numero di telefono** selezionare la voce **Interno**, **Selezione passante** o **Interno/DISA**.
7) Fare clic su **Applica**, quindi su **OK**.

10.3.2.10 Come configurare il prefisso del fascio

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee/Rete** > **Fascio**.
4) Nella struttura dei menu fare clic sul fascio che si desidera modificare in **Fascio**.
5) Fare clic sulla scheda **Cambia parametri del gruppo di linee**.

6) Selezionare una delle seguenti opzioni:
   - Se si desidera che il numero di telefono visualizzato per la chiamata in arrivo comprenda il codice del fascio, selezionare la casella di controllo **Prefisso fascio in entrata** nell'area **Flags del fascio**.
   - Se non si desidera che il numero di telefono visualizzato per la chiamata in arrivo comprenda il codice del fascio, deselezionare la casella di controllo **Prefisso fascio in entrata** nell'area **Flags del fascio**.
   - Se si desidera che il numero di telefono visualizzato per la chiamata in uscita comprenda il codice del fascio, selezionare la casella di controllo **Prefisso fascio in uscita** nell'area **Flags del fascio**.
   - Se non si desidera che il numero di telefono visualizzato per la chiamata in uscita comprenda il codice del fascio, deselezionare la casella di controllo **Prefisso fascio in uscita** nell'area **Flags del fascio**.
7) Fare clic su **Applica**, quindi su **OK**.

10.3.2.11 Come definire un fascio per la connessione di rete e inserire un secondo codice di linea urbana

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee/Rete** > **Fascio**.
4) Nella struttura dei menu fare clic sulla voce che si desidera modificare in **Fascio**.
5) Nel campo **Codice di linea urbana (2° CLU)** selezionare il valore desiderato.
6) Fare clic sulla scheda **Cambia parametri del gruppo di linee**.
7) Nell'elenco a discesa **Tipo di fascio**, selezionare la voce **PABX**.
8) Fare clic su **Applica**, quindi su **OK**.

10.3.3 Controllo del segnale di linea

Quando viene stabilita una connessione tramite la linea esterna analogica, è possibile inviare le cifre composte alla linea urbana solo quando viene riconosciuto il tono di composizione (tono acustico). Siccome il tempo necessario prima dell'arrivo del tono di composizione varia a seconda degli operatori di rete, è necessario monitorare l'arrivo del tono di composizione.

La configurazione del tempo di controllo del segnale di linea e del tempo di selezione delle cifre viene eseguita tramite Manager E.

Ritardo del controllo del segnale di linea

Il monitoraggio del tono di composizione può iniziare immediatamente o dopo una pausa. In alcuni casi, può essere necessario riprodurre ulteriori toni per l'utente dopo l'impegno della linea, ad esempio per informarlo che sulla linea esterna è stato attivato l'inoltro chiamata. Per questi casi, è possibile impostare

un ritardo di tempo per il controllo del segnale di linea (pausa prima della composizione, 1-9 secondi). Le cifre digitate vengono inviate alla linea urbana solo dopo la pausa.

Nota: Nota per Brasile:

Se vengono utilizzate la selezione DTMF di dispositivi terminali analogici in combinazione con linee esterne analogiche (TLAx e TML8W) e la selezione a impulsi dopo il controllo del segnale di linea, possono insorgere problemi con il controllo della composizione se come prefisso internazionale si sceglie quello del Brasile. In questo caso i segnali DTMF dei terminali analogici vengono inviati direttamente alle linee urbane analogiche. Tutti i segnali DTMF che vengono selezionati prima della ricezione del tono di composizione vanno persi. Di conseguenza, in questi casi, per consentire il funzionamento corretto è necessario abilitare nel terminale la ricerca automatica del percorso (LCR) il metodo di composizione e il controllo della composizione.

Tempo di controllo del segnale di linea

Il tempo di attesa per il segnale di linea è configurabile. Se non si rileva alcun tono di linea dopo il periodo configurato, la linea viene messa fuori servizio. Il sistema controlla ad intervalli ciclici se il segnale di linea è di nuovo disponibile. In questo caso, la linea viene rimessa in servizio.

Tempo di selezione delle cifre

È possibile impostare dopo quanti secondi dal riconoscimento del tono di selezione deve essere inviata la prima cifra composta (impostazione predefinita: 0 secondi).

Analisi del secondo tono di composizione

Il sistema di comunicazione è in grado di riconoscere un ulteriore tono di composizione (2° segnale acustico). Ciò è importante per i gestori di reti pubbliche che in caso di chiamate internazionali trasmettono un secondo tono di composizione, ad esempio in Belgio dopo lo 00, in Francia dopo il 16 o il 19. Per la Germania questa funzione non si applica.

10.3.3.1 Come configurare il ritardo per il controllo del segnale di linea

Prerequisiti

È presente una porta analogica con linea esterna analogica.

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee/Rete** > **Fascio**.
4) Nella struttura dei menu fare clic sul fascio analogico che si desidera modificare in **Fascio**.
5) Fare clic sulla scheda **Cambia parametri del gruppo di linee**.

6) Se il monitoraggio delle chiamate deve avvenire immediatamente, nell'area **Pausa inizio sel.**, selezionare il pulsante di opzione **Nessuna pausa**.
7) Se il monitoraggio delle chiamate deve essere effettuato solo dopo un tempo di ritardo, nell'area **Pausa inizio sel.** selezionare il tempo di ritardo in secondi.
8) Fare clic su **Applica**, quindi su **OK**.

10.3.3.2 Come configurare il tempo di controllo del segnale di linea

Prerequisiti

È stato inserito un modulo linea esterna analogica.

Passo a passo

1) Dal PC Admin accedere a Manager E.
2) Nella barra dei menu, fare clic su **File | Trasferisci**.
3) Selezionare la scheda **Comunicazioni**.
4) Nell'area **Accesso**, selezionare il pulsante di opzione in base al tipo di collegamento del PC Admin al sistema di comunicazione.
5) Selezionare il pulsante di opzione **Leggere/scrivere CDB** quindi fare clic su **Sistema -> PC**.
6) Fare clic su **OK**. Il CDB verrà trasferito dal sistema di comunicazione a Manager E.
7) Terminato il trasferimento, fare clic su **OK**, quindi su **Chiudi**.
8) In Manager E, nella struttura dei menu della Visualizzazione sistema, fare clic su **Impostazioni** > **Parametri sistema** > **Parametri di tempo**.
9) Nell'elenco sottostante, in **Tempo di controllo del segnale di linea**, in **Base** e **Fattore**, inserire il tempo massimo di attesa prima del tono di linea(predefinito: Base = `1s`, Fattore = `10`).
10) Fare clic su **Applica**.
11) Nella barra dei menu, fare clic su **File | Trasferisci**.
12) Selezionare la scheda **Comunicazioni**.
13) Fare clic su **PC -> Sistema**, quindi su **OK**. Le impostazioni vengono importate nel sistema di comunicazione.
14) Fare quindi clic su **OK** e **Chiudi**.

10.3.3.3 Come configurare il tempo di selezione delle cifre

Prerequisiti

È stato inserito un modulo linea esterna analogica.

Passo a passo

1) Dal PC Admin accedere a Manager E.
2) Nella barra dei menu, fare clic su **File | Trasferisci**.
3) Selezionare la scheda **Comunicazioni**.
4) Nell'area **Accesso**, selezionare il pulsante di opzione in base al tipo di collegamento del PC Admin al sistema di comunicazione.

5) Selezionare il pulsante di opzione **Leggere/scrivere CDB** quindi fare clic su **Sistema -> PC**.
6) Fare clic su **OK**. Il CDB verrà trasferito dal sistema di comunicazione a Manager E.
7) Terminato il trasferimento, fare clic su **OK**, quindi su **Chiudi**.
8) In Manager E, nella struttura dei menu della Visualizzazione sistema, fare clic su **Impostazioni** > **Parametri sistema** > **Parametri di tempo**.
9) Nell'elenco sottostante, in **Tempo tra analisi HT e la composizione linea HKZ**, in **Base** e **Fattore**, definire dopo quanti secondi dal rilevamento del tono di linea deve essere inviata la prima cifra al centralino (predefinito: Base = `10ms`, Fattore = `0`).
10) Fare clic su **Applica**.
11) Nella barra dei menu, fare clic su **File | Trasferisci**.
12) Selezionare la scheda **Comunicazioni**.
13) Fare clic su **PC -> Sistema**, quindi su **OK**. Le impostazioni vengono importate nel sistema di comunicazione.
14) Fare quindi clic su **OK** e **Chiudi**.

10.3.3.4 Come attivare o disattivare la valutazione del secondo tono di composizione

Prerequisiti

È presente una porta analogica con linea esterna analogica.

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee/Rete** > **Fascio**.
4) Nella struttura dei menu fare clic sul fascio analogico che si desidera modificare in **Fascio**.
5) Fare clic sulla scheda **Cambia parametri del gruppo di linee**.
6) Se si desidera attivare l'analisi del secondo tono di composizione, nell'area **Flags del fascio**, selezionare la casella di controllo **Valutazione 2º tono acustico**.
7) Se si desidera disattivare l'analisi del secondo tono di composizione, nell'area **Flags del fascio**, deselezionare la casella di controllo **Valutazione 2º tono acustico/Controllo della linea**.
8) Fare clic su **Applica**, quindi su **OK**.

10.4 Assegnazione priorità accesso linea esterna con funzione LCR attivata

Sulla base della priorità di accesso alla linea esterna viene definita la sequenza dei diversi provider (ISDN/analogico o ITSP).

Per l'accesso alla linea esterna, solitamente è necessario digitare il codice "0". All'interno di questo Codice viene configurata la priorità dei diversi provider (in

base ai dati preimpostati). In questo modo, una conversazione in corso può avvenire inizialmente tramite ITSP, quindi in caso esito negativo dell'accesso alla linea esterna, tramite ISDN.

10.4.1 Come priorizzare l'accesso alla linea esterna

Con la procedura guidata Configurazione della **Linea ISDN / analogica / ITSP**, è possibile configurare la sequenza di accesso alla linea esterna tramite ISDN/ analogico e ITSP.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**. Sono configurati diversi ITSP.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Linea esterna ISDN / analogica / ITSP**. La procedura guidata visualizza una panoramica di box, slot e porte analogiche.
4) Fare clic su **OK & Avanti**.
5) Fare clic più volte su **OK & Avanti** fino a raggiungere la finestra **Priorità per accesso a linea esterna**.
6) Nel campo **Tentativi di accesso alla linea esterna**, nell'elenco a discesa **Prima tramite**, selezionare il provider preferito per il primo tentativo di ottenere una linea esterna libera tramite il sistema di comunicazione.
7) Nell'elenco a discesa **Quindi mediante**, selezionare un secondo provider, tramite il quale eseguire il tentativo successivo per l'accesso alla linea esterna.
8) Nell'elenco a discesa successivo **Quindi mediante**, selezionare un terzo provider, tramite il quale eseguire il tentativo successivo per l'accesso alla linea esterna.
9) Fare clic su **OK & Avanti**, quindi su **Fine**.

11 Utenti

Un abbonato o una stazione è un partner di comunicazione collegato al sistema di comunicazione. In generale, a ogni stazione (a parte le stazioni virtuali) viene assegnato un terminale. Un terminale è, ad esempio, un telefono, un PC o un dispositivo fax. Le stazioni possono anche essere utenti dei client UC.

Esistono i seguenti tipi di stazioni:

- Stazioni IP (note anche come client IP)
- Stazioni SIP (un sottoinsieme delle stazioni IP)
- Stazioni UP0
- Utenti DECT
- Stazioni Mitel SIP-DECT
- Utenti ISDN
- Stazioni analogiche
- Stazioni di mobilità (stazioni mobili, vedi Mobility)
- Utenti virtuali

I dati degli abbonati (nome, numero di stazione, numero DID, indirizzo e-mail, ecc.) possono essere importati come file XML durante l'installazione iniziale (vedere Piano di composizione individuale). Inoltre, i dati degli abbonati possono essere esportati in un file XML (vedere Esportazione dei dati degli abbonati).

Procedura di ottenimento delle licenze per le stazioni

Tutte le stazioni sono soggette a licenza. Per cominciare, le stazioni possono essere configurate durante l'installazione iniziale o in un secondo momento utilizzando le procedure guidate delle stazioni. Una volta effettuata correttamente la configurazione, gli abbonati possono effettuare chiamate interne. Nella fase successiva, le licenze delle stazioni devono essere attivate e assegnate alle stazioni. Una volta assegnate correttamente le licenze, gli abbonati possono anche effettuare chiamate esterne.

Concetti correlati

Concessione della licenza alla pagina 291
Mobilità alla pagina 944

11.1 Piano di composizione

Un piano di composizione è una lista di tutti i numeri di telefono e codici disponibili nel sistema di comunicazione. Contiene fra l'altro i numeri di telefoni interni, quelli di selezione passante e quelli dei gruppi. Nel sistema di comunicazione, i numeri di telefono e i codici sono preimpostati con valori predefiniti. All'occorrenza, questi valori possono essere singolarmente modificati.

Durante la configurazione di numeri di telefono o codici può venire visualizzato un messaggio di errore se il numero desiderato è già assegnato. Con il supporto del piano di numerazione è possibile verificare quali numeri di telefono sono ancora disponibili.

11.1.1 Piano di composizione predefinito

Il piano di composizione predefinito contiene tutti i numeri telefonici e i codici configurati nel sistema di comunicazione con i valori predefiniti.

I valori predefiniti possono all'occorrenza essere modificati. Alcuni numeri di telefono possono essere completamente eliminati in modo da non venire visualizzati nella panoramica del piano di composizione.

Piano di composizione predefinito per piattaforme hardware e soft switch:

Tipo di numero di telefono	X1	X3/X5/X8/S	Azione
Numeri di telefono dell'utente interno	11-30	100-742	eliminabile
Nr. di selezione passante	11 -30	100-742	eliminabile
Numeri di telefono gruppo 1-90 Numeri di telefono gruppo 91-800	31-40 -	350-439 non preassegnati	eliminabile
Numero di telefono linee	700-703	ab 7801	eliminabile
Codici del fascio (codici esterni): Fsc 1 (linea ISDN, analogica) Fsc 8 (UC Suite) Fsc 12-15 (linea ITSP) Fsc 16 (Rete)	 0 = mondo / 9 = USA - non preassegnati non preassegnati	 0 = mondo / 9 = USA 851 855-858 859	solo modificabile
Codice di posto (Posto di rinvio) Interno	9 = mondo 0 = USA	9 = mondo 0 = USA	solo modificabile
Codice di posto (Posto di rinvio) Selezione passante	0 = mondo – = USA	0 = mondo – = USA	solo modificabile
Numeri di telefono per utenti in linea	non preassegnati	749	solo modificabile
Numero di telefono per accesso remoto	non preassegnati	non preassegnati	solo modificabile
Numero di telefono per i messaggi vocali UC Smart UC Suite	351 -	351 non preassegnati	solo modificabile solo modificabile
Numeri di telefono conferenze	-	non preassegnati	solo modificabile
Numero di telefono per parcheggio	-	non preassegnati	solo modificabile

Tipo di numero di telefono	X1	X3/X5/X8/S	Azione
Numeri di telefono AutoAttendant	-	non preassegnati	solo modificabile
Numero di telefono per posto operatore	9 = mondo 0 = USA	9 = mondo 0 = USA	solo modificabile
Sostituzione per "*" (nei codici)	75	75	eliminabile
Sostituzione per "#" (nei codici)	76	76	eliminabile
Codici di servizio			solo modificabile

11.1.2 Piano di composizione personalizzato

Il sistema di comunicazione consente di configurare un piano di composizione personalizzato. A tale scopo è possibile modificare i valori predefiniti dei numeri di telefono e dei codici. In seguito alla ricarica del sistema di comunicazione, vengono ripristinati i valori predefiniti.

Sono utili le seguenti azioni:

- Cancella numeri di telefono predefiniti: tranne per alcune eccezioni (numeri di telefono predefiniti speciali), è possibile cancellare i numeri di telefono predefiniti. Questi numeri di telefono sono contrassegnati con "eliminabile" nella colonna "Azione" della tabella Piano di composizione predefinito.
- Modifica numeri di telefono predefiniti speciali: questi numeri di telefono non possono essere eliminati. Si possono invece modificare i valori assegnati a questi numeri di telefono. Questi numeri di telefono sono contrassegnati con "solo modificabili" nella colonna "Azione" della tabella Piano di composizione predefinito.
- Importa numeri di telefono e dati utente: tramite un file XML si possono importare i dati utente durante l'installazione iniziale. In questo modo si importano anche il numero di telefono e il numero di interno dell'utente. Normalmente, ciò viene eseguito durante l'installazione iniziale.

Importazione dei dati degli utenti tramite file XML

Un piano di composizione personalizzato può essere importato nel sistema di comunicazione durante l'installazione iniziale come file XML in formato UTF-8.

Il programma di amministrazione OpenScape Business Assistant mette a disposizione in **Centro assistenza** > **Documenti** > **Modelli CSV** il file `csv-templates.zip`. Questo file zip contiene i seguenti file e la relativa descrizione.

- `portdata_xml_import_empty.xml`

  Questo modello contiene registri senza record di esempio È quindi possibile aggiungere nuovi record dati con Microsoft Excel.
- `portdata_xml_import_example.xml`

  Questo modello contiene registri con record di esempio È quindi possibile sovrascrivere questi record dati con Microsoft Excel. I record non necessari devono essere eliminati.

- `portdata_xml_import_syntax.txt`

  Descrizione in inglese e tedesco per la corretta creazione dei record.

11.1.2.1 Come cancellare o modificare i numeri di telefono predefiniti

Alcuni numeri di telefono predefiniti si possono cancellare e ridefinire tramite le procedure guidate. Per quanto riguarda i numeri di telefono predefiniti speciali, non eliminabili, è possibile modificarne i valori preassegnati.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

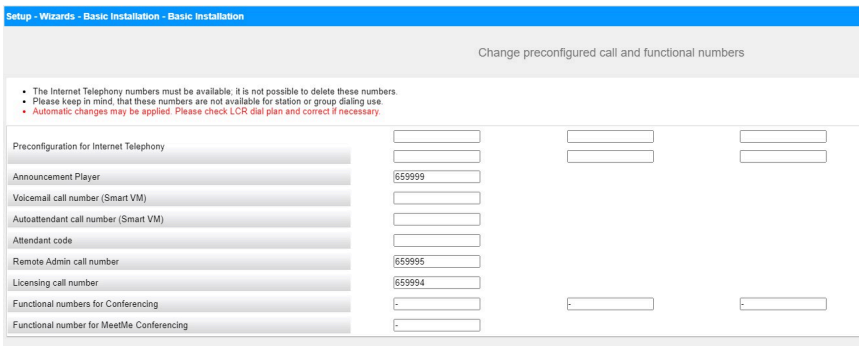
Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Fare clic su **Modifica**, per avviare la procedura guidata **Installazione di base**.
3) Fare clic su **Avanti**.

Nota: Per visualizzare una panoramica dei numeri di telefono attualmente configurati, selezionare **Mostra configurazione utenti** quindi fare clic su **Esegui funzione**.

---

4) Selezionare **Cancella tutti numeri di telefono**.
5) Nella domanda di sicurezza, selezionare la casella di controllo **Cancella tutti numeri di telefono**.
6) Fare clic su **Esegui funzione**.



7) Modificare come necessario i campi dei valori preassegnati ai numeri di telefono predefiniti speciali.
8) Fare clic su **OK**. I numeri di telefono vengono eliminati e vengono applicate le eventuali modifiche ai numeri di telefono predefiniti speciali.
9) Fare clic su **Annulla**, per chiudere la procedura guidata **Installazione di base**.

11.1.2.2 Come modificare i numeri di telefono predefiniti speciali

Per funzioni speciali, è possibile modificare numeri di telefono predefiniti.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

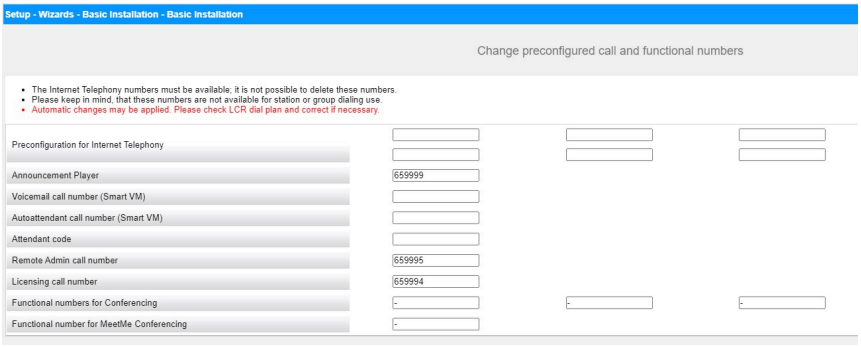
Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Fare clic su **Modifica**, per avviare la procedura guidata **Installazione di base**.
3) Fare clic su **Avanti**.

Nota: Per visualizzare una panoramica dei numeri di telefono attualmente configurati, selezionare **Mostra configurazione utenti** quindi fare clic su **Esegui funzione**.

---

4) Attivare **Modifica numeri di telefono e funzionali pre-configurati**.
5) Fare clic su **Esegui funzione**.



6) Immettere nei campi i numeri di telefono e i codici desiderati, quindi fare clic su **OK**. I nuovi numeri di telefono e codici vengono memorizzati.

Nota: I numeri di telefono configurati in questa sezione non possono essere utilizzati come numeri di telefono utente, di selezione passante o dei gruppi.

---

7) Fare clic su **Annulla**, per chiudere la procedura guidata **Installazione di base**.

11.1.2.3 Come importare numeri di telefono e dati utente

Tramite un file XML è possibile importare dati utente predefiniti.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Esiste un file XML in formato UTF-8 con i dati inseriti. Un modello XML è disponibile in **Centro assistenza** > **Documenti** > **Modelli CSV**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Fare clic su **Modifica**, per avviare la procedura guidata **Installazione di base**.

3) Fare clic su **Avanti**.

Nota: Per visualizzare una panoramica dei numeri di telefono attualmente configurati, selezionare **Mostra configurazione utenti** quindi fare clic su **Esegui funzione**.

4) Attivare il pulsante di opzione **Configurazione utente importando file XML**.

5) Fare clic su **Esegui funzione**.

6) Selezionare con **Sfoglia** il file XML creato e fare clic su **Apri**.

7) Fare quindi clic su **OK**. I dati utente vengono importati.

8) Fare clic su **Annulla**, per chiudere la procedura guidata **Installazione di base**.

11.2 Requisiti per la telefonia LAN

Per telefonia LAN si intendono le comunicazioni di utenti IP nell'ambito della rete interna (LAN). Per garantire la qualità della trasmissione voce nei sistemi di telefonia basati su LAN, le reti IP utilizzate e il sistema di comunicazione devono soddisfare specifici requisiti. La qualità voce e l'affidabilità della comunicazione dipendono dalla tecnologia di rete implementata.

Per garantire una trasmissione completa e una buona qualità voce, i segnali voce vengono compressi tramite codec audio digitalizzati e contrassegnati in base a specifiche procedure (Quality of Service), in modo che la trasmissione voce acquisisca priorità rispetto alla trasmissione dati.

Requisiti

- LAN con almeno 100 Mbit/sec. e full duplex
- Ciascun componente nella rete IP deve essere collegato a una propria porta e a uno switch o a un router; non si possono utilizzare HUB.
- Ritardo massimo per un fascio 50 (One Way Delay); ritardo massimo complessivo 150 ms
- Perdita massima pacchetti 3%; se si utilizzano Fax/Modem tramite G.711, la perdita pacchetti non deve superare lo 0,05%.
- Jitter massimo 20 ms
- Supporto per Quality of Service (QoS): IEEE 802.p, DiffServ (RFC 2474) o ToS (RFC 791)
- Utilizzo massimo rete 40%

11.2.1 Codec audio

Codec audio identifica un programma che codifica la voce in pacchetti dati digitali (pacchetti IP) e viceversa. A seconda del codec audio utilizzato, i dati possono essere compressi in diversa misura. La compressione consente di trasmettere i pacchetti IP con una larghezza di banda inferiore rispetto ai pacchetti non compressi. La decodifica dei pacchetti dati può portare a una perdita della qualità voce e della continuità della riproduzione.

Per una conversione appropriata dati-voce dopo il trasporto, il destinatario deve utilizzare lo stesso Codec del mittente.

Codec audio supportati

Vengono supportati i seguenti Codec audio:

- G.729A, G.729AB: codifica voce 8 Kbit/s - buona qualità voce.
- G.711 (A-law e µ-law): codifica voce a 56 o 64 Kbit/sec. - qualità voce molto buona. G.711 viene impostato anche nelle reti fisse (ISDN).

Ai Codec audio è possibile assegnare priorità da 1 (alta) a 4 (bassa). Il sistema di comunicazione tenta automaticamente di utilizzare un codec audio a priorità elevata per ogni connessione. Se si utilizza un Codec audio a bassa compressione (buona qualità voce), il carico della rete risulta elevato. In caso di utilizzo intenso della telefonia IP, il trasferimento dati su una rete già sovraccarica può comportare un peggioramento della qualità voce.

Con alcuni codec, il sistema di comunicazione può attivare il riconoscimento delle pause vocali (VAD, Voice Activity Detection). In caso di pause prolungate il carico di rete può diminuire.

Per ciascun Codec è possibile definire la dimensione del frame (dimensioni dei pacchetti IP) con un valore da 10 a 90 millisecondi. In questo modo si definisce la frequenza di campionamento per il segnale voce nei pacchetti IP. I valori più alti (ad es. 90 ms) indicano da un lato un comportamento migliore dei dati nell'overhead dei pacchetti IP, dall'altro un maggiore ritardo nella trasmissione.

Esiste la possibilità di disattivare i codec G.729, che consumano molte risorse, e di utilizzare i codec G.711. In questo modo si ottimizza il numero di chiamate parallele eseguibili. Se viene attivata questa funzione, è necessario eseguire un riavvio.

Nei sistemi OSBiz X il payload termina nel sistema, quindi gli utenti parlano con un codec, che è supportato dal sistema. Ad esempio, il telefono HFA ha prima impostato il codec G.722. Il sistema non supporta il codec G.722 e il codec G.711 è stato impostato come prima opzione. In questo caso, i due utenti parleranno con il codec G.711. Per quanto riguarda i sistemi OSBiz S, gli utenti parlano con il codec G.722, mentre c'è un payload end-to-end.

11.2.1.1 Come configurare i parametri Codec audio

Prerequisiti

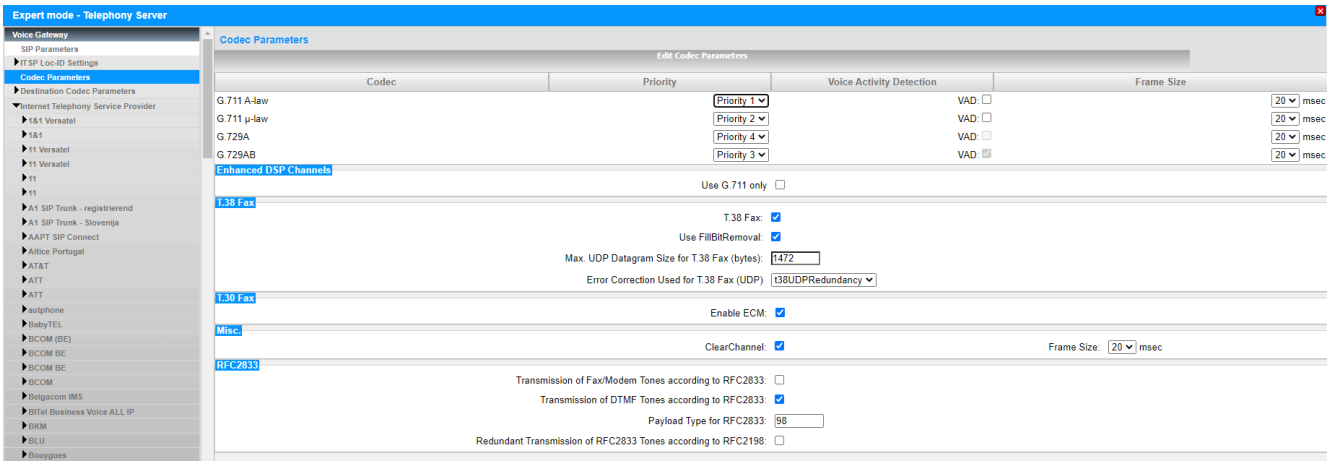
Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Server telefonia** > **Gateway voce**.

3) Nella struttura dei menu fare clic su **Parametri Codec**.



4) Assegnare al codec audio desiderato una priorità da 1 (alta) a 4 (bassa) tramite l'elenco a discesa **Priorità**.
5) Attivare/disattivare l'opzione **Riconoscimento delle pause vocali (VAD)** per il codec audio desiderato.
6) Definire in **Dimensione del frame** le dimensioni del pacchetto voce IP per il codec audio.

Nota: Occorre inserire lo stesso valore per tutti i codec, ad esempio 20 msec. Non è supportato configurare valori diversi per ciascun codec.

---

7) Se si desidera utilizzare solo i due codec audio G.711, nell'area **Canali DSP avanzati**, selezionare la casella di controllo **Usa solo G.711**.
8) Fare clic su **Applica**, quindi su **OK**.

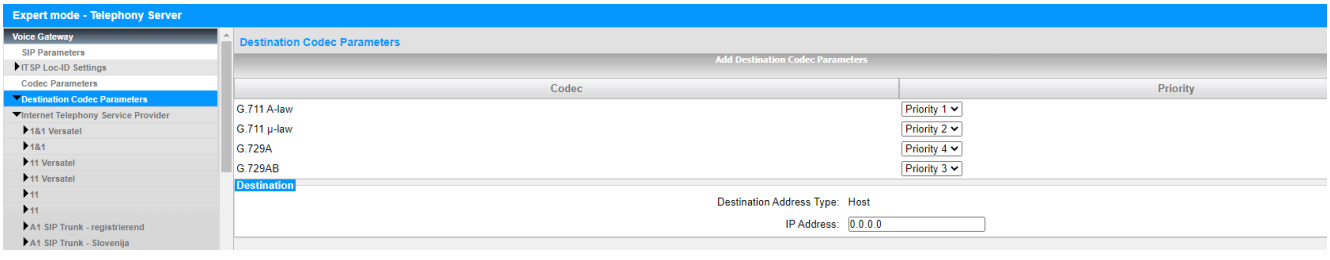
11.2.1.2 Come assegnare i parametri codec audio a una destinazione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Server telefonia** > **Gateway voce**.
3) Nella struttura dei menu fare clic su **Parametri Codec di destinazione**.



4) Assegnare al codec audio desiderato una priorità da 1 (alta) a 4 (bassa) tramite l'elenco a discesa **Priorità**.

5) Nel campo **Indirizzo IP**, inserire l'indirizzo IP della destinazione a cui deve essere assegnata la priorità precedentemente impostata del codec audio (ad esempio, `192.168.1.10`).
6) Fare clic su **Applica**, quindi su **OK**.

11.2.2 Trasmissione di toni secondo RFC2833

La trasmissione dei toni DTMF e dei toni fax/modem secondo RFC2833 può essere abilitata o disabilitata.

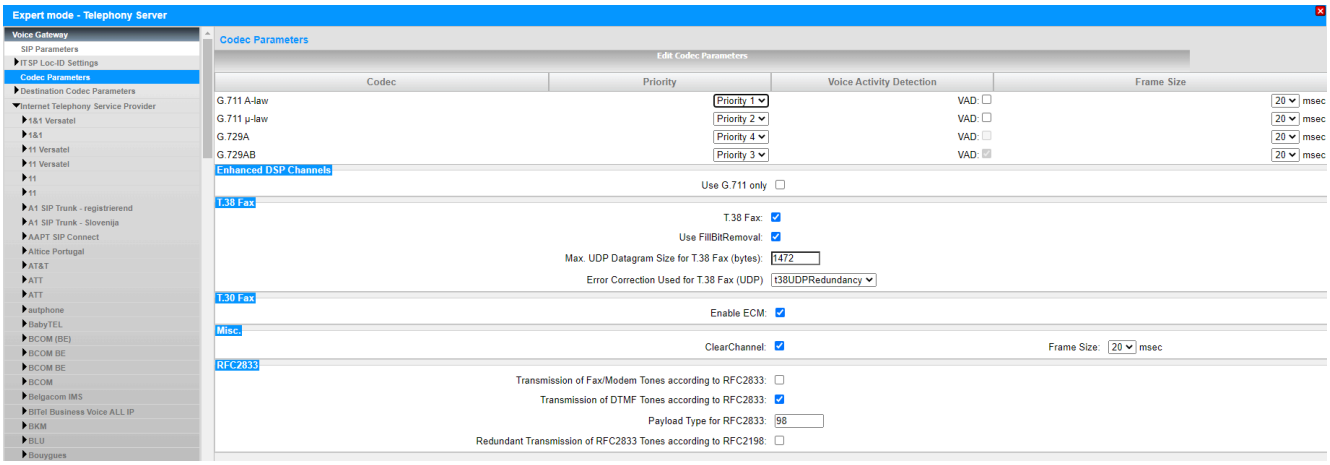
11.2.2.1 Come attivare o disattivare la trasmissione di toni fax/modem secondo RFC2833

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **Gateway voce**.
3) Nella struttura dei menu fare clic su **Parametri Codec**.



4) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Trasmissione di toni fax/modem secondo RFC2833**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Trasmissione di toni fax/modem secondo RFC2833**.
5) Fare clic su **Applica**, quindi su **OK**.

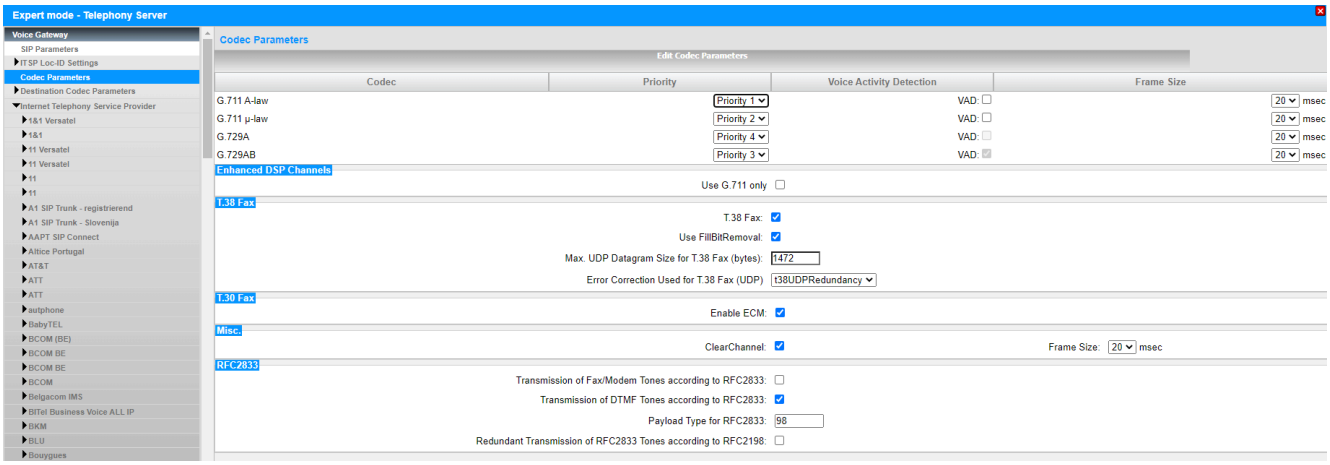
11.2.2.2 Come attivare o disattivare la trasmissione DTMF secondo RFC2833

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **Gateway voce**.
3) Nella struttura dei menu fare clic su **Parametri Codec**.



4) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Trasmissione di toni DTMF secondo RFC2833**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Trasmissione di toni DTMF secondo RFC2833**.
5) Fare clic su **Applica**, quindi su **OK**.

11.2.3 Quality of Service

Quality of Service (QoS) riunisce diverse procedure per garantire la massima qualità possibile e l'assenza di perdite nella trasmissione di pacchetti dati (pacchetti IP). Per ottenere una buona qualità voce nelle trasmissioni voce, grazie a QoS i pacchetti IP voce nelle reti IP vengono gestiti con priorità rispetto alle altre applicazioni.

Per l'attribuzione della priorità i pacchetti IP vengono dotati di uno speciale contrassegno (Punto codice). Le informazioni di priorità determinano una suddivisione in diverse classi. Se i componenti presenti nella rete IP (ad es. sistema di comunicazione, utenti SIP e router Internet) supportano QoS, è possibile assegnare a tali classi larghezze di banda differenziate per il trasporto dei pacchetti IP voce.

Classi di priorità secondo DiffServ

Per la priorizzazione secondo il processo DiffServ, vengono definiti diversi punti di codice per il campo Type of Service (ToS) per la suddivisione della trasmissione dei pacchetti IP in diverse classi.

- Punto codice Expedited Forwarding (EF): garantisce una larghezza di banda costante. Per i pacchetti IP contrassegnati con questo punto codice è sempre disponibile la stessa larghezza di banda. Un volta raggiunto il valore di larghezza di banda impostato, tutti i pacchetti che superano tale valore vengono scartati.

- Punto codice Assured Forwarding (AF): garantisce una larghezza di banda minima. I pacchetti IP contrassegnati con questo punto codice presentano una priorità inferiore rispetto agli EF e devono dividersi la larghezza di banda non utilizzata da EF. Un volta raggiunto il valore impostato di larghezza di banda, tutti i pacchetti IP che superano tale valore vengono scartati.

  Per AF sono riservate quattro classi: AF1x (priorità più bassa), AF2x, AF3x e AF4x (priorità alta), dove x sta per uno dei tre livelli di dropping: basso (1), medio (2) e alto (3). I pacchetti a bassa priorità vengono memorizzati in un buffer per un periodo più lungo, i pacchetti ad alta priorità vengono espulsi dopo un breve tempo se non possono essere inoltrati.
- Best Effort (BE; massimo sforzo): i pacchetti IP senza etichetta (campo ToS = 00) sono trattati con la priorità più bassa.

Classi di priorità secondo la Precedenza IP

Oltre al processo DiffServ, sono disponibili diverse definizioni precedenti che assegnano una priorità in base al campo ToS. Per adeguare il sistema di comunicazione alle impostazioni eventualmente richieste dalla rete del cliente, è possibile selezionare ad esempio le classi da 3 a 7 (CS3-CS7) per la precedenza IP.

Singole classi di priorità

Se nella rete del cliente non viene utilizzata alcuna delle possibilità previste, è anche possibile impostare direttamente il valore ToS in modo manuale. Il valore impostato può assumere i valori 0-63 nel sistema decimale e copiato nei 6 superiori del byte ToS (ad esempio 41 = 101-001-00 = 0xA4).

Tabella delle classi di priorità possibili

Classe di priorità	Valore ToS binario	Valore ToS esadecimale
AF (Assured Forwarding)		
AF11	001-010-00	28
AF12	001-100-00	30
AF13	001-110-00	38
AF21	010-010-00	48
AF22	010-100-00	50
AF23	010-110-00	58
AF31	011-010-00	68
AF32	011-100-00	70
AF33	011-110-00	78
AF41	100-010-00	88
AF42	100-100-00	90
AF43	100-110-00	98
EF (Expedited Forwarding)		
EF	101-110-00	B8
Best Effort (BE; massimo sforzo)		

Classe di priorità	Valore ToS binario	Valore ToS esadecimale
BE	000-000-00	00
CS (Class Selector)		
CS3	011-000-00	60
CS4	100-000-00	80
CS5	101-000-00	A0
CS6	110-000-00	C0
CS7	111-000-00	E0
Inserimento manuale	xxx-xxx-00	0-63 (decimale)

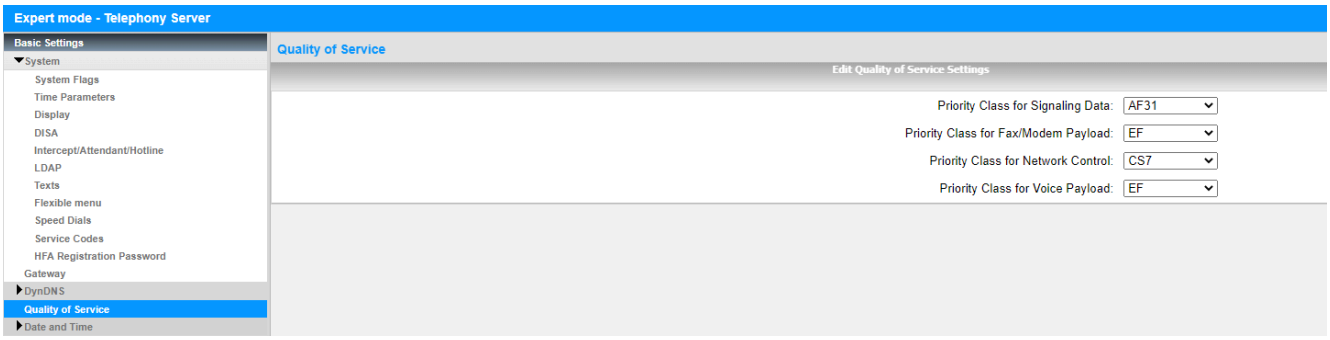
11.2.3.1 Come configurare la Quality of Service

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Quality of Service**.



4) Nell'elenco a discesa **Classe di priorità per dati di segnalazione** selezionare la classe desiderata.
5) Nell'elenco a discesa **Classe di priorità per payload fax/modem** selezionare la classe desiderata.
6) Nell'elenco a discesa **Classe di priorità per controllo di rete** selezionare la classe desiderata.
7) Nell'elenco a discesa **Classe di priorità per payload voce** selezionare la classe desiderata.
8) Fare clic su **Applica**, quindi su **OK**.

11.3 Utente IP

Gli utenti IP sono collegati al sistema di comunicazione tramite la LAN. Di norma un utente IP corrisponde a un telefono LAN o WAN.

Sono supportati i seguenti protocolli IP:

- Protocollo che dipende dal produttore del sistema di comunicazione

  Il sistema di comunicazione utilizza il protocollo CorNet-IP (CorNet-Internet-Protocol), sviluppato sulla base di H.323, per telefonia LAN sulle reti interne. Con CorNet-IP è possibile utilizzare tutti i servizi di telefonia del sistema di comunicazione.
- SIP (Session Initiation Protocol)

  SIP viene normalmente integrato per la telefonia Internet, ma non solo. È infatti possibile utilizzarlo anche nella telefonia su reti interne. SIP non consente però di utilizzare tutti i servizi del sistema di comunicazione.

Esistono i seguenti tipi di utenti IP:

- **Client di sistema**: un client di sistema è un utente IP che può utilizzare tutti i servizi del sistema di comunicazione tramite il protocollo CorNet-IP. Ad esempio si può trattare di un telefono di sistema IP, quale OpenStage 60 HFA o di un PC con software CTI come OpenScape Personal Edition.
- **Client SIP**: un client SIP è un utente IP che utilizza il protocollo SIP. Tramite il protocollo SIP, può utilizzare solo un numero limitato di funzioni del sistema di comunicazione. Un client SIP può essere ad esempio un telefono SIP come OpenStage 15 S.
- **DeskShare User**: Un DeskShare User è un utente IP che può accedere a un altro telefono di sistema IP (Mobile Login) e può utilizzarlo come se fosse il suo (compreso il numero di telefono).
- **Utente RAS**: un utente RAS (Remote Access Service User) può accedere alla rete IP tramite linea ISDN. Mediante tale utente è possibile eseguire la manutenzione remota del sistema di comunicazione.

Per ogni utente IP collegato è necessaria una licenza apparecchio "IP User".

Due utenti IP sono riservati per utenti in linea e per l'accesso remoto tramite ISDN. Questi utenti IP non necessitano di licenza apparecchio. Se uno o più di questi tre utenti riservati non è più necessario, tali utenti possono essere deconfigurati in utenti IP normali utilizzando la Modalità esperti. Tuttavia per questi utenti IP sono necessarie licenze apparecchio.

Configurazione utenti IP

Le seguenti configurazioni possono essere eseguite per un utente IP:

- Configurazione dei parametri predefiniti con la procedura guidata **Terminali IP** (vedere Come configurare gli utenti IP).
- Configurazione di tutti i parametri (predefiniti e avanzati) tramite la Modalità esperti (vedere >Utente>Utente>Client IP).

I telefoni di sistema IP OpenScape Desk Phone vengono normalmente forniti con il software SIP. Non appena si configura un telefono di sistema OpenScape Desk Phone nel WBM come **client di sistema**, il software HFA memorizzato nel sistema di comunicazione viene automaticamente caricato nel telefono di sistema IP.

11.4 Stazioni SIP

Le stazioni SIP sono stazioni IP che utilizzano il Session Initiation Protocol (SIP) per comunicare. Le stazioni SIP possono utilizzare questo protocollo per accedere a un numero limitato di funzioni del sistema di comunicazione. Le stazioni SIP, come le stazioni IP, sono connesse al sistema di comunicazione attraverso la LAN.

Una stazione SIP è un telefono WLAN o un telefono LAN come l'OpenStage 15 S, ad esempio.

Per ogni stazione SIP collegata, è necessaria una licenza di stazione "Utente IP".

Autenticazione SIP

Al fine di garantire la sicurezza della rete interna, è importante che gli abbonati SIP siano autenticati sul sistema di comunicazione con i valori descritti di seguito. Questi valori devono essere configurati nel WBM del sistema di comunicazione per ogni utente SIP e anche per ogni telefono SIP. Per proteggersi dagli attacchi SIP, si raccomanda vivamente l'autenticazione!

- Password

  Password per l'autenticazione: assegnata liberamente; almeno 8 caratteri fino a un massimo di 20 caratteri. La password deve contenere almeno una lettera maiuscola, una lettera minuscola, una cifra e un carattere speciale. È necessario assegnare una password separata per ogni utente SIP.
- SIP ID d'utente / Nome d'utente

  Nome utente per l'autenticazione: preassegnato; può essere modificato se necessario, massimo 20 caratteri. Ad ogni utente SIP viene preassegnato un diverso ID utente SIP.
- Realm

  Zona o dominio per l'autenticazione: assegnato liberamente; può essere modificato se necessario, massimo 20 caratteri. Il realm per tutti gli abbonati SIP è preassegnato con lo stesso valore. Può essere modificato a seconda delle esigenze, ad esempio nel nome host o nel nome di dominio del sistema di comunicazione.

Configurazione delle stazioni SIP nel sistema di comunicazione

Per una stazione IP, è possibile eseguire le seguenti configurazioni nel WBM del sistema di comunicazione:

- Configurazione dei parametri standard con la procedura guidata **Telefoni IP** (vedere Come configurare le stazioni SIP).
- Configurazione di tutti i parametri (standard e avanzati in modalità Esperto (vedere Stazione>Stazione>Clienti IP).

Configurazione del telefono SIP

I dati utilizzati per l'autenticazione di un utente SIP sul sistema di comunicazione devono essere inseriti anche direttamente sul telefono SIP.

Configurazione dei dati di autenticazione sul telefono SIP (vedere Configurazione dei dati di autenticazione sul telefono SIP).

Funzionalità che si possono usare con i telefoni SIP

Le seguenti funzioni possono essere utilizzate con i telefoni SIP:

- Chiamate in entrata e in uscita con visualizzazione di numero e nome del chiamante
- Blocco, alternanza/collegamento, consultazione
- Trasferimento di chiamata (schermato/non schermato)
- Esecuzione di chiamate
- Deviazione immediata delle chiamate, su occupato e dopo il timeout
- Conferenza a tre
- Elenchi di chiamate, indicatore di messaggi in attesa
- Disattivazione della suoneria del telefono, rifiuto di chiamata, inoltro di chiamata
- Chiamata in attesa
- Appartenenza a gruppi (senza visualizzazione del numero del gruppo)
- Diverse chiamate interne, esterne e di richiamo
- LED della casella vocale - Indicazione di messaggio in attesa
- Composizione DTMF, ad esempio per il funzionamento delle caselle vocali
- Utilizzo dei client UC
- Aggiornamenti software automatici (quando si utilizza il DLI)

Nota: L'implementazione con un contact center multicanale non è stata rilasciata (ad esempio, il trasferimento a gruppi UCD).

A seconda del telefono, potrebbero esserci delle limitazioni alle funzioni disponibili; vedere il wiki all'indirizzo:

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

Le seguenti funzioni, che si attivano utilizzando i codici di servizio con * o #, possono essere utilizzate con i telefoni SIP:

- Ripristino di tutti i servizi: #0
- Deviazione di chiamata: *1xf (x = 1 - tutti, 2 - interni, 3 - esterni) (f = numero di inoltro)
- Deviazione di chiamata disattivata: #1
- Abbandono/partecipazione a un gruppo di ricerca: #85g/*85g (g = numero del gruppo, facoltativo - necessario in caso di gruppi multipli)
- Soppressione/abilitazione dell'ID di chiamata (CLIR): *86/#86
- Selezione diretta: * 7nnnn (nnnn = numero di chiamata rapida)
- Apertura porta: *61

Suggerimento: Si consiglia di utilizzare i codici di sostituzione * o # per una migliore compatibilità con i dispositivi SIP di terze parti. L'utente SIP deve inviare l'intera sequenza di codici di servizio come composizione in blocco.

Suggerimento: A differenza dei dispositivi HFA, sui dispositivi SIP non c'è interazione con l'utente o guida per le sequenze di codici di servizio. È necessario comporre subito l'intera sequenza di codici di servizio.

Funzionalità che si possono usare con i telefoni SIP e myPortal/ myAttendant

I telefoni SIP da utilizzare con myPortal e myAttendant devono soddisfare i seguenti requisiti:

- È supportato il 3PCC come da RFC 3725.
- È supportata la funzione di "avviso di chiamata".
- La funzione Non disturbare locale è disattivata.

La piena funzionalità delle funzioni dipende dal telefono SIP utilizzato e non può essere garantita. Con i telefoni SIP OpenStage è stato eseguito con successo un test delle funzioni elencate di seguito.

Funzionalità orientate alla connessione/alla chiamata:

- Esegui chiamata
- Reindirizzamento delle chiamate
- Esecuzione di chiamate
- Ripresa delle chiamate
- Conferenza controllata dall'applicazione
- Messa in attesa una chiamata
- Alternanza (commutazione/collegamento)
- Consultazione
- Disconnetti
- Trasferisci

Funzionalità orientate al telefono:

- Non disturbare
- Inoltro di chiamata

11.5 Utenti UP0

Un utente UP0 utilizza per la trasmissione del segnale digitale una linea $U_{P0/E}$. Gli utenti UP0 sono collegati tramite interfacce UP0 al sistema di comunicazione e sono telefoni di sistema quali ad esempio OpenStage 60T. Gli utenti UP0 possono utilizzare tutte le funzioni del sistema di comunicazione.

Per un utente UP0, sono disponibili le seguenti opzioni di connessione:

- OpenScape Business X1

  alle interfacce $U_{P0/E}$della scheda madre.
- OpenScape Business X3/X5

  Alle interfacce $U_{P0/E}$ della scheda madre o se vi sono diversi terminali UP0, al modulo $U_{P0/E}$ aggiuntivo.
- OpenScape Business X8

  A moduli $U_{P0/E}$ aggiuntivi.
- OpenScape Business S

  Nessun collegamento possibile.

Per ogni utente UP0 collegato è necessaria una licenza apparecchio "TDM User". Anche i telefoni di sistema collegati in modalità slave hanno necessità di una licenza.

Configurazione dell'utente UP0

Le seguenti configurazioni possono essere eseguite per un utente UP0:

- Configurazione dei parametri predefiniti con la procedura guidata **Terminali UP0** (vedere Come configurare gli utenti UP0).
- Configurazione di tutti i parametri (predefiniti e avanzati) tramite la Modalità esperti (vedere Utenti>Utenti>Utente UP0).

11.6 Utenti DECT

Un utente DECT utilizza per la trasmissione i segnali digitali di una stazione base cordless. Un utente DECT è un telefono DECT.

Per un utente DECT, sono disponibili le seguenti opzioni di connessione:

- OpenScape Business X1W/X1R/X3W/X3R/X5R

  Utente base cordless su un'interfaccia $U_{P0/E}$ della scheda madre.
- OpenScape Business X8

  Utente base cordless su uno o più moduli SLMUC.
- OpenScape Business S

  Stazione base DECT IP nella LAN

Il collegamento di una stazione base cordless viene definito soluzione cordless integrata. Sono quindi disponibili quasi tutte le funzioni del sistema di comunicazione.

L'integrazione della stazione base DECT IP nella rete interna viene denominata Cordless IP. Poiché in questo caso, può essere utilizzato solo il protocollo SIP, non tutte le funzioni del sistema di comunicazione sono disponibili.

Per ogni utente DECT collegato è necessaria una licenza apparecchio "TDM User".

Per la descrizione e configurazione della soluzione cordless integrata, vedere Soluzione cordless integrata.

Configurazione utenti DECT

Le seguenti configurazioni possono essere eseguite per un utente DECT:

- Configurazione dei parametri standard con la procedura guidata **Terminali DECT** (vedere Come configurare gli utenti DECT).
- Configurazione di tutti i parametri (predefiniti e avanzati) tramite la Modalità esperti (vedere Utente>Utente>Utenti DECT>Utenti DECT).

Gli utenti DECT IP vengono configurati come normali utenti SIP.

11.7 Stazioni Mitel SIP DECT

Per le stazioni Mitel SIP DECT, sono disponibili le seguenti opzioni di connessione:

- Sistemi OpenScape Business S
- Hardware OpenScape Business V3 (OCCe)

Provisioning delle stazioni Mitel SIP DECT RFP

Il processo comprende i seguenti passaggi generali:

1) Configurare il DHCP con un indirizzo IP statico per la stazione base OMM.
2) La stazione base ottiene un indirizzo IP e avvia l'applicazione OMM.
3) Configurare la stazione base attraverso la sua interfaccia web.
4) La stazione base recupera automaticamente i file di configurazione da OpenScape Business.
5) Quando un portatile si collega, la stazione base recupera anche il file di configurazione dell'utente e configura il portatile.

Configurazione delle stazioni Mitel SIP DECT tramite WBM

È necessario eseguire le seguenti operazioni di configurazione:

1) Abilitare il server DHCP e fornire un indirizzo IP statico per la stazione base OMM (vedere Interfacce di rete > Scheda madre > Modalità DHCP > Server DHCP > Indirizzi IP statici).
2) Configurazione dei parametri standard con la procedura guidata Dispositivi Mitel SIP DECT (vedere Come configurare le stazioni Mitel SIP DECT).
3) Configurazione delle stazioni SIP e dei relativi parametri tramite la modalità Esperto (vedere Come configurare le stazioni SIP tramite la Modalità Esperto).

11.8 Utenti ISDN

Un utente ISDN serve per la trasmissione dei segnali digitali del bus S_0. Pertanto viene denominato anche apparecchio S_0. L'utente ISDN viene collegato al sistema di comunicazione tramite le interfacce S_0

Per un utente S_0, sono disponibili le seguenti opzioni di connessione:

- OpenScape Business X1

  in un'interfaccia S_0 della scheda madre.
- OpenScape Business X3/X5

  a un'interfaccia S_0 della scheda madre o a un modulo S_0.
- OpenScape Business X8

  a uno o più moduli S_0.
- OpenScape Business S

  A gateway o adattatori aggiuntivi richiesti

È possibile collegare i seguenti apparecchi ISDN:

- Telefono ISDN
- Fax di gruppo 4
- Modem ISDN
- PC con scheda ISDN

Si possono definire i seguenti tipi di utenti ISDN:

- Standard: per telefono ISDN, fax gruppo 4, modem ISDN o PC con scheda ISDN

- Fax: necessario per la configurazione del tasto "Info da fax/segreteria telefonica". Ad esempio, se viene collegato un PC con scheda ISDN e software fax al bus S_0 e si assegna a tale dispositivo il tipo "Fax" è possibile configurare su ciascun terminale un tasto "Info da fax/segreteria telefonica". Quando il tasto si illumina segnala la ricezione di un fax.
- Segreteria telefonica: necessario per la risposta a una chiamata quando la segreteria ha già accettato la conversazione. Ad esempio se viene collegato un Gigaset ISDN con segreteria telefonica e viene assegnato al dispositivo il tipo "Segreteria telefonica" su ogni terminale è possibile rispondere a una chiamata già accettata dalla segreteria telefonica. A tale scopo sul terminale deve essere programmato un tasto con il numero di telefono interno del Gigaset.

Per ogni utente ISDN collegato è necessaria una licenza apparecchio "TDM User".

Collegamento degli utenti ISDN all'interfaccia S_0

Per poter collegare un utente ISDN al sistema di comunicazione, deve essere presente almeno un'interfaccia S_0 destinabile al collegamento utente ISDN o alla connessione ISDN punto - punto, e configurata come bus S_0 interno (bus S_0 Euro).

Nota: In caso di connessione ISDN punto - multipunto, dove più utenti ISDN vengono collegati a un'interfaccia S_0 (fino a 8 utenti ISDN), ciascun utente ISDN deve essere associato a un numero MSN univoco. Questa assegnazione deve avvenire nel menu di configurazione del terminale ISDN.

Configurazione utenti ISDN

Le seguenti configurazioni possono essere eseguite per un utente ISDN:

- Configurazione dei parametri predefiniti con la procedura guidata **Terminali ISDN** (vedere Come configurare gli utenti ISDN).
- Configurazione di tutti i parametri (predefiniti e avanzati) tramite la Modalità esperti (vedere Utenti>Utenti>Utenti ISDN).

Consentire per i numeri MSN solo i numeri configurati

L'amministratore può definire che ulteriori numeri MSN su un bus S0 possano essere configurati solo per i numeri interni esistenti. In questo caso è possibile impedire a utenti non autorizzati di aggiungere un numero MSN, in quanto con un altro numero MSN, il bus S0 si bloccherebbe; senza questa misura cautelativa, il sistema di comunicazione assegnerebbe per tale numero MSN un numero interno libero al bus S0.

Cambiamento del bus

Il sistema di comunicazione consente di parcheggiare una chiamata in corso sul bus S_0, di staccare successivamente il terminale, ricollegarlo su un’altra posizione del bus e continuare la conversazione – cambiamento del bus (Terminal Portability TP). Sull’apparecchio parcheggiato appare un'informazione sul display. Per l'intera procedura sono disponibili tre minuti.

Questa funzione non è disponibile per i servizi come telefax, telex o trasmissione dei dati.

11.8.1 Come configurare l'interfaccia S_0 per utenti ISDN

Con la procedura guidata **Linea ISDN / analogica / ITSP** è possibile configurare più interfacce S_0 in modo da poter collegare a esse i telefoni ISDN.

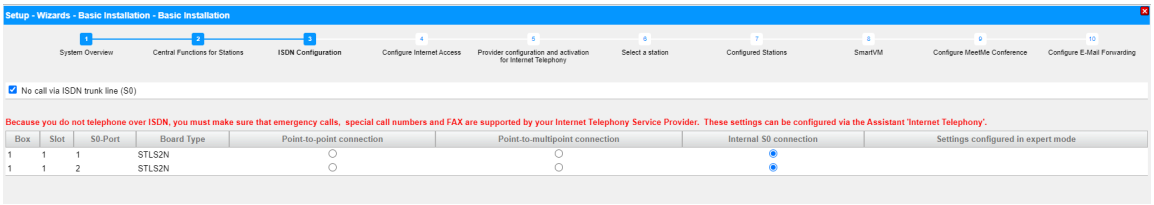
Prerequisiti

Sono disponibili una o più interfacce S_0 libere.

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Nella procedura guidata **Linea ISDN / analogica / ITSP** fare clic su **Modifica**.
4) Fare clic su **OK & Avanti**. Vengono visualizzate le interfacce S_0 (porte S_0) disponibili.



5) Lasciare la casella di controllo **No telefonia tramite linea esterna ISDN (S0)** come impostata.
6) Nelle interfacce S_0 desiderate selezionare il pulsante di opzione interfaccia **S0 interna**.

Nota: Queste interfacce S_0 non sono più utilizzabili per l'accesso alla linea esterna ISDN.

---

7) Fare clic su **OK & Avanti** finché non viene visualizzato il messaggio di conferma che la modifica del servizio è completata.
8) Fare clic su **Fine**.

11.8.2 Come consentire solo numeri configurati per MSN

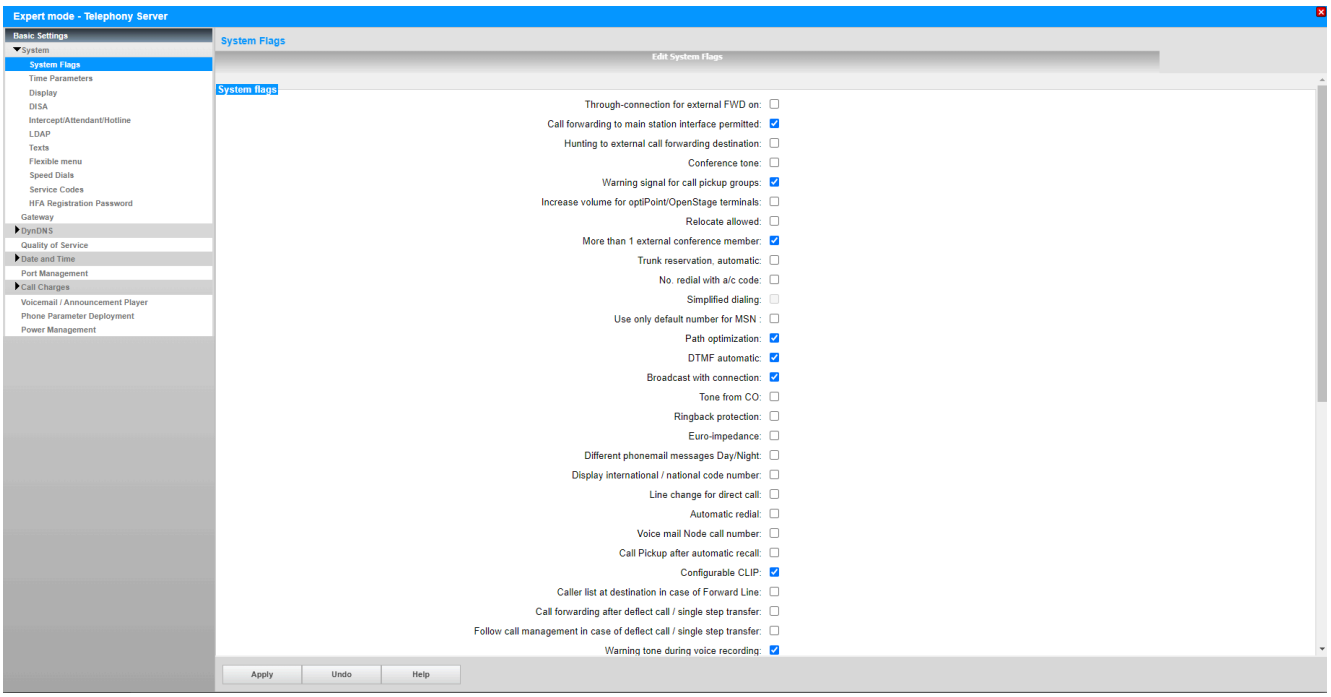
Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Impostazioni di base**.

3) Nella struttura dei menu fare clic su **Impostazione di base** > **Flag di** > **sistema**.



4) Se si desidera consentire solo i numeri configurati per MSN, selezionare la casella di controllo **Usare per MSN solo numeri installati**.
5) Se si desidera consentire per i numeri MSN non solo i numeri configurati, deselezionare la casella di controllo **Usare per MSN solo numeri installati**.
6) Fare clic su **Applica**, quindi su **OK**.

11.9 Utenti analogici

Un utente analogico (utente a/b) utilizza una linea a due conduttori per la trasmissione del segnale analogico. Nel sistema di comunicazione gli utenti analogici vengono collegati tramite l'interfaccia a/b.

Per un utente analogico, sono disponibili le seguenti opzioni di connessione:

- OpenScape Business X1

  a un'interfaccia analogica sulla scheda madre.
- OpenScape Business X3/X5

  a un'interfaccia analogica sulla scheda madre o a un modulo analogico.
- OpenScape Business X8

  a uno o più moduli analogici.
- OpenScape Business S

  A gateway o adattatori aggiuntivi richiesti

È possibile collegare i seguenti utenti analogici:

- Telefono analogico
- Fax analogico (gruppo 3)
- Segreteria telefonica

- Modem da 9600 bit/s
- Apparecchio porta
- Altoparlante

Si possono definire i seguenti tipi di utenti analogici:

- Standard: per telefono analogico, gruppo fax 3, segreteria telefonica o altoparlante
- Fax: necessario per la configurazione del tasto "Info da fax/segreteria telefonica". Ad esempio, se viene collegato un gruppo fax 3 e si assegna a tale dispositivo il tipo "Fax" è possibile configurare su ciascun terminale un tasto "Info da fax/segreteria telefonica". Quando il tasto si illumina segnala la ricezione di un fax.
- Segreteria telefonica: necessario per la risposta a una chiamata quando la segreteria ha già accettato la conversazione. Ad esempio se viene collegato un Gigaset con segreteria telefonica e viene assegnato al dispositivo il tipo "Segreteria telefonica" su ogni terminale è possibile rispondere a una chiamata già accettata dalla segreteria telefonica. A tale scopo sul terminale deve essere programmato un tasto con il numero di telefono interno del Gigaset.
- Modem: i modem analogici con velocità fissa di 56 kbit/s o superiore non sono supportati, in quanto tale velocità o un velocità superiore non può essere elaborata.

Per ogni utente analogico collegato è necessaria una licenza apparecchio "TDM User".

Reperibilità di un fax analogico nel sistema con il numero di fax utilizzato finora

Siccome non è possibile deviare un dispositivo fax analogico su un numero fax del sistema, è possibile adottare la seguente soluzione: il numero fax finora usato viene configurato nel sistema e riceve i messaggi fax in arrivo. Per i dispositivi fax analogici viene configurata una porta con il numero utilizzato finora come CLIP. L'opzione CLIP impostabile deve essere selezionata. I fax per destinazioni esterne mostrano il numero precedente come mittente; i destinatari interni vedono il numero interno del dispositivo fax.

Configurazione dell'utente analogico

Le seguenti configurazioni possono essere eseguite per un utente analogico:

- Configurazione dei parametri predefiniti con la procedura guidata **Terminali analogici** (vedere Come configurare gli utenti analogici).
- Configurazione di tutti i parametri (predefiniti e avanzati) tramite la Modalità esperti (vedere Utenti>Utenti>Utenti analogici).

11.10 Utenti virtuali

Gli utenti virtuali si comportano come utente reali ma non sono associati ad alcun terminale fisico.

Gli utenti virtuali sono necessari ad esempio per l'integrazione di telefoni cellulari e per l'inoltro di chiamate. Gli utenti virtuali devono essere configurati come reali per essere utilizzati per la segnalazione delle chiamate.

Configurazione di utenti virtuali

La configurazione dei parametri degli utenti virtuali avviene tramite la Modalità esperti (vedere Utenti>Utenti>Utenti virtuali).

11.11 Programmazione dei tasti

Ciascun telefono di sistema è dotato di un numero preciso di tasti funzione. Alcuni tasti sono associati a una funzione. Queste associazioni si possono modificare e i tasti non associati ad alcuna funzione possono essere programmati con le funzioni desiderate.

Per la programmazione dei tasti sono disponibili le seguenti possibilità:

- Programmazione dei tasti tramite WBM

  Nel WBM, tramite la procedura guidata **Programmazione dei tasti**, è possibile programmare i tasti dei telefoni di sistema collegati.

  Con la procedura guidata è possibile configurare la mappatura tasti per un utente, anche se per tale utente non è stato ancora collegato alcun telefono di sistema.
- Programmazione dei tasti tramite client UC

  Gli utenti Client UC **myPortal for Desktop**, **myPortal for Outlook** e **myAttendant** possono programmare i tasti del telefono del sistema anche tramite i Client UC (consultare le istruzioni per l'uso dei Client UC).
- Programmazione dei tasti direttamente sul telefono

  Nei telefoni di sistema dotati di display alcuni tasti funzione si possono programmare direttamente sul telefono.

Programmazione dei tasti funzione su livelli differenti

I tasti funzione del telefono di sistema possono essere programmati due volte, sul primo e sul secondo livello. Il primo livello può essere programmato con tutte le funzioni offerte. Il secondo livello può essere programmato con numeri di telefono esterni. Per poter utilizzare il secondo livello, sul telefono di sistema deve essere configurato un tasto Shift. Il LED del tasto funzione corrisponde sempre al primo livello.

Nota: Nel caso di un **utente, non è possibile copiare la programmazione dei tasti poiché la funzionalità di assegnazione automatica dei tasti è specifica a MULAP e non può essere copiata su nessun altro utente. Per attivare la copia dei tasti, occorre rimuovere manualmente il prefisso ** da questi utenti.

11.11.1 Come programmare i tasti funzione nei telefoni del sistema

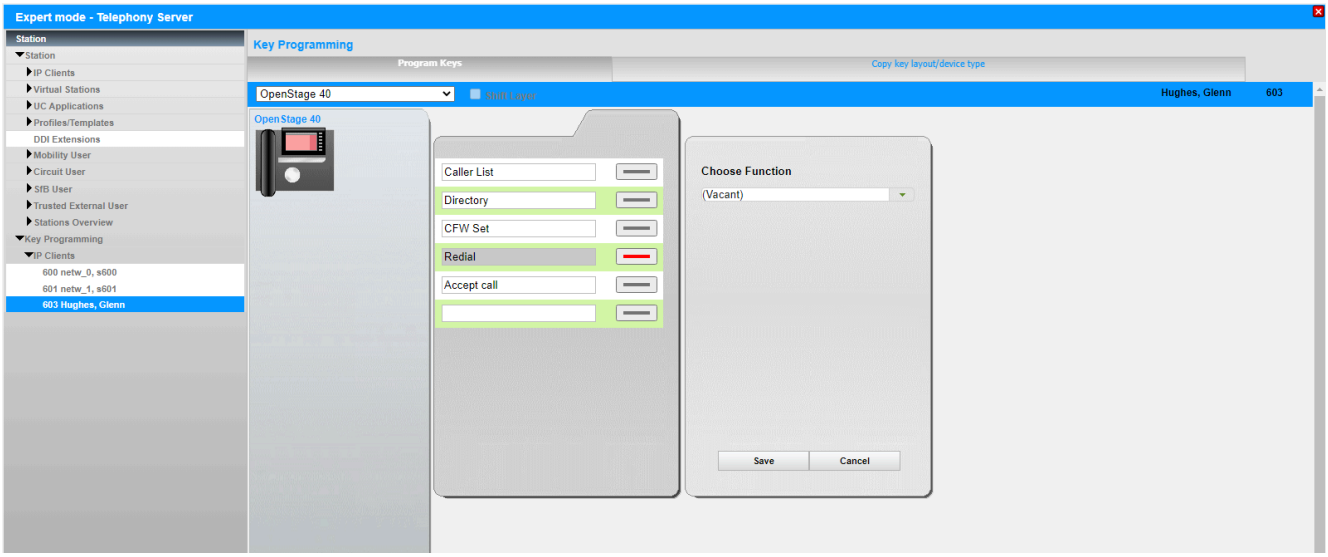
Con la procedura guidata **Programmazione tasti** è possibile configurare i tasti funzione dei telefoni del sistema.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Telefoni / utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Programmazione tasti**. Viene visualizzata la lista di tutti gli utenti.
4) Nella riga dell'utente desiderato fare clic su **Modifica**.
5) Assegnare all'utente il telefono di sistema:
   - Se a un utente è già collegato un telefono di sistema, viene visualizzata una rappresentazione semplificata del telefono di sistema.
   - Se a un utente non è ancora stato collegato alcun telefono di sistema, selezionare il telefono di sistema da collegare dall'elenco a discesa. Viene visualizzata una rappresentazione semplificata del telefono di sistema selezionato.
6) In tale rappresentazione del telefono di sistema, fare clic sul campo tasti desiderato. Vengono visualizzati i tasti funzione del campo tasti selezionato con le funzioni attualmente assegnate.



7) Assegnare le funzioni ai tasti funzione:
   a) Nel tasto funzione da assegnare, fare clic sull'icona del tasto. Viene visualizzato un elenco a discesa con le funzioni disponibili.
   b) Nell'elenco a discesa **Seleziona funzione** selezionare una delle opzioni presentate.
   c) Alcune funzioni richiedono informazioni aggiuntive. Se necessario, selezionare o inserire i dati necessari.
   d) Fare clic su **Salva**.
   e) Nel campo **Cambia etichette predefinite** modificare, se necessario, l'etichetta del tasto funzione.

Nota: Se è stata selezionato un telefono di sistema con assegnazione automatica delle etichette ai tasti (ad

esempio OpenStage 60 HFA), tale testo viene importato nel telefono di sistema.

f) Fare clic su **Salva**.

g) Se si desidera programmare altri tasti funzione, ripetere il passo 7.

8) Se un tasto funzione è stato configurato come tasto **Shift**, selezionare la casella di controllo **Shift**. Assegnare al secondo livello dei tasti funzione i numeri di telefono esterni, come descritto al passo 7.

9) Fare clic su **Applica configurazione dei tasti**.

10) Se si desidera utilizzare la programmazione tasti appena definita per altri o per tutti i telefoni del sistema, selezionare la casella di controllo relativa ai telefoni di sistema desiderati, fare clic su **Applica**, quindi su **OK** e **OK & Avanti**.

11) Se si desidera utilizzare la programmazione tasti appena definita solo per il telefono di sistema selezionato, per sicurezza fare clic prima su **Deseleziona tutti gli utenti**, quindi su **OK & Avanti**.

12) Fare clic su **Avanti**, quindi su **Fine**.

11.12 Profilo apparecchio

I profili contengono i valori e le proprietà degli utenti (apparecchi). Un profilo può essere assegnato a più membri. A tutti i membri di un profilo si applicano gli stessi valori e proprietà.

I profili utente possono essere assegnati a utenti con telefoni di sistema. È possibile creare fino a 20 profili apparecchio. I profili apparecchio possono essere esportati ed importati sia singolarmente che collettivamente. I file sono di tipo `xml`.

Ogni utente può essere membro di un solo profilo. Se vengono variati i valori e le proprietà di un utente e se questo è membro di un profilo, questo verrà eliminato dal profilo.

11.13 Configurazione degli utenti

Per gli utenti si possono definire valori specifici (ad es. Numero di telefono, Nome e Interno) e proprietà (ad es. tipo della segnalazione chiamata).

La configurazione di un utente si suddivide in configurazione standard e avanzata. Le impostazioni predefinite possono essere configurate tramite le procedure guidate da un utente con il profilo **Advanced**. Le impostazioni avanzate possono essere effettuate solo in Modalità esperti da un utente con il profilo **Expert**.

Le impostazioni standard si possono modificare comodamente in una lista per tutti gli utenti dello stesso tipo (ad es. utenti IP o utenti analogici). Le impostazioni aggiuntive (ad es. la segnalazione delle chiamate o il flag utente) possono essere modificate singolarmente per ciascun utente.

Gli utenti virtuali vengono configurati per interno in Modalità esperti (sia per le impostazioni standard che per quelle avanzate).

Sebbene il profilo **Basic** non possa essere utilizzato per configurare gli utenti, può essere usato per modificare i nomi degli utenti.

Per gli utenti collegati a un sistema di comunicazione deve essere disponibile un piano di composizione. I numeri di telefono, i nomi e i numeri di selezione passante di tutti gli utenti configurati possono essere visualizzati in Modalità esperti selezionando **Utenti** > **Estensioni selezione passante**.

Gli MSN non forniti dal provider di servizi né dal sistema devono essere eliminati, in caso contrario possono insorgere conflitti con MSN o numeri utente di telefonia Internet. Gli MSN messi a disposizione dal provider di telefonia Internet (ITSP) devono essere assegnati agli utenti in fase di configurazione dell'ITSP (vedere Configurazione di un ITSP).

Importante: La modifica di un numero di telefono utente reimposta la Smart VM (casella vocale) eventualmente configurata per tale utente. Tutti i messaggi vocali personali, i messaggi di benvenuto e gli annunci vanno persi e la password viene reimpostata.

Impostazioni predefinite

Le impostazioni predefinite devono essere controllate per ciascun utente e, se necessario, modificate.

- **Numero di telefono, Nome, Interno**

  Di norma ciascun utente viene assegnato a un numero di telefono (ad es. 101). A questo numero l'utente è raggiungibile internamente. Nei telefoni di sistema questo numero di telefono viene visualizzato sul proprio display e su quello del partner di comunicazione. Se si desidera che per le chiamate esterne venga visualizzato un numero diverso dal proprio, è possibile configurare un numero alternativo.

  Ad ogni utente può inoltre essere assegnato un numero di interno. Tramite questo numero l'utente è raggiungibile direttamente dall'esterno. L'utente ad esempio può essere raggiungibile internamente al numero 101 ed esternamente all'interno `3654321` (MSN nelle connessioni punto - multipunto) o `<numero sistema>-101` (connessione punto - punto). Alla prima installazione in una connessione punto - punto è possibile definire se il numero di telefono interno deve essere automaticamente utilizzato anche come selezione passante. Il numero di selezione passante può essere comunque diverso dal numero interno. Se si utilizza la telefonia Internet, è possibile definire un numero di selezione passante aggiuntivo tramite il quale l'utente è raggiungibile per la telefonia Internet. Questo numero di telefono viene messo a disposizione da un Internet Telephony Service Provider.

  Ad ogni utente può essere assegnato un nome Questo nome viene visualizzato sul display del partner di comunicazione (solo per i telefoni di sistema).

  Se esiste un piano di composizione, i numeri di telefono, i numeri interni e i nomi degli utenti devono essere adeguati al piano di composizione.

- **Tipo**

  Per ciascun utente è possibile selezionare un tipo. Un utente IP può, ad esempio, essere di tipo **client di sistema** o **client SIP**, un utente analogico può essere un telefono o un fax analogico e un utente ISDN può essere un telefono o un fax ISDN.

- **Numero fax, numero di connessione passante del fax.**

  Se si desidera configurare una casella fax per l'utente (utilizzabile ad es. con il client UC myPortal for Desktop o myPortal for Outlook) indicare un numero di fax (per la ricezione dei fax interni) e un numero di selezione passante fax (per la ricezione dei fax esterni).
- **Autorizzazioni**

  A un utente può essere assegnata una classe di abilitazione tra le 15 diverse classi disponibili. Ciò determina se l'utente può ricevere ed eseguire chiamate esterne o quali numeri di telefono può comporre e quali no (vedere Autorizzazioni (controllo della composizione)).
- **Gruppi di risposta per assente**

  Ciascun utente può essere assegnato a un gruppo di risposta per assente.
- **Lingua, segnalazione della chiamata**

  È possibile impostare la lingua per i comandi dei menu dei telefoni di sistema collegati.

  È possibile selezionare il suono del tono di chiamata per le chiamate esterne e interne.
- **Casella vocale (solo con UC Smart)**

  Con la soluzione di comunicazione unificata UC Smart, per ogni utente è possibile configurare una casella vocale e scegliere tra diversi annunci di benvenuto. Per ulteriori informazioni sulla casella vocale, vedere Casella vocale (SmartVM)

  Con la soluzione di comunicazione unificata UC Suite, a ogni utente viene automaticamente assegnata una casella vocale. In questo caso quindi non sono presenti impostazioni per la casella vocale.
- **Flag utente**

  I flag utente di ciascun utente possono essere modificati. Per una descrizione dei flag utente, vedere >Utenti>Utente>Parametri utente.

Impostazioni avanzate

La Modalità esperti consente di configurare qualsiasi impostazione per tutti i tipi di utente. Le impostazioni avanzate possono essere mantenute come tali per il funzionamento standard e modificate solo se necessario. Per informazioni su impostazioni avanzate, vedere Utenti.

Concetti correlati

Autorizzazioni (controllo della composizione) alla pagina 752
Testo in più lingue alla pagina 1230

11.13.1 Come configurare gli utenti IP

La procedura guidata **Terminali IP** consente di configurare utenti IP (telefoni LAN e WAN).

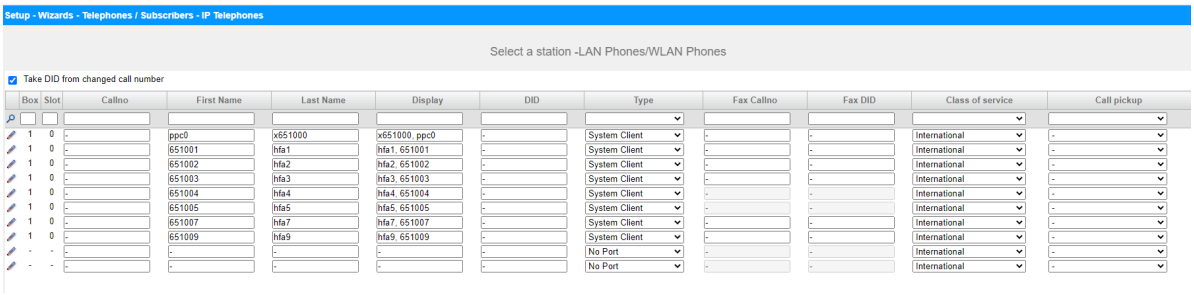
Prerequisiti

Per il funzionamento dei telefoni WLAN è necessaria una rete LAN wireless operativa.

Si è connessi a WBM con il profilo **Advanced**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Telefoni / utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Terminali IP**. Viene visualizzato un elenco di tutti gli utenti IP.



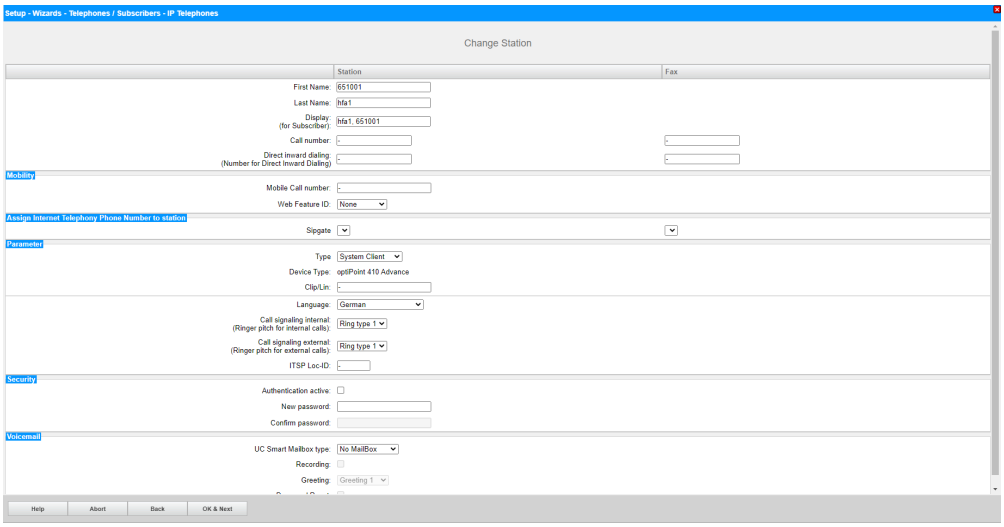
4) Se l'utente deve ricevere automaticamente il numero interno come selezione passante, selezionare il pulsante di opzione **Acquisisci DID dal numero di telefono modificato**.
5) Se si desidera che il numero di selezione passante dell'utente sia diverso dal numero di telefono, nella riga dell'utente desiderato, in corrispondenza di **DID**, immettere un numero di selezione passante per l'utente:
   - solo con connessioni punto - punto:

     Fare clic sul campo desiderato e immettere tramite tastiera il numero di selezione passante. Questo numero può coincidere con il numero interno.
   - solo con connessioni punto - multipunto:

     Nell'elenco a discesa selezionare un MSN. L'utente può ad es. essere raggiunto da chiamate interne sul numero interno 101 e dall'esterno tramite l'MSN 654321.
   - connessione punto - punto e connessione punto - multipunto:

     Nel campo desiderato selezionare una voce dall'elenco a discesa **xxx - modificabile** (xxx indica il numero interno) e immettere tramite tastiera il numero di selezione passante o selezionare un MSN dall'elenco a discesa.
6) Quando l'utente riceve come interno un numero utente di telefonia Internet, disattivare il pulsante di opzione **Acquisisci DID dal numero di telefono modificato**, dall'elenco accanto a questo pulsante di opzione selezionare il provider di servizi di telefonia Internet, quindi nella riga all'utente desiderato, dal menu a discesa **DID**, scegliere il numero di telefono dell'utente di telefonia Internet.
7) Nella riga appropriata dell'utente desiderato, immettere in **N° tel** un numero dell'utente interno. Si può utilizzare il numero di telefono pre-assegnato o immetterne uno diverso, ancora libero.
8) Nella riga dell'utente desiderato immettere in **Nome** un nome nel formato `Cognome, nome` o `Nome Cognome`.
9) Nella riga dell'utente desiderato, selezionare dall'elenco a discesa **Tipo** il tipo di utente IP (ad es. **Client di sistema** o **Deskshare User**).

10) Se per l'utente deve essere configurata una casella fax (utilizzabile ad esempio con i client UC **myPortal for Desktop** o **myPortal for Outlook**, procedere come segue:
   a) Nella riga dell'utente desiderato, nel campo **Fax N° tel**, inserire il numero di fax interno desiderato, mediante il quale l'utente potrà ricevere messaggi fax interni.
   b) Se per la casella fax deve essere configurato un numero interno, nella riga dell'utente desiderato, nel campo **DID fax**, inserire il numero di fax esterno desiderato, mediante il quale l'utente potrà ricevere messaggi fax esterni.
11) Nella riga dell'utente selezionato, dall'elenco a discesa **Abilitazione**, selezionare il gruppo di abilitazione desiderato.
12) Per aggiungere l'utente a un gruppo di risposta, selezionare dall'elenco a discesa **Gruppo di risposta alle chiamate** nella riga dell'utente desiderato.
13) Se necessario procedere a ulteriori impostazioni:
   a) Nella riga del terminale desiderato, fare clic sull'icona a forma di matita **Modifica**.



   b) Assegnare un **Numero cellulare** e selezionare **Web Feature ID** dall'elenco a discesa nell'area **Connessione mobile**.
   c) Nel campo **Clip/Lin** immettere un numero di telefono (selezione passante o MSN), che deve essere visualizzato sul display dell'utente chiamato al posto del proprio numero quando si effettua una chiamata esterna.

Nota: Questo servizio deve essere autorizzato dal gestore di rete.

Nota: Configurare almeno un numero DID. In caso contrario, il sistema non tiene conto del numero CLIP del chiamante e il numero interno della chiamata viene

formattato e inviato come numero di chiamata per la chiamata esterna.

d) Nell'elenco a discesa **Lingua** selezionare la lingua da utilizzare per i comandi dei menu del telefono.
e) Dall'elenco a discesa **Segnalazione della chiamata interna** assegnare all'utente uno degli otto possibili toni di segnalazione chiamate interne. In questo modo l'utente invia agli altri utenti interni un tono di chiamata diverso in base al quale può essere differenziato (standard: Suoneria 1).
f) Nell'elenco a discesa **Segnalazione della chiamata esterna**, selezionare e assegnare uno dei tre possibili toni di segnalazione chiamate esterne (standard: Suoneria 1).
g) Nel campo **ID Loc ITSP**, immettere il numero di indice dell'ID posizione dell'ITSP.
h) Solo con UC Smart: Dal menu a discesa selezionare **Tipo mailbox UC Smart** se l'utente deve ricevere una mailbox standard o una mailbox posto operatore (AutoAttendant).
i) Solo con UC Smart e mailbox predefinita: Se un chiamante può lasciare un messaggio nella casella vocale, selezionare la casella di controllo **Registrare**.
j) Solo con UC Smart: Dall'elenco a discesa **Annuncio**, selezionare un annuncio di benvenuto.
k) Solo con UC Smart: Se la password della casella vocale deve essere reimpostata, selezionare la casella di controllo **Reset password**.

Nota:

Se una casella vocale viene riconfigurata, la casella di controllo **Reset password** non deve essere selezionata. Consente di reimpostare la password per la casella vocale. In caso di riconfigurazione, l'utente deve cambiare comunque la password iniziale della casella vocale al primo accesso.

l) Se l'utente è connesso a Internet, l'Autenticazione DEVE essere attivata e OCCORRE immettere password sicure per tutti gli utenti IP. Controllare l'elenco flag **Autenticazione attiva** e completare i campi **Nuova password** e **Conferma password**.
m) Fare clic su **OK & Avanti**.
n) Modificare i flag utente in base alle necessità. Per una descrizione dei flag utente, vedere Capitolo 24.3.7.10 Utenti > Utenti > Parametri utente.
o) Fare clic su **OK & Avanti**.

14) Se si desidera configurare un altro utente, ripetere i passi da 5 a 13.
15) Fare clic su **OK & Avanti**. Viene visualizzato l'elenco di tutti gli utenti IP configurati. Se necessario è possibile stampare la lista degli utenti IP facendo clic su **Stampa**.
16) Fare clic su **OK & Avanti**, quindi su **Fine**.

11.13.2 Come configurare gli utenti SIP

La procedura guidata **Terminali IP** consente di configurare utenti SIP (telefoni LAN e WAN).

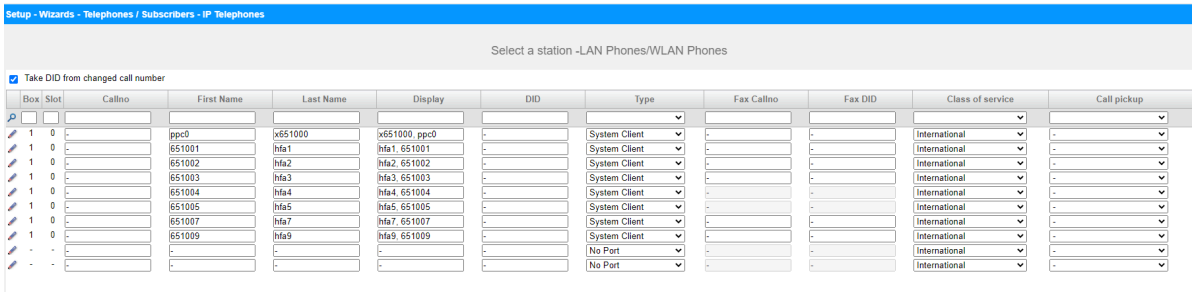
Prerequisiti

Per il funzionamento dei telefoni WLAN è necessaria una rete LAN wireless operativa.

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Telefoni / utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Terminali IP**. Viene visualizzato un elenco di tutti gli utenti IP. Questo elenco include tutti gli utenti SIP.



4) Se l'utente deve ricevere automaticamente il numero interno come selezione passante, selezionare il pulsante di opzione **Acquisisci DID dal numero di telefono modificato**.
5) Se si desidera che il numero di selezione passante dell'utente sia diverso dal numero di telefono, nella riga dell'utente desiderato, in corrispondenza di **DID**, immettere un numero di selezione passante per l'utente:
   - solo con connessioni punto - punto:

     Fare clic sul campo desiderato e immettere tramite tastiera il numero di selezione passante. Questo numero può coincidere con il numero interno.
   - solo con connessioni punto - multipunto:

     Nell'elenco a discesa selezionare un MSN. L'utente può ad es. essere raggiunto da chiamate interne sul numero interno 101 e dall'esterno tramite l'MSN 654321.
   - connessione punto - punto e connessione punto - multipunto:

     Nel campo desiderato selezionare una voce dall'elenco a discesa **xxx - modificabile** (xxx indica il numero interno) e immettere tramite tastiera il numero di selezione passante o selezionare un MSN dall'elenco a discesa.
6) Quando l'utente riceve come interno un numero utente di telefonia Internet, disattivare il pulsante di opzione **Acquisisci DID dal numero di telefono modificato**, dall'elenco accanto a questo pulsante di opzione selezionare il provider di servizi di telefonia Internet, quindi nella riga all'utente desiderato, dal menu a discesa **DID**, scegliere il numero di telefono dell'utente di telefonia Internet.
7) Nella riga appropriata dell'utente desiderato, immettere in **N° tel** un numero dell'utente interno. Si può utilizzare il numero di telefono pre-assegnato o immetterne uno diverso, ancora libero.

8) Nella riga dell'utente desiderato immettere in **Nome** un nome nel formato `Cognome, nome` o `Nome Cognome`.

9) Nella riga dell'utente desiderato, nell'elenco **Tipo**, selezionare il tipo **Client SIP**.

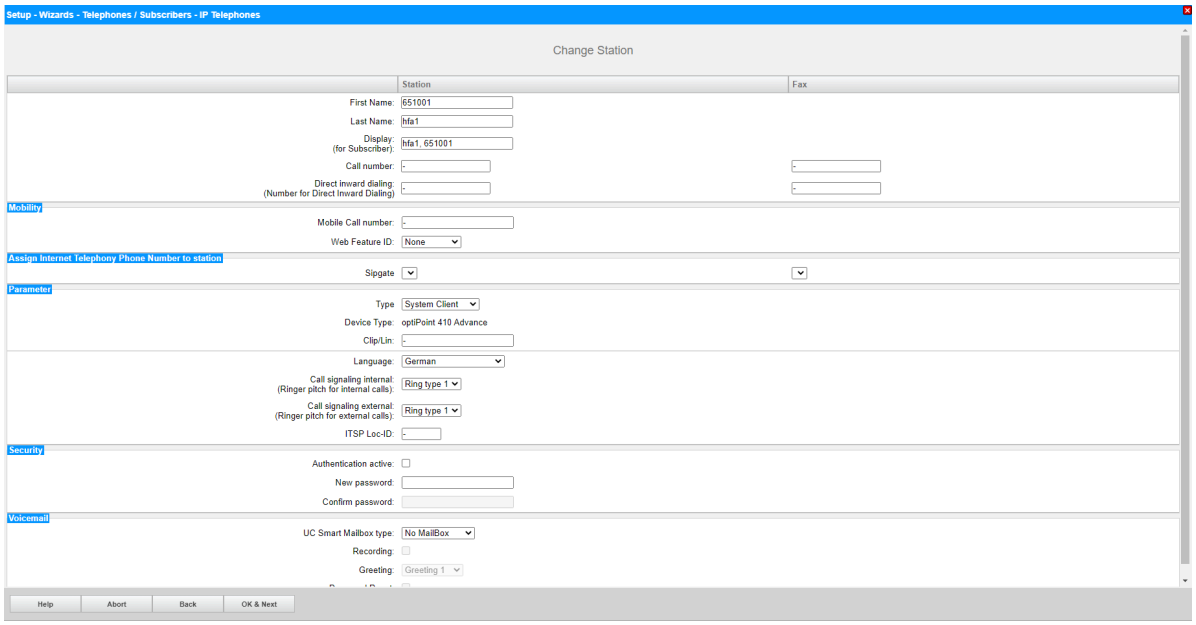
10) Se per l'utente deve essere configurata una casella fax (utilizzabile ad esempio con i client UC **myPortal for Desktop** o **myPortal for Outlook**, procedere come segue:
    a) Nella riga dell'utente desiderato, nel campo **Fax N° tel**, inserire il numero di fax interno desiderato, mediante il quale l'utente potrà ricevere messaggi fax interni.
    b) Se per la casella fax deve essere configurato un numero interno, nella riga dell'utente desiderato, nel campo **DID fax**, inserire il numero di fax esterno desiderato, mediante il quale l'utente potrà ricevere messaggi fax esterni.

11) Nella riga dell'utente selezionato, dall'elenco a discesa **Abilitazione**, selezionare il gruppo di abilitazione desiderato.

12) Per aggiungere l'utente a un gruppo di risposta, selezionare dall'elenco a discesa **Gruppo di risposta alle chiamate** nella riga dell'utente desiderato.

13) Configurare i dati per la registrazione SIP:

a) Nella riga del terminale desiderato, fare clic sull'icona a forma di matita **Modifica**.



b) Nell'area **Sicurezza**, immettere la password da utilizzare per l'autenticazione dell'utente SIP nei campi **Password** e **Conferma password**.

c) Nel campo **SIP ID d'utente / Nome d'utente** immettere un nome utente di propria scelta per l'autenticazione del'utente SIP, ad esempio SIP 120.

d) In **Realm** immettere un nome a scelta per la zona corrispondente, ad esempio OSBIZ-SIP. Questo valore dovrebbe essere uguale tutti i client SIP.

Nota: I valori della password, ID utente e realm qui definiti devono essere inseriti anche sul telefono SIP.

---

14) Se necessario procedere a ulteriori impostazioni:

a) Se il telefono SIP deve essere utilizzato insieme a un telefono cellulare dual-mode, inserire nell'area `Mobility` in **Num. cellulare** il codice linea esterna e di seguito il numero di telefono del cellulare (es. **0016012345678**). Inoltre, nell'elenco a discesa **Web Feature ID**, selezionare questo client SIP. (Vedere Telefonia dual mode).

b) Assegnare un numero DID per la telefonia Internet a ogni utente e, se lo si desidera, alla casella fax nell'area **Interno diretto per telefoni Internet**. A tal fine, selezionare i numeri DID dagli elenchi a discesa degli ITSP desiderati. Per ogni ITSP attivo, verrà presentato un elenco a discesa per l'utente e uno per la casella fax.

Nota: Il campo **Interno per telefonia DSL** non è visibile se la telefonia Internet non è stata configurata o non è attivo alcun Internet Telephony Service Provider.

---

c) Nel campo **Clip/Lin** immettere un numero di telefono (selezione passante o MSN), che deve essere visualizzato sul display dell'utente

chiamato al posto del proprio numero quando si effettua una chiamata esterna.

Nota: Questo servizio deve essere autorizzato dal gestore di rete.

Nota: Configurare almeno un numero DID. In caso contrario, il sistema non tiene conto del numero CLIP del chiamante e il numero interno della chiamata viene formattato e inviato come numero di chiamata per la chiamata esterna.

d) Nell'elenco a discesa **Lingua** selezionare la lingua da utilizzare per i comandi dei menu del telefono.
e) Dall'elenco a discesa **Segnalazione della chiamata interna** assegnare all'utente uno degli otto possibili toni di segnalazione chiamate interne. In questo modo l'utente invia agli altri utenti interni un tono di chiamata diverso in base al quale può essere differenziato (standard: Suoneria 1).
f) Nell'elenco a discesa **Segnalazione della chiamata esterna**, selezionare e assegnare uno dei tre possibili toni di segnalazione chiamate esterne (standard: Suoneria 1).
g) Solo con UC Smart: Dal menu a discesa selezionare **Tipo mailbox UC Smart** se l'utente deve ricevere una mailbox standard o una mailbox posto operatore (AutoAttendant).
h) Solo con UC Smart e mailbox predefinita: Se un chiamante può lasciare un messaggio nella casella vocale, selezionare la casella di controllo **Registrare**.
i) Solo con UC Smart: Dall'elenco a discesa **Annuncio**, selezionare un annuncio di benvenuto.
j) Solo con UC Smart: Se la password della casella vocale deve essere reimpostata, selezionare la casella di controllo **Reimposta password**.

Nota: Se una casella vocale viene riconfigurata, la casella di controllo **Reset password** non deve essere selezionata. Consente di reimpostare la password per la casella vocale. In caso di riconfigurazione, l'utente deve cambiare comunque la password iniziale della casella vocale al primo accesso.

k) Fare clic su **OK & Avanti**.
l) Modificare i flag utente in base alle necessità. Per una descrizione dei flag utente, vedere Utenti > Utenti > Parametri utente.
m) Fare clic su **OK & Avanti**.

15) Se si desidera configurare un altro utente, ripetere i passi da 5 a 14.
16) Fare clic su **OK & Avanti**. Viene visualizzato l'elenco di tutti gli utenti IP configurati. Se necessario è possibile stampare la lista degli utenti IP facendo clic su **Stampa**.
17) Fare clic su **OK & Avanti**, quindi su **Fine**.

11.13.3 Come configurare le stazioni UP0

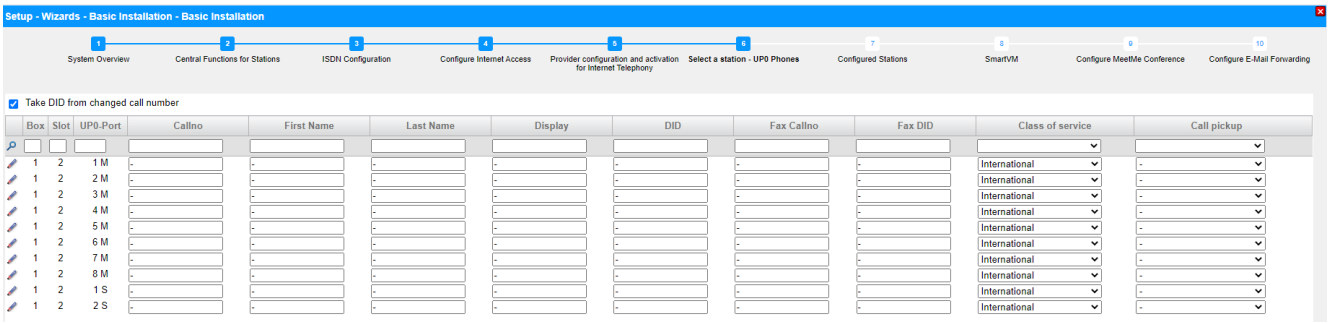
È possibile utilizzare la procedura guidata **Dispositivi UP0** per configurare le stazioni UP0.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Telefoni/ Abbonati**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Dispositivi UP0**. Viene visualizzato l'elenco di tutte le stazioni UP0.



4) Se si desidera che il numero di chiamata interna venga assegnato automaticamente alla stazione come numero di chiamata diretta, attivare il pulsante di opzione **Recuperare il DID dal numero di chiamata modificato**.
5) Se si desidera che il numero di selezione passante dell'utente sia diverso dal numero di telefono, nella riga dell'utente desiderato, in corrispondenza di **DID**, immettere un numero di selezione passante per l'utente:
   - solo con connessioni punto - punto:

     Fare clic sul campo desiderato e immettere tramite tastiera il numero di selezione passante. Questo numero può coincidere con il numero interno.
   - solo con connessioni punto - multipunto:

     Nell'elenco a discesa selezionare un MSN. L'utente può ad es. essere raggiunto da chiamate interne sul numero interno 101 e dall'esterno tramite l'MSN 654321.
   - connessione punto - punto e connessione punto - multipunto:

     Nel campo desiderato selezionare una voce dall'elenco a discesa **xxx - modificabile** (xxx indica il numero interno) e immettere tramite tastiera il numero di selezione passante o selezionare un MSN dall'elenco a discesa.
6) Se si desidera assegnare alla stazione un numero di telefono di telefonia Internet come numero di selezione diretta, lasciare deselezionato il pulsante di opzione **Recupera DID da numero di chiamata modificato** e selezionare invece il fornitore di servizi di telefonia Internet dall'elenco accanto al pulsante di opzione. Selezionare quindi il numero di telefono

di telefonia Internet dall'elenco a discesa **DID** nella riga della stazione desiderata.

7) Nella riga appropriata dell'utente desiderato, immettere in **N° tel** un numero dell'utente interno. Si può utilizzare il numero di telefono pre-assegnato o immetterne uno diverso, ancora libero.

8) Nella riga dell'utente desiderato immettere in **Nome** un nome nel formato `Cognome, nome` o `Nome Cognome`.

9) Se per l'utente deve essere configurata una casella fax (utilizzabile ad esempio con i client UC **myPortal for Desktop** o **myPortal for Outlook**, procedere come segue:

a) Nella riga dell'utente desiderato, nel campo **Fax N° tel**, inserire il numero di fax interno desiderato, mediante il quale l'utente potrà ricevere messaggi fax interni.

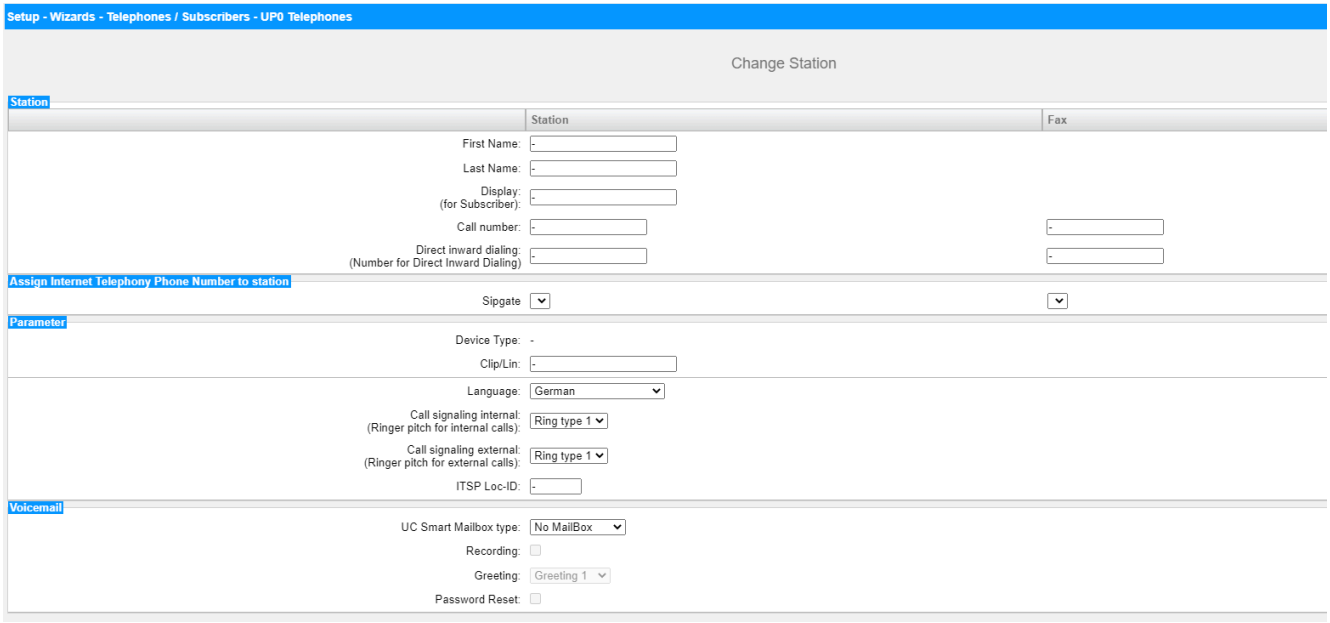
b) Se si desidera configurare un numero DID per la casella fax, nella riga dell'abbonato desiderato inserire nel campo **DID fax** il numero di fax esterno a cui l'abbonato può ricevere fax dall'esterno.

10) Nella riga dell'utente selezionato, dall'elenco a discesa **Abilitazione**, selezionare il gruppo di abilitazione desiderato.

11) Per aggiungere l'utente a un gruppo di risposta, selezionare dall'elenco a discesa **Gruppo di risposta alle chiamate** nella riga dell'utente desiderato.

12) Se necessario, effettuare ulteriori impostazioni:

a) Nella riga del terminale desiderato, fare clic sull'icona a forma di matita **Modifica**.



b) In **Interno per telefonia Internet** scegliere un numero interno dall'elenco a discesa. Per ciascun ITSP attivo viene visualizzato un elenco a discesa.

Nota: Il campo **DID per telefonia Internet** non è visibile se la telefonia Internet non è stata configurata o non è attivo alcun provider di servizi di telefonia Internet.

---

c) Nel campo **Clip/Lin** immettere un numero di telefono (selezione passante o MSN), che deve essere visualizzato sul display dell'utente chiamato al posto del proprio numero quando si effettua una chiamata esterna.

Nota: Questa funzione deve essere autorizzata dal provider di rete.

Nota: Deve essere configurato almeno un numero DID. In caso contrario, il sistema non tiene conto del numero CLIP del chiamante e il numero interno della chiamata viene formattato e inviato come numero di chiamata per la chiamata esterna.

---

d) Nell'elenco a discesa **Lingua** selezionare la lingua da utilizzare per i comandi dei menu del telefono.

e) Dall'elenco a discesa **Segnalazione della chiamata interna** assegnare all'utente uno degli otto possibili toni di segnalazione chiamate interne.

In questo modo l'utente invia agli altri utenti interni un tono di chiamata diverso in base al quale può essere differenziato (standard: Suoneria 1).

f) Nell'elenco a discesa **Segnalazione della chiamata esterna**, selezionare e assegnare uno dei tre possibili toni di segnalazione chiamate esterne (standard: Suoneria 1).

g) Solo con UC Smart: Selezionare se l'abbonato deve ricevere una casella postale predefinita o una casella postale di assistenza (AutoAttendant) nell'elenco a discesa **Tipo di casella postale UC Smart**.

h) Solo con UC Smart e la casella postale predefinita: Se il chiamante può lasciare un messaggio nella casella vocale, selezionare la casella **Registrazione**.

i) Solo con UC Smart: Selezionare il messaggio di benvenuto dall'elenco a discesa **Messaggio di benvenuto**.

j) Solo con UC Smart: Se la password della casella vocale deve essere reimpostata, selezionare la casella di controllo **Reimposta password**.

Nota: La casella di controllo **Reimposta password** deve essere deselezionata quando si configura una nuova casella vocale. Serve per reimpostare la password della casella vocale. Quando viene creata una nuova casella vocale, l'abbonato deve comunque cambiare la password iniziale quando accede per la prima volta alla sua casella vocale.

---

k) Fare clic su **OK & Avanti**.

l) Modificare i flag utente in base alle necessità. Per una descrizione dei flag di stazione, vedere Stazione > Stazione > Parametri stazione.

m) Fare clic su **OK & Avanti**.

13) Se si desidera configurare un'altra stazione, ripetere i passaggi da 5 a 12.

14) Fare clic su **OK & Avanti**. Viene visualizzato l'elenco di tutte le stazioni UP0 configurate. Se necessario, è possibile stampare l'elenco delle stazioni UP0 con **Stampa**.

15) Fare clic su **OK & Avanti**, quindi su **Fine**.

11.13.4 Come configurare gli utenti DECT

È possibile utilizzare la procedura guidata **Dispositivi DECT** per configurare le stazioni DECT (telefoni DECT).

Prerequisiti

Una stazione base è collegata a un'interfaccia UP0 o a una scheda SLC installata.

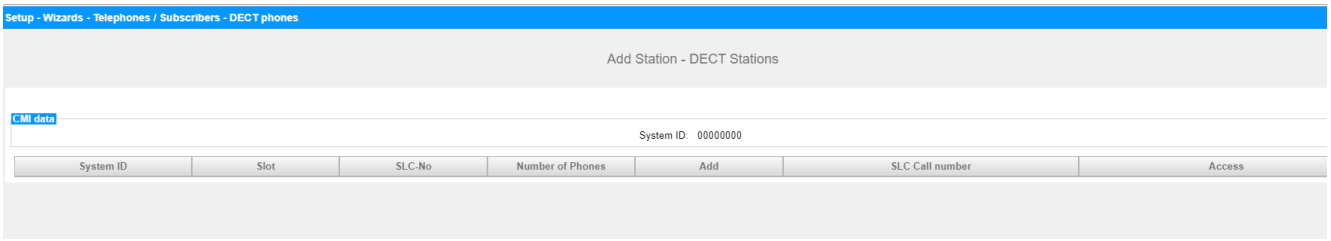
Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.

2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Telefoni/ Abbonati**.

3) Fare clic su **Modifica** per avviare la procedura guidata **Telefoni DECT**. Viene visualizzato l'elenco di tutte le stazioni DECT.



4) Se si desidera che il numero di chiamata interna venga assegnato automaticamente alla stazione come numero di chiamata diretta, attivare il pulsante di opzione **Recuperare il DID dal numero di chiamata modificato**.

5) Se si desidera che il numero di selezione passante dell'utente sia diverso dal numero di telefono, nella riga dell'utente desiderato, in corrispondenza di **DID**, immettere un numero di selezione passante per l'utente:

   - solo con connessioni punto - punto:

     Fare clic sul campo desiderato e immettere tramite tastiera il numero di selezione passante. Questo numero può coincidere con il numero interno.
   - solo con connessioni punto - multipunto:

     Nell'elenco a discesa selezionare un MSN. L'utente può ad es. essere raggiunto da chiamate interne sul numero interno 101 e dall'esterno tramite l'MSN 654321.
   - connessione punto - punto e connessione punto - multipunto:

     Nel campo desiderato selezionare una voce dall'elenco a discesa **xxx - modificabile** (xxx indica il numero interno) e immettere tramite tastiera il numero di selezione passante o selezionare un MSN dall'elenco a discesa.

6) Se si desidera assegnare alla stazione un numero di telefono di telefonia Internet come numero di selezione diretta, lasciare deselezionato il pulsante di opzione **Recupera DID da numero di chiamata modificato** e selezionare invece il fornitore di servizi di telefonia Internet dall'elenco accanto al pulsante di opzione. Selezionare quindi il numero di telefono di telefonia Internet dall'elenco a discesa **DID** nella riga della stazione desiderata.

7) Nella riga appropriata dell'utente desiderato, immettere in **N° tel** un numero dell'utente interno. Si può utilizzare il numero di telefono pre-assegnato o immetterne uno diverso, ancora libero.

8) Nella riga dell'utente desiderato immettere in **Nome** un nome nel formato `Cognome, nome` o `Nome Cognome`.

9) Se per l'utente deve essere configurata una casella fax (utilizzabile ad esempio con i client UC **myPortal for Desktop** o **myPortal for Outlook**, procedere come segue:

   a) Nella riga dell'utente desiderato, nel campo **Fax N° tel**, inserire il numero di fax interno desiderato, mediante il quale l'utente potrà ricevere messaggi fax interni.

   b) Se si desidera configurare un numero DID per la casella fax, nella riga dell'abbonato desiderato inserire nel campo **DID fax** il numero di fax esterno a cui l'abbonato può ricevere fax dall'esterno.

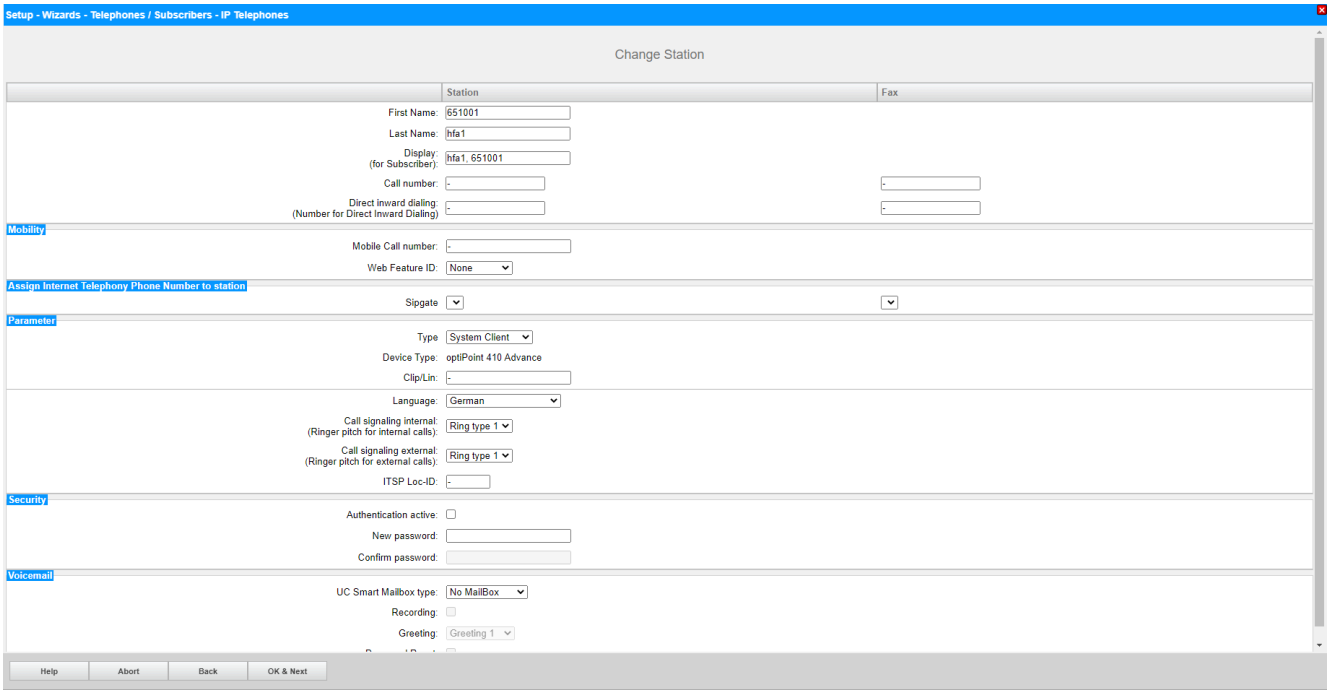
10) Nella riga dell'utente selezionato, dall'elenco a discesa **Abilitazione**, selezionare il gruppo di abilitazione desiderato.

11) Per aggiungere l'utente a un gruppo di risposta, selezionare dall'elenco a discesa **Gruppo di risposta alle chiamate** nella riga dell'utente desiderato.

12) Se si desidera modificare il codice (PIN) del telefono DECT, immettere il nuovo codice nella riga dell'utente desiderato in **Codice mobile**. L'utente DECT deve accedere all'utente base con questo codice.

13) Se necessario, effettuare ulteriori impostazioni:

a) Nella riga del terminale desiderato, fare clic sull'icona a forma di matita **Modifica**.



b) In **Interno per telefonia Internet** scegliere un numero interno dall'elenco a discesa. Per ciascun ITSP attivo viene visualizzato un elenco a discesa.

Nota: Il campo **DID per telefonia Internet** non è visibile se la telefonia Internet non è stata configurata o non è attivo alcun provider di servizi di telefonia Internet.

---

c) Nel campo **Clip/Lin** immettere un numero di telefono (selezione passante o MSN), che deve essere visualizzato sul display dell'utente chiamato al posto del proprio numero quando si effettua una chiamata esterna.

Nota: Questa funzione deve essere autorizzata dal provider di rete.

Nota: Deve essere configurato almeno un numero DID. In caso contrario, il sistema non tiene conto del numero CLIP del chiamante e il numero interno della chiamata

viene formattato e inviato come numero di chiamata per la chiamata esterna.

d) Nell'elenco a discesa **Lingua** selezionare la lingua da utilizzare per i comandi dei menu del telefono.
e) Dall'elenco a discesa **Segnalazione della chiamata interna** assegnare all'utente uno degli otto possibili toni di segnalazione chiamate interne. In questo modo l'utente invia agli altri utenti interni un tono di chiamata diverso in base al quale può essere differenziato (standard: Suoneria 1).
f) Nell'elenco a discesa **Segnalazione della chiamata esterna**, selezionare e assegnare uno dei tre possibili toni di segnalazione chiamate esterne (standard: Suoneria 1).
g) Solo con UC Smart: Selezionare se l'abbonato deve ricevere una casella postale predefinita o una casella postale di assistenza (AutoAttendant) nell'elenco a discesa **Tipo di casella postale UC Smart**.
h) Solo con UC Smart e la casella postale predefinita: Se il chiamante può lasciare un messaggio nella casella vocale, selezionare la casella **Registrazione**.
i) Solo con UC Smart: Selezionare il messaggio di benvenuto dall'elenco a discesa **Messaggio di benvenuto**.
j) Solo con UC Smart: Se la password della casella vocale deve essere reimpostata, selezionare la casella di controllo **Reimposta password**.

Nota: La casella di controllo **Reimposta password** deve essere deselezionata quando si configura una nuova casella vocale. Serve per reimpostare la password della casella vocale. Quando viene creata una nuova casella vocale, l'abbonato deve comunque cambiare la password iniziale quando accede per la prima volta alla sua casella vocale.

k) Fare clic su **OK & Avanti**.
l) Modificare i flag utente in base alle necessità. Per una descrizione dei flag di stazione, vedere Stazione > Stazione > Parametri stazione.
m) Fare clic su **OK & Avanti**.

14) Se si desidera configurare un'altra stazione, ripetere i passaggi da 5 a 13.
15) Fare clic su **OK & Avanti**. Viene visualizzato l'elenco di tutte le stazioni DECT configurate. Se necessario, è possibile stampare l'elenco delle stazioni DECT con **Stampa**.
16) Fare clic su **OK & Avanti**, quindi su **Fine**.

Attività correlate

Come effettuare la prima configurazione dei telefoni DECT alla pagina 969

11.13.5 Come configurare le stazioni Mitel SIP DECT tramite provisioning

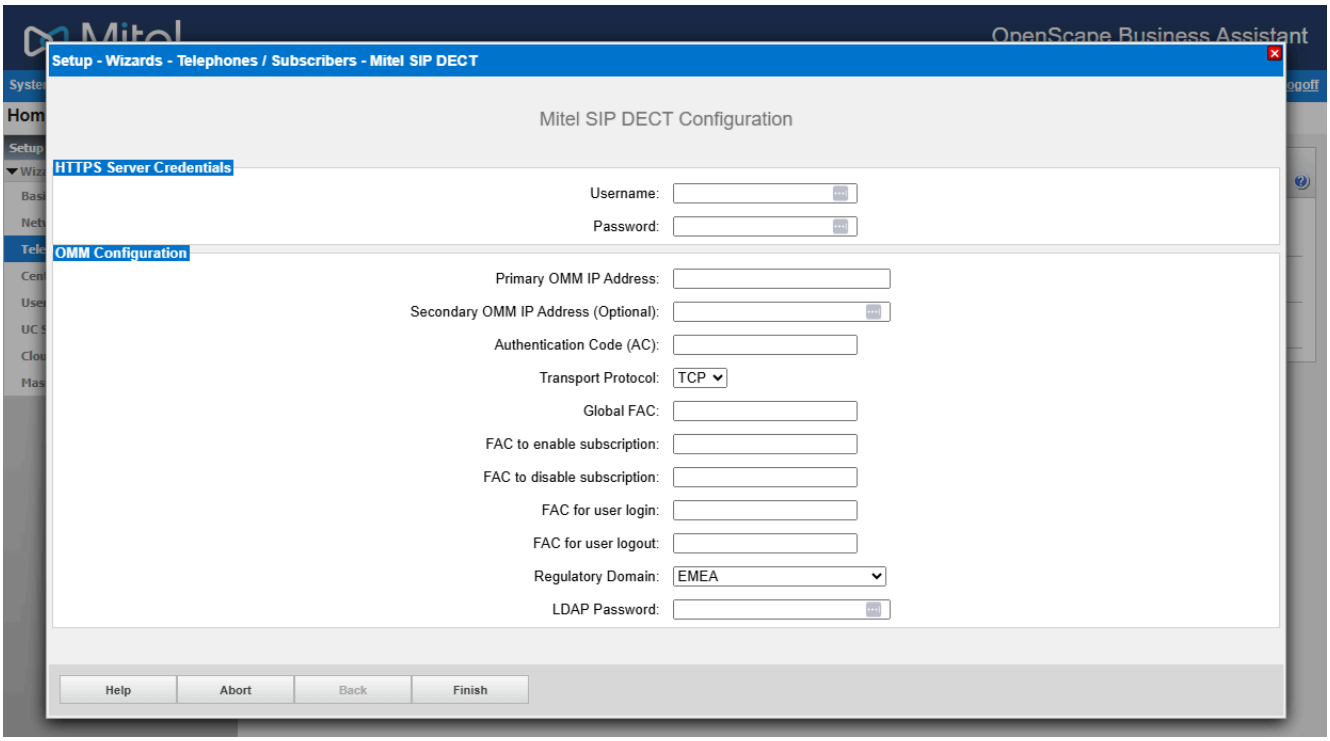
È possibile utilizzare la procedura guidata **Mitel SIP DECT** per configurare i dispositivi Mitel SIP-DECT e connettersi a Open Mobility Manager (OMM).

Prerequisiti

L'indirizzo MAC del dispositivo SIP DECT RFP è noto.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperto > Interfacce di rete > DHCP**.
2) Fare clic per abilitare **Server DHCP**.
3) Nella barra di navigazione, fare clic su **Server DHCP > Indirizzi IP statici**.
4) Nella finestra **Indirizzi IP statici**, fare clic sulla scheda **Aggiungere un indirizzo IP statico**.
5) Inserire le informazioni richieste come descritto in Interfacce di rete > Scheda madre > Modalità DHCP > Server DHCP > Indirizzi IP statici.
6) Fare clic su **Applica**.
7) Nella barra di navigazione, fare clic su **Configurazione**.
8) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Telefoni/ Abbonati**.
9) Fare clic su **Modifica**, per avviare la procedura guidata **Mitel SIP DECT**.



10) In **Credenziali server HTTPS**, fornire le credenziali di accesso al server.
    a) Impostare il **Nome utente** e la **Password**.
11) In **Configurazione OMM**:
12) Fornire l'**Indirizzo IP OMM primario** e l'**Indirizzo IP OMM secondario (facoltativo)** dell'OMM.
13) Impostare il **Codice di autenticazione (AC)**.
14) In **Protocolli di trasporto**, scegliere dal menu a discesa uno dei seguenti valori:
    - TCP
    - UDP
    - TLS

15) Impostare i vari Codici di accesso alle funzioni (FAC) nei seguenti campi:
    a) **FAC globale**
    b) **FAC per abilitare la sottoscrizione**
    c) **FAC per l'accesso dell'utente**
    d) **FAC per la disconnessione dell'utente**
16) In **Dominio normativo**, scegliere uno dei seguenti valori dal menu a discesa:
    - EMEA
    - USA
    - Brasile
    - Taiwan
    - Radio 1910 - 1927 MHz 250 Mw
17) Fornire la **Password LDAP** per accedere alla directory interna degli utenti di OpenScape Business.
18) Fare clic su **Fine**.
    Vengono generati i file di configurazione necessari dall'applicazione OMM.
19) Configurare una stazione SIP come descritto in Come configurare le stazioni SIP tramite la Modalità Esperto.
20) Collegare il dispositivo Mitel SIP DECT RFP alla rete. Attendere qualche istante affinché il dispositivo riceva un indirizzo IP dal server DHCP.
21) Connettersi all'applicazione OMM e configurare la stazione base, come descritto nella "*Guida alla configurazione del Mitel SIP DECT Phone*".

11.13.5.1 Come configurare le stazioni SIP in modalità Esperto

È possibile utilizzare la **Modalità Esperto** per configurare le stazioni SIP.

Prerequisiti

Si è connessi a WBM con il profilo **Esperto**.

Passo a passo

1) Nella struttura di navigazione, fare clic su **Modalità Esperto** > **Server telefonia** > **Stazione**.
2) Nella nuova finestra, fare clic per espandere **Stazione** e selezionare **Client IP**. Viene visualizzato l'elenco di tutte le stazioni IP/SIP.
3) Nella colonna **Tipo**, selezionare **Client SIP**.
4) Fare clic su **Applica**.
5) Fare clic sulla freccia blu accanto al numero di chiamata della stazione IP, nella colonna **CallNo**.
6) Nella finestra **Modifica parametri stazione**, selezionare **Dispositivo Mitel SIP DECT** dal menu a discesa **Provisioning dei dispositivi**.
   Appare l'opzione **Configurazione di Mitel SIP DECT**.

7) Nell'opzione **Configurazione di Mitel SIP DECT**, impostare quanto segue:
   a) Inserire il **PIN** del dispositivo.
   b) In **Blocco tasti abilitato**, abilitare (Sì) o disabilitare (No) il blocco dei tasti del dispositivo.
   c) In **PIN blocco tasti**, inserire il PIN per il blocco dei tasti.
   d) In **Ora blocco tasti**, inserire l'ora in cui il PIN del blocco tasti avrà effetto.
   e) In **Mostra directory personale**, scegliere se la directory personale è visibile (Sì) o meno (No).
8) Fare clic su **Applica**.
9) Passare alla scheda **Modifica dati client del punto di lavoro**.
10) In **Parametri**, configurare i valori come descritto in Parametri stazione.
11) Fare clic su **Applica**.

11.13.6 Come configurare gli utenti ISDN

La procedura guidata **Terminali ISDN** consente di configurare utenti ISDN (ad esempio, telefoni o fax ISDN).

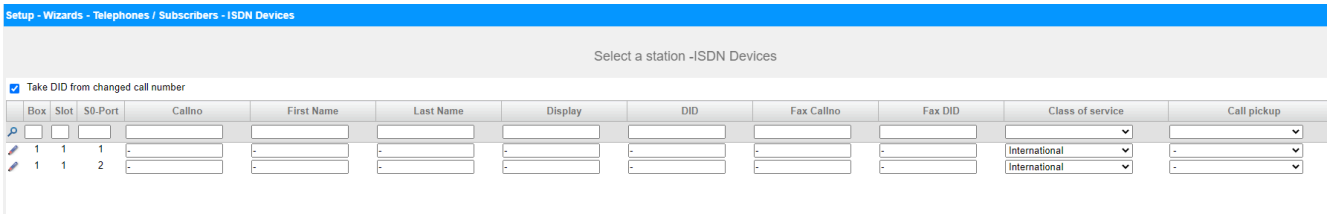
Prerequisiti

È disponibile almeno un'interfaccia S_0 libera. Se viene utilizzata la porta S_0 di una piattaforma hardware, questa deve essere configurata come porta S_0 interna.

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Telefoni / utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Terminali ISDN**. Viene visualizzato un elenco di tutti i terminali ISDN.



4) Se si desidera che il numero di selezione passante dell'utente sia uguale al numero di telefono, selezionare il pulsante di opzione **Acquisisci DID dal numero di telefono modificato**.

5) Se si desidera che il numero di selezione passante dell'utente sia diverso dal numero di telefono, nella riga dell'utente desiderato, in corrispondenza di **DID**, immettere un numero di selezione passante per l'utente:

- solo con connessioni punto - punto:

  Fare clic sul campo desiderato e immettere tramite tastiera il numero di selezione passante. Questo numero può coincidere con il numero interno.
- solo con connessioni punto - multipunto:

  Nell'elenco a discesa selezionare un MSN. L'utente può ad es. essere raggiunto da chiamate interne sul numero interno 101 e dall'esterno tramite l'MSN 654321.
- connessione punto - punto e connessione punto - multipunto:

  Nel campo desiderato selezionare una voce dall'elenco a discesa **xxx - modificabile** (xxx indica il numero interno) e immettere tramite tastiera il numero di selezione passante o selezionare un MSN dall'elenco a discesa.

6) Nella riga appropriata dell'utente desiderato, immettere in **N° tel** un numero dell'utente interno. Si può utilizzare il numero di telefono pre-assegnato o immetterne uno diverso, ancora libero.

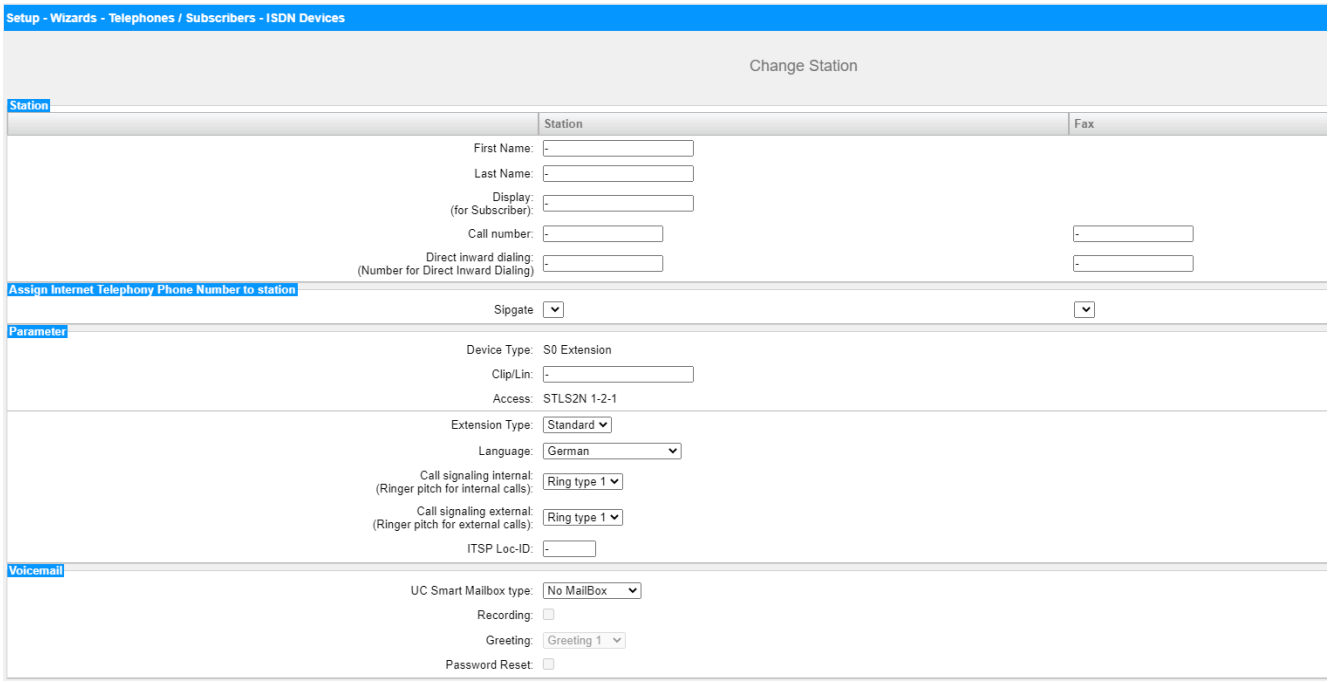
7) Nella riga dell'utente desiderato immettere in **Nome** un nome nel formato `Cognome, nome` o `Nome Cognome`.

8) Nella riga dell'utente selezionato, dall'elenco a discesa **Abilitazione**, selezionare uno dei gruppi di abilitazione desiderati.

9) Per aggiungere l'utente a un gruppo di risposta, selezionare dall'elenco a discesa **Gruppo di risposta alle chiamate** nella riga dell'utente desiderato.

10) Se necessario procedere a ulteriori impostazioni:

a) Nella riga del terminale desiderato, fare clic sull'icona a forma di matita **Modifica**.



b) In **Interno per telefonia Internet** scegliere un numero interno dall'elenco a discesa. Per ciascun ITSP attivo viene visualizzato un elenco a discesa.

Nota: Il campo **Interno per telefonia DSL** non è visibile se la telefonia Internet non è stata configurata o non è attivo alcun Internet Telephony Service Provider.

---

c) Nel campo **Clip/Lin** immettere un numero di telefono (selezione passante o MSN), che deve essere visualizzato sul display dell'utente chiamato al posto del proprio numero quando si effettua una chiamata esterna.

Nota: Questo servizio deve essere autorizzato dal gestore di rete.

Nota: Configurare almeno un numero DID. In caso contrario, il sistema non tiene conto del numero CLIP del chiamante e il numero interno della chiamata viene formattato e inviato come numero di chiamata per la chiamata esterna.

---

d) Nell'elenco a discesa **Tipo di periferica**, selezionare il tipo del terminale ISDN (`Standard` o `Fax`).

e) Mantenere la selezione predefinita nell'elenco a discesa **Lingua**. Nel caso dei terminali ISDN questa impostazione non ha alcun significato.

f) Dall'elenco a discesa **Segnalazione della chiamata interna** assegnare all'utente uno degli otto possibili toni di segnalazione chiamate interne.

In questo modo l'utente invia agli altri utenti interni un tono di chiamata diverso in base al quale può essere differenziato (standard: Suoneria 1).

g) Nell'elenco a discesa **Segnalazione della chiamata esterna**, selezionare e assegnare uno dei tre possibili toni di segnalazione chiamate esterne (standard: Suoneria 1).

h) Solo con UC Smart: Dal menu a discesa selezionare **Tipo mailbox UC Smart** se l'utente deve ricevere una mailbox standard o una mailbox posto operatore (AutoAttendant).

i) Solo con UC Smart e mailbox predefinita: Se un chiamante può lasciare un messaggio nella casella vocale, selezionare la casella di controllo **Registrare**.

j) Solo con UC Smart: Dall'elenco a discesa **Annuncio**, selezionare un annuncio di benvenuto.

k) Solo con UC Smart: Se la password della casella vocale deve essere reimpostata, selezionare la casella di controllo **Reimposta password**.

Nota: Se una casella vocale viene riconfigurata, la casella di controllo **Reset password** non deve essere selezionata. Consente di reimpostare la password per la casella vocale. In caso di riconfigurazione, l'utente deve cambiare comunque la password iniziale della casella vocale al primo accesso.

---

l) Fare clic su **OK & Avanti**.

m) Modificare i flag utente in base alle necessità. Per una descrizione dei flag utente, vedere Utenti > Utenti > Parametri utente.

n) Fare clic su **OK & Avanti**.

11) Se si desidera configurare un altro utente, ripetere i passi da 5 a 10.

12) Fare clic su **OK & Avanti**. Viene visualizzato l'elenco di tutti gli utenti ISDN configurati. Se necessario è possibile stampare la lista degli utenti ISDN facendo clic su **Stampa**.

13) Fare clic su **OK & Avanti**, quindi su **Fine**.

11.13.7 Come configurare gli utenti analogici

La procedura guidata **Terminali analogici** consente la configurazione dei dispositivi analogici collegati (ad esempio, telefoni o fax analogici).

Prerequisiti

È disponibile almeno un'interfaccia analogica libera.

Sui dispositivi analogici è attivato DTMF.

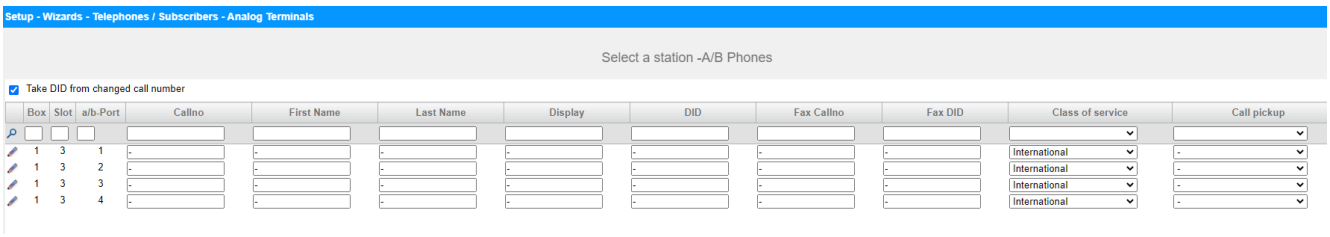
Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.

2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Telefoni / utenti**.

3) Fare clic su **Modifica**, per avviare la procedura guidata **Terminali analogici**. Viene visualizzato un elenco di tutti i terminali analogici.



4) Se si desidera che il numero di selezione passante dell'utente sia uguale al numero di telefono, selezionare il pulsante di opzione **Acquisisci DID dal numero di telefono modificato**.

5) Se si desidera che il numero di selezione passante dell'utente sia diverso dal numero di telefono, nella riga dell'utente desiderato, in corrispondenza di **DID**, immettere un numero di selezione passante per l'utente:

   - solo con connessioni punto - punto:

     Fare clic sul campo desiderato e immettere tramite tastiera il numero di selezione passante. Questo numero può coincidere con il numero interno.
   - solo con connessioni punto - multipunto:

     Nell'elenco a discesa selezionare un MSN. L'utente può ad es. essere raggiunto da chiamate interne sul numero interno 101 e dall'esterno tramite l'MSN 654321.
   - connessione punto - punto e connessione punto - multipunto:

     Nel campo desiderato selezionare una voce dall'elenco a discesa **xxx - modificabile** (xxx indica il numero interno) e immettere tramite tastiera il numero di selezione passante o selezionare un MSN dall'elenco a discesa.

6) Nella riga appropriata dell'utente desiderato, immettere in **N° tel** un numero dell'utente interno. Si può utilizzare il numero di telefono pre-assegnato o immetterne uno diverso, ancora libero.

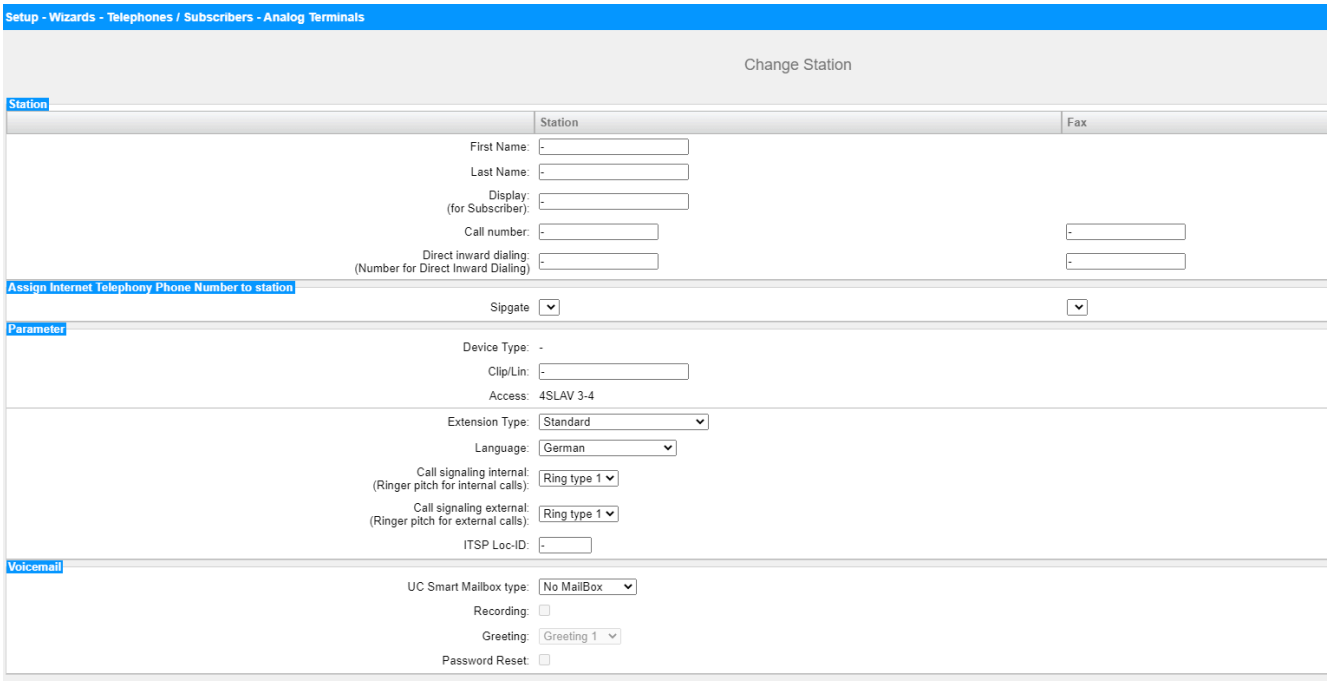
7) Nella riga dell'utente desiderato immettere in **Nome** un nome nel formato `Cognome, nome` o `Nome Cognome`.

8) Nella riga dell'utente selezionato, dall'elenco a discesa **Abilitazione**, selezionare uno dei gruppi di abilitazione desiderati.

9) Per aggiungere l'utente a un gruppo di risposta, selezionare dall'elenco a discesa **Gruppo di risposta alle chiamate** nella riga dell'utente desiderato.

10) Se necessario procedere a ulteriori impostazioni: - Se viene configurato un modem analogico, occorre selezionare l'opzione **Modem**:

a) Nella riga del terminale desiderato, fare clic sull'icona a forma di matita **Modifica**.



b) In **Interno per telefonia Internet** scegliere un numero interno dall'elenco a discesa. Per ciascun ITSP attivo viene visualizzato un elenco a discesa.

Nota: Il campo **Interno per telefonia DSL** non è visibile se la telefonia Internet non è stata configurata o non è attivo alcun Internet Telephony Service Provider.

---

c) Nel campo **Clip/Lin** immettere un numero di telefono (selezione passante o MSN), che deve essere visualizzato sul display dell'utente chiamato al posto del proprio numero quando si effettua una chiamata esterna.

Nota: Questo servizio deve essere autorizzato dal gestore di rete.

Nota: Configurare almeno un numero DID. In caso contrario, il sistema non tiene conto del numero CLIP del chiamante e il numero interno della chiamata viene

formattato e inviato come numero di chiamata per la chiamata esterna.

d) Nell'elenco a discesa **Tipo di periferica**, selezionare il tipo di terminale analogico (ad es. fax).

   Se viene configurato un modem analogico, occorre selezionare l'opzione **Modem**.

e) Mantenere la selezione predefinita nell'elenco a discesa **Lingua**. Nel caso dei terminali analogici questa impostazione non ha alcun significato.

f) Dall'elenco a discesa **Segnalazione della chiamata interna** assegnare all'utente uno degli otto possibili toni di segnalazione chiamate interne. In questo modo l'utente invia agli altri utenti interni un tono di chiamata diverso in base al quale può essere differenziato (standard: Suoneria 1).

g) Nell'elenco a discesa **Segnalazione della chiamata esterna**, selezionare e assegnare uno dei tre possibili toni di segnalazione chiamate esterne (standard: Suoneria 1).

h) Solo con UC Smart: Dal menu a discesa selezionare **Tipo mailbox UC Smart** se l'utente deve ricevere una mailbox standard o una mailbox posto operatore (AutoAttendant).

i) Solo con UC Smart e mailbox predefinita: Se un chiamante può lasciare un messaggio nella casella vocale, selezionare la casella di controllo **Registrare**.

j) Solo con UC Smart: Dall'elenco a discesa **Annuncio**, selezionare un annuncio di benvenuto.

k) Solo con UC Smart: Se la password della casella vocale deve essere reimpostata, selezionare la casella di controllo **Reimposta password**.

   Nota: Se una casella vocale viene riconfigurata, la casella di controllo **Reset password** non deve essere selezionata. Consente di reimpostare la password per la casella vocale. In caso di riconfigurazione, l'utente deve cambiare comunque la password iniziale della casella vocale al primo accesso.

l) Fare clic su **OK & Avanti**.

m) Modificare i flag utente in base alle necessità. Per una descrizione dei flag utente, vedere Utenti > Utenti > Parametri utente.

n) Fare clic su **OK & Avanti**.

11) Se si desidera configurare un altro utente, ripetere i passi da 5 a 10.

12) Fare clic su **OK & Avanti**. Viene visualizzato l'elenco di tutti gli utenti analogici configurati. Se necessario è possibile stampare la lista degli utenti analogici facendo clic su **Stampa**.

13) Fare clic su **OK & Avanti**, quindi su **Fine**.

11.13.8 Come modificare i nomi degli utenti

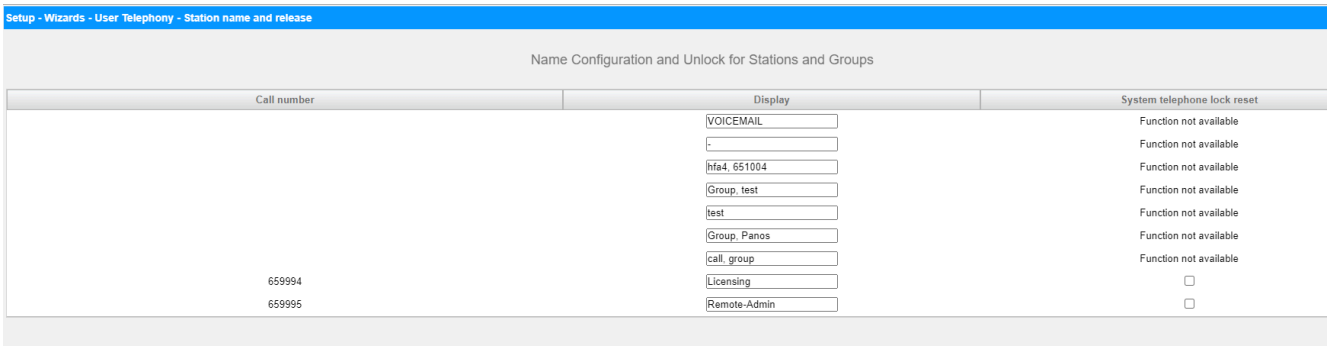
Con la procedura guidata **Nome utente e rilascio** è possibile modificare i nomi degli utenti.

Prerequisiti

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Nome utente e rilascio**.



4) Fare clic sulla colonna **Visualizza** nel campo dell'utente desiderato e modificare il nome dell'utente nel formato `Cognome, nome` o `Nome Cognome`.
5) Se si desidera modificare il nome di altri utenti, ripetere il passo 4.
6) Fare clic su **OK & Avanti**, quindi su **Fine**..

11.14 Configurazione dei profili apparecchio

I profili apparecchio contengono i valori e le proprietà degli utenti IP (apparecchi).

Con la procedura guidata **Profili** un amministratore con il profilo **Advanced** può eseguire le seguenti configurazioni:

- Creazione di un nuovo profilo
- Visualizzazione dei profili e dei relativi membri
- Aggiunta di membri a un profilo
- Eliminazione di membri da un profilo
- Esportazione o importazione dei singoli profili

Tramite la Modalità esperti, un amministratore con il profilo **Expert**può eseguire anche le seguenti configurazioni:

- Modifica dei valori e delle impostazioni di un profilo esistente
- Importazione ed esportazione di tutti i profili

I profili apparecchio già creati non possono essere cancellati ma solo sovrascritti.

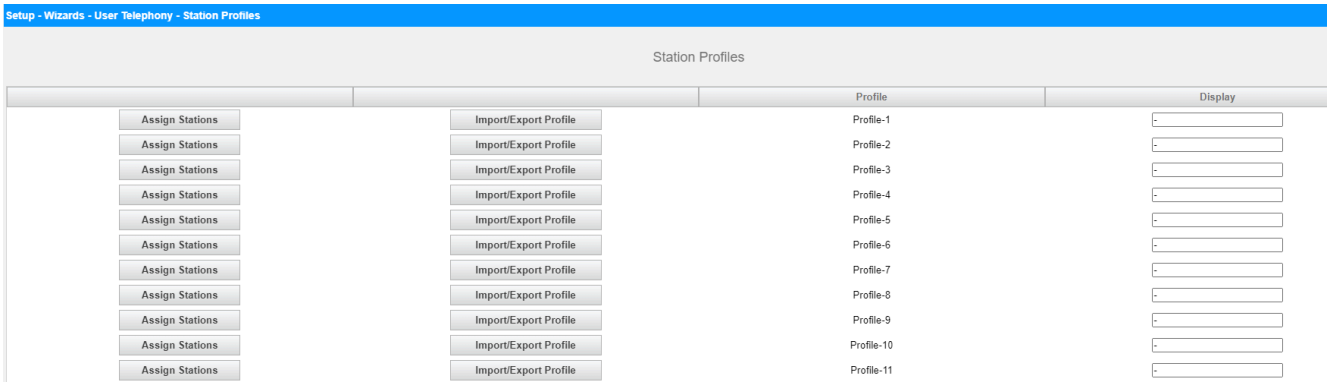
11.14.1 Come creare un nuovo profilo apparecchio

Prerequisiti

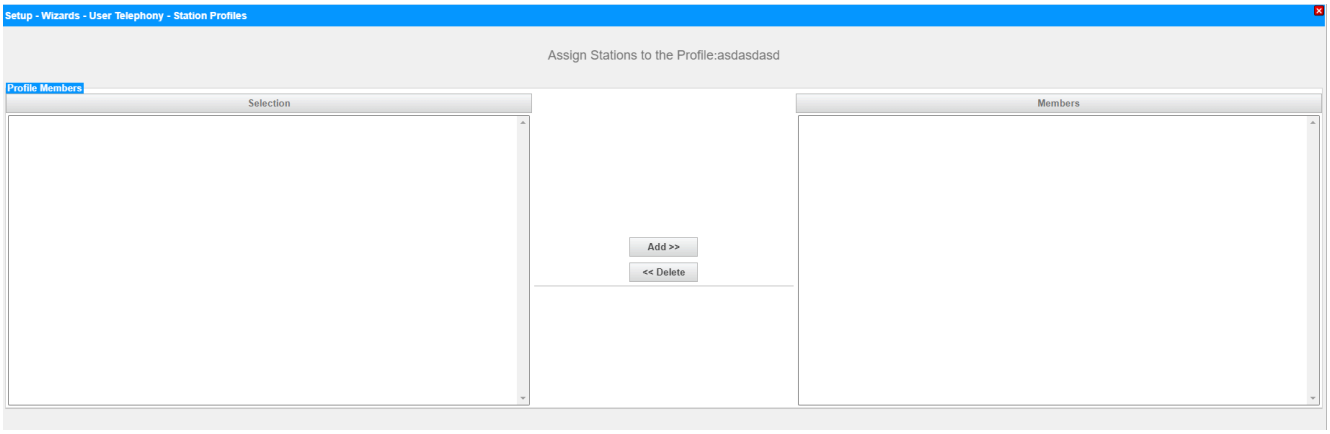
Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Profili utente**. Vengono visualizzati tutti i profili utente disponibili.



4) Nella riga del profilo utente desiderato, alla colonna **Visualizza**, indicare un nome a scelta per il profilo (max. 16 caratteri).
5) Nella riga del profilo utente desiderato, fare clic su **Assegna utenti**.



6) Dalla tabella **Membri profilo** selezionare i membri desiderati (è consentita la selezione multipla), quindi premere **Aggiungi**. Questi utenti sono assegnati al profilo apparecchio e non possono venire assegnati ad altri profili apparecchio.
7) Fare clic su **OK**.
8) Fare clic su **OK & Avanti**. Vengono visualizzati tutti i profili apparecchio disponibili e i relativi membri.
9) Fare clic su **OK & Avanti**, quindi su **Fine**.

11.14.2 Come visualizzare un profilo apparecchio e i relativi membri

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Profilo utente**. Vengono visualizzati tutti i profili utente disponibili.
4) Fare clic su **OK & Avanti**. Vengono visualizzati tutti i profili apparecchio disponibili e i relativi membri.

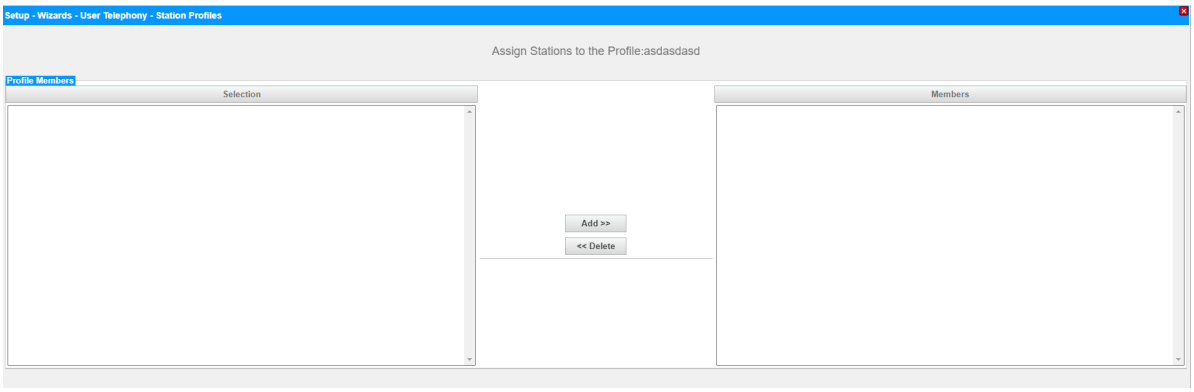
11.14.3 Come aggiungere membri a un profilo apparecchio

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Profilo utente**. Vengono visualizzati tutti i profili apparecchio disponibili e i relativi membri.
4) Nella riga del profilo apparecchio desiderato, fare clic su **Assegna utente**.



5) Dall'elenco **Membri profilo** selezionare i membri desiderati (è consentita la selezione multipla), quindi premere **Aggiungi**. Questi utenti sono assegnati al profilo apparecchio e non possono venire assegnati ad altri profili apparecchio.
6) Fare clic su **OK**.
7) Fare clic su **OK & Avanti**. Vengono visualizzati tutti i profili apparecchio disponibili e i relativi membri.
8) Fare clic su **OK & Avanti**, quindi su **Fine**.

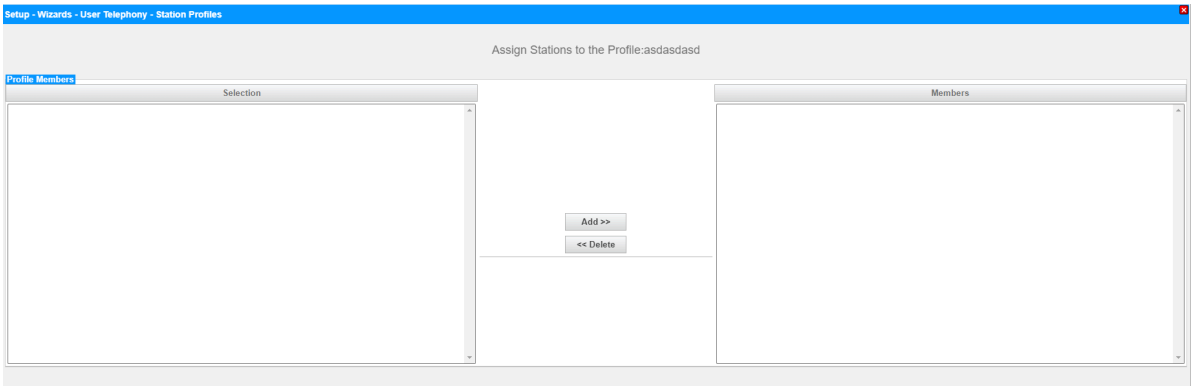
11.14.4 Come cancellare i membri da un profilo apparecchio

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Profilo utente**. Vengono visualizzati tutti i profili apparecchio disponibili e i relativi membri.
4) Nella riga del profilo apparecchio desiderato, fare clic su **Assegna utente**.



5) Dall'elenco **Membri** selezionare i membri desiderati (è consentita la selezione multipla), quindi premere **Elimina**. A questi utenti può essere assegnato un altro profilo apparecchio.
6) Fare clic su **OK**.
7) Fare clic su **OK & Avanti**. Vengono visualizzati tutti i profili apparecchio disponibili e i relativi membri.
8) Fare clic su **OK & Avanti**, quindi su **Fine**.

11.14.5 Come importare o esportare i profili dei singoli utenti

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Profilo utente**. Vengono visualizzati tutti i profili apparecchio disponibili e i relativi membri.
4) Nella riga del profilo apparecchio desiderato, fare clic su **Importa/esporta profilo**.
5) Se si desidera esportare il profilo apparecchio, fare clic su **Download** e salvare il file in una rubrica a scelta.
6) Se si desidera importare il profilo apparecchio, fare clic su **Sfoglia**, navigare fino al punto in cui è memorizzato i file e caricarlo nel sistema di comunicazione.
7) Fare clic su **OK**.

8) Fare clic su **OK & Avanti**. Vengono visualizzati tutti i profili apparecchio disponibili e i relativi membri.
9) Fare clic su **OK & Avanti**, quindi su **Fine**.

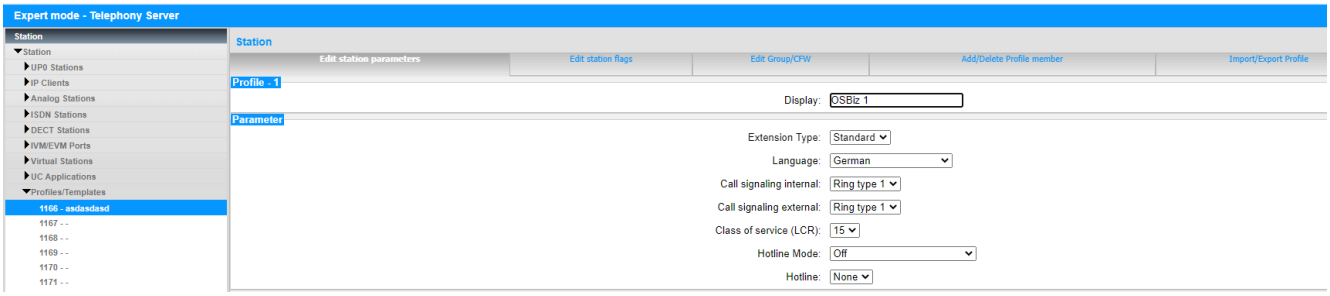
11.14.6 Come modificare i valori e le impostazioni di un profilo apparecchio

Prerequisiti

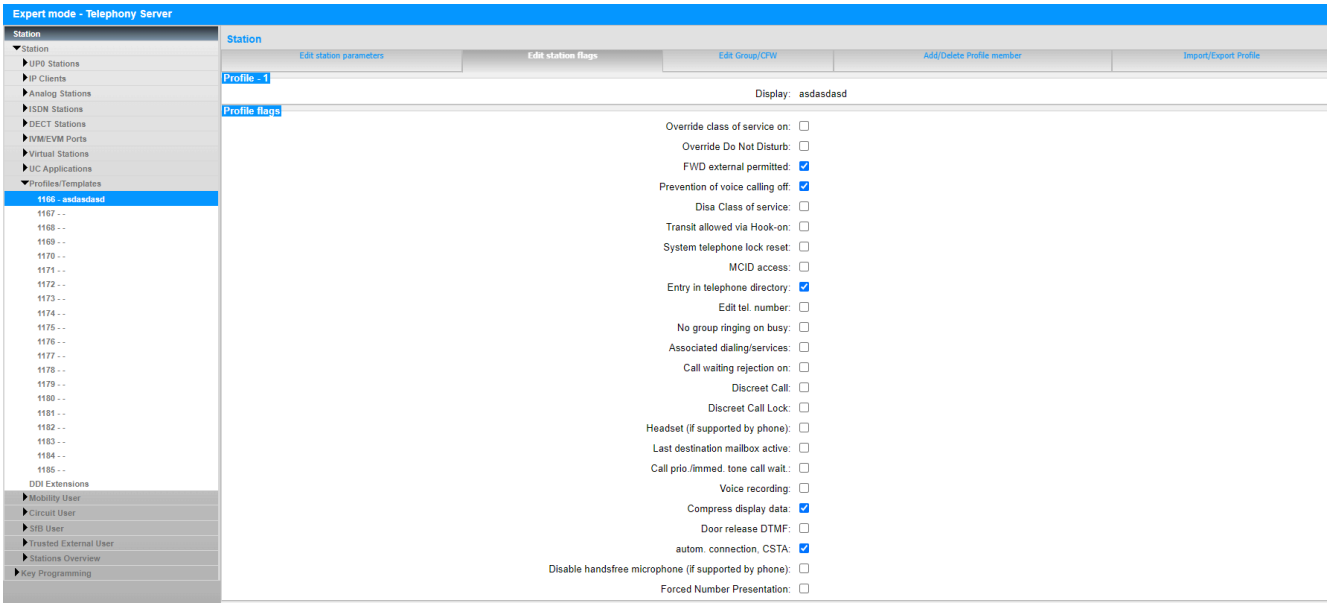
Si è connessi al WBM con il profilo **Expert**.

Passo a passo

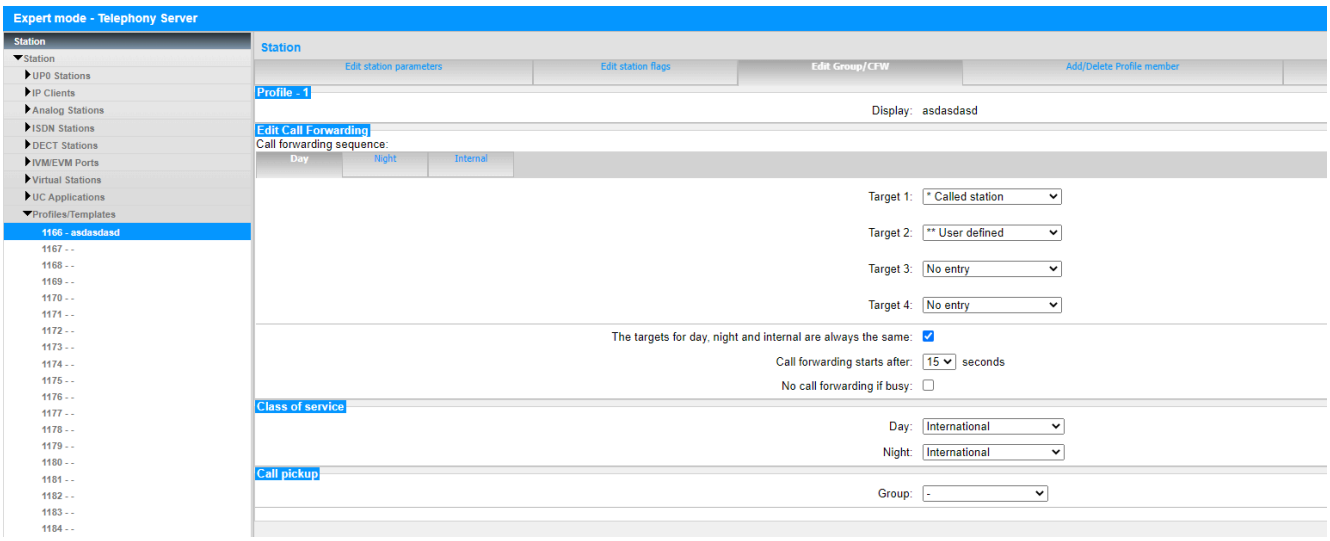
1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Utenti**.
3) Nella struttura dei menu fare clic su **Utente** > **Profili/Modelli**.
4) Nella struttura dei menu, fare clic sul numero profilo utente.



5) Se necessario, nella scheda **Parametri dell'utente**, nel campo **Nome** modificare il nome del profilo utente (max. 16 caratteri), quindi premere **Applica**.
6) Se necessario, nella scheda **Parametri dell'utente**, modificare il parametro utente desiderato per il profilo utente, quindi premere **Applica**.



7) Se necessario, nella scheda **Flag utente**, modificare il parametro utente desiderato per il profilo utente, quindi premere **Applica**.



8) Se necessario, nella scheda **Modifica gruppo/CFW**, modificare gli inoltri di chiamata desiderati per il profilo utente, quindi premere **Applica**.
9) Fare clic su **Applica**.

11.14.7 Come importare o esportare i profili di tutti gli utenti

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Nella struttura dei menu fare clic su **Utente** > **Profili/Modelli**.
4) Fare clic sulla scheda **Importa/Esporta tutti i profili**.
5) Se si desidera esportare tutti i profili apparecchio, fare clic su **Download** e salvare il file in una rubrica a scelta.
6) Se si desidera importare tutti i profili apparecchio di un file, fare clic su **Sfoglia**, navigare fino al punto in cui è memorizzato il file e caricarlo nel sistema di comunicazione.

11.15 Configurazione dati di autenticazione nel telefono SIP

I dati per l'autenticazione di un utente SIP nel sistema di comunicazione devono essere inseriti direttamente nel telefono SIP. A tale scopo, devono essere utilizzati dati inseriti nel WBM di ogni utente SIP.

I seguenti dati devono essere copiati dal WBM e registrati sul telefono SIP (in ogni telefono SIP extra):

- Password

  Password per l'autenticazione.
- SIP ID d'utente / Nome d'utente

  Nome utente per l'autenticazione.
- Realm

  Zona o dominio per l'autenticazione.

La configurazione può essere eseguita tramite il WBM del telefono SIP o direttamente sul display del telefono SIP.

11.15.1 Come configurare i dati di autenticazione tramite il WBM del telefono SIP

Prerequisiti

Il telefono SIP è collegato alla LAN.

Il PC Admin ha accesso al WBM del telefono SIP.

Si conosce l'indirizzo IP del telefono SIP.

La configurazione descritta nell'esempio si riferisce a un OpenStage 60 SIP.

Passo a passo

1) Sul PC Admin, avviare il browser Web e richiamare la pagina di accesso del WBM del telefono SIP al seguente indirizzo:

`https://<Indirizzo IP del telefono SIP>`

Nota: Se il WBM non si avvia, verificare la connessione LAN e ripetere la procedura. Se il problema persiste, verificare se l'indirizzo IP viene bloccato dal proprio firewall. Per informazioni più precise, consultare la documentazione del firewall.

---

2) Se il browser Web segnala un problema con un certificato di sicurezza, installare il certificato (nell'esempio Internet Explorer V10).

a) Chiudere il browser Web.

b) Aprire il browser Web con i diritti di amministratore facendo clic con il pulsante destro del mouse sull'icona del browser, quindi nel menu di scelta rapida selezionare la voce **Esegui come amministratore**.

c) Consentire il controllo dell'ID utente.

d) Richiamare la pagina di accesso del WBM del telefono SIP al seguente indirizzo:

```
https://<Indirizzo IP del telefono SIP>
```

e) fare clic su **Continua caricamento del sito Web**.

f) Fare clic sul messaggio **Errore certificato** nella barra di navigazione del browser Web.

g) Fare clic su **Mostra certificati**.

h) Fare clic su **Installa certificato** (visibile solo con i privilegi di amministratore).

i) Selezionare l'opzione **Computer locale** e confermare con **Avanti**.

j) Selezionare l'opzione **Salva tutti i certificati nella seguente memoria**, fare clic su **Ricerca** e immettere le **Autorità di certificazione radice attendibili**.

k) Confermare con **OK** e successivamente con **Avanti** e **Fine**.

l) Confermare l'importazione del certificato con **OK** e chiudere la finestra del certificato con **OK**.

m) Chiudere il browser Web.

n) Avviare di nuovo il browser Web (senza i diritti di amministratore) e richiamare la pagina di accesso del WBM del telefono SIP al seguente indirizzo:

```
https://<Indirizzo IP del telefono SIP>
```

3) Al primo accesso viene chiesto di inserire una password.

a) Per proteggere il sistema dall'uso improprio, nei campi **Nuova password** e **Conferma password** immettere la nuova password. Prestare attenzione alle lettere maiuscole e minuscole e allo stato del tasto **Num**. La password viene visualizzata come una serie di asterischi (*).

Nota: Tale password deve essere di almeno 6 caratteri e contenere un numero. Annotarsi esattamente la nuova password.

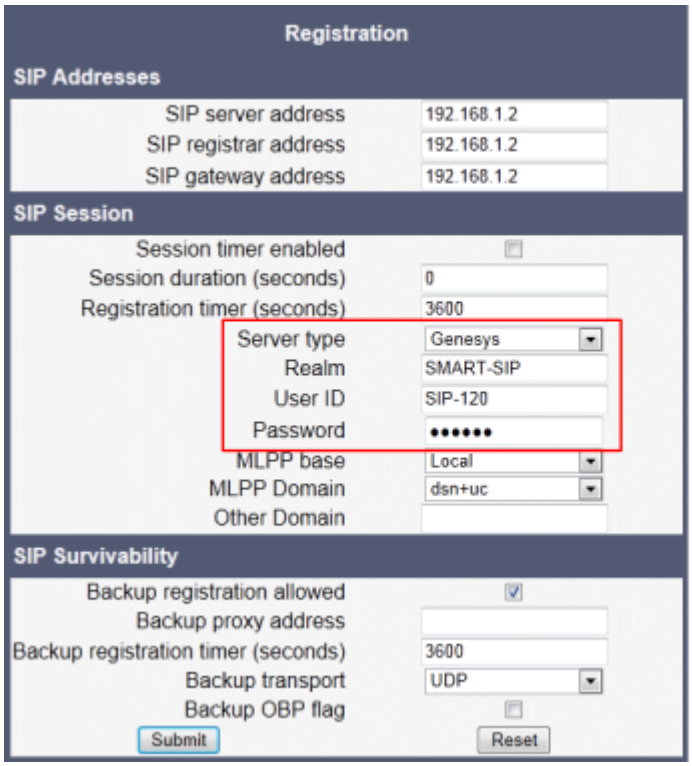
---

4) Fare clic su **OK**.

5) Fare clic sulla scheda**Pagina amministratore (Admin)**.

6) Inserire la password di amministratore (predefinita: 123456), quindi fare clic su **Accesso**..

7) Selezionare **Sistema** > **Registrazione**.



8) Nell'area **Sessione SIP**, dall'elenco a discesa **Tipo server** selezionare la voce **Genesys**.

9) Nel campo **Realm**, immettere la voce Realm specificata nella configurazione dell'utente SIP nel WBM del sistema di comunicazione (ad esempio `SMART-SIP`).

10) Nel campo **ID utente** inserire l'ID utente utilizzato per la configurazione dell'utente SIP nel WBM del sistema di comunicazione (ad esempio, `SIP-120`).

11) Nel campo **Password**, immettere la password specificata nella configurazione dell'utente SIP nel WBM del sistema di comunicazione.

12) Fare clic su **Submit**. Le modifiche vengono salvate.

13) Disconnettersi dal WBM utilizzando il pulsante **Disconnessione**.

11.15.2 Come configurare i dati di autenticazione sul display del telefono SIP

Prerequisiti

I dati di autenticazione (ID utente, password e dominio) sono noti.

La configurazione descritta nell'esempio si riferisce a un OpenStage 80 SIP.

Passo a passo

1) Per accedere alla modalità di amministrazione del telefono di sistema, premere, sul telefono, il tasto corrispondente al menu delle impostazioni/applicazioni.

2) Sfogliare nella scheda da `Impostazioni` a `Admin` e confermare con il tasto OK.
3) Immettere la password di amministratore (predefinita: `123456`) e confermare con il tasto OK.
4) Sfogliare fino a `System` (Sistema) e confermare con il tasto OK.
5) Sfogliare fino a `Registration` (Registrazione) e confermare con il tasto OK.
6) Sfogliare fino a `SIP session` (Sessione SIP) e confermare con il tasto OK.
7) Sfogliare fino a `Server type` (Tipo server) e confermare con il tasto OK.
8) Sfogliare fino a `Genesys` e confermare con il tasto OK.
9) Sfogliare fino a `Realm` e confermare con il tasto OK.
10) Immettere la voce Realm specificata nella configurazione dell'utente SIP nel WBM del sistema di comunicazione (ad esempio, `SMART-SIP`). Confermare con l'icona OK.
11) Sfogliare fino a `User ID` (ID utente) e confermare con il tasto OK.
12) Inserire l'ID utente indicato nella configurazione dell'utente SIP tramite il WBM del sistema di comunicazione (ad esempio, `SIP-120`). Confermare con l'icona OK.
13) Sfogliare fino a `Password` e confermare con il tasto OK.
14) Immettere la password specificata nella configurazione dell'utente SIP nel WBM del sistema di comunicazione. Confermare con l'icona OK.
15) Confermare la richiesta dopo aver salvato le modifiche premendo `Salva` e confermando con il tasto OK.
16) Utilizzando il pulsante Indietro, tornare al menu `Admin`.
17) Quando il telefono di sistema richiede un riavvio in seguito alle modifiche apportate, nel menu `Admin` viene visualizzata la voce `Riavvia`. Confermare `Riavvia` con il tasto OK e poi `Sì` sempre con il tasto OK. Il telefono di sistema effettua un riavvio e accede al sistema di comunicazione.

11.16 Esportazione dei dati degli utenti

I dati importanti degli utenti possono essere esportati un file XML.

Oltre ai dati dell'utente, quali ad esempio il nome e il numero di telefono degli utenti, gli indirizzi di posta elettronica e il tipo di telefono, il file XML può contenere anche altre informazioni, quali ad esempio numeri di gruppo e assegnazioni delle licenze.

Il file XML può essere modificato con un programma di tipo foglio di calcolo, ad esempio Microsoft Office Excel.

Un modello con record dati e descrizioni di esempio è disponibile nel file `csv-templates.zip` in **Centro assistenza** > **Documenti** > **Modelli CSV**.

11.16.1 Come esportare i dati degli utenti

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Configurazione**.
3) Nella struttura dei menu, fare clic su **Configurazione** > **Configurazione porta**.
4) Fare clic sulla scheda **Esportazione della configurazione**.
5) Premere il pulsante **Download**.
6) Confermare la richiesta di conferma con **OK**.
7) Fare clic su **Salva** quindi selezionare la posizione di memorizzazione del file XML.
8) Infine fare clic su **Salva**.

12 UC Smart

UC Smart è integrato in tutti i modelli di OpenScape Business (con e senza UC Booster) e offre funzioni di comunicazione unificata quali ad esempio stato presenza, messaggi vocali e conferenze.

Client per UC Smart

Le funzionalità di UC Smart possono essere utilizzate con i seguenti client:

- myPortal @work
- myPortal to go (come UC Mobile App o Web Edition)
- Application Launcher
- OpenScape Business Attendant / BLF
- Client WSI di terzi

I limiti di espansione dipendono dal modello di OpenScape Business utilizzato e dalle eventuali varianti OpenScape Business UC Booster installate.

Particolarità di UC Smart con OpenScape Business S

L'architettura di sistema di OpenScape Business S presenta le seguenti limitazioni:

- Il numero di messaggi vocali non viene visualizzato sul display del telefono (MWI).
- La casella vocale (SmartVM) non supporta le funzioni Fax, Occupato o Riconoscimento silenzio. Le connessioni fax in entrata non possono essere inoltrate a un dispositivo fax standard dopo la risposta da parte della casella SmartVM. La casella SmartVM registra per 2 minuti.
- In caso di inoltro delle connessioni tramite Company AutoAttendant (Posto operatore automatico azienda) a utenti occupati, il chiamante riceve il tono di occupato. Non è possibile lasciare un messaggio vocale.
- Se viene richiesto l'inoltro di un messaggio vocale al numero di telefono memorizzato nella casella SmartVM inoltrato (Calling Party Number), tale numero deve essere identico a quello configurato nella casella SmartVM dell'utente.
- Sia con l'UC Booster Server che con OpenScape Business S, per il collegamento alla casella vocale (SmartVM) vengono occupate linee SIPQ. Per queste linee non sono richieste licenze.
- In caso di annunci simultanei, vengono occupati canali MEB.
- Per le chiamate voce alla casella vocale (SmartVM) o ad AutoAttendant, sono disponibili 60 canali MEB.

Nota: Dopo le modifiche alla configurazione di utenti, gruppi, Mobility o altri parametri di sistema quali i codici di accesso alle linee, è necessario sincronizzare i dati UC per UC Smart o UC Suite. La sincronizzazione avviene cinque minuti dopo l'ultima modifica alla configurazione. Se una modifica alla configurazione ha luogo prima della scadenza del timer dei 5 minuti, quest'ultimo viene riavviato. I dati UC possono essere obsoleti fino all'avvio della sincronizzazione.

Concetti correlati

Funzioni UC alla pagina 92

12.1 Impostazioni di base per UC Smart

Le impostazioni di base di UC Smart possono essere personalizzate.

I client UC Smart possono essere attivati o disattivati. Se si utilizza UC Smart, deve essere disattivata la UC Suite.

Impostazione della password

L'amministratore deve assegnare a tutti gli utenti di UC Smart una password iniziale e comunicare tale password agli utenti. La password iniziale può essere la stessa per tutti gli utenti o diversa per ciascun utente. La password iniziale, deve essere modificata dall'utente al suo primo accesso a un client UC Smart. Senza l'assegnazione di una password iniziale, l'utente non può accedere a un client UC Smart.

La password inserita da parte dell'utente deve soddisfare i rigorosi criteri previsti per la creazione di password.

Impostazioni avanzate per conferenze controllate dalle applicazioni (opzionale)

L'amministratore configura nel WBM, durante l'installazione iniziale, il **Numero funzionale per conferenza MeetMe** (numero di accesso MeetMe) e almeno un **Numero funzionale per conferenza** (sala conferenze).

Per i sistemi OpenScape Business X, il numero di accesso MeetMe deve essere assegnato a una lista destinazioni chiamata in cui la prima voce è vuota e la seconda corrisponde al numero della casella vocale (SmartVM).

Per i sistemi OpenScape Business S, il numero di accesso MeetMe deve essere assegnato a una lista destinazioni chiamata in cui la prima voce corrisponde al numero della casella vocale (fascio Application Suite).

Infine, occorre assegnare al numero di accesso MeetMe anche una casella vocale standard.

La descrizione della configurazione è disponibile qui: Come configurare le conferenze controllate da applicazioni.

Assegnazioni delle licenze

L'amministratore deve assegnare a ciascun utente UC Smart User un licenza Utente UC.

In via opzionale possono essere assegnate altre licenze per:

- Casella vocale (utile anche senza UC Smart)
- Conferenza
- Application Launcher

12.1.1 Come attivare UC Smart

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Selezione applicazione**.
3) Se si desidera utilizzare UC Smart senza UC Booster Server, fare clic su **Pacchetto con UC Smart**.
4) Se si desidera utilizzare la UC Smart con UC Booster Server, fare clic su **Pacchetto con UC Smart su OSBiz UC Booster Server**, quindi nel campo **Indirizzo IP di OSBiz UC Booster Server**, inserire l'indirizzo IP del server Linux esterno.
5) Fare clic su **Applica**.

Passaggi successivi

Come configurare UC Smart

12.1.2 Come configurare UC Smart

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

In Modalità esperti, in **Selezione applicazione** il **Pacchetto con UC Smart** è attivato.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **UC Smart**.
4) Nella struttura dei menu, fare clic su **Amministrazione** > **Impostazioni di base**.
5) In **Attiva/disattiva UC Smart** selezionare la casella di controllo **Attiva**.
6) Assegnare la password iniziale in **Politica per le password**:
   a) In **Password Smart UC iniziale a livello di sistema**, fare clic su **Configura**.
   b) Nel campo **Password UC Smart iniziale per tutto il sistema** inserire la password iniziale per tutti gli utenti UC Smart.
   c) Fare clic su **Applica**.
7) Definire le linee guida per le password in **Politica per le password**:

   Nota: Per informazioni dettagliate sulle linee guida per la password, fare clic sull'icona **i**.

   - Se si desidera che le password degli utenti soddisfi i rigorosi criteri previsti per le password (opzione consigliata), selezionare la casella di controllo **Gli utenti devono immettere una password sicura**.
   - Se non si desidera che le password degli utenti soddisfi i rigorosi criteri previsti per le password (opzione non consigliata), deselezionare la casella di controllo **Gli utenti devono immettere una password sicura**.

8) Definire l'accesso al sistema in **Impostazioni di accesso**:
   - Se si desidera attivare l'accesso crittografato ai client UC Smart per il sistema (opzione consigliata se si utilizza myPortal to go tramite Internet), selezionare la casella di controllo **HTTPS**.
   - Se si desidera attivare l'accesso non crittografato ai client UC Smart per il sistema (opzione non consigliata se si utilizza myPortal to go tramite Internet), selezionare la casella di controllo **HTTP**.
9) Selezionare la casella di controllo **Salvare i dati di accesso nel terminale** se i dati di accesso devono essere salvati anche nel telefono.
10) Fare clic su **Applica**.

12.1.3 Come configurare le conferenze controllate da applicazioni

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

In Modalità esperti, in **Selezione applicazione** il **Pacchetto con UC Smart** è attivato.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Fare clic su **Modifica**, per avviare la procedura guidata **Installazione di base**.
3) Ignorare la finestra **Panoramica** premendo **OK&Avanti**. Viene visualizzata la finestra **Funzioni centrali per gli utenti**.
4) Attivare **Modifica numeri di telefono e funzionali pre-configurati**.
5) Fare clic su **Esegui funzione**. Viene visualizzata la finestra **Modifica numeri di telefono e funzionali pre-configurati**.
6) Se necessario, modificare il **Numero funzionale per conferenza MeetMe** in base alle proprie necessità.
7) Assegnare almeno un **Numero funzionale per conferenza** per la sala conferenze.
8) Fare quindi clic su **OK**. Si torna alla finestra **Funzioni centrali per gli utenti**.
9) Fare clic su **OK & Avanti**.
10) Terminare la procedura guidata confermando tutte le altre finestre con **OK&Avanti**.
11) Nella barra di navigazione fare clic su **Modalità esperti**.
12) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
13) Nella struttura dei menu fare clic su **Chiamate in entrata** > **Inoltri di chiamata**.
14) Fare clic sulla scheda **Elenchi destinazioni chiamata - Definizione**.

15) Per OpenScape Business X definire la Lista destinazioni chiamata per il numero di accesso MeetMe come segue:
    a) In **Lista destinazioni chiamata** selezionare una lista destinazioni chiamata libera, ad esempio `500`.
    b) Selezionare innanzitutto come prima destinazione **Nessuna voce** e come seconda destinazione il numero della casella vocale (ad esempio, `Gruppo VOICEMAIL 351`).
16) Per OpenScape Business S definire la Lista destinazioni chiamata per il numero di accesso MeetMe come segue:
    a) In **Lista destinazioni chiamata** selezionare una lista destinazioni chiamata libera, ad esempio `500`.
    b) Selezionare Destinazione esterna come Prima destinazione (percorso: Suite applicazione) e inserire il numero chiamata della casella vocale nel campo "Destinazione esterna".
17) Fare clic su **Applica**, quindi su **OK**.
18) Chiudere la finestra.
19) Nella barra di navigazione fare clic su **Modalità esperti**.
20) Nella struttura di navigazione, fare clic su **Telefonia** > **Connessione**.
21) Nella struttura dei menu fare clic su **Interfacciamenti** > **SmartVM**.
22) Fare clic sulla scheda **Modifica caselle postali SmartVM**.
23) Nella colonna **Numero mailbox**inserire in un campo libero il numero di accesso MeetMe per il quale occorre aggiungere la casella vocale.
24) Fare clic su **Applica**, quindi su **OK**.

12.1.4 Come rilevare gli indirizzi IP dei componenti del sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Selezione applicazione**.

   In **Selezione applicazione**, vengono visualizzati gli indirizzi IP di diversi componenti del sistema, tra cui, ad esempio, **UC Smart**, **Application Launcher**, **CSTA Connector**, **Open Directory Service**, **UC Suite** e **Web Collaboration**.

Concetti correlati

Impostazioni di base per UC Suite alla pagina 530

12.1.5 Come controllare lo stato di UC Smart

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

In Modalità esperti, in **Selezione applicazione** il **Pacchetto con UC Smart** è attivato.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **UC Smart**.
4) Nella struttura dei menu fare clic su **Amministrazione** > **Stato**.

   In **Server applicazioni** vengono visualizzate informazioni di stato su UC Smart, ad esempio **Stato**, **Versione**, **Switch telefono**, **Database**, **EVM**, **Punti di monitoraggio mancanti**, **Utenti attivi**, **Connessioni attive**, **Connessioni HTTPS attive**, **Utente Mobility Entry**, **Utente senza terminale** e **Utente bloccato**.

12.2 Client UC Smart

I client UC Smart sono interfacce che offrono funzioni di comunicazione unificata.

Il sistema offre i seguenti client UC Smart per i seguenti dispositivi:

Tipo client	Client	Tipo di terminale
Client di comunicazione	myPortal @work	PC
Client mobile	myPortal to go (UC Smart) (vedere Mobilità alla pagina 944)	Smartphone, tablet-PC
Client di comunicazione	OpenScape Desk Phone CP 400/600/600E/ 700/700X/710 HFA (client integrato nel software del telefono)	OpenScape Desk Phone CP 400/600/600E/ 700/700X/710 HFA

12.2.1 myPortal @work

myPortal @work è un'applicazione di comunicazione unificata (Microsoft Windows e Mac OS X) che combina tutte le funzionalità e i servizi necessari, come la composizione rapida tramite elenchi telefonici, preferiti, conversazioni e informazioni sullo stato di presenza dei colleghi, in un'unica soluzione progettata per accelerare la comunicazione quotidiana, migliorare il lavoro di team ed entrare in contatto veloce con colleghi, clienti e partner.

myPortal @work può essere utilizzato nella modalità UC Smart o UC Suite. A seconda della modalità, le caratteristiche offerte nell'interfaccia utente sono diverse. Non è possibile modificare la modalità operativa, in quanto è impostata dall'amministratore del sistema. In caso di dubbi sulla modalità operativa corrente del client myPortal @work, richiedere le informazioni all'amministratore di sistema.

myPortal @work offre un client di telefonia Voice over IP (VoIP) integrato. Se l'opzione VoIP è attivata, le caratteristiche relative alle chiamate vocali del client myPortal @work usano la funzionalità VoIP.

Nota: Per usare la funzionalità Voce over IP (VoIP), l'utente deve essere configurato come client di sistema.

Per l'uso di Voice over IP (VoIP) remoto con Del DispositivoSistema@Home, vedere 1 Configurazione del DispositivoSistema@Home

La funzionalità VoIP supporta una serie di funzioni in aggiunta alle funzioni UC:

- Esecuzione di una chiamata
- Risposta a una chiamata
- Termine di una chiamata
- Consultazione
- Trasferimento dopo la risposta
- Trasferimento nascosto
- Devia
- Devia a casella vocale
- Richiamata automatica (la visualizzazione della notifica per una richiamata non è ancora supportata)
- Richiamata alternata
- Attivazione/disattivazione silenziamento (solo per la funzionalità VoIP)
- Conferenza sistema
- Rifiuto dell'avviso di chiamata
- Richiamata automatica su occupato
- Non disturbare (DND)
- DTMF
- Risposta per assente

Nota: Poiché il client myPortal@Work non supporta la funzionalità di inviare toni DTMF a un altro utente, l'invio di un tono DTMF tramite il comando CSTA "generateDigits" non è rispettivamente supportato e tale richiesta sarà negata e respinta dal sistema.

Lavoro in team:

Il client myPortal @work VoIP può inoltre essere usato in:

- Gruppo (ad es., Lineare, Chiamata in attesa)
- MULAP come membro MULAP

Per il sistema di comunicazione è supportata anche la crittografia segnalazione e payload (SPE). Il client VoIP usa lo stack di sicurezza moderno WebRTC, quindi permette un trasferimento di dati sicuro mediante DTLS.

Nota: Anche la configurazione SDES ITSP è supportata.

I codici di servizio possono essere avviati dalla barra di ricerca ma non sono supportati in caso di problemi. Non viene fornito feedback sull'esecuzione corretta o non corretta dei codici di servizio, pertanto si consiglia vivamente di utilizzare le opzioni di input fornite dall'interfaccia utente di myPortal @work per controllare le caratteristiche rispettive.

myPortal @work in modalità UC Suite può essere usato non solo come sistema indipendente ma anche in combinazione con myPortal for Desktop/Outlook, myAgent, myAttendant Client (CTI, preferiti e conversazioni). Anche le licenze Utente UC esistenti possono essere usate con myPortal @work.

La descrizione seguente si riferisce principalmente a myPortal@word in modalità UC Smart. Le differenze rispetto alla modalità UC Suite sono descritte nelle Istruzioni per l'uso di myPortal @work.

myPortal @work supporta solitamente le seguenti caratteristiche:

- Stato presenza
- Deviazione di chiamata basata sullo stato
- Rubriche compresa la ricerca per nome
- Preferiti
- Conversazioni: nel client vengono visualizzate fino a 25 conversazioni e ogni conversazione ha fino a 50 voci
- Conferenze
- Tasto di scelta rapida composizione/Tasto di scelta rapida ricerca/ Collegamenti ipertestuali telefonici
- Funzioni chiamata tramite:
  1) Dispositivo telefonico associato
  2) Client Integrated Voice over IP
- Controllo casella vocale
- Zoom In / Zoom Out
- Condivisione schermo tramite collaborazione Web Collaboration (opzionale)

Uso di myPortal @work in ambiente Microsoft Terminal Server

myPortal @work viene rilasciato per le funzionalità UC e CTI negli ambienti Microsoft Terminal Server con le seguenti limitazioni:

- I collegamenti ipertestuali telefonici e la funzionalità Fai clic per chiamare non sono supportati
- La funzionalità Avvia applicazione al lancio non è supportata
- Il caricamento dell'immagine dell'utente non è supportato
- Le funzionalità Ancora/Disancora, Blocca/Sblocca e Riduci a icona sulla barra delle applicazioni sono limitate
- La funzionalità VoIP non è supportata

12.2.1.1 Requisiti richiesti per myPortal @work

Per poter utilizzare il client UC, il PC client deve disporre di una dotazione hardware e software adeguata. In base alla configurazione, per l'installazione e gli aggiornamenti automatici sono necessari diritti di amministratore. La gamma di funzioni utilizzabili dipende dalle licenze utilizzate.

I requisiti seguenti sono necessari per installare myPortal @work:

- Diritti di amministratore
- Programma di configurazione software di myPortal @work
- Indirizzi IP e porte del sistema di comunicazione
- Indirizzo FQDN o IP, porta per connessione WAN (Dispositivo@Home)

- Dati di accesso (Utente e Password) per il proprio account utente UC nel sistema di comunicazione
- Informazioni sull'account di casella vocale (facoltativo)
- Numero di telefono MULAP nel caso di assegnazione di più numeri (facoltativo)
- Windows OS e Apple Mac OS X

Nota: È necessario attivare TLS 1.2 in Opzioni Internet (nel Pannello di controllo) e installare o attivare manualmente le patch più recenti di Microsoft.

Se non si eseguono le azioni precedenti, l'accesso HTTPS viene respinto.

Telefoni

myPortal @work può essere utilizzato in combinazione con i seguenti telefoni:

Nota: myPortal @work può anche essere utilizzato come sistema indipendente, usando la funzionalità VoIP, senza un dispositivo fisico.

- OpenStage HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/410/710 HFA
- Telefoni analogici
- Telefoni ISDN
- Openscape Personal Edition HFA
- OpenStage M3 (OpenScape Business Cordless)
- OpenScape DECT Phone S6/SL6/R6 (OpenScape Business Cordless)

Sono supportati i dispositivi precedenti (ad esempio, optiPoint 410/420/500 e Gigaset M2/SL3/S4/SL4/S5). I dispositivi Optiset E non possono essere utilizzati. Per i dispositivi testati e approvati, consultare le rispettive release note.

Nota: Il client integrato OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA non presenta pre-requisiti particolari, tranne la configurazione e la licenza client standard.

I "Preferiti" nel menu telefonico contengono dei tasti programmabili liberamente e non sono collegati ai Preferiti UC. È possibile trovare i dettagli relativi a tali tasti e le istruzioni nella documentazione del dispositivo.

Nota: Con i telefoni analogici e DECT, non è supportato il LED mailbox e la visualizzazione di informazioni a display è supportata solo in modo limitato.

Browser Web

Per la programmazione dei pulsanti dei telefoni sul client UC sono stati approvati i seguenti browser Web:

- Microsoft Internet Explorer Versione 10 (o successiva)
- Mozilla Firefox 19 (o successivo)
- Google Chrome

File di installazione

L'amministratore può scaricare i file di installazione dal **Centro assistenza** > **Software** e metterli a disposizione degli utenti, ad esempio tramite un'unità di rete.

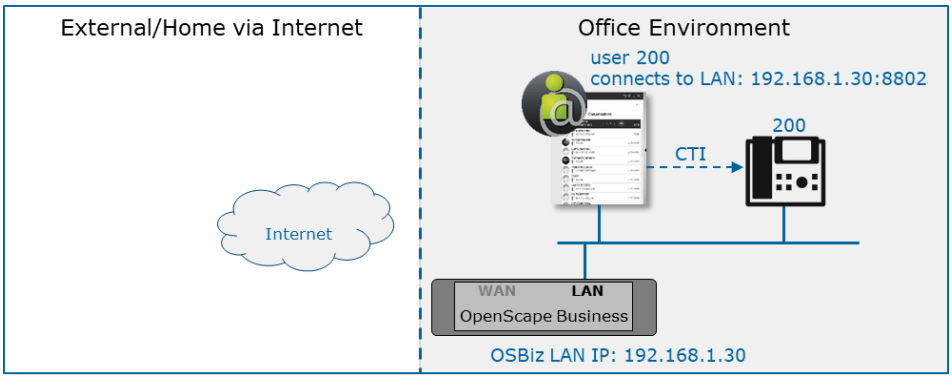
12.2.1.2 Configurazione utente myPortal @work

myPortal @work è una combinazione di un client UC e un client VoIP e queste due funzionalità richiedono le seguenti configurazioni/licenze basate su diverse modalità UC (Smart/UC Suite) e casi d'uso.

Nota: Quando un account utente myPortal @work viene bloccato dopo diversi tentativi di accesso errati, in modalità UC Suite, non è visibile nella Rubrica utente di UC Suite. È possibile visualizzare gli utenti di myPortal @work bloccati in **Modalità esperti > Web Services > Web Services Assistant > Gestione utenti** ma si possono sbloccare questi account in **Modalità esperti > OpenScape Business UC Suite > Rubrica utente**.

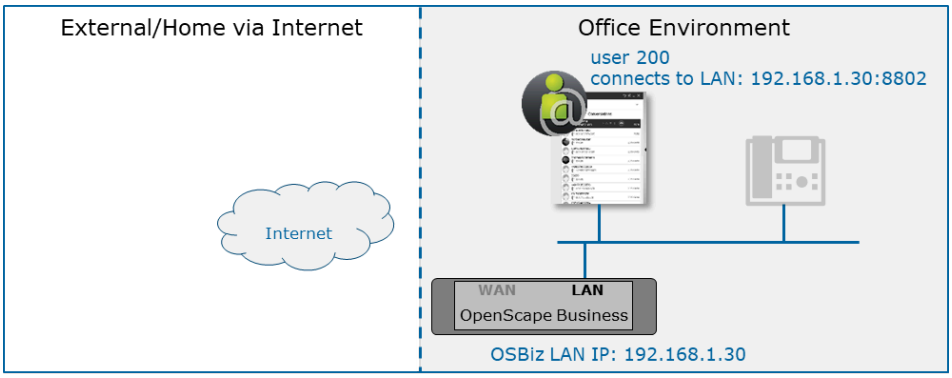
Configurazione LAN locale - Solo client UC e CTI

myPortal @work viene utilizzato come client UC e CTI per un telefono da scrivania associato senza VoIP.



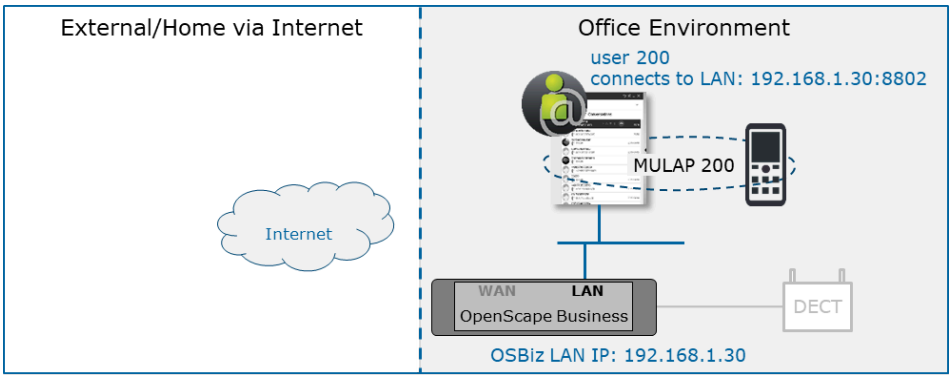
- Licenze: Utente UC o Utente Groupware
- Accesso a myPortal @work: nella schermata di accesso, impostare il proprio nome utente/password/indirizzo IP LAN:8802

Configurazione LAN locale - Client UC e VoIP



- Licenze: Licenza Utente IP e Utente UC o Groupware
- Accesso a myPortal @work: nella schermata di accesso, impostare il proprio nome utente/password/indirizzo IP LAN:8802
- Registrazione di myPortal @work VoIP: Dopo aver effettuato correttamente l'accesso, occorre andare su Impostazioni > VoIP> Attiva VoIP
- La connettività STUN nel client non è necessaria per le connessioni interne pure. Tuttavia, si rende necessaria in alcuni scenari ibridi con altri utenti che utilizzano myPortal @work VoIP tramite Internet pubblico. Per verificare la connettività STUN, andare su Impostazioni > VoIP > Impostazioni ICE avanzate > Verifica stato ICE.

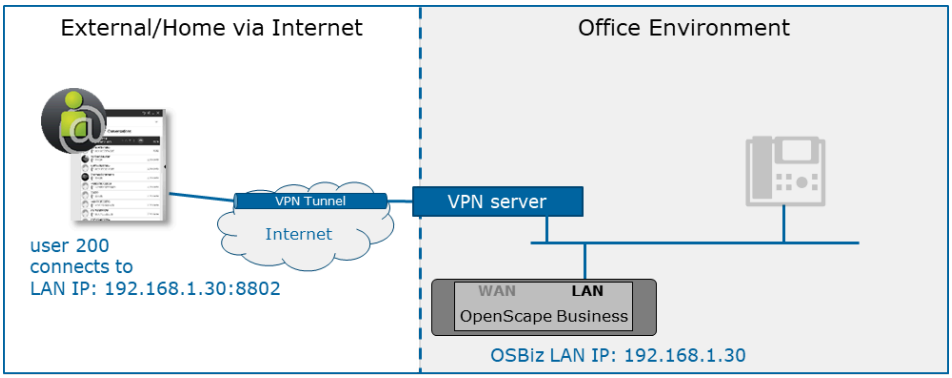
Configurazione utente MULAP (LAN locale)



- Licenze:
  - myPortal @work: Licenza Utente IP e Utente UC o Groupware
  - altro dispositivo MULAP - in questo esempio DECT: Licenza Utente TDM o Utente IP (la configurazione MULAP è consigliata per la combinazione con dispositivi TDM o DECT, ma può essere utilizzata anche con un dispositivo IP. In caso di dispositivo IP, vedere anche le sezioni Utente Deskshare tramite LAN locale alla pagina 493 e Utente Deskshare remoto tramite VPN alla pagina 494).
- Accesso a myPortal @work: nella schermata di accesso, impostare il proprio nome utente/password del numero MULAP/indirizzo IP LAN:8802
- Registrazione di myPortal @work VoIP: Dopo aver effettuato correttamente l'accesso, occorre andare su Impostazioni > VoIP> selezionare il telefono assegnato e infine Attiva VoIP
- La connettività STUN nel client non è necessaria per le connessioni interne pure. Tuttavia, si rende necessaria in alcuni scenari ibridi con altri utenti che

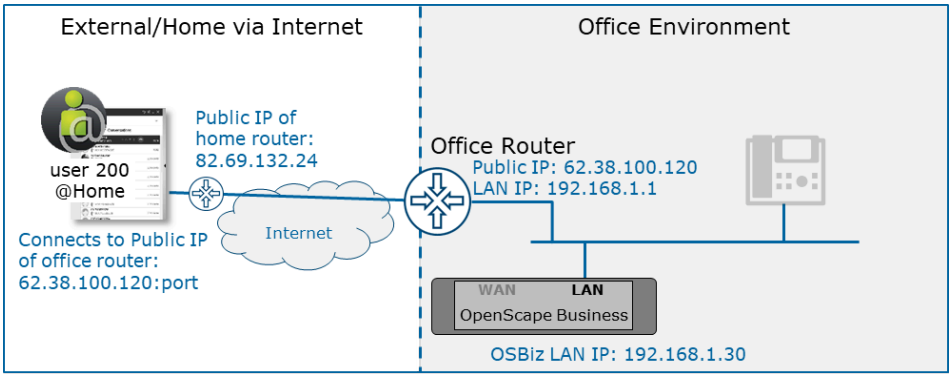
utilizzano myPortal @work VoIP tramite Internet pubblico. Per verificare la connettività STUN, andare su **Impostazioni > VoIP > Impostazioni ICE avanzate > Verifica stato ICE**.

Utente domestico con configurazione della connessione VPN



- Licenze: Licenza Utente IP e Utente UC o Groupware
- Accesso a myPortal @work: nella schermata di accesso, impostare il proprio nome utente/password/indirizzo IP LAN:8802
- Registrazione di myPortal @work VoIP: Dopo aver effettuato correttamente l'accesso, occorre andare su Impostazioni > VoIP> Attiva VoIP
- La connettività STUN è obbligatoria. Per verificare la connettività STUN, andare su Impostazioni > VoIP > Impostazioni ICE avanzate > Verifica stato ICE.

myPortal @work tramite Internet pubblico

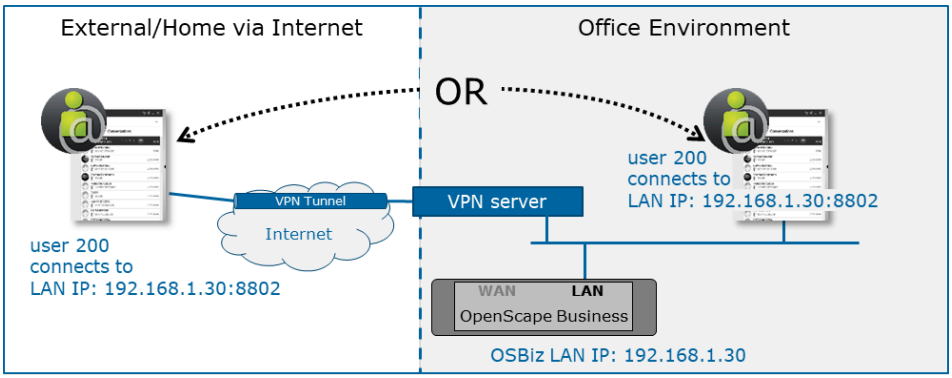


- Licenze: Licenza Utente IP e Utente UC o Groupware
- Accesso a myPortal @work: nella schermata di accesso, impostare il proprio nome utente/password/indirizzo IP pubblico:porta configurata dall'amministratore.
- Registrazione di myPortal @work VoIP: Dopo aver effettuato correttamente l'accesso, occorre andare su Impostazioni > VoIP> Attiva VoIP
- Preparare l'ambiente di rete come descritto nel capitolo Passaggi di configurazione per utilizzare myPortal @work via Internet alla pagina 496
- Il flag SBC non è richiesto per myPortal @work. È necessario solo se si utilizza un dispositivo hardware.
- Non utilizzare l'interfaccia WAN OSBiz per la connessione a Internet quando si utilizza myPortal @work tramite IP pubblico. In caso contrario, l'SBC interno rileverà l'indirizzo IP pubblico dell'interfaccia WAN e lo utilizzerà

nella comunicazione tra client e OSBiz, comportando problemi di payload. Configurazione proposta: Connettere l'ITSP tramite l'interfaccia LAN. È possibile farlo tramite il normale router ISP o tramite un secondo router e route statiche.

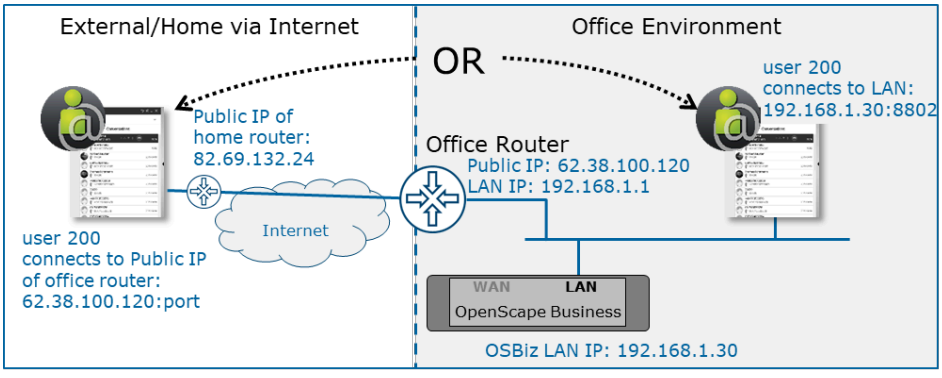
- È necessaria la connettività STUN. Per verificare la connettività STUN, andare su Impostazioni > VoIP > Impostazioni ICE avanzate > Verifica stato ICE.

Utente domestico con configurazione VPN e LAN locale (ad es. spostamento dall'ufficio a casa e viceversa)



- Licenze: Licenza Utente IP e Utente UC o Groupware
- Accesso a myPortal @work: nella schermata di accesso, impostare il proprio nome utente/password/indirizzo IP LAN:8802
- Registrazione di myPortal @work VoIP: Dopo aver effettuato correttamente l'accesso, occorre andare su Impostazioni > VoIP> Attiva VoIP
- myPortal @work può essere utilizzato in entrambi gli ambienti senza modificare le impostazioni.
- È obbligatoriamente necessaria la connettività STUN. Per verificare la connettività STUN, andare su Impostazioni > VoIP > Impostazioni ICE avanzate > Verifica stato ICE.

myPortal @work tramite configurazione Internet pubblico e LAN locale (ad es. spostamento dall'ufficio a casa e viceversa)



- Licenze: Licenza Utente IP e Utente UC o Groupware
- Accesso a myPortal @work: nella schermata di accesso, impostare il proprio nome utente/password/indirizzo IP LAN:8802 e indirizzo IP pubblico:porta configurata dall'amministratore. Configurando entrambi gli indirizzi non è necessario utilizzare un secondo profilo quando ci si sposta dall'ufficio a casa e viceversa.

- Registrazione di myPortal @work VoIP: Dopo aver effettuato correttamente l'accesso, occorre andare su Impostazioni > VoIP> Attiva VoIP
- Preparare l'ambiente di rete come descritto nel capitolo Passaggi di configurazione per utilizzare myPortal @work via Internet alla pagina 496
- Il flag SBC non è richiesto per myPortal @work. È necessario solo se si utilizza un dispositivo hardware.

Per la registrazione VoIP

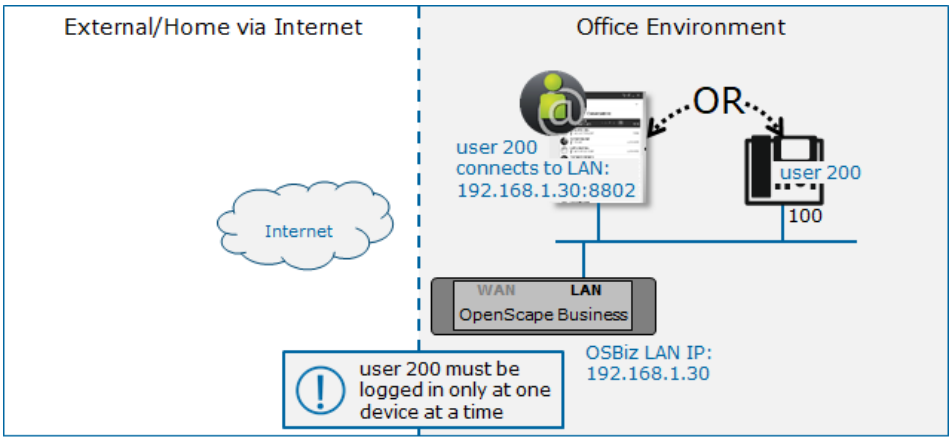
Nel caso in cui si utilizzi sia l'utente locale che quello domestico, l'utente deve disporre di una sola connessione VoIP a casa o in ufficio.

Per UC

Quando l'utente desidera essere connesso in UC contemporaneamente in più di un luogo:

- Modalità UC Smart: Il client UC può essere connesso contemporaneamente da casa e dall'ufficio, ma in questo scenario è supportato un solo client VoIP e la registrazione della funzionalità VoIP dell'altro client deve essere annullata.
- Modalità UC Suite: Verificare il paragrafo "Combinazione di myPortal @work con altri client UC Suite e configurazione della licenza". È consentito un solo client myPortal @work.

Utente Deskshare tramite LAN locale



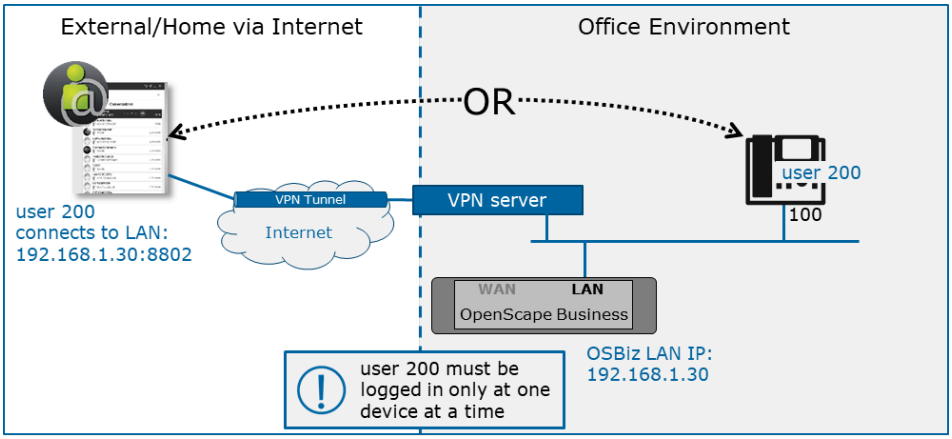
- Licenze: Licenza Deskshare e licenza Utente UC o Groupware
- Accesso a myPortal @work: nella schermata di accesso, impostare l'accesso del nome utente dell'interno Deskshare/password/indirizzo IP LAN:8802
- Registrazione di myPortal @work VoIP: Dopo aver effettuato correttamente l'accesso, occorre andare su Impostazioni > VoIP> Attiva VoIP

Esempio: Il dispositivo utilizza un numero fittizio = "100" Connettersi a "100" con il telefono da scrivania come Deskshare, ad es. 200 utilizzando il codice di servizio *9419.

Per utilizzare myPortal @work con l'utente 200, il telefono da scrivania viene disconnesso automaticamente e torna al numero fittizio "100". Quando si torna di nuovo al telefono da scrivania, assicurarsi che myPortal @work non sia registrato (# l'utente deve uscire dall'applicazione o disconnettersi).

Utente Deskshare remoto tramite VPN

La stessa configurazione descritta nel capitolo Utente Deskshare tramite LAN locale alla pagina 493 è supportato anche per l'utente domestico tramite VPN.



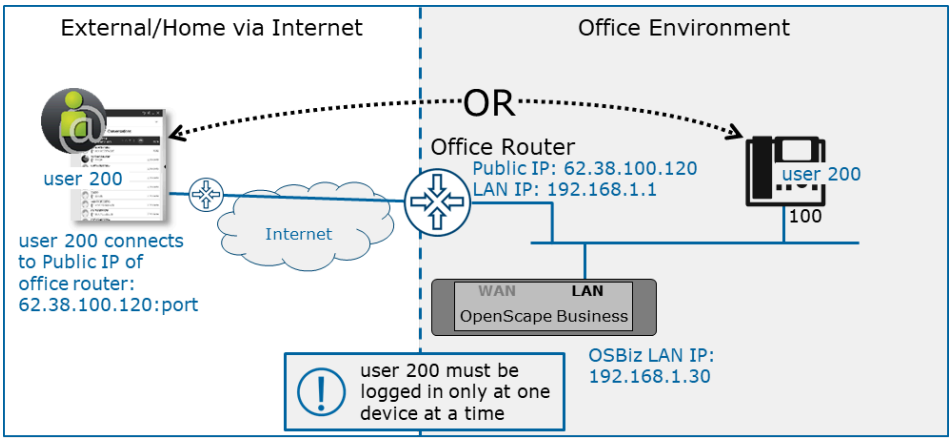
- Licenze: Licenza Deskshare e licenza Utente UC o Groupware
- Accesso a myPortal @work: nella schermata di accesso, impostare l'accesso del nome utente dell'interno Deskshare/password/indirizzo IP LAN:8802
- Registrazione di myPortal @work VoIP: Dopo aver effettuato correttamente l'accesso, occorre andare su Impostazioni > VoIP> Attiva VoIP

Esempio: Il dispositivo utilizza un numero fittizio = "100" Connettersi a "100" con il telefono da scrivania come Deskshare, ad es. 200 utilizzando il codice di servizio *9419.

Per utilizzare myPortal @work con l'utente 200, il telefono da scrivania viene disconnesso automaticamente e torna al numero fittizio "100". Quando si torna di nuovo al telefono da scrivania, assicurarsi che myPortal @work non sia registrato (# l'utente deve uscire dall'applicazione o disconnettersi).

Utente Deskshare remoto tramite Internet pubblico

La stessa configurazione descritta nel capitolo Utente Deskshare tramite LAN locale alla pagina 493 è tecnicamente possibile anche con utenti domestici tramite Internet pubblico. Tuttavia, questa configurazione non è ancora completamente testata e quindi descritta in via preliminare in questa versione del documento.



- Licenze: Licenza Deskshare e licenza Utente UC o Groupware
- Accesso a myPortal @work: nella schermata di accesso, impostare l'accesso del nome utente dell'interno Deskshare/password/indirizzo IP LAN:8802
- Registrazione di myPortal @work VoIP: Dopo aver effettuato correttamente l'accesso, occorre andare su Impostazioni > VoIP> Attiva VoIP

Esempio: Il dispositivo utilizza un numero fittizio = "100" Connettersi a "100" con il telefono da scrivania come Deskshare, ad es. 200 utilizzando il codice di servizio *9419.

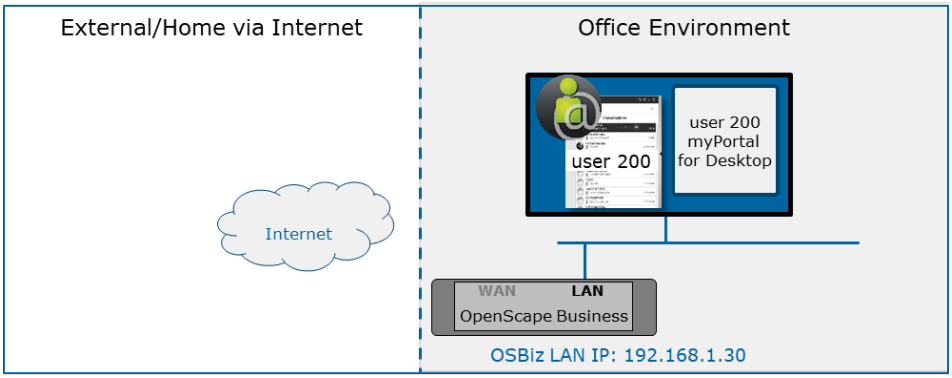
Per utilizzare myPortal @work con l'utente 200, il telefono da scrivania viene disconnesso automaticamente e torna al numero fittizio "100". Quando si torna di nuovo al telefono da scrivania, assicurarsi che myPortal @work non sia registrato (# l'utente deve uscire dall'applicazione o disconnettersi).

Combinazione di myPortal @work con altri client UC Suite e configurazione della licenza

Nota: Le configurazioni descritte in questo capitolo sono supportate anche per l'utente domestico tramite VPN.

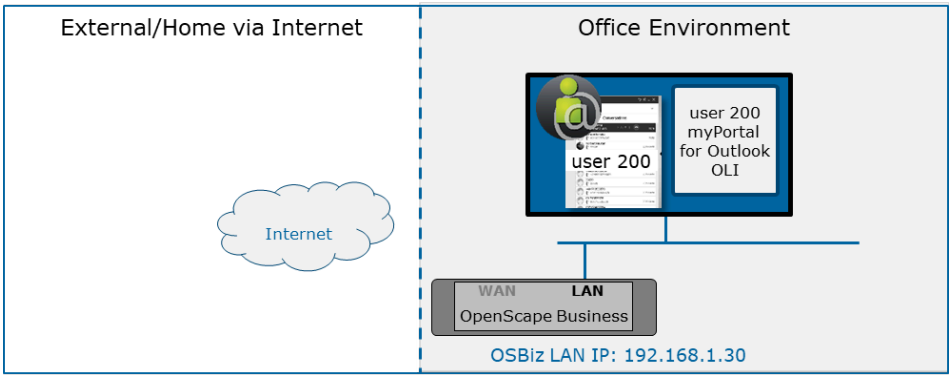
Licenza Utente UC

Lo stesso utente può essere connesso in parallelo con myPortal @work e myPortal for Desktop.



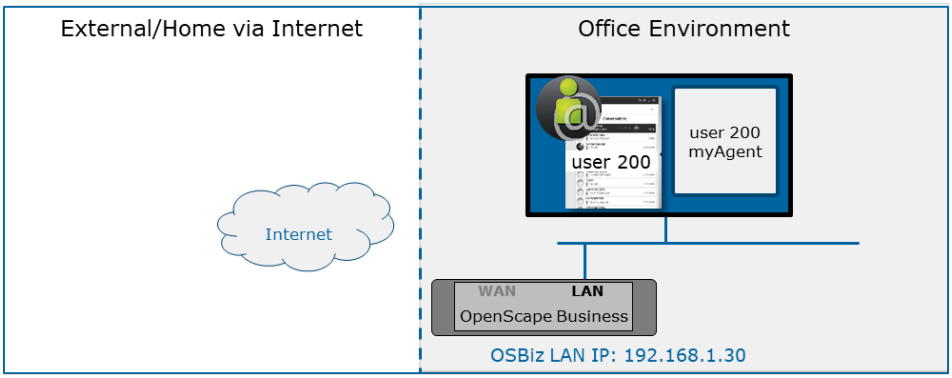
Licenza Groupware

Lo stesso utente può essere connesso in parallelo con myPortal @work e OLI.



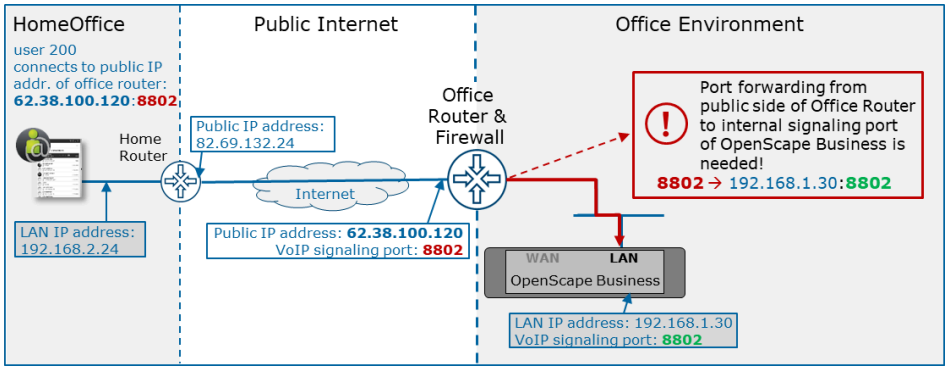
Combinazione di licenza IP, Utente UC e myAgent

myAgent e myPortal @work VoIP possono essere utilizzati come softphone in parallelo.



12.2.1.3 Passaggi di configurazione per utilizzare myPortal @work via Internet

Per poter utilizzare myPortal @work da Internet, OpenScape Business deve quindi essere accessibile anche da Internet. Per tutti gli esempi di questo capitolo, si presume il seguente scenario di rete di base.



Descrizione dello scenario di rete

OpenScape Business si trova all'interno dell'ambiente dell'ufficio, che è connesso a Internet tramite il router dell'ufficio. Questo router è accessibile da Internet tramite l'indirizzo IP pubblico "62.38.100.120" o tramite un nome DNS.

Il client myPortal @work è connesso alla LAN all'interno di una rete domestica o esterna, che è connessa a Internet tramite un router separato. Il router esterno è accessibile da Internet con l'indirizzo IP pubblico "82.69.132.24".

Passaggi di configurazione

Per utilizzare il client myPortal @work su OpenScape Business tramite Internet, è necessario configurare di conseguenza i seguenti componenti.

OpenScape Business all'interno dell'ufficio

Supporto STUN attivo sul sistema se non è già stato fatto per un ITSP.

Configurare l'utente myPortal @work (il flag SBC non è necessario per il VoIP)

Router dell'ufficio

Poiché il client myPortal @work deve raggiungere OpenScape Business da Internet e viceversa, è necessario eseguire la seguente configurazione sul router dell'ufficio perché ciò avvenga:

- Inoltro alla porta HTTPS dalla porta esterna (il valore predefinito è 8802) alla porta interna 8802 del sistema
  - Porta esterna (l'impostazione predefinita è 8802) -> Router per ufficio -> 192.168.1.30:8802

Per ulteriori informazioni, vedere anche il capitolo Porte e impostazioni firewall alla pagina 497

myPortal @work/ router esterno

Il client myPortal @work deve connettersi all'indirizzo IP pubblico o DNS del router Internet dell'ufficio sulla porta esterna, che è per impostazione predefinita 8802 (visto l'inoltro alla porta configurato in precedenza, questo punterà a OpenScape Business all'interno della rete dell'ufficio).

Nella maggior parte dei casi non è necessario configurare nulla di aggiuntivo sul router esterno, ma in caso di problemi, vedere il capitolo Porte e impostazioni firewall alla pagina 497.

12.2.1.4 Altri suggerimenti & impostazioni di configurazione

Impostazioni del server STUN

Per maggiori informazioni su come configurare il server STUN, vedere il capitolo "Configurazione STUN" nella guida "Come configurare il sistema device@home" e OpenScape Business V3, myPortal @work, Guida utente sezione "Come aggiungere un server STUN"

Cuffie

È possibile utilizzare ogni dispositivo audio/microfono rilevato nel sistema operativo.

Integrazione cuffie Jabra/Plantronics

In caso di problemi con l'integrazione cuffie Jabra, eseguire l'applicazione con i diritti di amministratore.

Per utilizzare l'integrazione cuffie Jabra, il dispositivo Jabra deve essere impostato come dispositivo microfono principale in myPortal @work.

Per l'integrazione di Plantronics, è necessario installare l'hub Plantronics.

Porte e impostazioni firewall

Fondamentalmente, per le segnalazioni myPortal @work è necessario configurare le seguenti porte:

- Funzionalità UC & segnalazione WebRTC/VoIP: 8802
- Porta server STUN predefinita: 3478. Se è configurato un server STUN personalizzato, potrebbe essere necessaria una porta diversa.

La configurazione delle porte per il payload WebRTC/VoIP dipende dal tipo di firewall utilizzato nell'ambiente del cliente. Per eseguire myPortal @work in un ambiente di rete del cliente, è fondamentale comprendere e verificare il tipo

di firewall utilizzato, se con stato o senza stato, e configurare le impostazioni firewall insieme all'amministratore IT responsabile.

Per comprendere meglio le differenze tra i due tipi di firewall, leggere quanto segue:

- I firewall senza stato sono progettati per proteggere le reti in base a informazioni statiche come origine e destinazione.
- Un firewall con stato è un firewall che monitora lo stato completo delle connessioni di rete attive. Ciò significa che i firewall con stato analizzano costantemente il contesto completo del traffico e dei pacchetti di dati.

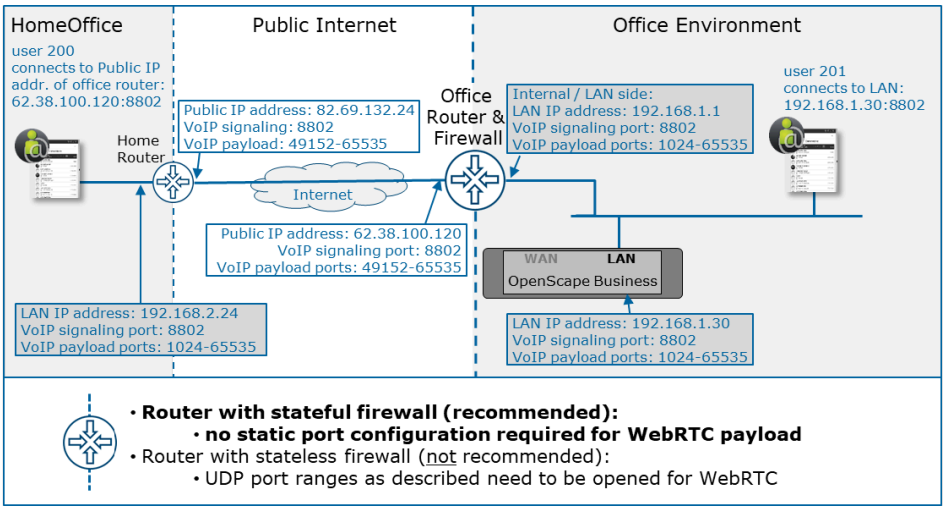
Per ulteriori informazioni su questi tipi di firewall, fare riferimento a Internet o alla documentazione tecnica pertinente come fonte di informazioni.

Si presuppone che verrà utilizzato un dispositivo firewall/NAT con stato per proteggere meglio le reti dei clienti privati, ossia che questo dispositivo deve consentire connessioni interne in uscita verso la loro destinazione.

Il dispositivo firewall/NAT bloccherà eventuali pacchetti in entrata, a meno che non appartengano a una sessione già stabilita (su una porta temporanea/dinamica) precedentemente stabilita in uscita.

In termini di utilizzo della porta, non è necessario configurare nulla all'interno del dispositivo firewall/NAT poiché questo verrà gestito e negoziato automaticamente quando si utilizza un firewall con stato.

L'utilizzo di un firewall con stato è il percorso consigliato e più sicuro per eseguire soluzioni VoIP basate su WebRTC.



In termini di firewall senza stato (che non sarà consigliato per il VoIP), è necessario aprire il seguente intervallo di porte di origine UDP per i dispositivi all'interno della rete del cliente per il traffico payload interno: 1024-65535.

Per tutto il traffico payload scambiato via Internet, la tecnologia WebRTC utilizza le porte dell'intervallo di porte UDP di 49152-65535. Per ulteriori informazioni, fare riferimento alla documentazione tecnica pertinente come fonte di informazioni.

Ciascun dispositivo di rete sul percorso tra gli endpoint di payload coinvolti deve essere configurato di conseguenza (ad es. router, firewall, NAT, proxy, ecc.).

Dato l'ampio intervallo di porte da aprire, il firewall senza stato non può essere raccomandato per il VoIP.

Tabella 4:

	Firewall con stato	Firewall senza stato da aprire in modo statico
Porta di segnalazione WebRTC/VoIP	8802	8802
Payload WebRTC/VoIP Intervallo di porte UDP all'interno della LAN locale, ovvero all'interno dell'ambiente del cliente	dinamico[4]	1024-65535
Payload WebRTC/VoIP Intervallo di porte UDP utilizzato su Internet pubblico	dinamico[4]	49152-65535

Limitazioni su VoIP

- In scenari con più chiamate (ad es. trasferimento, conferenza, avviso di chiamata in attesa) si consiglia di disattivare l'integrazione cuffie in caso di errore. Disattivando il flag dell'integrazione cuffie all'interno di myPortal @work, non è possibile utilizzare solo la funzionalità di controllo delle chiamate delle cuffie, ma le cuffie possono comunque essere utilizzate come dispositivo audio.
- La funzionalità "Postazioni libere" di myAgent (l'agente può selezionare il telefono da utilizzare tramite un menu a discesa durante la procedura di accesso), ovvero la selezione libera di un dispositivo fisico da parte di un agente, non è supportata in combinazione con myPortal @work.
- La configurazione NAT simmetrico non è supportata.
- I firewall restrittivi non sono supportati.

12.2.1.5 Guida alla risoluzione dei problemi

Timeout connessione

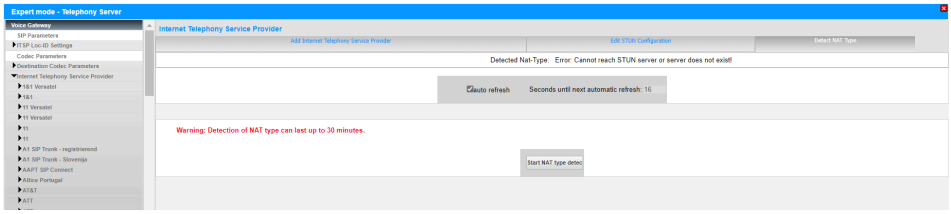
- Come utente domestico con connessione VPN, occorre verificare che l'utente possa accedere all'indirizzo LAN del sistema e connettersi all'indirizzo LAN: porta 8802. Messaggio di risoluzione dei problemi: Messaggio di errore "time out connessione". Azione: verificare se l'utente connesso tramite VPN dispone di un IP locale dalla rete VPN.
- Come utente autonomo, verificare che nessun altro dispositivo o client VoIP myPortal @work sia registrato con lo stesso numero di stazione. Controllare anche in **WBM > Modalità esperti > Web Services Assistant** le connessioni aperte.

Nessun payload

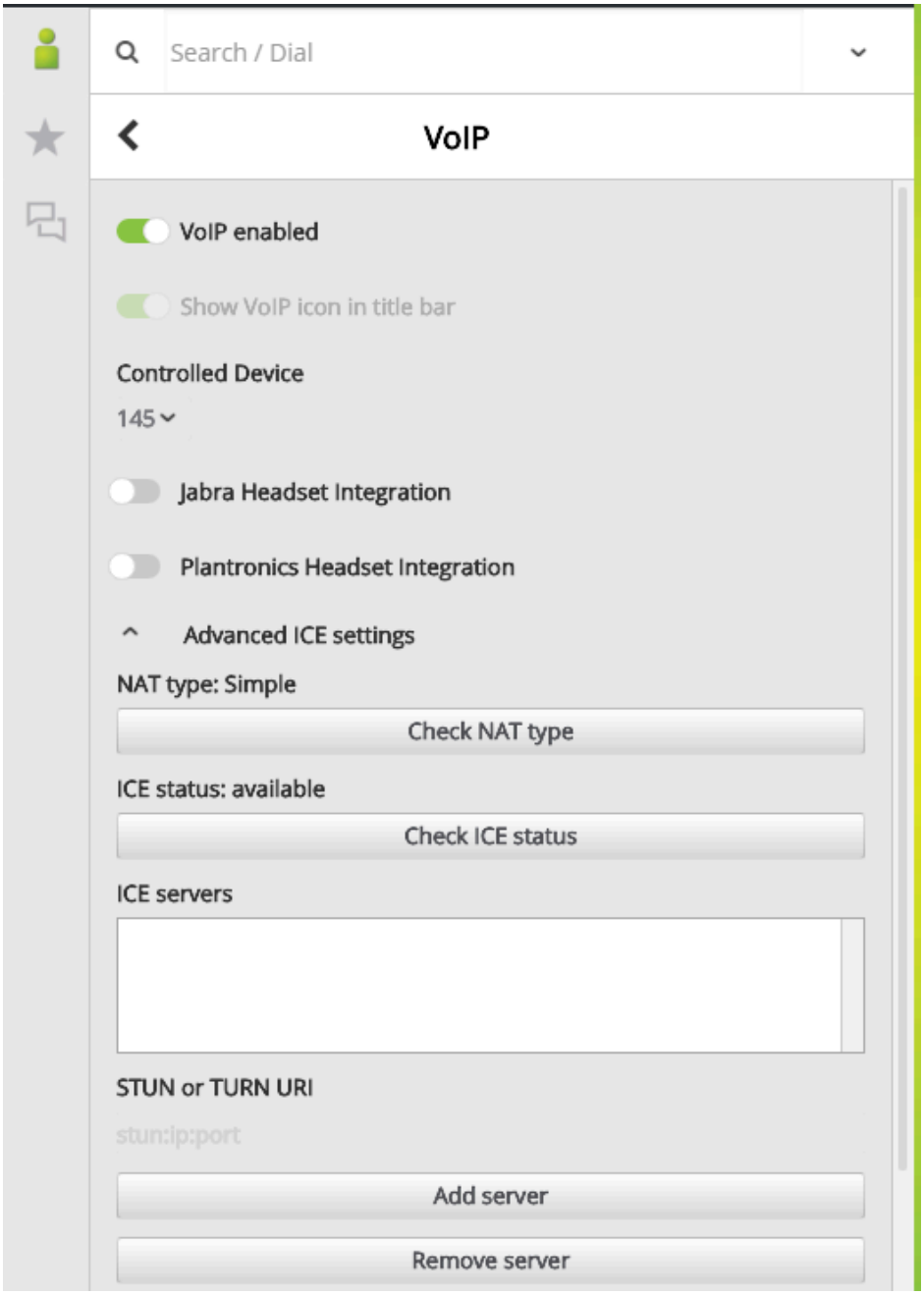
In caso di problema permanente di assenza di payload:

[4] Nessuna azione di configurazione necessaria; le porte verranno prese dinamicamente dallo stesso intervallo di porte UDP elencato per il firewall senza stato

- Verificare che le porte consentite siano aperte sul firewall. Per ulteriori informazioni, vedere il capitolo Porte e impostazioni firewall alla pagina 497.
- Controllare la configurazione del firewall NAT. La configurazione NAT simmetrico non è supportata.
- È possibile rilevare il tipo di NAT dal sistema in **WBM > Modalità esperti > Gateway voce > Rileva tipo di NAT**.
- Controllare la connettività del server STUN nel sistema.



- Verificare la connettività ICE in myPortal @work: **Impostazioni > VoIP > Impostazioni ICE avanzate**. Nel caso in cui "Tipo NAT" e/o "Stato ICE" non siano quelli visualizzati di seguito, le impostazioni di rete/firewall devono essere verificate dall'amministratore.



Eseguire "Controllare tipo NAT" > Tipo NAT: semplice

Eseguire "Verifica stato ICE" > Stato ICE: disponibile

- Disattivare l'integrazione cuffie da myPortal @work ed eseguire nuovamente lo scenario.
- Selezionare nuovamente i dispositivi audio dalle impostazioni VoIP.

12.2.1.6 Ulteriori suggerimenti

SIP ALG (gateway a livello di applicazione)

Se si verifica uno dei seguenti problemi, verificare che su uno dei router coinvolti sia attivato un SIP ALG. Esistono alcune categorie di sintomi per cui SIP ALG potrebbe influire sulle connessioni VoIP. Non è sempre evidente, soprattutto perché spesso questi problemi si verificano silenziosamente senza che gli utenti se ne accorgano.

- Audio unidirezionale (solo una persona può sentire l'altra)
- Il client non squilla quando viene chiamato
- Le chiamate cadono dopo la connessione
- Le chiamate finiscono direttamente nella casella vocale senza alcun motivo noto

12.3 Utente di UC Smart

Gli utenti di UC Smart sono utenti che utilizzano i client UC di UC Smart.

Le seguenti impostazioni sono disponibili per i client UC Smart in UC Smart Assistant:

Impostazioni	Spiegazione
Impostazioni	
Utente	Le impostazioni qui vengono solo visualizzate.
Nome	Le impostazioni qui vengono solo visualizzate.
Password	Password per client UC Smart e UC Smart Assistant.
Lingua	Lingua dell'interfaccia utente.
L'utente deve indicare una nuova password	Le impostazioni qui vengono solo visualizzate.
Accesso UC Smart Assistant	Autorizzazione per l'uso di UC Smart Assistant nel browser Web da parte dell'utente per i compiti di configurazione.
Configurato come utente Mobility	Le impostazioni qui vengono solo visualizzate.
Licenza casella vocale	Le impostazioni qui vengono solo visualizzate.
Servizi associati	Le impostazioni qui vengono solo visualizzate.
Dettagli del profilo	
Numero telefono Mobile	Numero di cellulare del partecipante in formato canonico (ad es. `+39 173 1234567`).
Numero di telefono privato/ esterno	Numero di telefono aggiuntivo dell'utente in formato canonico (ad es. `+39 051 987654321`).
Indirizzo e-mail	Indirizzo e-mail dell'utente
Da casella vocale a e-mail	Attivazione/disattivazione dell'avviso tramite e-mail all'arrivo di un nuovo messaggio vocale.

Impostazioni	Spiegazione
Visibilità presenza	Consente di impostare se lo Stato presenza deve essere visibile per partecipanti interni ed esterni o solo per gli interni o per nessun tipo di partecipante.
Informazioni sulla licenza	
Visualizza le licenze assegnate all'utente	

12.3.1 Come configurare un utente di UC Smart

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

In Modalità esperti, in **Selezione applicazione** il **Pacchetto con UC Smart** è attivato.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **UC Smart**.
4) Nella struttura dei menu, fare clic su **Amministrazione** > **Impostazioni di base**.
5) Nell'elenco **Utenti**, selezionare l'utente desiderato.
6) Nell'area **Impostazioni** e nel campo **Dati d. profilo** immettere i dati dell'utente.
7) Fare clic su **Applica**.
8) Se si desidera configurare altri utenti, ripetere i passi da 5 a 7.

12.3.2 Come modificare la password per un utente di UC Smart

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Il **Pacchetto con UC Smart** è stato attivato in **Selezione applicazione** in modalità Esperto.

Nota: Occorre ricordare che per impostazione predefinita, gli utenti UC Smart devono modificare di nuovo la propria password quando questa viene modificata dall'amministratore. Se non lo si desidera, dopo la modifica della password, disattivare il flag "L'utente deve modificare la password".

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Smart**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **UC Smart**.

4) Nella struttura dei menu, fare clic su **Amministrazione** > **Gestione utenti**.
5) Nell'area **Utente**, selezionare l'utente in questione.

> **Nota:** Per motivi di sicurezza, una password costituita da 5 asterischi (*****), non sarà accettata dal sistema.

6) Nell'area **Impostazioni**, in **Password**, inserire la nuova password.
7) Fare clic su **Applica**.
8) Se si desidera reimpostare la password di altri utenti, ripetere i passi da 5 a 7.

Passaggi successivi

Informare l'utente o gli utenti in questione della nuova password.

12.4 Stato presenza (presenza)

Lo stato presenza fornisce informazioni relative alla disponibilità degli utenti interni nella rubrica interna (anche utenti Mobility Entry). Inoltre, lo stato presenza consente di controllare la disponibilità degli utenti interni con la deviazione di chiamata basata sullo stato.

Un utente può modificare il proprio stato presenza tramite myPortal @work o myPortal to go. A ogni modifica dello stato presenza, a eccezione di **Ufficio**, è possibile definire il momento del ritorno in **Ufficio** previsto, se necessario.

L'utente può scegliere uno dei seguenti stati:

- **Ufficio**
- **Riunione**
- **Malattia**
- **Pausa**
- **Uscito**
- **Vacanza**
- **Pranzo**
- **Già uscito**
- **Non disturbare**

> **Nota:** L'amministratore di sistema può abilitare/disabilitare la visibilità dello stato "malato" all'interno dell'amministrazione del sistema. Vedere OpenScape Business UC Suite > Server

Le chiamate possono essere deviate in base allo stato a varie destinazioni, tra cui la casella vocale personale. Se un utente dispone di una casella vocale personale, può inoltrare le chiamate a una mailbox di gruppo o di sistema.

12.5 Rubriche e diario

Le rubriche, e il diario consentono di organizzare contatti e chiamate.

12.5.1 Rubriche

Le rubriche consentono di organizzare i contatti di un utente. Gli utenti possono accedere ai contatti con i client UC Smart.

Il sistema fornisce le seguenti rubriche, che supportano queste funzioni con la priorità sottoindicata per il numero di ricerca (il numero di ricerca è supportato solo per le chiamate esterne e se CO/ITSP non fornisce il nome):

Rubrica	Client UC Smart	Telefono di sistema con Display
Rubrica personale	Con l'Assistente personale, è possibile importare i contatti di Outlook.	
Rubrica interna	Contiene tutti gli utenti interni e i gruppi (con i relativi numeri di telefono aggiuntivi) per i quali è attiva la visualizzazione nel sistema. Gli utenti interni con telefoni di sistema visualizzati con i relativi stati presenza. Condizione essenziale per la visualizzazione dello stato presenza di un utente è che l'utente in questione l'abbia autorizzata.	Contiene tutti gli utenti interni e i gruppi per i quali è attiva la visualizzazione nel sistema.
Elenco dei Preferiti	Contiene i contatti selezionati dall'utente dalla rubrica personale e interna. Gli utenti interni con un telefono di sistema vengono visualizzati con lo stato presenza. Condizione essenziale per la visualizzazione dello stato presenza di un utente è che l'utente in questione l'abbia autorizzata.	
Rubrica di sistema	Contiene tutti i numeri di selezione breve centrali.	

Nota: Inserire ove possibile i numeri di telefono nelle rubriche sempre in formato canonico.

Nota: L'aggiunta o la rimozione di un contatto UC può richiedere vari minuti (**e** fino a 30 minuti) fino all'applicazione delle modifiche su tutti i client e dispositivi per via dei meccanismi di memorizzazione nella cache utilizzati. In alternativa è possibile riavviare il sistema per rendere **immediatamente** effettive le modifiche.

12.5.1.1 Come configurare le rubriche dei telefoni del sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È possibile selezionare quali rubriche sono disponibili per i telefoni di sistema con display.

Passo a passo

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony Server** > **Basic Settings** in the navigation tree.
3) Nella struttura dei menu, fare clic su **Sistema** > **Display**.
4) Nell'elenco a discesa **Rubrica**, selezionare una delle seguenti opzioni:
   - Se devono essere disponibili i contatti personali e le rubriche interna, esterna, di rete e LDAP, selezionare **Tutte**.
   - Se devono essere disponibili solo i contatti personali e le rubriche interna, esterna e di rete, selezionare **Interne**.
   - Se deve essere disponibile solo la rubrica LDAP, selezionare **LDAP**.
   - Se non deve essere disponibile alcuna rubrica, selezionare **No**.

   Nota: L'utente può attivare la gestione delle richieste di ricerca da parte della Rubrica unificata selezionando **Rubrica telefonica interna tramite Rubrica unificata**. When the flag is deactivated and there is no access to Unified Directory, the list view at the phone-book menu, implemented for the OpenScape Desk Phone CP 200/205/210, is not available.
5) Fare clic su **Applica**.

Passaggi successivi

Se si è selezionato **Tutti** o **LDAP**, assicurarsi che sia disponibile una corrispondente rubrica LDAP (ad esempio Open Directory Service) per i telefoni di sistema.

12.5.2 Rubrica interna

La rubrica interna contiene i dettagli di contatto degli utenti interni e dei gruppi MULAP del sistema di comunicazione. I client Smart UC hanno accesso alla rubrica interna.

L'amministratore ha accesso illimitato a tutti i dati nella rubrica interna. Gli utenti possono comporre i numeri di telefono direttamente da quest'ultima.

La visualizzazione nella rubrica interna di utenti e gruppi interni dipende dal parametro utente **Registrazione in elenco telef.** (configurabile nel WBM tramite la procedura guidata utente).

Nel sistema di reti si utilizza la rubrica interna a livello di nodo.

Concetti correlati

Chiamata di gruppo alla pagina 680

12.5.2.1 Come attivare o disattivare un utente nella rubrica interna

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Navigare nella struttura dei menu in **Utente** > **Utente** > **…** fino all'utente desiderato (Indice - Numero di telefono - Nome).
4) Fare clic sulla scheda **Modifica i flag dell'utente**.
5) Selezionare una delle seguenti opzioni:
   - Se il nome di un utente deve essere visualizzato nella rubrica del sistema, selezionare la casella di controllo **Registrazione in elenco telef.**
   - Se il nome dell'utente non deve essere visualizzato nella rubrica del sistema, deselezionare la casella di controllo **Registrazione in elenco telef**.
6) Fare clic su **Applica**, quindi su **OK**.

12.5.3 Elenco dei Preferiti

L'elenco dei Preferiti contiene i contatti selezionati dall'utente provenienti dalla rubrica personale o interna. I client UC Smart hanno accesso all'elenco dei Preferiti.

Un utente UC Smart può chiamare direttamente un contatto dall'elenco dei Preferiti. Se un utente interno riceve una chiamata, verrà visualizzato lo stato di chiamata dell'utente. L'utente UC Smart può quindi rispondere a questa chiamata. Inoltre, viene visualizzato lo stato presenza degli utenti interni.

12.5.4 Rubrica del sistema

La rubrica del sistema contiene tutti i numeri di selezione breve centrali a cui è stato assegnato un nome. I client UC Smart hanno accesso alla rubrica del sistema.

L'amministratore può disattivare la visualizzazione dei singoli utenti o numeri di selezione breve con nome.

12.5.5 Rubrica unificata

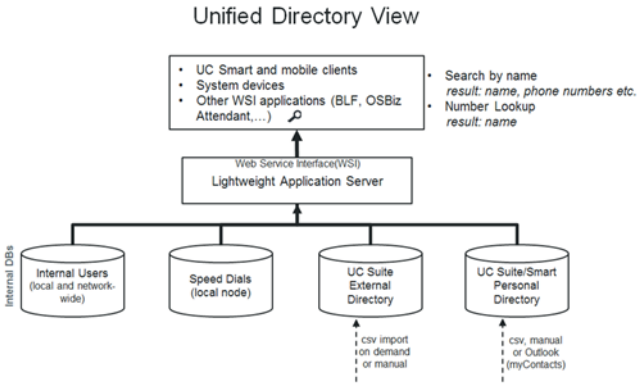
OpenScape Business fornisce diverse origini dati per memorizzare e recuperare dati relativi a utenti o contatti, a partire dai dati degli utenti interni nella configurazione per utenti interni, tramite l'elenco di selezione breve, fino alle varie rubriche delle applicazioni UC.

Ogni origine dati in OpenScape Business viene utilizzata da un'applicazione client specifica, installata nel SW di sistema sui dispositivi di telefonia o in

un'applicazione client UC. In base alle origini dati e ai client utilizzati, i dati recuperati e la loro presentazione possono variare.

Il servizio "Rubrica unificata" in OpenScape Business consente di applicare comuni funzioni di ricerca e risoluzione di nomi alle origini dati di OpenScape Business esistenti. Fornisce lo stesso risultato di ricerca o la stessa informazione di risoluzione del nome a tutti i dispositivi del sistema e ai client OpenScape Business.

Il servizio Rubrica unificata è accessibile tramite l'interfaccia Web Service (WSI) da client esterni quali myPortal to go oppure internamente tramite meccanismi di elaborazione chiamate (ad es. dai telefoni OpenStage).



Rubrica unificata utilizza le seguenti rubriche e database interni di OpenScape Business:

- Rubrica utente interno (in rete)
- Elenchi di selezione breve
- Rubrica personale UC Smart (opzionale)
- UC Suite Rubrica esterna (facoltativo)
- Contatti personali di Outlook (se importati tramite myContacts)

Il servizio Rubrica unificata è disponibile in ogni sistema OpenScape Business dalla release V2R2 in avanti. Non richiede pre-requisiti HW-SW o di licenza specifici.

Per ottenere i risultati migliori nell'utilizzo di Rubrica unificata, è necessario attenersi ad alcune regole a proposito dei formati dei numeri di telefono e del modo di scrivere i nomi.

12.5.5.1 Caratteristiche

Dispositivi / Client supportati

Il servizio Rubrica unificata fornisce:

- Ricerca nella rubrica di varie origini dati interne di OpenScape Business
- Offerta unificata del risultato della ricerca a tutti i client supportati
- Ricerca del numero di telefono / Risoluzione del nome in varie origini dati interne
- Offerta unificata dei risultati di risoluzione del nome per tutti i client supportati
- Accesso a dati esterni tramite l'interfaccia WebServices (WSI)

Le funzioni sono disponibili per i sistemi a nodo singolo come descritto di seguito. Nelle reti di OpenScape Business, la disponibilità delle funzioni dipende principalmente dal tipo di connessione dei fasci, dispositivi e client nella rete.

Rubrica unificata supporta i seguenti client / dispositivi di sistema di Unify che utilizzano le interfacce specificate:

Dispositivo/Client	Interfaccia utente/ Protocollo	Commenti
Telefoni OpenStage	Elaborazione chiamate / Protocollo CorNet	WSI / HTTP(S) è opzionale in OpenStage 60/80 per le immagini dei chiamanti
OpenScape Deskphone IP	Elaborazione chiamate / Protocollo CorNet	WSI / HTTP(S) è opzionale in DeskPhone IP 55 per le immagini dei chiamanti
Dispositivi cordless (CMI)	Elaborazione chiamate / Protocollo CMI	
CP 100/110 /200/205/210/ 405	Elaborazione chiamate / Protocollo CorNet	
DeskPhone CP400/ 600/600E/ 700/700X/710	WSI / HTTP(S)	
myPortal @work	WSI / HTTP(S)	
myPortal to go	WSI / HTTPS	
OpenScape Business Attendant / BLF	Elaborazione chiamate / Protocollo CorNet	WSI / HTTP(S) è opzionale

Nota: I client UC Suite myPortal, myAttendant e myAgent utilizzano propri meccanismi per la ricerca nella rubrica e la risoluzione dei nomi.

Funzione di ricerca

La ricerca nella Rubrica unificata viene sempre eseguita tramite l'interfaccia utente del dispositivo / client specifico. I criteri di ricerca e il set di caratteri utilizzati possono essere soggetti a limitazioni, in base ai client in uso.

Una volta inserito il criterio, la ricerca viene effettuata nelle directory successive

- Rubrica utente interno (in rete)
- Elenchi di selezione breve
- Rubrica personale UC Smart (opzionale)
- UC Suite Rubrica esterna (facoltativo)
- Contatti personali di Outlook (se importati tramite myContacts)

Tutte le corrispondenze all'interno delle directory precedenti vengono visualizzate come risultati di ricerca insieme alla relativa origine. I risultati possono contenere il set di dati di contatto completo o solo una parte di esso. La profondità di informazioni dei risultati dipende dall'origine dati.

Nota: La ricerca del nome del gruppo in myportal @work non è supportata in modalità UC Suite. È supportata solo la ricerca di utenti con licenza (licenza base) e gruppi MULAP con licenza (UC Entry).

I risultati vengono presentati ai dispositivi o ai clienti in base alle capacità dei display.

	Rubrica utente interna	Destinazione di selezione breve	Rubrica personale UC Smart	Rubrica esterna UC Suite	Contatti Outlook personali (tramite myContacts)
Cognome	X	---	X	X	X
Nome	X	---	X	X	X
Nome breve/ visualizzato	X	X	---	---	---
N° tel. ufficio	---	---	X	X	X
Nº tel. abitazione/ interno	---	---	X	---	X
N. cellulare	---	---	X	X	X
Ind. e-mail	---	---	X	X	X
Nome società	---	---	X	X	X
Città	---	---	---	---	---
Immagine contatto	---	---	X	---	X
Anteprima immagine contatto	---	---	X	---	X

Ricerca numero di telefono

La ricerca del numero di telefono nella Rubrica unificata risolve il chiamante trasferito (CLI) cercando il numero in tutte le origini dati interne supportate. La ricerca viene eseguita nei seguenti campi del numero di telefono:

- Numero dell'ufficio
- Numero cellulare
- Numero dell'abitazione

La ricerca del numero di telefono viene attivata, di solito, in caso di chiamate in entrata e in uscita, con la possibilità di considerare ulteriori funzioni specifiche di routing e inoltro.

Per ottenere risultati nel più breve tempo possibile, viene implementata una definizione fissa delle priorità delle origini dati utilizzate per la ricerca del

numero di telefono. Il risultato può contenere solo il cognome, nome, nome visualizzato oppure, se disponibili, i dati di contatto completi.

Tabella 5: Origini dati supportate e definizione di priorità

Priorità	Origini dati	Nota
1	Nome CO/ITSP (inviato dal provider)	Il pre-requisito è attivare il flag "Nome in CO".
2	Elenco di selezione breve	
3	Contatti personali	
4	Dettaglio utente UC	

I dati recuperati vengono presentati nel dispositivo dell'utente e/o nel client UC. La profondità delle informazioni dipende dalle capacità dei display.

- **Chiamate in entrata**

  Scenario supportato per i sistemi a nodo singolo:

  – Chiamata di base
  – Chiamata di gruppo / Chiamata MULAP
  – Segnalazione delle chiamate
  – Trasferimento di chiamata a passaggio singolo (SSCT)
  – Trasferimento monitorato/con consultazione
  – Deviazione di chiamata incondizionata (CFU = Call Forwarding Unconditional)
  – Deviazione di chiamata su mancata risposta (CFNR = Call Forwarding No Reply)
  – Deviazione di chiamata su occupato (CFB = Call Forwarding Busy)
  – Trasferimento nascosto
  – Risposta per assente

  Nota: La risposta per assente è diversa dal gruppo di risposta per assente. Nel gruppo di risposta per assente, quando un numero esterno viene salvato nella directory unificata, il nome del chiamante non viene mostrato dai membri del gruppo.

  Lo scenario supportato per le situazioni multinodo (di rete) è una chiamata tramite gateway.
- **Chiamata in uscita**

  Nel caso di una chiamata in uscita, la ricerca del numero di telefono dell'utente chiamato viene eseguita solo una volta.

  Lo scenario supportato per i sistemi a nodo singolo è una chiamata base a un numero esterno.

La presentazione dei risultati della ricerca del numero di telefono dipende dalle capacità dei display dei telefoni.

12.5.5.2 Regole e convenzioni

È necessario osservare alcune convenzioni relative a formati di numeri e nomi nelle origini dati per ottenere risultati ottimali utilizzando il servizio Unified Directory.

Formato numero supportato

Tutti i numeri di telefono esterni nelle origini dati devono essere inseriti nel formato canonico che include codice paese e prefisso interurbano, ad es. +4989700712345

L'elenco di selezione rapida supporta solo il formato selezionabile del sistema, ad es. 0089700712345 o 0004989700712345

Quando sono configurati numeri di selezione rapida per l'accesso tramite LDAP, è necessario abilitare l'opzione di conversione del numero per visualizzare il nome del contatto quando il numero è in formato canonico. Per ulteriori informazioni su come abilitare la conversione del numero, vedere Come aggiungere un'origine dati esterna per Open Directory Service alla pagina 1181.

Formati nome supportati

È necessario osservare le convenzioni seguenti relative a formati di nomi e set di caratteri:

- **Formato nome di selezione rapida**

  La ricerca del nome nell'elenco di selezione rapida è supportata solo se si utilizzano regole di configurazione specifiche. I nomi e i cognomi devono essere inseriti nel campo del nome esistente utilizzando lo schema seguente:

  <Cognome>, <Nome> (separati da virgola)
- **Utenti interni in caso di migrazioni**

  La migrazione a V2R1 e versioni successive con utenti interni che non seguono queste regole di configurazione non sarà supportata nel modo previsto. Ciò significa che l'amministratore deve convertire i nomi interni nello schema seguente prima della migrazione:

  <Cognome>, <Nome> (separati da virgola)

Disponibilità di modifiche di directory

Dopo la creazione, l'aggiornamento o l'eliminazione di contatti nelle varie origini dati, la visualizzazione di tutte le modifiche nei risultati di ricerca numero di telefono può richiedere fino a 10 minuti.

12.5.5.3 Capitolo 11.5.5.3 Limiti funzionali

Le Rubriche unificate sono soggette ai seguenti limiti funzionali:

Ricerca del nome

- Supporto dei nomi di gruppi

  Non è possibile eseguire ricerche di nomi di gruppi (non i nomi MULAP) in tutti i tipi di configurazioni

- Supporto di caratteri speciali

  Nella maggior parte dei dispositivi l'utente può eseguire ricerche utilizzando i caratteri standard "a-z". I caratteri speciali (diacritici) come i caratteri tedeschi Ä, ä, Ö, ö, Ü, ü, ß non sono accessibili tramite l'interfaccia utente del dispositivo di telefonia.

  Pertanto, un semplice risultato di ricerca dei caratteri include anche caratteri speciali. Una ricerca di uno qualsiasi dei caratteri "acdegilnorstuyz" trova i caratteri speciali corrispondenti "àáâãåäąăçćčďđèéêëęě#ìíîĩĺľłñńóôőõříśšşťùúûůűüýÿžźż"

  nei risultati di ricerca.

  Nota: La ricerca della rubrica con il carattere jolly all'inizio della stringa di ricerca, ad esempio <*jo*>, è supportata solo per gli utenti interni.

- Supporto del formato dei nomi di selezione breve

  La ricerca del nome nell'elenco di selezione rapida è supportata solo se si utilizzano regole di configurazione specifiche. I nomi e i cognomi devono essere inseriti nel campo del nome esistente utilizzando uno dei seguenti schemi

  – <Cognome>, <Nome> (separati dalla virgola)
  – <Nome> <Cognome> (separati da uno spazio, in questo caso)

Presentazione di nomi

I contatti personali in UC Smart e quelli provenienti dalla rubrica esterna non in linea nei quali la somma delle lunghezze del nome e del cognome supera i 24 caratteri vengono abbreviati a 24 caratteri in totale, per l'adattamento alla larghezza del display dei dispositivi.

Ricerca numero di telefono

La funzione di ricerca del numero di telefono (recupero del nome del contatto in base al numero del chiamante) non è supportata nella Rubrica unificata per i dispositivi SIP e S0.

12.5.5.4 Rubrica unificata nei sistemi di rete

Il servizio Rubrica unificata è attivo in ogni nodo di una rete OpenScape Business e utilizza le origini dati del proprio sistema. I dispositivi di telefonia e il client utilizzano sempre il servizio Rubrica unificata nel proprio nodo.

Pertanto, la disponibilità dei contatti nell'ambito della rete dipende dal tipo di contenuto dell'origine dati.

Tabella 6: Origine dati locale e in rete

Origine dati	Dati locali	Dati in rete
Rubrica utente interno	X	X
Elenchi di selezione breve	X	---

Origine dati	Dati locali	Dati in rete
Rubrica personale UC Smart	X	---
Rubrica personale UC Smart	X	---
Contatti personali di Outlook (tramite myContacts)	X	---

Ricerca numero di telefono

Negli scenari di rete la funzionalità di ricerca del numero di telefono non viene utilizzata. In tali scenari, il nome viene trasportato fra i nodi di rete mediante normali meccanismi di rete.

Per gli utenti interni si utilizza il Nome visualizzato configurato, per cui la ricerca è superflua.

12.5.6 Diario

Il diario è l'elenco di tutte le chiamate in arrivo e in uscita di un utente. Tramite il diario, un utente può chiamare in modo rapido e semplice il contatto o rispondere alle chiamate perse.

All'utente UC Smart vengono mostrate al massimo le ultime 100 chiamate.

Cartella per i vari tipi di chiamata

Le chiamate possono essere suddivise nei seguenti gruppi:

- **Aperte**
- **Perse**
- **Accettate**
- **Tutte le chiamate**

Dettagli della chiamate

Ogni chiamata viene visualizzata con una data e un'ora e, se disponibile, un numero di telefono. Se una rubrica contiene ulteriori informazioni su un numero di telefono, ad esempio **Cognome** e **Nome**, vengono visualizzati anche tali dati. Vengono inoltre visualizzati i parametri **Direzione** e **Durata** della chiamata oltre agli eventuali inoltri o alla risposta per assente.

12.6 Chiamate

Per le chiamate, il formato del numero è di particolare importanza.

12.6.1 Formati dei numeri di telefono

Per l'indicazione dei numeri di telefono sono disponibili diversi formati.

Formato	Descrizione	Esempio
classico	Inizia con + e contiene sempre l'indicativo del paese, il codice località e il resto del numero di telefono. Il carattere spazio e seguenti caratteri speciali + ( ) / - : ; sono consentiti.	+49 (89) 7007-98765
selezionabile	Ovvero, come il numero verrebbe composto in un telefono di sistema dell'ufficio, sempre con codice di linea urbana.	• 321 (interno) • 0700798765 (propria rete urbana) • 0089700798765 (rete urbana esterna) • 0004989700798765 (estero)

Suggerimento: Ove possibile utilizzare sempre il formato canonico dei numeri di telefono. In ogni situazione un numero di telefono è completo e univoco, oltre a essere coerente sulla rete e per gli utenti mobili.

Mediante selezione manuale (formato selezionabile) di un numero di telefono esterno, è necessario comporre sempre il codice di accesso linea urbana.

Quando si seleziona un numero di telefono esterno in formato componibile dalla rubrica, mediante il dialer sul desktop e il dialer dagli appunti per certi client UC, il sistema di comunicazione inserisce automaticamente il codice di linea urbana (fascio 1).

Nota: Per le chiamate entro il territorio degli Stati Uniti tramite CSTA a un numero di telefono in formato canonico, il numero viene convertito nel formato componibile.

12.6.2 Requisiti per ricevere chiamate VoIP su myPortal to go utilizzando CallKit sull'iPhone

Le notifiche delle chiamate VoIP iOS si basano sul meccanismo APNS di Apple.

Questo servizio richiede quanto segue:

- Un server DNS configurato che risolve i nomi dei domini pubblici da Internet.
- Accesso a Internet per il sistema OpenScape Business (porta TCP/443 in uscita) per inviare le notifiche di chiamata APNS.
- Il software di sistema deve essere aggiornato all'ultima versione principale/secondaria/di correzione rilasciata. L'ultima versione del sistema è importante perché il servizio APNS richiede certificati specifici che scadono quando si esegue il software di sistema precedente.

12.7 Conferenze

Durante una conferenza più partecipanti (inclusi utenti esterni) possono comunicare contemporaneamente tra loro. La funzione Gestione conferenze permette di condurre in modo rapido e semplice le conferenze nonché di programmarle in anticipo.

Conferenze controllate da telefono e da applicazioni

Gli utenti possono tenere conferenze, sia tramite telefono che tramite le applicazioni myPortal UC Smart.

Gli utenti possono avviare una conferenza controllata tramite telefono nelle modalità descritte di seguito e successivamente gestirla sempre tramite telefono:

- chiamare i partecipanti desiderati e connetterli alla conferenza
- estendere una chiamata in consultazione convertendola in una conferenza
- estendere una seconda chiamata convertendola in una conferenza

Le conferenze controllate tramite applicazioni possono essere tenute, controllate e gestite tramite Gestione conferenze. Per utilizzare la funzione Gestione conferenze, è necessaria una licenza apposita.

Differenze tra i tipi di conferenze:

	Conferenza controllata telefonicamente	**Conferenza controllata da applicazioni**
Direzione della connessione dal punto di vista del sistema	• In uscita	• In entrata (selezionata dal partecipante)
Autenticazione dei partecipanti alla conferenza	-	• PIN personale (ID conferenza) • PIN ospite (opzionale)
Invito predefinito ai partecipanti alla conferenza	-	• Nome conferenza • Numero di accesso (MeetMe) • PIN personale (ID conferenza) • PIN ospite (opzionale)
Numero max. di partecipanti per conferenza	8	16

Conferenza pianificata

Le conferenze pianificate sono create come conferenze permanenti. In caso di necessità, la conferenza può essere proseguita senza definire un'ulteriore scadenza. Le conferenze pianificate non occupano alcun canale conferenza se nessun partecipante è entrato in conferenza. La sequenza di composizione del numero è determinata dalla disponibilità dei canali conferenza.

Al primo accesso tramite WBM, gli amministratori possono modificare il numero di accesso (MeetMe) definito per le conferenze. Ai partecipanti viene mostrato il numero di accesso con il quale possono entrare nella conferenza. Pertanto dovranno autentificarsi utilizzando il proprio PIN personale o, se consentito, il PIN ospite.

Moderatori

Chi avvia la conferenza diventa automaticamente il moderatore e può:

- Creare, modificare ed eliminare le conferenze pianificate.
- Aggiungere e eliminare partecipanti alla conferenza.

  I partecipanti eliminati non restano nella conferenza.
- Disconnettere partecipanti dalla conferenza.

  I partecipanti che sono usciti dalla conferenza possono entrarvi di nuovo.
- Definire un altro partecipante interno dello stesso nodo come moderatore
- Lasciare la conferenza senza concluderla immediatamente.

  Se il moderatore in carica esce dalla conferenza, la conferenza viene conclusa entro 5 minuti.
- Concludere le conferenze attive.
- Avviare da una conferenza attiva una sessione di Web Collaboration.
- Inviare inviti predefiniti a tutti i partecipanti alla conferenza o solo a singoli partecipanti.

Tutti i partecipanti interni di uno stesso nodo possono diventare moderatori. Per poterlo essere, tuttavia, è richiesta una licenza per conferenze.

I partecipanti alla conferenza i cui dati di contatto sono stati inseriti manualmente vengono gestiti come utenti partecipanti e non possono essere impostati come moderatori.

Partecipanti alla conferenza

I partecipanti alla conferenza possono uscire dalla conferenza e rientrarvi di nuovo. Inoltre, possono prendere parte a una sessione di Web Collaboration già avviata. Finché nella conferenza vi è un solo partecipante, verrà riprodotta musica durante l'attesa. Il numero massimo di partecipanti esterni alla conferenza è limitato, tra l'altro, dal numero di linee urbane disponibili.

Conclusione automatica senza moderatore

Se il moderatore in carica lascia la conferenza, gli utenti ricevono un messaggio informativo in cui si comunica che la conferenza sarà conclusa entro 5 minuti.

Avviso ai partecipanti alla conferenza

Il moderatore può inviare a tutti o ad alcuni partecipanti alla conferenza un invito tramite e-mail. A tal fine è necessario che sul PC client sia installato un programma di posta elettronica. Gli indirizzi di posta elettronica noti vengono automaticamente inseriti nella lista di distribuzione. Un invito a tutti i partecipanti alla conferenza contiene solo un PIN ospite generico (se consentito), mentre in caso di inviti ai singoli utenti viene inviato anche un PIN personale.

In alternativa, è possibile copiare negli Appunti un testo di invito predefinito per utilizzarlo in altri programmi (ad esempio nelle chat).

12.8 Web Collaboration

Per conferenze telefoniche e telefonate, myPortal supporta l'integrazione del prodotto separato Web Collaboration che offre funzioni di collaborazione simultanea multimediale. Ciò offre un accesso rapido a funzioni quali

condivisione desktop e applicazioni, condivisione di file, co-browsing, whiteboarding, URL Push, chat con IM e chat video con più utenti.

Web Collaboration può essere avviato da un utente durante una telefonata tramite la finestra della chiamata del client PC UC o dal moderatore durante una conferenza attiva dalla conferenza stessa. Si apre una pagina Web in cui può essere avviato il download del client Web Collaboration. Non è necessario installare in locale Web Collaboration sul client PC UC. Se sul client PC UC è disponibile un programma di posta elettronica, agli interlocutori si può inviare un'e-mail con il collegamento al client Web Collaboration. Per informazioni su Web Collaboration, consultare la relativa documentazione del prodotto Web Collaboration.

Quando si elimina o si conclude una conferenza, la relativa sessione di Web Collaboration viene automaticamente eliminata.

Integrazione di Web Collaboration

Per poter integrare Web Collaboration, l'amministratore deve inserire nel WBM il numero di licenza e la password per la connessione hosted di tale prodotto. Il produttore offre il server di Web Collaboration su Internet sotto forma di servizio (server pubblico). Il numero di licenza e la password vengono trasmessi tramite una connessione https sicura. Per impostazione predefinita, a questo scopo viene utilizzata la porta TCP 5100. Non sono supportati server di Web Collaboration locali.

Nota: Per l'utilizzo di Web Collaboration, i client PC UC e il sistema di comunicazione devono disporre di una connessione a Internet. Le connessioni tramite proxy non sono supportate dal sistema di comunicazione.

Instant Messaging e Web Collaboration

Le funzioni di instant messaging del sistema e di una sessione di Web Collaboration sono indipendenti una dall'altra: i messaggi istantanei di un client PC UC non vengono visualizzati in una sessione di Web Collaboration dello stesso partecipante e viceversa.

12.8.1 Come configurare la connessione al server di Web Collaboration (server pubblico)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È disponibile un accesso a Internet.

Per una connessione sicura al server di Web Collaboration (server pubblico) è necessaria una chiave di licenza e una password.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Web Services**.
3) Nella struttura dei menu selezionare **Web Services** > **Web Collaboration**.
4) Selezionare il pulsante di opzione **Server pubblico**.

5) Nel campo **Numero licenza** immettere il numero di licenza per la connessione sicura al server di Web Collaboration (server pubblico).
6) Nel campo **Password** immettere la password per la connessione sicura al server di Web Collaboration (server pubblico).

Nota: Se si desidera testare la funzione Web Collaboration per 5 minuti, utilizzare il pulsante di opzione **Server pubblico (modalità demo/valutazione)**. A tal fine è necessario un numero di licenza e una password.

---

7) Fare clic su **Applica**, quindi su **OK**.

12.8.2 Come disattivare la connessione al server di Web Collaboration

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Web Services**.
3) Nella struttura dei menu selezionare **Web Services** > **Web Collaboration**.
4) Selezionare il pulsante di opzione **Nessun server di Web Collaboration**.
5) Fare clic su **Applica**, quindi su **OK**. L'opzione per l'avvio di una sessione di Web Collaboration nel client UC è disattivata.

12.9 Invio messaggi immediato

Per Invio messaggi immediato si intende la comunicazione mediante messaggi istantanei (chat).

12.9.1 Invio messaggi immediato

Con i messaggi istantanei, è possibile chattare con altri utenti di UC Smart.

I messaggi istantanei inviati e ricevuti vengono visualizzati dall'utente e dai suoi interlocutori in una finestra di dialogo. Selezionando un destinatario, il client mostra se questo è attualmente online. Se il proprio interlocutore non è in linea, non è possibile trasmettere a quest'ultimo messaggi istantanei. La pagina panoramica Messaggi istantanei mostra gli stream più recenti. Il sistema salva un numero limitato di messaggi istantanei. Vengono visualizzati al massimo gli ultimi 100 messaggi istantanei di un utente.

12.10 Casella vocale (SmartVM)

La casella vocale (chiamata anche SmartVM) riproduce per i chiamanti un annuncio di benvenuto e chiede se desiderano lasciare un messaggio o essere connessi a un interno. Gli utenti interni possono accedere alla casella vocale

tramite un telefono e con il client UC Smart. Gli utenti che desiderano utilizzare una casella vocale, richiedono una licenza VoiceMail.

Tipi di casella vocale

Di seguito sono elencati i diversi tipi di casella vocale.

- Mailbox predefinita:

  La mailbox predefinita è la casella vocale personale di un utente. Può rispondere alle chiamate, riprodurre un annuncio personalizzato o standard per il chiamante e chiedere al chiamante se desidera lasciare un messaggio. La mailbox predefinita dell'utente può essere configurata tramite telefono o tramite il cliente UC Smart (ad esempio, con la registrazione di un annuncio di benvenuto personalizzato).
- Mailbox di gruppo:

  La mailbox di gruppo ha le stesse caratteristiche della mailbox standard, tranne che non è assegnata a un singolo utente, ma a un gruppo di utenti. I messaggi per una mailbox di gruppo possono essere registrati solo se almeno un membro del gruppo dispone di una licenza VoiceMail. Le informazioni della casella vocale vengono mostrate a tutti gli utenti del gruppo che dispongono di una licenza VoiceMail. È possibile ascoltare i messaggi utilizzando il menu del telefono della casella vocale personale del membro del gruppo.
- Mailbox posto operatore (AutoAttendant/Company AutoAttendant):

  La mailbox posto operatore riproduce un annuncio di benvenuto per i chiamati con o senza la successiva opzione di commutazione. Company AutoAttendant è una forma speciale di mailbox posto operatore. Qui, il chiamante può essere automaticamente inoltrato (ad esempio al posto operatore) o inoltrato a un utente (ad esempio all'assistenza o alla hotline) mediante la composizione di un numero di telefono interno o di un numero di selezione breve (cifre 0-9). Tali scelte devono essere illustrate da appositi messaggi. Inoltre è possibile configurare una destinazione di rinvio alla quale il chiamante verrà inoltrato se questo non seleziona alcuna cifra o seleziona una cifra errata (non assegnata). L'amministratore può configurare fino a 100 mailbox posto operatore.
- Mailbox annuncio:

  La funzione annuncio viene configurata mediante assegnazione di un indice annunci a una porta annunci e l'impostazione di una casella vocale con il numero di telefono della porta annunci. Come annuncio viene utilizzato l'annuncio di benvenuto della casella postale. A seconda del tipo di annuncio, la riproduzione può avvenire una sola volta (annuncio) o ciclicamente (musica). Il menu del telefono di una casella vocale può essere utilizzato solo da un altro telefono in quanto non vi è alcun telefono associato. Pertanto, per la casella postale annunci deve essere usato un PIN diverso da quello della casella vocale del telefono utilizzato.
- Casella postale sistema:

  Come mailbox di sistema viene utilizzata la casella vocale con il numero di telefono del gruppo di ricerca di SmartVM. La mailbox di sistema deve essere una mailbox standard (nessun AutoAttendant) con attivata la registrazione vocale. Le informazioni della casella vocale vengono mostrate al possessore della casella stessa con l'indice 1 visualizzato, che potrà anche interrogarla. Questa prima casella vocale non può essere una mailbox di gruppo, una mailbox posto operatore o una mailbox annuncio. Se la

mailbox di sistema non viene utilizzata, non deve essere configurata alcuna mailbox con il numero di telefono del gruppo di ricerca SmartVM.

Funzioni della casella vocale

- Comando e controllo tramite telefono

  (dall'esterno: è necessario un numero di telefono proprio)
- Selezione manuale o automatica di diversi annunci di benvenuto
- Menu telefonico (Telephone User Interface, TUI) con struttura menu commutabile a livello di sistema:
  - Menu telefono, UC Smart: **SmartVM** (simile a EVM)
  - Menu telefono, UC Suite: **OSO** (simile a UC Suite)
- Fino a 320 caselle vocali configurabili per sistema
- Fino a 32 ore di capacità di registrazione vocale per sistema
- Fino a 100 messaggi memorizzati per casella vocale
- Fino a 2 minuti di durata per il tempo di registrazione di un messaggio vocale per casella vocale
- Fino a 10 possibili processi simultanei di risposta o smistamento delle chiamate
- Annuncio/musica prima della risposta
- Riproduzione di annunci personali
- Inoltro di chiamate fax tramite riconoscimento automatico tono fax a una destinazione fax preconfigurata

---

Nota: Per informazioni sul menu telefonico, consultare la guida rapida dell'interfaccia utente telefonica (TUI) di UC Smart e di UC Suite.

Impostazioni per il codice

Prima dell'utilizzo iniziale della casella vocale è necessario che ogni utente modifichi il codice preassegnato (predefinito: `123456`).

Il codice è costituito da una sequenza di sei cifre. Non deve essere costituito da cifre ripetute (ad esempio `333333`) o da una sequenza ordinata di cifre (ad esempio `987654`). Dopo sei tentativi non riusciti di inserire il codice, l'accesso alla corrispondente casella vocale viene bloccato finché la password non viene reimpostata dall'amministratore. Dopo due tentativi di inserimento di una password non corretta nel menu del telefono, la connessione viene interrotta.

Porte

La casella vocale utilizza le porte S_0 500-509 con i numeri di telefono assegnati 739-748. Per impostazione predefinita, le porte 504 e 505 vengono assegnate al Company AutoAttendant (numero 352), mentre le restanti 8 porte al gruppo di ricerca casella vocale (numero 351). Il numero di telefono 351 è il numero di telefono generale della casella vocale, tramite il quale è accessibile il menu del telefono.

Controllo della selezione

Per impostazione predefinita, le porte della casella vocale, per ragioni di sicurezza, sono solo semiabilitate alla linea urbana. Le seguenti funzioni

richiedono l'assegnazione di un gruppo di abilitazione con accesso alla linea esterna:

- Come chiamare il mittente di un messaggio vocale
- Ascolto dei messaggi vocali tramite l'utente Mobility tramite richiamata
- Trasferimento a destinazione esterna tramite Company AutoAttendant

Messaggi di benvenuto/Annunci

I singoli messaggi di benvenuto (= annunci) sono riprodotti nel sistema tramite telefono o con il WBM. Per la configurazione tramite telefono, viene composto il numero di telefono della casella vocale, quindi seguendo le istruzioni dell'interfaccia della casella vocale, è possibile registrare un nuovo messaggio di benvenuto tramite telefono.

I messaggi di benvenuto possono essere caricati nel sistema, salvati ed eliminati separatamente per ogni casella vocale tramite la Modalità esperti.

Nota: Per la riproduzione di messaggi vocali tramite numeri di telefono esterni (ad es. riproduzione tramite telefono cellulare attivata da myPortal to go), è necessario regolare la classe di servizio delle porte Smart VM. Si consiglia di utilizzare un "elenco consentito" per numeri così conosciuti.

12.10.1 Configurazione della casella vocale (SmartVM)

La configurazione della casella vocale (SmartVM) contiene la configurazione delle caselle di posta predefinite/di gruppo e delle mailbox posto operatore.

Le impostazioni generali per la casella vocale (SmartVM) vengono eseguite tramite la procedura guidata **SmartVM**, ad esempio la modifica del numero di telefono della casella vocale per adattarlo a un piano di composizione a 4 cifre.

Le impostazioni speciali per la casella vocale (SmartVM) e la configurazione di mailbox standard/di gruppo e di mailbox posto operatore vengono eseguite tramite la Modalità esperti.

Nota: La modifica di un numero reimposta la casella vocale dell'utente in questione. Tutti i messaggi vocali personali, i messaggi di benvenuto e gli annunci vanno persi e la password viene reimpostata.

È possibile caricare, salvare ed eliminare singoli annunci di benvenuto in SmartVM, oltre a salvare e ripristinare annunci di benvenuto e messaggi di una o di tutte le caselle vocali. Inoltre, è possibile consultare la guida all'uso nella lingua caricata e visualizzare le 10 caselle vocali con la maggior parte dei messaggi e lo spazio occupato da messaggi e annunci di benvenuto.

Per informazioni sulla configurazione di mailbox posto operatore, consultare il capitolo Attendant - AutoAttendant - Company AutoAttendant (UC Smart).

Assegnazione delle mailbox agli utenti

Se la casella vocale (SmartVM) è configurata, gli utenti possono essere assegnati alla propria mailbox standard. Ciò è possibile tramite

- un inoltro chiamata per l'utente utilizzando un elenco destinazioni di chiamata (configurato dall'amministratore). In questo caso, la chiamata nella sequenza viene successivamente inoltrata alle destinazioni chiamata selezionate (ad esempio, in primo luogo all'utente e dopo il tempo stabilito, alla mailbox).
- una deviazione chiamata al telefono dell'utente (l'utente può effettuarla esso stesso). In questo caso, la chiamata passa direttamente alla mailbox.

  Se l'utente è membro di un gruppo di ricerca e se il gruppo di ricerca riceve una chiamata, tale chiamata non viene inoltrata alla casella vocale del gruppo di ricerca.

12.10.1.1 Come attivare o disattivare la casella vocale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

UC Smart è attivo.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Interfacciamenti**.
3) Nella struttura dei menu fare clic su **Interfacciamenti** > **SmartVM**.
4) Fare clic sulla scheda **Modifica parametri SmartVM**.
5) Per disattivare la funzione casella vocale, selezionare la casella di controllo **Disattivazione EVM**.
6) Per attivare la funzione casella vocale, deselezionare la casella di controllo **Disattivazione EVM**.
7) Fare clic su **Applica**, quindi su **OK**.

12.10.1.2 Come configurare la casella vocale (SmartVM)

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **SmartVM**.
4) Selezionare la casella di controllo **Attiva SmartVM**.

5) Se necessario, modificare le impostazioni generali della mailbox di sistema alla colonna **Voicemail**:
   a) Se necessario, nel campo **Numero di telefono** modificare il numero della casella vocale (predefinito: `351`), per adattarlo ad esempio a un piano di composizione a 4 cifre.
   b) Se necessario, nel campo **DID** modificare il numero interno della casella vocale (predefinito: `351`), per adattarlo ad esempio a un piano di composizione a 4 cifre.
   c) Se necessario, nel campo **Nome** modificare il nome della casella vocale (predefinito: `VOICEMAIL`).
6) Se necessario, modificare le impostazioni generali per la mailbox posto operatore alla colonna **AutoAttendant**:
   a) Se necessario, nel campo **Numero di telefono** modificare il numero della casella vocale (predefinito: `352`), per adattarlo ad esempio a un piano di composizione a 4 cifre.
   b) Se necessario, nel campo **DID** modificare il numero interno della casella vocale (predefinito: `352`), per adattarlo ad esempio a un piano di composizione a 4 cifre.
   c) Se necessario, nel campo **Nome** modificare il nome della casella vocale (predefinito: `AutoAttendant`).
7) Fare clic su **OK & Avanti**.
8) Se necessario, nella riga della porta desiderata, nel campo **N° tel.** modificare il numero di telefono della porta (predefinito: `739-748`), per adattarlo ad esempio a un piano di composizione a 4 cifre.
9) Se necessario, nella riga della porta desiderata, nel campo **Nome** modificare il nome della porta (predefinito: `SmartVM 1-10`).
10) Se necessario, nella riga della porta desiderata, nell'elenco a discesa **Tipo** modificare il tipo di porta:
    - **Phone Mail (n° tel. a 5 cifre)**: la porta è assegnata alle mailbox predefinite e alle mailbox posto operatore del tipo AutoAttendant. Le porte di questo tipo sono incluse automaticamente nel gruppo di ricerca 351.
    - **Predefinita**: la porta è assegnata alle mailbox posto operatore del tipo Company AutoAttendant e alle mailbox annuncio. Le porte di questo tipo sono incluse automaticamente nel gruppo di ricerca 352.
11) Se necessario, nella riga della porta desiderata, nell'elenco a discesa **Modo** modificare il modo della porta:
    - **Annuncio**: un annuncio/messaggio di benvenuto viene riprodotto una volta.
    - **Musica su attesa**: un messaggio di benvenuto/annuncio/brano musicale viene riprodotto a ciclo continuo.
    - **Company AutoAttendant**: dopo la riproduzione del messaggio di benvenuto/annuncio vi è la possibilità di inoltro al posto operatore.
12) Fare clic su **OK & Avanti**.
13) Dal menu a discesa **Selezione casella postale**, selezionare la mailbox desiderata. Vengono quindi visualizzati i campi per la configurazione degli annunci di benvenuto.
14) Se si desidera utilizzare i propri annunci di benvenuto per la mailbox selezionata, fare clic su **Ricerca**, navigare fino alla posizione in cui sono

salvati i file (formato: wave, PCM, 16 bit, 8 kHz, mono) e fare clic su **Carica**. Gli annunci di benvenuto selezionati vengono caricati nel sistema.

Nota: Gli annunci di benvenuto già caricati possono essere salvati ed eliminati.

---

15) Se si desidera configurare annunci di benvenuto per altre mailbox, ripetere i punti dal 13 al 14.
16) Fare clic su **OK & Avanti**.
17) Modificare i parametri generali solo all'occorrenza. Per una descrizione dei parametri generali, vedere Interfacciamenti>SmartVM .
18) Fare clic su **OK & Avanti**, quindi su **Fine**.

12.10.1.3 Come aggiungere una mailbox standard per un utente

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

All'utente corrispondente deve essere assegnata una licenza casella vocale.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Interfacciamenti**.
3) Nella struttura dei menu fare clic su **Interfacciamenti** > **SmartVM**.
4) Fare clic sulla scheda **Modifica caselle postali SmartVM**.
5) Nel campo **Numero mailbox**, immettere il numero di telefono dell'utente per il quale deve essere aggiunta la mailbox.
6) Dall'elenco a discesa **Annuncio**, selezionare un annuncio di benvenuto.
7) Se un chiamante può lasciare un messaggio nella casella vocale, selezionare la casella di controllo **Registrare**.
8) Assicurarsi che la casella di controllo **AutoAttendant** sia deselezionata.
9) Se una casella vocale viene riconfigurata, la casella di controllo **Reset password** non deve essere selezionata. Consente di reimpostare la password per la casella vocale. In caso di riconfigurazione, l'utente deve cambiare comunque la password iniziale della casella vocale al primo accesso.
10) Fare clic su **Applica**, quindi su **OK**.

12.10.1.4 Come modificare il gruppo di abilitazione per la porta della casella vocale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

UC Smart è attivo.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione, fare clic su **Telefonia** > **Classi di autorizzazione**.
3) Nella struttura dei menu, fare clic su **Classi di autorizzazione** > **Stazione** > **EVM** quindi sulla porta della casella vocale desiderata.
4) Nella scheda **Modifica gruppo di abilitazione**, selezionare dall'elenco a discesa **Gruppo di abilitazione Giorno** o **Gruppo di abilitazione Notte** il gruppo di abilitazione desiderato per la modalità giorno e la modalità notte.
5) Fare clic su **Applica**, quindi su **OK**.

Nota: I testi della porta EVM vengono generati in base alla procedura guidata **Configurazione di base** > **Prefisso internazionale del sistema**.

12.10.1.5 Come modificare la struttura del menu del telefono per la casella vocale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

UC Smart è attivo.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Interfacciamento**.
3) Nella struttura dei menu, fare clic su **Interfacciamento** > **SmartVM**.
4) Fare clic sulla scheda **Modifica parametri SmartVM**.
5) Se si desidera che la struttura del menu del telefono sia simile a quella di OpenScape Office, dal menu a discesa **Interfaccia utente telefono** selezionare la voce **OSO**.
6) Fare clic su **Applica**, quindi su **OK**.

12.10.1.6 Come caricare, salvare ed eliminare i singoli annunci di benvenuto

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

UC Smart è attivo.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Configurazione**.
3) Nella struttura dei menu, fare clic su **Configurazione** > **Configurazione SmartVM** > **Operazioni su file**.
4) Fare clic sulla scheda **Dati degli annunci**.
5) Nell'elenco a discesa **Selezione casella postale** selezionare la casella postale desiderata.
6) Se si desidera caricare in SmartVM un file di benvenuto salvato in precedenza o un file wave, nell'annuncio di benvenuto desiderato fare clic

su **Ricerca**, quindi navigare fino al punto in cui è memorizzato il relativo file. Fare quindi clic su **Carica**.

Nota: Il file wave da caricare deve essere nel seguente formato: PCM, 16 bit, 8 khz, mono. Durante il caricamento ha luogo la conversione del file Wave. A seconda delle dimensioni, l'operazione può durare alcuni minuti.

---

7) Se si desidera salvare un annuncio di benvenuto esistente, nell'annuncio desiderato fare clic su **Salva** e salvare il file VMA in una posizione a scelta.

8) Se si desidera eliminare un annuncio di benvenuto esistente, nell'annuncio desiderato fare clic su **Cancella** e confermare con **OK**.

12.10.1.7 Come salvare e reimpostare gli annunci di benvenuto e i messaggi

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

UC Smart è attivo.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Manutenzione** > **Configurazione**.

3) Nella struttura dei menu, fare clic su **Configurazione** > **Configurazione SmartVM** > **Operazioni su file**.

4) Se si desidera salvare gli annunci di benvenuto e i messaggi:

a) Fare clic sulla scheda **Backup**.

b) Selezionare la casella di controllo **Messaggi** se oltre agli annunci di benvenuto devono essere salvati anche i messaggi.

c) Copiare le caselle vocali da salvare dall'elenco **Caselle postali disponibili** all'elenco **Caselle postali per backup**.

d) Fare clic su **Applica**. Gli annunci di benvenuto (e i messaggi se è selezionato il flag **Messaggi**) delle caselle vocali da salvare vengono salvati in un file di backup (*.tar). Salvare il file in una posizione di memoria a scelta.

5) Se si desidera ripristinare gli annunci di benvenuto e i messaggi:

a) Fare clic sulla scheda **Ripristina**.

b) Fare clic su **Sfoglia**, quindi navigare fino alla posizione di memorizzazione del file di backup (*.tar) e fare clic su **Apri**.

c) Fare clic su **Carica**, quindi su **OK**. Vengono visualizzate le caselle vocali contenute nel file di backup.

d) Copiare le caselle vocali da ripristinare dall'elenco **Caselle postali disponibili** all'elenco **Caselle postali per ripristino**.

e) Selezionare la casella di controllo **Messaggi** se oltre agli annunci di benvenuto devono essere salvati anche i messaggi.

f) Se la casella di controllo**Inclusione** è deselezionata, vengono sovrascritti solo gli annunci di benvenuto della casella vocale selezionata per i quali è stato creato un file di backup. Se la casella di controllo **Messaggi** è

selezionata, vengono aggiunti anche i messaggi contenuti nei dati di backup. I messaggi già esistenti vengono mantenuti.

g) Se la casella di controllo **Inclusione** è selezionata, prima del ripristino vengono cancellati tutti gli annunci di benvenuto e i messaggi delle caselle vocali selezionate in SmartVM. Se solo selezionate caselle vocali che non contengono dati di backup, vengono eliminate anche queste! I messaggi di benvenuto contenuti nei dati di protezione vengono trasmessi. Se è selezionata la casella di controllo **Messaggi**, vengono trasferiti anche i messaggi contenuti nei dati di backup.

h) Fare clic su **Carica**, quindi su **OK**. Gli annunci di benvenuto e i messaggi delle caselle vocali selezionate vengono ripristinati.

12.10.2 Servizio informativo per nuovi messaggi

Se lo si desidera, il sistema può informare tramite e-mail un utente di UC Smart dell'arrivo di un nuovo messaggio vocale.

Requisiti per il servizio informativo

- L'invio di e-mail (inoltro e-mail) deve essere configurato nel sistema dall'amministratore.
- L'indirizzo di posta elettronica dell'utente deve essere noto al sistema. L'amministratore può importare tutti gli indirizzi e-mail nel WBM durante l'installazione iniziale tramite un file XML o immettere un indirizzo e-mail per ciascun utente in UC Smart Assistant (vedere la Come configurare un utente di UC Smart). In alternativa, l'utente stesso può inserire il proprio indirizzo e-mail nel relativo client UC Smart.
- È stata assegnata all'utente una licenza casella vocale.
- Il servizio **Da casella vocale a e-mail** è attivato. L'amministratore può attivare la funzione per ciascun utente di UC Smart Assistant (Come attivare o disattivare gli avvisi tramite e-mail). In alternativa, l'utente stesso può attivare la funzione utilizzando il proprio client UC Smart.

L'utente di UC Smart riceve un'e-mail con il messaggio vocale sotto forma di file WAV (16 bit, mono), comprendente data e ora di ricezione, durata del messaggio vocale e se disponibile, il numero di telefono e il nome del mittente. L'indirizzo corrispondente viene utilizzato come mittente.

12.10.2.1 Come attivare o disattivare gli avvisi tramite e-mail

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

In Modalità esperti, in **Selezione applicazione** il **Pacchetto con UC Smart** è attivato.

L'indirizzo e-mail dell'utente è stato inserito nei dettagli del suo profilo.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.

2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.

3) Fare clic su **Modifica**, per avviare la procedura guidata **UC Smart**.

4) Nella struttura dei menu, fare clic su **Amministrazione** > **Impostazioni di base**.
5) Nell'elenco **Utenti**, selezionare l'utente desiderato.
6) Selezionare una delle seguenti opzioni:
   a) Se si desidera attivare il servizio informativo di notifica per i nuovi messaggi, nell'area **Dati d. profilo** selezionare la casella di controllo **Da casella vocale a e-mail**.
   b) Se si desidera disattivare il servizio informativo di notifica per i nuovi messaggi, nell'area **Dati d. profilo** deselezionare la casella di controllo **Da casella vocale a e-mail**.
7) Fare clic su **Applica**.
8) Se si desidera configurare altri utenti, ripetere i passi da 5 a 7.

13 UC Suite

La UC Suite offre servizi di comunicazione unificata, quali ad esempio stato presenza e CallMe, conferenze e messaggi vocali e fax nei client myPortal for Desktop e myPortal for Outlook. myAttendant offre inoltre funzioni per console posto operatore.

Nota: Per il modello hardware OpenScape Business X3/X5/X8, la soluzione di comunicazione unificata UC Suite richiede l'hardware UC Booster (UC Booster Card o UC Booster Server). Con OpenScape Business S (Soft switch) la soluzione di comunicazione unificata UC Suite è già integrata.

Nota: Dopo le modifiche alla configurazione di utenti, gruppi, Mobility o altri parametri di sistema quali i codici di accesso alle linee, è necessario sincronizzare i dati UC per UC Smart o UC Suite. La sincronizzazione avviene cinque minuti dopo l'ultima modifica alla configurazione. Se una modifica alla configurazione ha luogo prima della scadenza del timer dei 5 minuti, quest'ultimo viene riavviato. I dati UC possono essere obsoleti fino all'avvio della sincronizzazione. Durante la sincronizzazione, l'applicazione UC e l'API di Web Services Interface non sono disponibili e la connessione di qualsiasi client UC si interrompe finché i dati UC non vengono sincronizzati. Le connessioni vengono ripristinate automaticamente al termine della sincronizzazione dei dati UC.

13.1 Impostazioni di base per UC Suite

Le impostazioni di base della UC Suite possono essere personalizzate.

La UC Suite può essere attivata o disattivata. Se si utilizza la UC Suite, UC Smart deve essere disattivato.

Inoltre, è possibile verificare prima della composizione tutte le chiamate UC avviate dal sistema (ad esempio tramite il servizio CallMe), per assicurarsi che l'utente UC che richiede il servizio disponga dell'abilitazione per quel tipo di chiamata. Se l'utente UC non dispone della necessaria abilitazione, la chiamata non viene eseguita.

Nota: Se si utilizzano applicazioni CSTA, è necessario impostare il parametro di codice per tutte le linee attive.

Attività correlate

Come rilevare gli indirizzi IP dei componenti del sistema alla pagina 484

13.1.1 Come attivare UC Suite

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Selezione applicazione**.
3) Nella struttura dei menu fare clic su **Scelta applicazioni** > **Scelta applicazioni**.
4) Selezionare una delle seguenti opzioni:
   - Se si desidera utilizzare la UC Suite con UC Booster Card, fare clic su **Pacchetto con UC Suite**.
   - Se si desidera utilizzare UC Suite con UC Booster Server, fare clic su **Pacchetto con UC Suite su OSBiz UC Booster Server** e, inoltre, inserire l'indirizzo IP del server Linux esterno nel campo **Indirizzo IP di OSBiz UC Booster Server**.
5) Fare clic su **Applica**.

13.1.2 Come limitare l'abilitazione per le chiamate UC effettuate a livello di sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Sistema** > **Flag di sistema**.
4) Se prima della composizione di chiamate UC effettuate dal sistema è necessario verificare se l'utente UC Suite che richiede di effettuare la chiamata possiede l'abilitazione per quella chiamata particolare, nell'area **Restrizione per le chiamate UC** selezionare la casella di controllo **Restrizione per le chiamate UC**.
5) Se prima della composizione di chiamate UC effettuate dal sistema non è necessario verificare se l'utente UC Suite che richiede di effettuare la chiamata possiede l'abilitazione per quella chiamata particolare, nell'area **Restrizione per le chiamate UC** deselezionare la casella di controllo **Restrizione per le chiamate UC**.
6) Fare clic su **Applica**.

13.2 Client UC Suite

I client UC Suite rappresentano pratiche interfacce che offrono funzioni di comunicazione unificata complete.

Il sistema offre i seguenti client UC Suite per i seguenti dispositivi:

Tipo client	Client	Tipo di terminale
Client di comunicazione	myPortal for Desktop	PC
	myPortal for Outlook	
	myPortal@work	
	Fax Printer	
	myAttendant	
Client mobile	myPortal to go (UC Suite) (vedere Mobility)	Smartphone, tablet-PC
Client del Contact Center	myAgent (vedere Contact Center multimediale)	PC
	myReports (vedere Contact Center multimediale)	

Gli utenti che dispongono di un indirizzo e-mail, riceveranno un messaggio e-mail di benvenuto con istruzioni per i primi passi da eseguire per utilizzare il programma.

Impostazioni individuali degli utenti

Le singole impostazioni degli utenti per myPortal for Desktop vengono salvate sul PC in file .INI. Viene inoltre creato un file .INI per ogni utente. Le impostazioni dei singoli utenti di myPortal for Outlook, myAttendant e Fax Printer sono salvate nel registro di sistema del PC. In questo modo, i vari utenti possono utilizzare le applicazioni myPortal for Desktop, myPortal for Outlook, myAttendant e Fax Printer tramite un PC (Desk Sharing). Ciò ne consente inoltre l'uso in ambienti Windows Terminal Server e Citrix Server. In questo modo, più utenti possono accedere alle applicazioni dai propri PC senza necessità di installazione locale.

13.2.1 myPortal for Desktop

myPortal for Desktop è un client per la comunicazione unificata sul proprio PC. Oltre a comodi ausili di composizione con Rubriche, Preferiti, informazioni sullo stato di presenza degli altri utenti, questo strumento offre anche l'accesso a messaggi vocali e fax.

myPortal for Desktop offre le seguenti funzioni:

- Rubriche
- Elenco dei Preferiti

- Diario
- Dialer sul desktop
- Finestre popup
- Stato presenza
- Servizio CallMe con ONS (servizio One Number)
- Deviazione di chiamata basata sullo stato
- Posto operatore automatico personale
- Gestione conferenze
- Registrazione di conferenze
- Registrazione di chiamate
- Invio messaggi immediato
- Messaggi vocali e fax

13.2.2 myPortal @work

myPortal @work è un'applicazione di comunicazione unificata che combina tutte le funzionalità e i servizi necessari, come la composizione conveniente tramite rubriche, preferiti, conversazioni e informazioni sullo stato di presenza dei colleghi, in un'unica soluzione progettuale per accelerare la comunicazione quotidiana, migliorare il lavoro di squadra e entrare in contatto veloce con colleghi, clienti e partner.

Nota: Quando il client VoIP myportal@work viene utilizzato in combinazione con altri client UC Suite, si consiglia di utilizzare la messa in attesa per consultazione da myportal@work anziché la messa in attesa comune dai client UC Suite.

---

myPortal @work può essere utilizzato sia con le soluzioni UC Smart che UC Suite. Per ulteriori informazioni, vedere myPortal @work.

13.2.3 myPortal for Outlook

myPortal for Outlook è il client per comunicazione unificata di Microsoft Outlook (plugin) analogo a myPortal for Desktop.

Oltre alle funzioni offerte da myPortal for Desktop, myPortal for Outlook offre anche le seguenti funzioni aggiuntive:

- Come eseguire chiamate di contatti di Outlook
- Come creare un contatto di Outlook dal mittente di un messaggio vocale
- Come inviare messaggi vocali tramite e-mail
- Come inviare messaggi fax tramite e-mail

13.2.4 Fax Printer

Fax Printer è un'applicazione Windows per l'invio di messaggi fax da altre applicazioni Windows, quali ad esempio, Microsoft Word, con creazione delle singole copertine fax.

Fax Printer è costituito dai seguenti componenti:

- Fax Printer Cover Editor
- Fax Printer Driver - con le seguenti funzioni:
  - Invio fax ai singoli destinatari
  - Rubriche
  - Uso di copertina centralizzata
  - Uso di intestazioni predefinite
  - Fax tipo
  - Controllo tramite l'interfaccia utente
  - Controllo tramite la riga di comando

13.2.5 myAttendant

myAttendant è un'applicazione di comunicazione unificata che consente lo svolgimento di funzioni per posto operatore. Oltre a comodi ausili per le funzioni di posto operatore, composizione con Rubriche, Preferiti, Informazioni sullo stato di presenza degli altri utenti, questo strumento offre anche l'accesso a messaggi vocali e fax. Le funzionalità di instant messaging supportano la comunicazione con utenti interni.

myAttendant offre i seguenti servizi:

- Funzioni posto operatore
- Rubriche
- Diario
- Finestre popup
- Modifica dello stato presenza di utenti interni
- Registrazione di chiamate
- Centro messaggi
- Pulsanti utente
- Gestione di messaggi vocali e fax
- Invio messaggi immediato
- Funzioni team
- Gestione conferenze

13.2.6 Requisiti richiesti per client PC della UC Suite

Per utilizzare i client PC di UC Suite, questi ultimi devono disporre di una dotazione hardware e software adeguata. In base alla configurazione, per l'installazione e gli aggiornamenti automatici sono necessari diritti di amministratore. La gamma di funzioni utilizzabili dipende dalle licenze utilizzate.

Nota: Rispettare scrupolosamente le istruzioni correnti contenute nel file `Readme first` che si trova nella stessa cartella dei file di installazione.

Telefoni

I PC client della UC Suite possono essere utilizzati insieme ai seguenti telefoni:

- OpenStage HFA e SIP

- OpenScape Desk Phone IP 35G/55G HFA e SIP
- OpenScape Desk Phone IP 35G Eco HFA e SIP
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA e SIP
- OpenScape Desk Phone CP 110/210/410/710 HFA e SIP
- Telefoni SIP con supporto per 3PCC
- Telefoni analogici
- Telefoni ISDN
- OpenScape Personal Edition HFA e SIP
- OpenStage M3 (OpenScape Business Cordless)
- OpenScape DECT Phone S6/SL6/R6 (OpenScape Business Cordless)
- optiPoint WL3 professional SIP

Sono supportati i dispositivi precedenti (ad esempio, optiPoint 410/420/500, Gigaset M2/SL3/S4/SL4/S5 e optiPoint WL2 SIP). I dispositivi Optiset E non possono essere utilizzati. Per i dispositivi testati e approvati, consultare le rispettive release note.

Nota: Il client integrato OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA non presenta pre-requisiti particolari, tranne la configurazione e la licenza client standard.

I "Preferiti" nel menu telefonico contengono dei tasti programmabili liberamente e non sono collegati ai Preferiti UC. È possibile trovare i dettagli relativi a tali tasti e le istruzioni nella documentazione del dispositivo.

Nota: Con i telefoni analogici e DECT, non è supportato il LED mailbox e la visualizzazione di informazioni a display è supportata solo in modo limitato.

Sistemi operativi

I PC client della UC Suite possono essere utilizzati insieme ai seguenti sistemi operativi:

- Microsoft Windows 11 (a 64 bit) tutte le versioni
- Microsoft Windows 10 (a 64 bit) tutte le versioni
- Apple macOS da 13 / 14 / 15.1 a 15.4

Suggerimento: Il sistema operativo utilizzato richiede sempre lo stato attuale di tutti gli aggiornamenti disponibili (service pack e patch).

Il supporto del PC client UC Suite per Microsoft Office 2003, Microsoft Windows XP e Microsoft Windows Server 2003 termina in concomitanza con il termine del supporto di questi prodotti da parte di Microsoft. Il prodotto sarà ancora supportato, ma non testato nei dettagli.

Per l'installazione in ambiente Windows sono necessari i diritti di amministratore di un PC client, tuttavia ciò non è necessario per l'aggiornamento automatico. L'interfaccia utente in lingua russa o cinese di myPortal for Outlook richiede che Windows venga installato nella versione russa o cinese.

myPortal for Desktop per Apple MAC presenta la stessa interfaccia disponibile in Microsoft Windows. Per motivi legati all'architettura del sistema operativo Mac OS di Apple le seguenti funzionalità non sono attualmente supportate:

- Invio di fax
- Outlook, Integrazione Entourage

myPortal for Outlook è supportato in ambienti Microsoft Office 365. Microsoft Office 365 è un'applicazione cloud. Ciò comprende tra l'altro un server Exchange per la distribuzione centralizzata di e-mail, oltre ai prodotti classici di Microsoft Office. OpenScape Business supporta Microsoft Office 365.

In Microsoft Office 365 possono essere utilizzate le seguenti funzioni:

- Integrazione del calendario di Exchange
- Inoltro e-mail

Browser Web

Per la programmazione dei pulsanti dei telefoni sui client UC sono stati approvati i seguenti browser Web:

- Microsoft Internet Explorer Versione 10 (o successiva)
- Microsoft Edge
- Mozilla Firefox 19 (o successivo)
- Google Chrome

Software aggiuntivo

Software aggiuntivo	myPortal for Desktop	myAttendant	myPortal for Outlook
Oracle Java JRE 1.8.x o versione successiva (32 bit/64 bit) OpenJDK V8 o versione successiva (32 bit/64 bit)	X	X	
Microsoft Outlook / Office • 2021 (32 bit/64 bit) + Office 365 • 2019 (32 bit/64 bit) • 2016 (32 bit/64 bit): supportato, ma non più parte del test di sistema; in caso di errore non verrà fornita alcuna correzione SW (fine del supporto da parte di OpenScape Business)			X
Accesso a Microsoft Exchange Server (per contatti e appuntamenti di Outlook) Exchange 2015 / 2013 / 2010 (64 Bit)	X		X
Microsoft .NET Framework >= 4.0 (a partire da Outlook 2010)			X

Nota: Per usare l'integrazione calendario di Exchange con Microsoft Small Business Server, in alcune circostanze può essere necessario disabilitare qui la FBA (Form Based Authentication).

Informazioni su Java 32 bit o 64 bit

Per usare la funzione di myPortal for Desktop "Importa contatti di Outlook all'avvio" con Microsoft Office 2013 nella versione a 64 bit, è necessaria l'installazione di Java nella versione a 64 bit. Se questa funzione non viene utilizzata, si consiglia Java nella versione a 32 bit, in quanto l'utilizzo della memoria è notevolmente inferiore. In generale, per questo motivo in tutte le altre installazioni è consigliata la versione a 32 bit di Oracle Java o OpenJDK.

Nota: L'uso continuo di Oracle Java con OpenScape Business non richiede modifiche. Se è richiesta una modifica della versione Java (ad esempio upgrade da Oracle Java 7 a Oracle Java 8 o Open JDK B8), è richiesta una reinstallazione del client di comunicazione.

Requisiti hardware minimi

- 2 GHz CPU
- RAM: 2 GB
- LAN 100 Mbit/s (consigliato: LAN 1 Gbit/s)
- Risoluzione del monitor XGA (1024x768), myPortal per Outlook: Risoluzione del monitor SVGA (800x600)

Nota: I monitor 4K non sono supportati per myPortal e myAttendant.

Microsoft Terminal Server, Citrix XenApp Server

I PC client UC Suite possono essere utilizzati in ambienti Microsoft Terminal Server e Citrix se vengono soddisfatti i requisiti riportati di seguito.

Suggerimento: Gli ambienti Terminal Server e Citrix Server, ivi compresi i servizi ospitati e gli ambienti virtuali, sono esclusi dall'ambito della fornitura.

Suggerimento: Gli ambienti Citrix Server possono decodificare non correttamente alcune lettere regionali (ad esempio l'umlaut tedesco).

Sistemi operativi:

- Microsoft Windows 2022 Server 64 bit
- Microsoft Windows 2019 Server 64 bit
- Microsoft Windows 2016 Server 64 bit
- Microsoft Windows 2025 Server 64 bit

Applicazioni di Office:

Microsoft Outlook / Office

- 2021 (32 bit/64 bit) + Office 365
- 2019 (32 bit/64 bit)

- 2016 (32 bit/64 bit): supportato, ma non più parte del test di sistema; in caso di errore non verrà fornita alcuna correzione SW (fine del supporto da parte di OpenScape Business)

Requisiti hardware:

il numero di client installabili dipende dalle prestazioni del server e dalla disponibilità di memoria. Se sul server sono utilizzate altre applicazioni, è necessario prendere in considerazione il relativo consumo di memoria.

File di installazione

Per mettere a disposizione degli utenti i file di installazione, sono disponibili le seguenti opzioni:

- L'amministratore scarica i file di installazione dal Servizio L'amministratore può scaricare i file di installazione dal **Centro assistenza** e fornirli agli utenti tramite un'unità di rete, ad esempio.
- L'amministratore scarica anche l'archivio del programma di installazione offline dall'esempio.
- L'amministratore può anche scaricare 'archivio del programma di installazione offline da **Centro assistenza** e i client possono installarlo offline.

13.2.7 Installazione/disinstallazione Silent per client PC UC Suite

L'installazione/disinstallazione Silent è un metodo basato su riga di comando per l'installazione/disinstallazione e la modifica automatiche su client PC della UC Suite senza necessità di inserire altri comandi.

Nota: Rispettare scrupolosamente le indicazioni contenute nel file `ReadMe first.rtf`.

L'installazione/disinstallazione Silent richiede i diritti di amministratore locale del PC in questione. L'installazione/disinstallazione Silent consente la registrazione della scadenza in un file.

Per l'installazione/disinstallazione Silent sono disponibili i seguenti parametri:

Parametri	Componenti
`/quiet`	Avvia la procedura d'installazione senza l'intervento dell'utente e senza interfaccia utente. Questo parametro richiede che sia già stato trovato l'archivio.
`/repository`	Imposta l'indirizzo IP o il nome host da utilizzare durante l'installazione. Ad esempio, `/repository=192.168.50.50`
`/installpath`	Imposta il percorso dei client installati. Il valore predefinito è: `C:\Program Files(x86)\communicationsclients\`

Parametri	Componenti
`/autostart`	Avvia la procedura d'installazione senza l'intervento dell'utente. Questo parametro richiede che sia già stato trovato l'archivio.
`/i`	Seleziona un prodotto da installare. I valori disponibili sono `OLI`, `myPortal`, `myAgent`, `FPD`, `myReports` e `all`. Ad esempio: `/i="OLI,FPD"`
`/u`	Seleziona un prodotto da rimuovere. Ad esempio: `/u="OLI,FPD"`
`/set`	Seleziona i prodotti che dovrebbero essere installati nel sistema. Questa opzione installerà i prodotti selezionati o, se sono già installati, li modificherà. Rimuoverà anche i prodotti non elencati nel set specificato. Ad esempio: `/set="OLI,FPD"`
`/repair`	Ripara i prodotti specificati. Ad esempio: `/repair="OLI,FPD"`

13.2.7.1 Come eseguire l'installazione Silent

Prerequisiti

Il PC soddisfa i requisiti descritti in Requisiti richiesti per client PC della UC Suite.

Si dispone dei diritti di amministratore locale del PC client.

Il file `CommunicationsClients.exe` è disponibile nel PC client.

Nota: Rispettare scrupolosamente le indicazioni contenute nel file `ReadMe first`.

Utilizzare le righe di comando nel seguente formato in un file batch o in una finestra con richiesta di input DOS.

Passo a passo

1) Se non si desidera registrare la scadenza, eseguire la seguente riga di comando:

   ```
   CommunicationsClients.exe /repository=<IP-address> /
   i=all /quiet
   ```

   In cui `<IP-address>` deve essere sostituito dall'IP dei client UC.

2) Se si desidera registrare una scadenza, ad esempio nel file `C:\ccinstall.log`, eseguire la seguente riga di comando:

   ```
   CommunicationsClients.exe /repository=<IP-address> /
   i="myPortal,FPD" /quiet /l="C:\ccinstall.log"
   ```

   In cui `<IP-address>` deve essere sostituito dall'IP dei client UC. Il comando summenzionato installa solo myPortal for Desktop e FaxPrinter. È possibile modificarlo per installare i client che si desidera.

13.2.7.2 Come eseguire la disinstallazione Silent

Prerequisiti

Il PC soddisfa i requisiti descritti in Requisiti richiesti per client PC della UC Suite.

Si dispone dei diritti di amministratore locale del PC client.

Il file `CommunicationsClients.exe` è disponibile nel PC client.

Nota: Rispettare scrupolosamente le indicazioni contenute nel file `ReadMe first`.

Utilizzare le righe di comando nel seguente formato in un file batch o in una finestra con richiesta di input DOS.

Passo a passo

1) Se dopo l'ultima installazione Silent viene eseguito un aggiornamento del sistema, è opportuno ripetere esattamente, con il nuovo file `CommunicationsClients.exe`, ogni riga di comando fino a quel momento eseguita con il file `CommunicationsClients.exe` esistente (come se si volesse reinstallare con il nuovo file `CommunicationsClients.exe` i componenti già installati). Successivamente è possibile la disinstallazione Silent.
2) Se non si desidera registrare la scadenza, selezionare una delle seguenti righe di comando:
   - Se si desidera disinstallare tutti i componenti:

     ```
     CommunicationsClients.exe /quiet /u=all
     ```
   - Se si desidera disinstallare più componenti, inserire i parametri corrispondenti sotto forma di elenco puntato separato da virgole dopo `/=`, ad esempio, myPortal for Desktop / myAttendant and Fax Printer:

     ```
     CommunicationsClients.exe /quiet /u="myPortal,FPD"
     ```
   - Se si desidera disinstallare solo un componente, inserire il parametro corrispondente dopo `/=`, ad esempio, myPortal for Desktop / myAttendant:

     ```
     CommunicationsClients.exe /quiet /u=myPortal
     ```

3) Se si desidera registrare una scadenza, ad esempio nel file `C:\ccuninstall.log`, selezionare una delle seguenti righe di comando:

- Se si desidera disinstallare tutti i componenti:

  ```
  CommunicationsClients.exe /quiet /l="C:
  \ccuninstall.log" /u=all
  ```

- Se si desidera disinstallare più componenti, inserire i parametri corrispondenti sotto forma di elenco puntato separato da virgole dopo `/=`, ad esempio, myPortal for Desktop / myAttendant and Fax Printer:

  ```
  CommunicationsClients.exe /quiet /l="C:
  \ccuninstall.log" /u="myPortal,FPD"
  ```

- Se si desidera disinstallare solo un componente, inserire il parametro corrispondente dopo `/=`, ad esempio, myPortal for Desktop / myAttendant:

  ```
  CommunicationsClients.exe /quiet /l="C:
  \ccuninstall.log" /u=myPortal
  ```

13.2.8 Aggiornamenti automatici

Gli aggiornamenti automatici assicurano che i client UC vengano mantenuti alla versione più recente disponibile.

Se è disponibile una nuova versione, verrà eseguito l'aggiornamento automatico o verrà notificata la disponibilità dell'aggiornamento. Può venire visualizzato un messaggio indicante che una o più applicazioni devono essere chiuse per eseguire l'aggiornamento automatico.

Nota: Si consiglia di eseguire sempre gli aggiornamenti automatici. Questo vale per il software necessario per specifici client UC.

Nota: L'aggiornamento automatico di myPortal @work non è supportato nei computer MacOS.

13.3 Utente e profilo utente della UC Suite

Gli utenti della UC Suite sono utenti che utilizzano i client UC della UC Suite. I profili utente memorizzano le impostazioni degli utenti della UC Suite.

13.3.1 Utenti della

Gli utenti della UC Suite utilizzano i client UC della UC Suite. Le impostazioni degli utenti della UC Suite possono essere configurate tramite la rubrica utente.

La rubrica utente contiene tutti gli utenti del sistema. Per l'utilizzo del client UC è necessario inserire altri dati nella rubrica utente.

Nell'indice utenti sono visualizzate le seguenti informazioni relative all'utente:

- Icona dello stato presenza

  L'amministratore può modificare lo stato presenza di qualsiasi utente.
- **Estensione**
- **Nome utente**

  Nota: Sebbene UCSuite consenta e supporti la modifica dei nomi utente per i propri client, tuttavia tali modifiche potrebbero influire sull'accesso di client non UCSuite, come myPortalToGo/myPortal@Work (ove applicabile), quindi non è consigliabile in tali situazioni.
- **Nome**

  Nome e cognome configurati per l'utente.
- **Reparto**

  Se all'utente è assegnato un reparto.
- **E-mail**

  Indirizzo e-mail
- **È agente**

  Livello di agente del Contact Center multimediale.
- **Casella vocale**

  L'utente può ricevere messaggi vocali.
- **Inoltro di chiamata**

  Per l'utente è configurata una deviazione di chiamata.

La funzionalità di ricerca è disponibile anche per i campi della rubrica utente.

Vengono configurate le seguenti impostazioni:

Valori e impostazioni	Parole chiave
Dati personali	
I miei dati personali	Nome proprio, nome utente, password, indirizzo e-mail, reparto, numero di telefono aggiuntivo
La mia immagine	La mia immagine Formati file supportati: BMP, JPG/JPEG/JFIFI, PNG. Dimensione massima del file: 10 MB
Livello utente	Ricezione di messaggi vocali: vedere Utenti Utente come posto operatore: vedere Utenti Utente come agente: vedere Utenti
Preferenze	
Aspetto	Colori interfaccia, lingua dell'interfaccia utente
Avvisi	Finestre popup
Collegamento calendario	Creazione automatica degli appuntamenti Outlook in caso di assenza, aggiornamento automatico dello stato presenza tramite appuntamenti Outlook/iCal

Valori e impostazioni	Parole chiave
Tasti di scelta rapida	Tasti di scelta rapida per le funzioni
Varie	Reset automatico dello stato presenza, metodo di trasferimento, tempo di conservazione per le voci del diario, indirizzo del server, tasti funzione del telefono
Regole di chiamata	
Destinazioni di inoltro	Deviazione di chiamata basata sullo stato
Motore regole	Deviazione di chiamata basata su regole
Comunicazioni	
Impostazioni casella vocale	Modalità registrazione o annuncio, lingua della casella vocale
Avviso VM	Servizio informativo per nuovi messaggi
Avviso fax	Servizio informativo per nuovi messaggi
Profili	
Occupato, Non rispondere, Riunione, Malattia, Pausa, Fuori sede, Vacanza, Pranzo, Abitazione	Profilo per AutoAttendant personale
Sensibilità	
Protezione e accesso	Recupero dei propri messaggi fax e vocali tramite il posto operatore, richiesta di immissione della password per la casella vocale
Visibilità presenza	Come modificare la visibilità del proprio stato presenza per gli Altri
Presenza casella vocale	Annuncio del proprio stato presenza per un chiamante esterno o per un chiamante specifico
Consenti ad altri utenti di copiare il mio layout BLF	Consenti ad altri utenti di copiare i gruppi e i pulsanti BLF Questa opzione non è disponibile per i profili già creati.
myAttendant	
Messaggi LAN	Modulo di testo di un messaggio istantaneo
DID	MSN
Comunicazioni	Inoltro di chiamata

Per informazioni più precise sulle impostazioni dell'utente, consultare il Manuale d'uso dei client UC, alle parole chiave riportate nella tabella.

Per impostazione predefinita, la lunghezza della password per l'utilizzo dei client UC è di sei caratteri. La lunghezza della password può essere modificata in base alle proprie necessità (6-10 caratteri). Il numero massimo di caratteri ripetuti è due e il numero massimo di caratteri progressivi è tre. Il nome dell'account (invertito o meno) non può fare parte della password e la modifica della password richiede la conoscenza della vecchia password. L'utente è

costretto a modificare la password predefinita dopo il primo utilizzo. Il numero massimo di tentativi di accesso errati è cinque. Un amministratore con il profilo **Advanced** può modificare la password di un utente (ad esempio, perché quest'ultimo l'ha dimenticata).

Nota: Il nome e il cognome di un utente presenti nella rubrica utente verranno sovrascritti se modificati tramite una procedura guidata o entrando in modalità esperti. Se invece il nome e il cognome di un utente vengono modificati nella rubrica utente, i dati dell'utente, visualizzati utilizzando una procedura guidata o in modalità esperti, non verranno sovrascritti. In questo caso esisteranno due diversi nomi utente per lo stesso utente. Inoltre, se la lunghezza del nome e quella del cognome sono superiori a 16 caratteri in totale, vengono interrotte a 16 per adattarle alla visualizzazione sul dispositivo.

Gli utenti per cui è stato configurato un indirizzo e-mail e che utilizzano myPortal for Desktop, riceveranno un messaggio e-mail di benvenuto con istruzioni per i primi passi da eseguire per utilizzare il programma.

Reset dei dati utente

Le impostazioni di un utente possono essere riportate ai valori predefiniti. Il reset dei dati di un utente cancellerà tutti i dati dell'utente, compresi il nome, cognome e nome utente.

A prescindere dal fatto che il nome o il cognome dell'utente siano impostati con **WBM** > **Modalità esperti** > **Server telefonia** > **Utente**, il reset di questo utente con UC Suite potrà assegnare il numero archiviato come Interno anche al campo **Nome**.

13.3.1.1 Come configurare gli utenti della UC Suite

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Rubrica utente**. Vengono visualizzati tutti gli utenti.
4) Selezionare l'utente desiderato e premere **Modifica**.
5) Modificare i dati dell'utente.
6) Fare clic su **Salva**. La finestra verrà automaticamente chiusa. Vengono visualizzati tutti gli utenti.
7) Se si desidera configurare altri utenti, ripetere i passi da 4 a 6.

13.3.1.2 Come reimpostare gli utenti della UC Suite

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Rubrica utente**. Vengono visualizzati tutti gli utenti.
4) Selezionare l'utente desiderato e premere **Reimposta utente**.
5) Fare clic su **Salva**. La finestra verrà automaticamente chiusa. Vengono visualizzati tutti gli utenti.
6) Se si desidera reimpostare altri utenti, ripetere i passi da 4 a 5.

13.3.1.3 Come configurare un utente della UC Suite come agente (myAgent)

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Rubrica utente**. Vengono visualizzati tutti gli utenti.
4) Fare clic nella riga con l'utente corrispondente.
5) Fare clic su **Modifica**.
6) Fare clic su **Dati personali** > **Livello utente**.
7) Selezionare una delle seguenti opzioni:

   Se l'agente deve essere permanentemente disponibile, selezionare la casella di controllo **Agente sempre disponibile**. L'agente rimane disponibile per chiamate, fax e e-mail, anche se non ha risposto a una chiamata, fax o e-mail.

   Se l'agente non deve essere permanentemente disponibile, deselezionare la casella di controllo **Agente sempre disponibile**. L'agente riceve lo stato non disponibile se non ha risposto a una chiamata, fax o e-mail.
8) Nell'elenco a discesa **Livello** selezionare il ruolo desiderato per l'agente: **Agente**, **Supervisore** o **Amministratore**.
9) Fare clic su **Salva**.
10) Se si desidera configurare altri utente come agenti, ripetere i passi da 4 a 9.

13.3.1.4 Come cambiare lo stato presenza per un utente della UC Suite

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Rubrica utente**. Vengono visualizzati tutti gli utenti.
4) Selezionare l'utente desiderato.
5) Fare clic sull'icona dello stato di presenza e selezionare lo stato di presenza pertinente dall'elenco a discesa. Se necessario, inserire l'orario di rientro nel formato `aaaa/mm/gg hh:mm`, per esempio, `2012/12/12 12:00`.
6) Fare clic su **Salva**.
7) Se si desidera cambiare lo stato presenza per un altro utente, ripetere i passi da 4 a 6.
8) Chiudere la finestra.

13.3.1.5 Come modificare la password per un utente della UC Suite

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Click on **Edit** to start the **User Directory** wizard. Vengono visualizzati tutti gli utenti.
4) Mark the corresponding user and click **Edit** > **Personal Details** > **My Personal Details**.
5) Nel campo **Password** fare clic su **Modifica**.
6) Enter the new password under **New**.
7) Enter the new password under **Confirm**.
8) Fare clic su **OK**. La finestra verrà automaticamente chiusa. Vengono visualizzati tutti gli utenti.
9) If you want to change the password of another user, repeat steps 4 through 8.

Passaggi successivi

Informare l'utente o gli utenti in questione della nuova password.

13.3.1.6 Come modificare la lunghezza della password per un utente della UC Suite

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) In the navigation bar, click on **Expert Mode**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**.
4) Fare clic su**Impostazioni generali**.
5) Enter the minimum required password length (6-10) for the future in the **Lengths** field, under the**Length of Password** area.
6) Fare clic su **Salva**.

13.3.2 Profili utente della UC Suite

I profili utente della UC Suite memorizzano le impostazioni degli utenti della UC Suite. A un profilo utente possono essere assegnati più utenti (membri). A tutti i membri di un profilo si applicano le stesse impostazioni.

Ogni utente può essere membro di un solo profilo utente. Modifiche dirette delle impostazioni di un utente, quindi non tramite il profilo assegnato, eliminazione automatica dell'utente dal profilo.

Se viene eliminata l'assegnazione di un utente a un profilo, le impostazioni rappresentate da questo profilo rimangono.

Quando un utente è già assegnato a un profilo, solo le modifiche agli elementi del profilo bloccato verranno applicate a tale utente. Se il simbolo di blocco appare sbloccato, le modifiche non verranno applicate.

Se viene eliminato l'intero profilo, gli utenti che vi erano assegnati conservano le impostazioni del profilo.

È possibile configurare i seguenti valori e impostazioni:

Opzioni di menu	Valori e impostazioni per
Dati personali	
I miei dati personali	Visibilità dei numeri di telefono
Preferenze	
Aspetto	Colori interfaccia, lingua dell'interfaccia utente
Avvisi	Finestre popup
Connettività Outlook	Creazione automatica degli appuntamenti Outlook in caso di assenza, aggiornamento automatico dello stato presenza tramite appuntamenti Outlook/ iCal

Opzioni di menu	Valori e impostazioni per
Tasti di scelta rapida	Attivazione e impostazione di combinazioni di tasti per accedere a varie funzionalità comunemente usate tramite la tastiera. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Varie	Reset automatico dello stato presenza, metodo di trasferimento, tempo di conservazione per le voci del diario, indirizzo del server
Regole di chiamata	
Destinazioni di inoltro	Deviazione di chiamata basata sullo stato
Comunicazioni	
Impostazioni casella vocale	Modalità registrazione o annuncio, lingua della casella vocale
Avviso VM	Servizio informativo per nuovi messaggi
Avviso fax	Servizio informativo per nuovi messaggi
Notifiche di chiamata senza risposta	Notification Service for Missed Calls
Profili	
Profili	Profile for personal AutoAttendant. Available status: Busy, No Answer, Meeting, Sick, Break, Out of Office, Holiday, Lunch, Home
Sensibilità	
Protezione e accesso	Recupero dei propri messaggi fax e vocali tramite il posto operatore, richiesta di immissione della password per la casella vocale
Visibilità presenza	Come modificare la visibilità del proprio stato presenza per gli Altri
Presenza casella vocale	Annuncio del proprio stato presenza per un chiamante esterno o per un chiamante specifico
Preferiti	
Preferiti	Gruppi Preferiti con un elenco di contatti che possono essere assegnati all'utente.

Per informazioni più precise sulle impostazioni del profilo, consultare il Manuale d'uso dei client UC, alle parole chiave riportate nella tabella.

13.3.2.1 Come aggiungere un profilo utente della UC Suite

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Profilo**. Vengono visualizzati tutti i profili utente e i relativi membri.
4) Fare clic su **Aggiungi**.
5) Nel campo **Nome** inserire il nome desiderato per il profilo.
6) Fare clic su **Salva**.
7) Configurare le impostazioni desiderate del profilo utente.
8) Fare clic su **Salva** e chiudere la finestra.

13.3.2.2 Come modificare un profilo utente della UC Suite

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Profilo**. Vengono visualizzati tutti i profili e i relativi utenti.
4) Selezionare il profilo desiderato.
5) Fare clic su **Modifica**.
6) Modificare i valori e le impostazioni desiderati.

   Nota: Fare clic su **Salva** per rendere effettive le modifiche prima di passare a un'altra voce di menu.

7) Infine fare clic su **Salva** e chiudere la finestra.

13.3.2.3 Come visualizzare il profilo utente della UC Suite

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Profilo**. Vengono visualizzati tutti i profili utente e i relativi membri.

13.3.2.4 Come aggiungere membri a un profilo utente della UC Suite

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Profilo**. Vengono visualizzati tutti i profili utente e i relativi membri.
4) Selezionare il profilo utente desiderato e premere il pulsante **Assegna utenti**.
5) Dall'elenco **Utenti disponibili** scegliere il membro desiderato.
6) Fare clic su **<-** per trasferirli nell'elenco **Utenti assegnati**.

   Vengono visualizzati tutti i profili utente e i relativi membri.
7) Chiudere la finestra.

13.3.2.5 Come eliminare i membri da un profilo utente della UC Suite

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Profilo**. Vengono visualizzati tutti i profili utente e i relativi membri.
4) Selezionare il profilo utente desiderato e premere il pulsante **Assegna utenti**.
5) Dall'elenco **Utenti assegnati** selezionare il membro corrispondente.
6) Fare clic su **->** per trasferirli nell'elenco **Utenti disponibili**.

   Vengono visualizzati tutti i profili utente e i relativi membri.
7) Chiudere la finestra.

13.3.2.6 Come eliminare un profilo utente della UC Suite

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Profilo**. Vengono visualizzati tutti i profili utente e i relativi membri.
4) Selezionare il profilo utente desiderato.

5) Fare clic su **Rimuovi**.
6) Confermare con **OK**. Vengono visualizzati tutti i profili utente e i relativi membri.
7) Chiudere la finestra.

13.4 Stato presenza e servizio CallMe

Lo stato presenza e il servizio CallMe mostrano la reperibilità degli utenti, ottimizzandola. Lo stato presenza consente di eseguire in modo semplice la deviazione di chiamata in base allo stato, nonché di deviare la chiamata come configurato in myPortal for Desktop e myPortal for Outlook facilmente in base a regole.

13.4.1 Stato presenza (presenza)

Lo stato presenza comunica la disponibilità degli utenti interni (anche utenti mobili) nell'elenco dei Preferiti, nella rubrica interna, nella sala conferenze virtuale e tramite annunci della casella vocale. Oltre a ciò con lo stato presenza è possibile controllare la reperibilità degli utenti interni tramite le funzioni di deviazione di chiamata basata sullo stato, sulle regole e sull'AutoAttendant personale.

Un utente può modificare il proprio stato presenza tramite myPortal for Desktop, myPortal for Outlook o il menu della casella vocale. Disattivando una deviazione di chiamata nel telefono, il proprio stato presenza torna a essere**Ufficio**. A ogni modifica dello stato presenza, a eccezione di **Ufficio** e **CallMe**, è possibile definire il momento del ritorno previsto in **Ufficio** o **CallMe**.

L'utente può scegliere uno dei seguenti stati:

- **Ufficio**
- **Riunione**
- **Malattia**
- **Pausa**
- **Fuori sede**
- **In vacanza**
- **Pranzo**
- **A casa**
- **Non disturbare**

Nota: L'amministratore di sistema può abilitare/disabilitare la visibilità dello stato "malato" all'interno dell'amministrazione del sistema. Vedere OpenScape Business UC Suite > Server

---

Deviazione sulla casella vocale

Quando lo stato presenza di un utente non è **Ufficio** o **CallMe**, per impostazione predefinita, il sistema di comunicazione devia le chiamate sulla casella vocale e comunica, mediante annunci basati sullo stato, il tipo di assenza e il momento previsto del ritorno.

Testo informativo

È possibile aggiungere un testo informativo a scelta al proprio stato presenza corrente, ad esempio durante una riunione: "Sono nella sala n. ...". Il testo informativo viene visualizzato nell'elenco dei Preferiti, nella rubrica interna e nella sala conferenze virtuale. Alla modifica del proprio stato presenza, il testo informativo viene cancellato.

Reset automatico dello stato presenza

Al termine del periodo di assenza pianificato, l'utente può ripristinare automaticamente lo stato **Ufficio**. In caso contrario, il sistema estende lo stato presenza corrente per intervalli di 15 minuti, fino a quando non viene modificato dall'utente.

Visibilità dello stato presenza

L'utente può definire se il proprio stato presenza (diverso da **Ufficio** e **CallMe**), il momento previsto del rientro e il testo informativo eventualmente da questo inserito possono essere visualizzati dai singoli utenti della rubrica interna.

Nota: Le impostazioni di visibilità non vengono applicate per gli utenti myAttendant, in quanto possono sempre vedere lo stato di presenza di altri utenti.

Aggiornamento automatico dello stato presenza tramite appuntamenti Outlook/iCal

L'utente può controllare in modo automatico il proprio stato presenza tramite appuntamenti (tuttavia non disdetti o solo proposti) inserendo parole chiave specifiche nell'oggetto. È possibile scegliere tra i seguenti calendari:

- Calendario di Exchange (sul Microsoft Exchange Server)

  L'aggiornamento automatico dello stato presenza tramite appuntamenti Outlook viene eseguito indipendentemente dal fatto che il proprio PC sia acceso o meno. Per poter utilizzare questa funzione, è necessario che l'amministratore abbia configurato l'integrazione del calendario di Exchange.

  Nota: Per maggiori dettagli sull'uso delle diverse versioni del server Microsoft Exchange, consultare il sito Unify Experts Wiki all'indirizzo: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

- Calendario di Outlook

  L'aggiornamento automatico dello stato presenza tramite appuntamenti Outlook richiede che sul PC siano aperti myPortal for Desktop o myPortal for Outlook.
- Calendario iCal (myPortal for Desktop)

È possibile utilizzare le seguenti parole chiave:

- **Riunione**
- **Malattia**
- **Pausa**
- **Fuori sede**
- **In vacanza**

- **Pranzo**
- **A casa**

Le parole chiave dipendono dalla lingua dell'interfaccia utente installata. Le parole chiave possono trovarsi in qualsiasi punto dell'oggetto. Se l'oggetto contiene più parole chiave, solo la prima sarà effettiva. Se questa funzione è attivata, il proprio stato presenza viene modificato automaticamente all'ora di inizio e di fine dell'appuntamento in questione. La verifica degli appuntamenti nel calendario avviene a intervalli di 30 secondi.

Nota: Se si attiva questa funzione, fare attenzione che qualsiasi appuntamento il cui oggetto contiene le parole chiave corrispondenti determinerà una modifica del proprio stato presenza. Può essere necessario modificare l'oggetto.

Nota: A seconda delle impostazioni di sistema da parte dell'amministratore, lo stato di presenza "malato" potrebbe non essere disponibile.

Creazione automatica di appuntamenti Outlook in caso di assenza (Windows)

L'utente può creare automaticamente appuntamenti di Outlook quando è assente, modificando il proprio stato presenza. L'oggetto del relativo appuntamento Outlook sarà costituito dal proprio stato presenza e dal testo "(Auto)", ad esempio, "Riunione (Auto)". L'ora di inizio e fine di un appuntamento corrisponde alle informazioni in myPortal for Desktop o myPortal for Outlook. L'ora di fine dell'appuntamento Outlook rimane invariata in caso di un eventuale ritorno ritardato. È possibile definire se gli appuntamenti Outlook devono essere salvati nel file PST locale o sul server Exchange. Se si desidera che il salvataggio avvenga nel file PST locale, è necessario che Outlook sia aperto al momento della creazione degli appuntamenti. Se si desidera che il salvataggio avvenga sul server Exchange, gli appuntamenti Outlook vengono creati indipendentemente dal fatto che Outlook sia aperto. Per poter utilizzare questa funzione, è necessario che l'amministratore abbia configurato l'integrazione del calendario di Exchange.

Nota: Per maggiori dettagli sull'uso delle diverse versioni del server Microsoft Exchange, consultare il sito Unify Experts Wiki all'indirizzo: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

Finestra popup quando si modifica dello stato presenza

L'utente può visualizzare le modifiche al proprio stato presenza tramite finestre popup.

13.4.2 Servizio CallMe

Con il servizio CallMe, un utente può definire un qualsiasi telefono in una postazione di lavoro alternativa come destinazione CallMe, alla quale sarà raggiungibile con il suo numero interno. L'utente può utilizzare myPortal for Desktop o myPortal for Outlook presso la postazione di lavoro

alternativa come se fosse in ufficio, e quindi eseguire anche chiamate in uscita dalla destinazione CallMe.

Chiamate in arrivo

Le chiamate in arrivo sul numero interno vengono deviate sulla destinazione CallMe. Al chiamante viene mostrato il numero interno dell'utente chiamato. In questo modo, le chiamate senza risposta vengono inoltrate alla casella vocale dopo 60 secondi.

Chiamata in uscita

Per le chiamate in uscita con myPortal for Desktop o myPortal for Outlook, il sistema di comunicazione crea due connessioni: prima il sistema di comunicazione chiama l'utente alla destinazione CallMe. Quando l'utente risponde, il sistema di comunicazione chiama la destinazione desiderata e connette assieme i due punti. Alla destinazione viene mostrato il numero interno originale del chiamante (servizio One Number).

Stato presenza

Se il servizio CallMe è attivato, nel display del proprio telefono viene visualizzato "`CallMe attivo`" (non applicabile ai telefoni analogici e DECT). Gli altri utenti vedono lo stato presenza **Ufficio**.

Attivazione

L'utente può attivare manualmente il servizio CallMe. Il servizio CallMe viene inoltre riattivato tramite reset automatico dello stato presenza dopo un'assenza, a condizione che prima di tale assenza fosse attivo. Non sono supportati i seguenti tipi di destinazioni CallMe:

- Gruppo
- Telefono su cui si effettua la deviazione

Visualizzazione della destinazione CallMe nell'elenco dei preferiti

Un utente può definire che nell'elenco dei preferiti di altri utenti dovrà essere visualizzato il numero di telefono della destinazione CallMe anziché il proprio numero di telefono.

Disattivazione

Il servizio CallMe rimane attivo fino alla modifica dello stato presenza dell'utente.

Nota: La funzione CallMe non deve essere utilizzata al momento di selezionare il numero o effettuare una chiamata a una conferenza aperta.

13.4.3 Deviazione di chiamata in base allo stato

La deviazione di chiamata in base allo stato consente all'utente di deviare i chiamanti sulla base del proprio stato presenza a uno dei propri numeri di telefono aggiuntivi o alla casella vocale.

Un utente può configurare la deviazione di chiamata in base al proprio stato per ogni stato presenza eccetto **Ufficio**, **CallMe** e **Non disturbare**. Se si desidera modificare il proprio stato presenza, il sistema di comunicazione attiva la deviazione di chiamata alla destinazione definita dall'utente, ad esempio, se si è fuori sede, al proprio telefono cellulare e mentre si è in vacanza al proprio sostituto.

13.4.4 Inoltro di chiamata basato su regole

Con la deviazione di chiamata basata su regola, l'utente può trasferire il chiamante sulla base di diverse condizioni o eccezioni in modo ancora più flessibile dell'inoltro di chiamata basato sullo stato.

Oltre a ciò, la deviazione di chiamata basata su regole supporta:

- Qualsiasi destinazione
- Stato presenza **Ufficio**, **Riunione, Malattia, Pausa, Fuori sede, Vacanza, Pranzo, A casa**

Nota: CallMe e **Non disturbare** non sono validi per l'inoltro di chiamate basate su regole.

Con la procedura guidata regole, l'utente può definire le regole e attivarle o disattivarle in qualsiasi momento. Una regola è attiva solo se per il proprio telefono non è definita una deviazione. La deviazione di chiamata basata sullo stato (ad eccezione della deviazione alla casella vocale) ha priorità rispetto all'inoltro di chiamata basato su regole.

Se una regola è attiva per l'inoltro di chiamata, il display del telefono mostra **"regola attiva"**.

All'arrivo di una chiamata, il sistema di comunicazione verifica la disponibilità di regole attive in base alla sequenza definita nella procedura guidata regole. Viene eseguita solo la prima regola disponibile. In questo caso, dopo uno squillo il sistema di comunicazione devia la chiamata alla destinazione impostata.

In una regola possono essere definiti più tipi di condizioni ed eccezioni (eccetto …). Tuttavia, non è possibile definire una condizione con un'eccezione dello stesso tipo. Ad esempio, non è possibile configurare una condizione del tipo "un certo giorno della settimana" con un'eccezione del tipo "escluso un certo giorno della settimana".

Tipi di condizioni ed eccezioni

- (eccetto) un certo stato presenza
- (eccetto) una certa persona (nella rubrica interna, nella rubrica esterna, nella rubrica personale o con un numero di telefono specifico)
- (eccetto) chiamate trasferite all'utente da una certa persona (nella rubrica interna, nella rubrica esterna, nella rubrica personale o con un numero di telefono specifico)
- (eccetto) di un certo tipo, ovvero **interne** o **esterne** o di un **contatto sconosciuto**
- (eccetto) in una data specifica (o più date)
- (eccetto) in certi giorni della settimana

- (eccetto) tra una data di inizio e una di fine
- (eccetto) tra un'ora di inizio e una di fine

13.5 Rubriche e diario

Le rubriche, l'elenco dei preferiti e il diario consentono di organizzare contatti e chiamate.

13.5.1 Rubriche

Le rubriche consentono di organizzare i contatti di un utente. Con i client UC Suite nonché con i telefoni di sistema dotati di display, gli utenti possono accedere ai contatti.

Il sistema fornisce le seguenti rubriche, che supportano queste funzioni con la priorità sottoindicata per il numero di ricerca (il numero di ricerca è supportato solo per le chiamate esterne e se CO/ITSP non fornisce il nome):

Rubrica	myPortal for Desktop, myAttendant, myAgent, Fax Printer	myPortal for Outlook	Telefono di sistema con Display
Contatti Outlook Contatti Mac OS (myPortal for Desktop)	All'occorrenza, l'utente può importare in Microsoft Windows i contatti di Outlook/Mac OS all'avvio di myPortal for Desktop.	Contiene i contatti personali Outlook di un utente. Solo l'utente stesso ha accesso in scrittura a questi dati.	Contiene i contatti personali Outlook di un utente. Solo l'utente stesso ha accesso in scrittura a questi dati.
Rubrica personale	All'avvio di myPortal for Desktop, l'utente ha la possibilità di importare i contatti Outlook o di Mac OS o di gestire i contatti personali manualmente. Non è possibile modificare i contatti importati.	-	Con l'Assistente personale, è possibile importare i contatti di Outlook.

Rubrica	myPortal for Desktop, myAttendant, myAgent, Fax Printer	myPortal for Outlook	Telefono di sistema con Display
Rubrica interna	La rubrica interna di UC Smart offre funzionalità aggiuntive con la UC Suite. Contiene: • Tutti gli utenti interni • Gruppi per i quali è attiva la visualizzazione nel sistema • Numeri di telefono aggiuntivi, se l'utente ha reso queste informazioni visibili agli altri utenti interni Gli utenti interni (con un telefono di sistema) vengono rappresentanti con il relativo stato presenza e possono essere contattati mediante messaggi istantanei. Condizione essenziale per la visualizzazione dello stato presenza di un utente è che l'utente in questione l'abbia autorizzata. Eventualmente viene visualizzata l'ora ritorno prevista. Inoltre può essere visualizzato testo informativo inserito dall'utente. Un utente ha accesso a questa rubrica in sola lettura. La rubrica interna include la rubrica del sistema. Tuttavia, le ricerche eseguite nella rubrica interna non includono i risultati della rubrica del sistema, ma solo le voci della rubrica interna.		Contiene tutti gli utenti interni e i gruppi per i quali è attiva la visualizzazione nel sistema.
Rubrica esterna	Contiene i contatti di una rubrica di utenti ed è configurata dall'amministratore. Un utente ha accesso a questa rubrica in sola lettura.		-
Cartella di Exchange pubblica (non utilizzabile con Office 365)	Contiene i contatti della cartella pubblica di Exchange, se questa è stata configurata dall'amministratore. Questi vengono visualizzati nella rubrica esterna. Per maggiori dettagli sull'uso delle diverse versioni del server Microsoft Exchange, consultare il sito Unify Experts Wiki all'indirizzo: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.		-
Rubrica esterna non in linea (LDAP)	Contiene i contatti di una rubrica di utenti LDAP ed è configurata dall'amministratore. La rubrica esterna non in linea può essere utilizzata solo per le ricerche. L'amministratore può attivare e disattivare la visualizzazione della rubrica esterna non in linea per i telefoni di sistema.		
Rubrica di sistema	Contiene tutti i numeri di sistema, gli utenti UC e non UC. Gli utenti non UC includono gli utenti senza licenze UC e le postazioni virtuali, come Fax e AutoAttendant. La rubrica di sistema non si applica a Fax Printer		Contiene tutti gli utenti interni e tutti i numeri di selezione breve centrali. L'amministratore può attivare e disattivare la visualizzazione di un utente nella rubrica del sistema.

Nota: I numeri di telefono memorizzati nelle impostazioni e in tutte le rubriche (interne, esterne, personali, Outlook, Exchange) devono essere inseriti in formato canonico per essere raggiungibili sia da UC che dal dispositivo.

Il codice di accesso non deve essere incluso nel numero.

Nota: L'aggiunta o la rimozione di un contatto UC può richiedere vari minuti (**e** fino a 30 minuti) fino all'applicazione delle modifiche su tutti i client e dispositivi per via dei meccanismi di memorizzazione nella cache utilizzati. In alternativa è possibile riavviare il sistema per rendere **immediatamente** effettive le modifiche.

Ricerca semplice

È possibile come utente eseguire ricerche nelle rubriche in base al **Nome**, **Cognome** o a un numero di telefono. La ricerca nelle rubriche viene eseguita nell'ordine indicato nella tabella in alto. È possibile cercare una parola intera o anche stringhe parziali, ad esempio una parte di un numero di telefono. Le opzioni di ricerca impostate rimangono effettive anche per le successive ricerche. Tutti i termini ricercati vengono salvati in un elenco, che l'utente può successivamente eliminare.

Ricerca avanzata

È possibile eseguire ricerche in base ai campi **Titolo**, **Nome**, **Cognome**, **Società**, **Interno**, **Num. società**, **Num. ufficio 1**, **Num. ufficio 2**, **Num. abitazione 1**, **Num. abitazione 2**, **Numero cellulare** e **E-mail** e limitare il numero massimo di risultati. L'interfaccia moderna di myPortal for Desktop non supporta la ricerca avanzata. In un dispositivo sono supportati solo **Num. ufficio 1**, **Num. abitazione 1**, **Numero cellulare**.

Ordinamento

I contatti in una rubrica di myPortal for Desktop e myPortal for Outlook possono essere disposti in ordine alfanumerico crescente o decrescente per colonne. L'interfaccia moderna di myPortal for Desktop non supporta l'ordinamento.

13.5.1.1 Come configurare le rubriche dei telefoni del sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È possibile selezionare quali rubriche sono disponibili per i telefoni di sistema con display.

Passo a passo

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony Server** > **Basic Settings** in the navigation tree.
3) Nella struttura dei menu, fare clic su **Sistema** > **Display**.

4) Nell'elenco a discesa **Rubrica**, selezionare una delle seguenti opzioni:
   - Se devono essere disponibili i contatti personali e le rubriche interna, esterna, di rete e LDAP, selezionare **Tutte**.
   - Se devono essere disponibili solo i contatti personali e le rubriche interna, esterna e di rete, selezionare **Interne**.
   - Se deve essere disponibile solo la rubrica LDAP, selezionare **LDAP**.
   - Se non deve essere disponibile alcuna rubrica, selezionare **No**.

   Nota: L'utente può attivare la gestione delle richieste di ricerca da parte della Rubrica unificata selezionando **Rubrica telefonica interna tramite Rubrica unificata**. When the flag is deactivated and there is no access to Unified Directory, the list view at the phone-book menu, implemented for the OpenScape Desk Phone CP 200/205/210, is not available.

5) Fare clic su **Applica**.

Passaggi successivi

Se si è selezionato **Tutti** o **LDAP**, assicurarsi che sia disponibile una corrispondente rubrica LDAP (ad esempio Open Directory Service) per i telefoni di sistema.

13.5.2 Rubrica interna

La rubrica interna contiene i dettagli di contatto dei utenti interni del sistema di comunicazione. I client UC Suite hanno accesso alla rubrica del sistema.

L'amministratore ha accesso illimitato a tutti i dati nella rubrica interna. Gli utenti possono comporre i numeri di telefono direttamente da quest'ultima.

L'amministratore può disattivare la visualizzazione di tutti gli utenti analogici o di quelli senza nome. In quest'ultimo caso, non verranno visualizzati gli utenti il cui nome inizia con -.

13.5.2.1 Come attivare o disattivare un utente analogico nella rubrica interna

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Nella struttura dei menu fare clic su **Server**.
4) Fare clic sulla scheda **Impostazioni generali**.

5) Nell'area **Estensioni analogiche**, nell'elenco a discesa **Modalità utente analogico**, selezionare una delle seguenti opzioni:
   - Se si desidera visualizzare tutti gli utenti analogici della rubrica interna, selezionare **Mostra tutti**.
   - Se si desidera visualizzare solo gli utenti analogici della rubrica interna che comprendono un nome, selezionare **Mostra solo utenti con nome**.

     Nota: Con questa impostazione, non verranno visualizzati gli utenti analogici il cui nome inizia con -.
   - Se non si desidera visualizzare gli utenti analogici della rubrica interna, selezionare **Non mostrato**.
6) Fare clic su **Salva**.

13.5.2.2 Come abilitare o disabilitare la ricerca solo nella rubrica interna

Quando si compone un numero utilizzando il nome, è possibile configurare il sistema per limitare la ricerca solo alla rubrica interna o per cercare in tutte le rubriche dell'ambiente di rete. Per impostazione predefinita, il sistema è configurato per eseguire la ricerca solo nella rubrica interna.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications> OpenScape Business UC Suite**.
3) Click **Servers** in the menu tree.
4) Click on the **General Settings** tab.
5) To enable searching only in the internal directory, select the check box **Dial by name search local extension only**, under the **Directory Server** area.

   Nota: The check box **Dial by name search local extension only** is enabled by default.

   Il sistema cerca ora solo nella rubrica interna quando si utilizza la composizione per nome. Quando viene raggiunta l'estensione locale, il sistema riproduce il nome del ricevitore (se precedentemente registrato).
6) To disable searching only in the internal directory, clear the check box **Dial by name search local extension only**, under the **Directory Server** area.

   Quando si utilizza la composizione per nome il sistema cerca ora in tutte le rubriche dell'ambiente di rete.

13.5.3 Rubrica esterna

La rubrica esterna contiene i contatti di utenti esterni al sistema di comunicazione.

I dati della rubrica esterna sono a disposizione di tutti gli utenti di tutti i client UC Suite e sui telefoni dotati di display. Gli utenti possono comporre un numero dalla rubrica esterna. Gli utenti dei client della UC Suite myAttendant e myAgent possono modificare i dati nella rubrica esterna.

Importazione di un file CSV

L'amministratore può importare i contatti da un file CSV nel formato UTF-8 dal file system locale o da una condivisione di rete nella rubrica esterna.

La riga di intestazione nel file CSV consente l'assegnazione del nome del campo del file CSV ai campi del sistema. Il file CSV può ad esempio essere strutturato come segue:

- Intestazione:

  "ID cliente","Cognome","Nome","Numero di telefono società","Nome società"
- Righe dati:

  "987654","Dubios","Natalie","+498977712345","Company"

Per l'importazione del file CSV nel sistema, è possibile assegnare i seguenti campi:

- ID cliente
- Titolo
- Nome
- Cognome
- Società
- Num. ufficio
- 2° num. ufficio
- Num. cellulare
- Abitazione
- Num. fax
- E-mail
- Città

Nota: Il nome del contatto verrà visualizzato nella cronologia delle chiamate, solo se si compilano entrambi i campi Nome e Cognome.

Dopo la modifica del modello CSV, il file deve essere salvato in formato UTF-8 per garantire l'importazione corretta degli eventuali caratteri speciali presenti.

Se durante l'importazione i dati devono essere sovrascritti, gli **ID cliente** devono essere identici.

Nota: Per un modello CSV e una descrizione della sintassi richiesta per l'importazione di dati per la rubrica esterna, vedere **Centro assistenza** > **Documenti** > **Modelli CSV**.

13.5.3.1 Come importare un file CSV dal file system locale nella rubrica esterna

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Nel file system locale è disponibile un file CSV di tipo adatto nella codifica UTF-8 con i dati per la rubrica esterna.

La lunghezza dei campi dei modelli CSV è soggetta ad alcune limitazioni. I limiti di lunghezza sono elencati di seguito:

- customer_business carattere variabile(50)
- customer_business2 carattere variabile(50)
- customer_home carattere variabile(50)
- customer_mobile carattere variabile(50)
- customer_title carattere variabile(20)
- customer_firstname carattere variabile(50)
- customer_surname carattere variabile(50)
- customer_company carattere variabile(255)
- customer_id carattere variabile(255)
- customer_xmppid carattere variabile(256)
- customer_fax carattere variabile(50)
- customer_email carattere variabile(255)
- customer_city carattere variabile(255)
- customer_street_address carattere variabile(2048)
- customer_import_source carattere variabile(256)

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Rubrica esterna**.
4) Fare clic sulla scheda **Importa directory esterna**.
5) Selezionare una delle seguenti opzioni:
   - Se si desidera caricare il file CSV del file system locale, selezionare il pulsante di opzione **File locale**, quindi nell'area **Carica file** selezionare il file CSV.
   - Se si desidera caricare il file CSV da una condivisione di rete, selezionare il pulsante di opzione **Cartella di Windows pubblica** e, nell'area **Cartella Windows pubblica**, inserire i dati per l'accesso alla condivisione di rete (nome del file CSV, nome di dominio, nome utente e una password per la condivisione).

     È possibile verificare la correttezza delle voci tramite il comando **Test**.
6) Nell'area **Caricamento file**, fare clic su **Scegli file** e selezionare il file desiderato.
7) Nel campo **Righe intestazione** immettere il numero di righe di intestazione del file CSV.
8) Inserire il **Separatore campi** utilizzato nel file CSV.

9) Selezionare una delle seguenti opzioni:

- Se si desidera eliminare i dati esistenti dalla directory esterna, selezionare la casella di controllo **Rimuovi rubrica prima dell'importazione**.
- Se non si desidera eliminare i dati esistenti dalla directory esterna, deselezionare la casella di controllo **Rimuovi rubrica prima dell'importazione**.

Nota: Il flag **Rimuovi rubrica prima dell'importazione** non rimuove i record se sono già utilizzati in altre funzioni, ad esempio chiamante VIP, ecc.

Nota: Il flag **Rimuovi dati prima dell'importazione** elimina solo i dati importati dall'importazione CSV. I dati importati manualmente non vengono cancellati per evitare perdite di dati impreviste. L'unico modo per eliminare i dati inseriti manualmente è cancellarli manualmente.

---

10) Nell'area **ID cliente duplicato**, definire come il sistema dovrà comportarsi durante l'importazione con gli ID cliente già disponibili:

- Se si desidera sovrascrivere i contatti disponibili con quelli del file CSV, selezionare **Aggiorna cliente esistente**.

Nota: CustomerID è l'identificatore che determina se due record sono duplicati. Pertanto, si considera che i record importati con un CustomerID esistente si riferiscano a un cliente esistente e verranno aggiornati. Il flag **Aggiorna cliente esistente** funziona solo quando l'CustomerID viene mappato durante l'importazione. Pertanto, si consiglia vivamente di affidarsi al modello fornito e di adattare i dati senza omettere gli identificatori univoci.

- Se si desidera mantenere i contatti esistenti, selezionare **Arresta importazione del record corrente**.

11) Fare clic su **Avanti**.

12) Dagli elenchi a discesa, selezionare sequenzialmente i campi del file CSV da associare ai campi corrispondenti del sistema. Se i campi non sono disponibili o non si desidera importare i dati, fare clic sull'opzione vuota.

13) Fare clic su **Avanti**.

14) Fare clic su **Importa**. Non chiudere tale finestra mentre il processo di importazione è in corso. Al termine dell'importazione, verrà visualizzato il numero di record importati.

13.5.3.2 Come aggiungere l'accesso a un database esterno per la rubrica esterna

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Sono disponibili i dati per l'accesso al database esterno.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Click on **Edit** to start the **External Directory** wizard.
4) Click on **Import External Directory** tab.
5) Click in the **File Upload** area on **Choose File** and select the desired file.

13.5.3.3 Come esportare un file CSV dalla rubrica esterna

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic sulla scheda **Esporta rubrica esterna**.
4) Selezionare una delle seguenti opzioni:
   - Se si desidera esportare un file CSV del file system locale, selezionare il pulsante di opzione **File locale** e fare clic sul pulsante **Avvia**.
   - Se si desidera esportare in una cartella di Windows pubblica, selezionare il pulsante di opzione **Cartella di Windows pubblica**. Immettere i valori richiesti nei campi seguenti:

     - **Nome del file**

     - **Nome utente**

     - **Dominio**

     - **Password**

     E fare clic sul pulsante **Avvia**.

13.5.4 Rubrica esterna non in linea (LDAP)

La rubrica esterna non in linea (LDAP) contiene i contatti di un server LDAP per myPortal for Desktop, myAgent, Fax Printer, myPortal for Outlook e per i telefoni di sistema con display.

Il sistema supporta la versione LDAP 2 con autenticazione.

LDAP (Lightweight Directory Access Protocol) è un protocollo di accesso a elenchi telefonici basato su TCP/IP, utilizzato dai servizi di accesso a elenchi telefonici tramite rete. LDAP sfrutta un formato univoco e diffuso a livello mondiale per rappresentare tutti i nomi e offre diversi layout e un sistema di assegnazione univoco tra i nomi e la relativa rappresentazione interna. L'amministratore dovrà definire questi dettagli assieme all'amministratore IT del cliente in fase di trattativa. LDAP è supportato dai sistemi operativi MS Windows e Linux.

In un ambiente Microsoft, Active Directory Server (ADS) ovvero il server Exchange funge anche da server LDAP. Con Microsoft Windows, i dati degli utenti possono essere gestiti con l'applicazione Active Directory o ESTOS

Metadir. Alla gestione di questi dati provvede normalmente l'amministratore IT del cliente.

Con Linux, i dati degli utenti possono essere gestiti ad esempio con OpenLdap.

L'uso di un browser LDAP (ad esempio, Freeware di Softerra) facilita la configurazione di un servizio elenchi telefonici LDAP.

I numeri di telefono sul server LDAP possono contenere come separatore solo "-" e lo spazio. Il sistema non è in grado di filtrare eventuali altri separatori.

In fase di configurazione di una rubrica esterna non in linea, l'amministratore può adattare la mappatura dei campi ai nomi del server LDAP utilizzato. Durante la ricerca del nome tramite il numero di telefono, i campi eliminati vengono ignorati. La ricerca viene sempre eseguita sulle ultime 4 posizioni del numero di telefono, precedute dal carattere jolly predefinito. È possibile disattivare la ricerca del nome mediante il numero di telefono all'arrivo delle chiamate.

Se la porta predefinita 389 è già occupata, è necessario configurare un'altra porta.

Nota: Per ulteriori informazioni, consultare il seguente indirizzo Internet: `http://wiki.unify.com`.

I dati delle rubriche esterne sono quindi a disposizione degli utenti tramite myPortal for Desktop, myAttendant, Fax Printer e myPortal for Outlook.

Telefoni di sistema con display

Tramite il menu, gli utenti possono scegliere fra la rubrica interna e l'elenco LDAP, a condizione che questi siano configurati per i telefoni di sistema. La rubrica LDAP supporta la ricerca nei relativi contatti e consente la successiva chiamata di un contatto.

Il nome contenuto nel server LDAP non viene visualizzato a display alla segnalazione della chiamata o durante la conversazione. Anche i numeri di telefono delle chiamate in arrivo non vengono sostituiti dal nome contenuto nel server LDAP (come per esempio nel caso della selezione breve).

Gli utenti del sistema possono essere chiamati dalla Rubrica LDAP soltanto se è stato configurato il relativo numero di selezione passante e se il medesimo corrisponde alla voce contenute nel database LDAP. I numeri di telefono contenuti nel server LDAP vengono instradati all'interno della rete solo se il numero di telefono interno e quello di selezione passante sono uguali.

13.5.4.1 Come aggiungere una rubrica esterna non in linea (LDAP) per client PC

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È necessario conoscere i dati di accesso per il server LDAP.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.

3) Fare clic sulla scheda **Config provider esterni**.
4) Selezionare una delle seguenti opzioni:
   - Se, per le chiamate esterne in arrivo, si desidera attivare nel diario la funzione di risoluzione dei numeri di telefono in nomi, selezionare la casella di controllo **Cerca per numero di telefono**.
   - Se, per le chiamate esterne in arrivo, si desidera disattivare nel diario la funzione di risoluzione dei numeri di telefono in nomi, deselezionare la casella di controllo **Cerca per numero di telefono**.
5) Fare clic su **Aggiungi**.
6) Immettere i dati di accesso del server LDAP:
   a) In **Nome** inserire il nome di questa rubrica esterna non in linea.
   b) Nel campo **Server**, indicare il nome o l'indirizzo IP del server LDAP.
   c) Nel campo **Porta**, immettere il numero di porta del server LDAP.
   d) In **Nome distinto base LDAP**, inserire il nome distinto della base LDAP, ad esempio `dc=example-for-a-domain, dc=net`.
   e) Inserire il **Nome utente**.
   f) Inserire la **Password**.
7) Nei campi seguenti, inserire le corrispondenti descrizioni dei campi del server LDAP: **Titolo**, **Nome**, **Cognome**, **Num. ufficio 1**, **Num. ufficio 2**, **Abitazione**, **Cellulare**, **Società**, **Num. società**, **Indirizzo postale**, **Stato, provincia o contea**, **Paese**, **Codice Postale**, **E-mail**, **Cercapersone**, **Numero di fax** e **Città**.
8) Fare clic su **Salva**.

13.5.4.2 Come eliminare la rubrica esterna non in linea (LDAP) per i client PC

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic sulla scheda **Config provider esterni**.
4) Fare clic sulla rubrica esterna non in linea da cancellare.
5) Fare clic su **Rimuovi**.

13.5.4.3 Come aggiungere una rubrica esterna non in linea (LDAP) per i telefoni di sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È necessario conoscere i dati di accesso per il server LDAP.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Server telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu, fare clic su **Sistema** > **LDAP**.
4) Immettere l'**Indirizzo IP del server LDAP**.
5) Inserire il **Numero porta accesso LDAP**.
6) Inserire il **Nome utente**.
7) Inserire la **Password**.
8) Nel campo **Confermare la password**, inserire la password.
9) In **Nome distinto base**, inserire il nome distinto della base LDAP del server LDAP, ad esempio `dc=esempio-di-dominio, dc=rete`.
10) Nel campo **Richiesta di ricerca** inserire la stringa di ricerca per il server LDAP, ad esempio `cn=$*`.
11) Nel campo **Attributo risultato Nome** inserire il nome per il server LDAP, ad esempio, `cn`.
12) Nel campo **Attributo risultato Numero di telefono** inserire il numero di telefono per il server LDAP, ad esempio, `Numerotelefono`.
13) Selezionare una delle seguenti opzioni per l'ordinamento dei risultati della ricerca:
    - Se si desidera ordinare i risultati della ricerca, selezionare la casella di controllo **Ordina risultati ricerca**.
    - Se non si desidera ordinare i risultati della ricerca, deselezionare la casella di controllo **Ordina risultati ricerca**.
14) Immettere il **Codice impegno LDAP**.
15) Inserire il **Prefisso numero telefono LDAP**.
16) Fare clic su **Applica**.

13.5.5 Rubrica di sistema

Per i client UC Suite, la rubrica di sistema contiene tutti i numeri di sistema, gli utenti UC e non UC. Gli utenti non UC includono gli utenti senza licenze UC e le stazioni virtuali, come Fax e AutoAttendant. Per i dispositivi, la rubrica di sistema contiene tutte le stazioni interne e tutti i numeri di selezione breve centrali.

L'amministratore può disattivare la visualizzazione dei singoli utenti o numeri di selezione breve con nome.

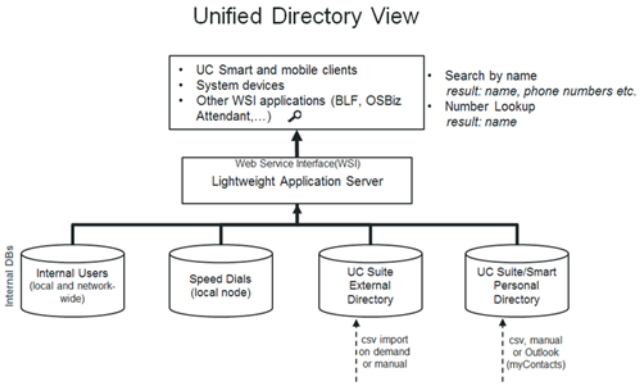
13.5.6 Rubrica unificata

OpenScape Business fornisce diverse origini dati per memorizzare e recuperare dati relativi a utenti o contatti, a partire dai dati degli utenti interni nella configurazione per utenti interni, tramite l'elenco di selezione breve, fino alle varie rubriche delle applicazioni UC.

Ogni origine dati in OpenScape Business viene utilizzata da un'applicazione client specifica, installata nel SW di sistema sui dispositivi di telefonia o in un'applicazione client UC. In base alle origini dati e ai client utilizzati, i dati recuperati e la loro presentazione possono variare.

Il servizio "Rubrica unificata" in OpenScape Business consente di applicare comuni funzioni di ricerca e risoluzione di nomi alle origini dati di OpenScape Business esistenti. Fornisce lo stesso risultato di ricerca o la stessa informazione di risoluzione del nome a tutti i dispositivi del sistema e ai client OpenScape Business.

Il servizio Rubrica unificata è accessibile tramite l'interfaccia Web Service (WSI) da client esterni quali myPortal to go oppure internamente tramite meccanismi di elaborazione chiamate (ad es. dai telefoni OpenStage).



Rubrica unificata utilizza le seguenti rubriche e database interni di OpenScape Business:

- Rubrica utente interno (in rete)
- Elenchi di selezione breve
- Rubrica personale UC Smart (opzionale)
- UC Suite Rubrica esterna (facoltativo)
- Contatti personali di Outlook (se importati tramite myContacts)

Il servizio Rubrica unificata è disponibile in ogni sistema OpenScape Business dalla release V2R2 in avanti. Non richiede pre-requisiti HW-SW o di licenza specifici.

Per ottenere i risultati migliori nell'utilizzo di Rubrica unificata, è necessario attenersi ad alcune regole a proposito dei formati dei numeri di telefono e del modo di scrivere i nomi.

13.5.6.1 Caratteristiche

Dispositivi / Client supportati

Il servizio Rubrica unificata fornisce:

- Ricerca nella rubrica di varie origini dati interne di OpenScape Business
- Offerta unificata del risultato della ricerca a tutti i client supportati
- Ricerca del numero di telefono / Risoluzione del nome in varie origini dati interne
- Offerta unificata dei risultati di risoluzione del nome per tutti i client supportati
- Accesso a dati esterni tramite l'interfaccia WebServices (WSI)

Le funzioni sono disponibili per i sistemi a nodo singolo come descritto di seguito. Nelle reti di OpenScape Business, la disponibilità delle funzioni dipende principalmente dal tipo di connessione dei fasci, dispositivi e client nella rete.

Rubrica unificata supporta i seguenti client / dispositivi di sistema di Unify che utilizzano le interfacce specificate:

Dispositivo/Client	Interfaccia utente/ Protocollo	Commenti
Telefoni OpenStage	Elaborazione chiamate / Protocollo CorNet	WSI / HTTP(S) è opzionale in OpenStage 60/80 per le immagini dei chiamanti
OpenScape Deskphone IP	Elaborazione chiamate / Protocollo CorNet	WSI / HTTP(S) è opzionale in DeskPhone IP 55 per le immagini dei chiamanti
Dispositivi cordless (CMI)	Elaborazione chiamate / Protocollo CMI	
CP 100/110 /200/205/210/ 405	Elaborazione chiamate / Protocollo CorNet	
DeskPhone CP400/ 600/600E/ 700/700X/710	WSI / HTTP(S)	
myPortal @work	WSI / HTTP(S)	
myPortal to go	WSI / HTTPS	
OpenScape Business Attendant / BLF	Elaborazione chiamate / Protocollo CorNet	WSI / HTTP(S) è opzionale

Nota: I client UC Suite myPortal, myAttendant e myAgent utilizzano propri meccanismi per la ricerca nella rubrica e la risoluzione dei nomi.

Funzione di ricerca

La ricerca nella Rubrica unificata viene sempre eseguita tramite l'interfaccia utente del dispositivo / client specifico. I criteri di ricerca e il set di caratteri utilizzati possono essere soggetti a limitazioni, in base ai client in uso.

Una volta inserito il criterio, la ricerca viene effettuata nelle directory successive

- Rubrica utente interno (in rete)
- Elenchi di selezione breve
- Rubrica personale UC Smart (opzionale)
- UC Suite Rubrica esterna (facoltativo)
- Contatti personali di Outlook (se importati tramite myContacts)

Tutte le corrispondenze all'interno delle directory precedenti vengono visualizzate come risultati di ricerca insieme alla relativa origine. I risultati possono contenere il set di dati di contatto completo o solo una parte di esso. La profondità di informazioni dei risultati dipende dall'origine dati.

Nota: La ricerca del nome del gruppo in myportal @work non è supportata in modalità UC Suite. È supportata solo la ricerca di utenti con licenza (licenza base) e gruppi MULAP con licenza (UC Entry).

I risultati vengono presentati ai dispositivi o ai clienti in base alle capacità dei display.

	Rubrica utente interna	Destinazione di selezione breve	Rubrica personale UC Smart	Rubrica esterna UC Suite	Contatti Outlook personali (tramite myContacts)
Cognome	X	---	X	X	X
Nome	X	---	X	X	X
Nome breve/ visualizzato	X	X	---	---	---
N° tel. ufficio	---	---	X	X	X
Nº tel. abitazione/ interno	---	---	X	---	X
N. cellulare	---	---	X	X	X
Ind. e-mail	---	---	X	X	X
Nome società	---	---	X	X	X
Città	---	---	---	---	---
Immagine contatto	---	---	X	---	X
Anteprima immagine contatto	---	---	X	---	X

Ricerca numero di telefono

La ricerca del numero di telefono nella Rubrica unificata risolve il chiamante trasferito (CLI) cercando il numero in tutte le origini dati interne supportate. La ricerca viene eseguita nei seguenti campi del numero di telefono:

- Numero dell'ufficio
- Numero cellulare
- Numero dell'abitazione

La ricerca del numero di telefono viene attivata, di solito, in caso di chiamate in entrata e in uscita, con la possibilità di considerare ulteriori funzioni specifiche di routing e inoltro.

Per ottenere risultati nel più breve tempo possibile, viene implementata una definizione fissa delle priorità delle origini dati utilizzate per la ricerca del numero di telefono. Il risultato può contenere solo il cognome, nome, nome visualizzato oppure, se disponibili, i dati di contatto completi.

Tabella 7: Origini dati supportate e definizione di priorità

Priorità	Origini dati	Nota
1	Nome CO/ITSP (inviato dal provider)	Il pre-requisito è attivare il flag "Nome in CO".
2	Elenco di selezione breve	
3	Contatti personali	
4	Dettaglio utente UC	

I dati recuperati vengono presentati nel dispositivo dell'utente e/o nel client UC. La profondità delle informazioni dipende dalle capacità dei display.

- **Chiamate in entrata**

  Scenario supportato per i sistemi a nodo singolo:

  – Chiamata di base
  – Chiamata di gruppo / Chiamata MULAP
  – Segnalazione delle chiamate
  – Trasferimento di chiamata a passaggio singolo (SSCT)
  – Trasferimento monitorato/con consultazione
  – Deviazione di chiamata incondizionata (CFU = Call Forwarding Unconditional)
  – Deviazione di chiamata su mancata risposta (CFNR = Call Forwarding No Reply)
  – Deviazione di chiamata su occupato (CFB = Call Forwarding Busy)
  – Trasferimento nascosto
  – Risposta per assente

  Nota: La risposta per assente è diversa dal gruppo di risposta per assente. Nel gruppo di risposta per assente, quando un numero esterno viene salvato nella directory unificata, il nome del chiamante non viene mostrato dai membri del gruppo.

  Lo scenario supportato per le situazioni multinodo (di rete) è una chiamata tramite gateway.
- **Chiamata in uscita**

  Nel caso di una chiamata in uscita, la ricerca del numero di telefono dell'utente chiamato viene eseguita solo una volta.

  Lo scenario supportato per i sistemi a nodo singolo è una chiamata base a un numero esterno.

La presentazione dei risultati della ricerca del numero di telefono dipende dalle capacità dei display dei telefoni.

13.5.6.2 Regole e convenzioni

È necessario osservare alcune convenzioni relative a formati di numeri e nomi nelle origini dati per ottenere risultati ottimali utilizzando il servizio Unified Directory.

Formato numero supportato

Tutti i numeri di telefono esterni nelle origini dati devono essere inseriti nel formato canonico che include codice paese e prefisso interurbano, ad es. +4989700712345

L'elenco di selezione rapida supporta solo il formato selezionabile del sistema, ad es. 0089700712345 o 0004989700712345

Quando sono configurati numeri di selezione rapida per l'accesso tramite LDAP, è necessario abilitare l'opzione di conversione del numero per visualizzare il nome del contatto quando il numero è in formato canonico. Per ulteriori informazioni su come abilitare la conversione del numero, vedere Come aggiungere un'origine dati esterna per Open Directory Service alla pagina 1181.

Formati nome supportati

È necessario osservare le convenzioni seguenti relative a formati di nomi e set di caratteri:

- **Formato nome di selezione rapida**

  La ricerca del nome nell'elenco di selezione rapida è supportata solo se si utilizzano regole di configurazione specifiche. I nomi e i cognomi devono essere inseriti nel campo del nome esistente utilizzando lo schema seguente:

  <Cognome>, <Nome> (separati da virgola)
- **Utenti interni in caso di migrazioni**

  La migrazione a V2R1 e versioni successive con utenti interni che non seguono queste regole di configurazione non sarà supportata nel modo previsto. Ciò significa che l'amministratore deve convertire i nomi interni nello schema seguente prima della migrazione:

  <Cognome>, <Nome> (separati da virgola)

Disponibilità di modifiche di directory

Dopo la creazione, l'aggiornamento o l'eliminazione di contatti nelle varie origini dati, la visualizzazione di tutte le modifiche nei risultati di ricerca numero di telefono può richiedere fino a 10 minuti.

13.5.6.3 Capitolo 11.5.5.3 Limiti funzionali

Le Rubriche unificate sono soggette ai seguenti limiti funzionali:

Ricerca del nome

- Supporto dei nomi di gruppi

  Non è possibile eseguire ricerche di nomi di gruppi (non i nomi MULAP) in tutti i tipi di configurazioni

- Supporto di caratteri speciali

  Nella maggior parte dei dispositivi l'utente può eseguire ricerche utilizzando i caratteri standard "a-z". I caratteri speciali (diacritici) come i caratteri tedeschi Ä, ä, Ö, ö, Ü, ü, ß non sono accessibili tramite l'interfaccia utente del dispositivo di telefonia.

  Pertanto, un semplice risultato di ricerca dei caratteri include anche caratteri speciali. Una ricerca di uno qualsiasi dei caratteri "acdegilnorstuyz" trova i caratteri speciali corrispondenti "àáâãåäąăçćčďđèéêëęě#ìíîïĺľłñńóôőõříśšşťùúûůüüýÿžźż"

  nei risultati di ricerca.

  Nota: La ricerca della rubrica con il carattere jolly all'inizio della stringa di ricerca, ad esempio <*jo*>, è supportata solo per gli utenti interni.

- Supporto del formato dei nomi di selezione breve

  La ricerca del nome nell'elenco di selezione rapida è supportata solo se si utilizzano regole di configurazione specifiche. I nomi e i cognomi devono essere inseriti nel campo del nome esistente utilizzando uno dei seguenti schemi

  – <Cognome>, <Nome> (separati dalla virgola)
  – <Nome> <Cognome> (separati da uno spazio, in questo caso)

Presentazione di nomi

I contatti personali in UC Smart e quelli provenienti dalla rubrica esterna non in linea nei quali la somma delle lunghezze del nome e del cognome supera i 24 caratteri vengono abbreviati a 24 caratteri in totale, per l'adattamento alla larghezza del display dei dispositivi.

Ricerca numero di telefono

La funzione di ricerca del numero di telefono (recupero del nome del contatto in base al numero del chiamante) non è supportata nella Rubrica unificata per i dispositivi SIP e S0.

13.5.6.4 Rubrica unificata nei sistemi di rete

Il servizio Rubrica unificata è attivo in ogni nodo di una rete OpenScape Business e utilizza le origini dati del proprio sistema. I dispositivi di telefonia e il client utilizzano sempre il servizio Rubrica unificata nel proprio nodo.

Pertanto, la disponibilità dei contatti nell'ambito della rete dipende dal tipo di contenuto dell'origine dati.

Tabella 8: Origine dati locale e in rete

Origine dati	Dati locali	Dati in rete
Rubrica utente interno	X	X
Elenchi di selezione breve	X	---

Origine dati	Dati locali	Dati in rete
Rubrica personale UC Smart	X	---
Rubrica personale UC Smart	X	---
Contatti personali di Outlook (tramite myContacts)	X	---

Ricerca numero di telefono

Negli scenari di rete la funzionalità di ricerca del numero di telefono non viene utilizzata. In tali scenari, il nome viene trasportato fra i nodi di rete mediante normali meccanismi di rete.

Per gli utenti interni si utilizza il Nome visualizzato configurato, per cui la ricerca è superflua.

13.5.6.5 Come importare i contatti nella directory unificata

L'importazione guidata dei contatti consente di importare i contatti nella directory direttamente da un file csv.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Directory unificata**.
3) Fare clic su **Modifica** accanto a **Importa contatti** per procedere con l'importazione dei contatti nella directory globale.
4) Nella sezione **Caricamento file** , fare clic su **Scegli file** e selezionare il file csv che si desidera caricare.

   Nota: La quantità massima di voci che è possibile importare è di 100.000 (30.000 per i sistemi integrati).

5) Nella sezione **Opzioni**, inserire il **Separatore file**. ';' o ',' sono voci valide.
6) Fare clic su **OK e avanti**.
7) Il backend elabora il file, leggere le intestazioni e le presenta insieme alle categorie predefinite della directory master nella pagina **Mappatura intestazioni CSV**. A questo punto, l'utente può abbinare le voci dei file csv per importare i relativi dati nelle categorie desiderate, diverse da quella predefinita.
8) Fare clic su **OK e avanti**.

9) Nella pagina **Panoramica dell'importazione**:

a) Selezionare una delle seguenti opzioni relative al file csv importato:

- Aggiungi contatti alla directory globale
- Elimina dalla directory globale tutti i contatti importati tramite CSV
- Elimina tutti i contatti dalla directory globale

b) Riguardo a **ID cliente duplicato**, selezionare una delle seguenti opzioni:

- Aggiorna cliente esistente
- Arresta importazione record corrente

Le voci che verranno aggiunte e quelle non sono state convalidate verranno presentate in due tabelle corrispondenti.

Nota: I record duplicati sono identificati da una combinazione dei campi Nome, Cognome, telefono aziendale ed e-mail. Questi campi non possono essere aggiornati automaticamente scegliendo "**Aggiorna cliente esistente**". Per aggiornare questi campi, scegliere di eliminare prima i record meno recenti nel passaggio 9a.

Il flag **"Aggiorna cliente esistente"** funziona solo quando l'ID cliente viene mappato durante l'importazione.

Solo il record con lo stesso **ID cliente** verrà considerato come "cliente esistente" e verrà aggiornato.

Il flag "**Rimuovi dati prima dell'importazione**" non rimuove i record se sono già utilizzati in altre funzioni, ad esempio come chiamante VIP, ecc.

ID cliente è l'unica chiave per determinare se il record è duplicato. Se l'ID cliente non è mappato, non c'è modo di evitare la duplicazione.

Pertanto, si consiglia vivamente ai clienti di affidarsi al modello fornito e di adattare i propri dati senza omettere gli identificatori univoci.

---

10) Fare clic su **OK e avanti**. Per questa operazione possono essere necessari diversi minuti.

11) La pagina **Importazione completata** informa sul numero di voci che sono state importate.

12) Fare clic su **Fine**.

13.5.6.6 Come modificare o aggiungere nuovi contatti alla directory unificata

La procedura guidata di modifica dei contatti consente di modificare i contatti già importati o di aggiungerne di nuovi.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.

2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **Directory unificata**.
3) Fare clic su **Modifica** accanto a **Modifica contatti** per procedere con la modifica dei contatti della directory globale.
4) Modificare i campi dei contatti desiderati. Il pulsante **Applica** diventa disponibile solo dopo aver modificato una voce.
5) Fare clic su **Aggiungi** per aggiungere manualmente un nuovo contatto.
6) Compilare i campi desiderati del nuovo contatto e fare clic sul pulsante **Applica**.

13.5.7 Reparti

I reparti raggruppano gli utenti presenti nella rubrica interna in base alle rispettive organizzazioni. La rubrica interna consente la ricerca o l'ordinamento in base al reparto.

13.5.7.1 Come aggiungere un reparto

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Click on **Edit** to start the **Departments** wizard.
4) Fare clic su **Aggiungi**.
5) Enter the **Department Name** of the Department.
6) Enter the **Hunt Group** identifier.
7) Fare clic su **Salva**.

13.5.7.2 Come assegnare un reparto ad un utente

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Click on **Edit** to start the **User Directory** wizard.
4) Selezionare l'utente corrispondente.
5) Click on **Edit** > **Personal Details** > **My Personal Details**.
6) Select the desired department from the list box in the **Department** field.
7) Fare quindi clic su **Salva**.

13.5.7.3 Come modificare un reparto

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Click on **Edit** to start the **Departments** wizard.
4) Nell'elenco di reparti, fare clic sul reparto corrispondente.
5) Clic su **Modifica**.
6) Enter the **Department Name** of the Department.
7) Enter the **Hunt Group** identifier.
8) Fare clic su **Salva**.

13.5.7.4 Come eliminare un reparto

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Reparti**.
4) Nell'elenco di reparti, fare clic sul reparto corrispondente.
5) Fare clic su **Rimuovi**.
6) Fare clic su **OK**.

13.5.8 Elenco dei Preferiti

L'elenco dei Preferiti consente all'utente di mantenere sempre in vista i contatti desiderati. In questo modo risulta molto semplice chiamarli. Tutti gli utenti interni (con telefono di sistema) e i relativi interlocutori esterni potranno vedere lo stato di presenza e potranno contattare tale utente tramite messaggi istantanei.

L'utente può aggiungere contatti da tutte le rubriche all'elenco dei Preferiti. Se i Preferiti non provengono da una rubrica interna, al posto dell'icona dello stato presenza viene visualizzata quella dell'origine del contatto.

L'elenco dei Preferiti consente di gestire i contatti dei gruppi. I contatti di tutti i gruppi possono essere ordinati in base al cognome, al nome o alla sequenza originale.

In caso di assenza di un utente interno, si vedrà il momento previsto per il rientro posizionando il puntatore del mouse sulla relativa voce, a condizione che tale utente abbia reso visibile il proprio stato presenza.

Nel caso di Preferiti con più numeri di telefono, è possibile definire un numero di telefono predefinito, al quale chiamare il contatto. Il numero di telefono

predefinito di un contatto dei Preferiti è riconoscibile nel menu di scelta rapida dal segno di spunta nella relativa casella di controllo.

13.5.9 Diario

Il diario è l'elenco di tutte le chiamate in arrivo e in uscita di un utente. Tramite il diario, un utente può chiamare in modo rapido e semplice il contatto o rispondere alle chiamate perse.

Cartella per i vari tipi di chiamata

Le chiamate sono suddivise nei seguenti gruppi:

- **Aperte**

  Contiene le chiamate non risposte e perse per le quali è stato trasmesso un numero di telefono. Non appena si risponde a una di queste chiamate, tutte le voci associate al numero di telefono corrispondente vengono eliminate dall'elenco.
- **Tutte le chiamate**
- **Perse**
- **Risposte**
- **Interne**
- **Esterne**
- **In arrivo**
- **In uscita**
- **Pianificate**

  Contiene tutte le chiamate pianificate come utente tramite appuntamenti specifici. Il servizio Chiamate pianificate non è disponibile per gli agenti del Contact Center. Perché il sistema di comunicazione esegua una chiamata pianificata, è necessario che myPortal for Desktop o myPortal for Outlook siano in esecuzione al momento dell'appuntamento, che lo stato di presenza dell'utente sia **Ufficio** o **CallMe** e che l'utente confermi l'esecuzione della chiamata in una finestra di dialogo. Nel caso l'utente sia occupato quando scade l'appuntamento per una chiamata pianificata, il sistema sposta la chiamata pianificata in avanti fino a quando l'utente non è di nuovo libero. myPortal for Desktop o myPortal for Outlook informano l'utente all'uscita di eventuali chiamate pianificate in attesa. All'avvio, myPortal for Desktop o myPortal for Outlook informano l'utente di eventuali appuntamenti nel frattempo scaduti per chiamate pianificate. Tali chiamate possono essere cancellate o ripianificate con un nuovo appuntamento.

Nell'interfaccia moderna di myPortal for Desktop non sono disponibili tutte le cartelle per i tipi di chiamata.

All'avvio dell'interfaccia moderna myPortal for Desktop, vengono caricate solo 100 voci del diario. In seguito e quando si verificano nuove chiamate in entrata, il numero nella cronologia delle chiamate supererà i 100 record.

Tempo di conservazione

Il sistema salva una registrazione delle chiamate nel diario per un periodo di tempo massimo, impostato dall'amministratore. Gli utenti possono ridurre questo tempo. Una volta trascorso tale periodo, il sistema cancella automaticamente le voci in questione.

Nota: Il tempo di conservazione definisce anche il tempo massimo per le analisi con myReports.

Raggruppamento in base al periodo

Le chiamate sono suddivise nei vari gruppi in base al tempo, ad esempio: Oggi, Ieri, ecc., Settimana scorsa, Mese scorso e Precedente. L'amministratore può definire per quanto tempo le chiamate resteranno memorizzate nel diario. Una volta trascorso tale periodo, le voci verranno automaticamente eliminate. Nell'interfaccia moderna di myPortal for Desktop non è disponibile la funzione di raggruppamento in base al periodo.

Dettagli chiamata

Ogni chiamata viene visualizzata con una data e un'ora e, se disponibile, un Numero di telefono. Se una rubrica contiene ulteriori informazioni su un numero di telefono, ad esempio **Cognome**, **Nome** e **Società**, vengono visualizzati anche tali dati. Nella maggior parte delle cartelle, vengono inoltre visualizzate le colonne **Direzione**, **Durata** e **Chiamata completata**. Nell'interfaccia moderna di myPortal for Desktop non sono disponibili tutti i dettagli delle chiamate.

Ordinamento

È possibile ordinare i dati delle chiamate nel diario in base ai valori alfanumerici di una qualsiasi colonna, in ordine crescente o decrescente.

Dopo aver ordinato il diario in base a una colonna, è possibile saltare alle prime voci che iniziano con un carattere particolare, ad esempio ai primi cognomi che iniziano con una "P". Inserendo altre cifre è possibile restringere ulteriormente la ricerca. Nell'interfaccia moderna di myPortal for Desktop non è disponibile la funzione di ordinamento.

Esporta

Gli utenti possono esportare il diario sotto forma di file CSV tramite myPortal for Desktop o myPortal for Outlook:

13.5.9.1 Come modificare il tempo di conservazione massimo per il diario

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**.
4) Click on **Maintenance**.
5) Enter the desired duration in days in the **Keep call history for** field, under the **Calls Information Maintenance** area.

Nota: Il tempo di conservazione definisce anche il tempo massimo per le analisi con myReports.

6) Fare clic su **Salva**.

13.6 Chiamate

Per le chiamate, sono a disposizione degli utenti funzioni pratiche, quali dialer sul desktop, finestra popup, registrazione di chiamate e conferenze.

13.6.1 Dialer sul desktop e dialer degli appunti

Il dialer sul Desktop e il dialer degli appunti consentono agli utenti con myPortal for Desktop (Windows) o myPortal per Outlook di richiamare una destinazione specifica o una destinazione copiata negli Appunti di Windows da diverse applicazioni Windows tramite combinazioni di tasti, ad esempio da un'e-mail di Outlook.

In base al tipo di stringa utilizzata, il dialer sul funziona nel modo seguente:

- Viene composto direttamente un numero di telefono in formato canonico.
- Viene selezionato un numero di telefono in formato selezionabile, a condizione che il sistema di comunicazione sia in grado di determinare se si tratta di una destinazione interna o esterna. In caso contrario viene richiesto all'utente di effettuare la scelta appropriata.
- Se una stringa contiene lettere, tale stringa verrà ricercata come Nome o Cognome.

Il dialer sul desktop e il dialer degli appunti vengono eseguiti dopo un tempo impostabile. Durante questo arco di tempo, è ancora possibile interrompere la composizione del numero. Se si modifica il valore predefinito da 3 s a 0 s, la composizione viene eseguita immediatamente. È possibile modificare tale valore nelle impostazioni dei client UC Suite.

Le applicazioni di Windows installate con i componenti standard di Windows, supportano normalmente il dialer sul desktop e il dialer degli appunti, ma non le applicazioni a 16 bit. Il dialer sul desktop è supportato solo con applicazioni a 32 bit.

13.6.2 Finestre popup

Le finestre popup dei client della UC Suite consentono all'utente di reagire con un singolo clic, ad esempio all'arrivo di una chiamata o di un nuovo messaggio vocale.

Le finestre popup vengono visualizzate nell'angolo in basso a destra dello schermo. Possono comparire diversi tipi di finestre popup. Le finestre popup per le chiamate e i messaggi mostrano il numero di telefono, il nome e l'immagine del chiamante, se disponibile. I pulsanti presenti nelle finestre popup variano in base alla situazione.

Le finestre popup possono essere ridotte a icona nella barra delle applicazioni. Quando vi sono più di tre finestre popup aperte per le chiamate, queste verranno automaticamente ridotte a icona nella barra delle applicazioni.

13.6.3 Registrazione di chiamate

Un utente può registrare le chiamate. Le chiamate registrate vengono visualizzate nella casella vocale.

Suggerimento: È necessario informare il proprio interlocutore che la conversazione verrà registrata. In alcuni paesi (ad esempio, la Francia), l'interlocutore viene automaticamente informato dal sistema della registrazione in corso.

Come amministratore è possibile consentire o impedire la registrazione di chiamate assieme alla registrazione di conferenze a livello di sistema. In via opzionale, è possibile configurare la riproduzione di un annuncio o di un tono di avviso all'inizio della registrazione.

Gli utenti possono gestire le registrazioni delle chiamate tramite myPortal for Desktop o myPortal for Outlook. Le chiamate registrate vengono visualizzate nella casella vocale con un punto rosso e mostrano, se disponibile, il numero di telefono dell'interlocutore.

La registrazione viene interrotta in caso di consultazione, attesa, trasferimento e avvio di una conferenza.

Nota: DTMF non è supportato durante la registrazione delle chiamate.

13.6.3.1 Come attivare e disattivare la registrazione di chiamate

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**.
4) Click on **Live Record**.
5) Selezionare una delle seguenti opzioni:
   - If you want to allow the recording of calls, select the **Live Record** check box.
   - If you want to prevent the recording of calls, clear the **Live Record** check box.
6) Fare clic su **Salva**.

Nota: Calls that have this functionality activated cannot be transferred or held.

13.6.3.2 Come attivare o disattivare l'annuncio relativo alla registrazione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**.
4) Click on **Live Record**.
5) Selezionare una delle seguenti opzioni:
   - If you want to play an announcement at the start of a recording, select the **Play prompt before recording** check box.
   - If you do not want to play an announcement at the start of a recording, clear the **Play prompt before recording** check box.
6) Fare clic su **Salva**.

13.6.3.3 Come attivare o disattivare il tono di avviso per la registrazione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**.
4) Click on **Live Record**.
5) Selezionare una delle seguenti opzioni:
   - Se si desidera riprodurre un tono di avviso all'inizio della registrazione, selezionare la casella di controllo **Riproduci tono di avviso prima della registrazione**.
   - Se non si desidera riprodurre un tono di avviso all'inizio della registrazione, deselezionare la casella di controllo **Riproduci tono di avviso prima della registrazione**.
6) Fare clic su **Salva**.

Nota: Please note that this process applies only to **Openscape Business S**. The activation of the Recording warning tone in **Openscape Business X** is controlled by the flag **Warning tone during voice recording** which can be found in **Expert Mode** > **Basic Settings** > **System Flags**.

13.7 Conferenze

Durante una conferenza più partecipanti (inclusi utenti esterni) possono comunicare contemporaneamente tra loro.

13.7.1 Gestione conferenze

Con Gestione conferenze, un utente può utilizzare diversi tipi di conferenze.

Tipi di conferenze

I diversi tipi di conferenza offrono le seguenti caratteristiche:

	AdHoc	**Pianificata**	**Permanente**	**aperte**
Uso	• Controllo tramite telefono • controllato tramite applicazione	• controllato tramite applicazione	• controllato tramite applicazione	• controllato tramite applicazione
Inizio	• manuale	• Pianificato	• manuale	• manuale
Fine	• manuale	• Pianificato • manuale	• manuale	• manuale
Durata della prenotazione di canali conferenze	• predefinito 1 ora	• Pianificato	• fino alla disattivazione o all'eliminazione della conferenza	• fino alla disattivazione o all'eliminazione della conferenza
Estensione	x	x	-	-
Frequenza	• manuale	• Pianificato	-	-
Direzione della connessione dal punto di vista del sistema	• in uscita	• in uscita • in arrivo	• in arrivo	• in arrivo
Insieme di partecipanti	• fisso	• fisso	• fisso	• aperte
Autenticazione del partecipante alla conferenza	-	• ID conferenza individuale (opzionale) • Password (opzionale)	• ID conferenza individuale (opzionale) • Password (opzionale)	• ID conferenza condiviso (opzionale)
Registrazione, se attivata nel sistema	• manuale (On Demand Conference Recording)	• (Auto Conference Recording) • manuale (On Demand Conference Recording)	• (Auto Conference Recording) • manuale (On Demand Conference Recording)	• (Auto Conference Recording) • manuale (On Demand Conference Recording)

	AdHoc	Pianificata	Permanente	aperte
Invito tramite e-mail con:	• Nome conferenza • Collegamento per la sessione di Web Collaboration	• Nome conferenza • Numero di accesso • ID conferenza • Password • Data e ora di inizio e fine della conferenza • Collegamento per la sessione di Web Collaboration	• Nome conferenza • Numero di accesso • ID conferenza • Password • Collegamento per la sessione di Web Collaboration	• Nome conferenza • Numero di accesso • ID conferenza • Password
Appuntamento di Outlook come allegato e-mail (.ics)	-	x	-	-

Conferenza controllata da applicazioni

Gli utenti possono avviare, gestire e controllare conferenze tramite Gestione conferenze di myPortal for Desktop o myPortal for Outlook.

Conferenza controllata telefonicamente

Gli utenti possono avviare una conferenza controllata tramite telefono nelle modalità descritte di seguito e successivamente gestirla sempre tramite telefono:

- chiamare i partecipanti desiderati e connetterli alla conferenza
- Estendere una chiamata in consultazione convertendola in una conferenza
- Estendere una seconda chiamata convertendola in una conferenza

Sala conferenze virtuale

In caso di conferenze controllate da applicazioni, nella sala conferenze virtuale gli utenti possono seguire la conferenza in forma grafica e in tempo reale; questo spazio consente inoltre al supervisore di gestire la conferenza. La sala conferenze virtuale mostra il numero di telefono, il nome e lo stato presenza dei partecipanti, se tali dati sono disponibili.

Numero di accesso

Accedendo come amministratore, è possibile modificare i numeri di accesso predefiniti nell'installazione di base per le sale conferenze. Gli utenti possono visualizzare il numero di accesso per una conferenza.

Supervisore conferenza

Il convocante della conferenza diventa automaticamente il supervisore conferenza finché non viene esplicitamente cambiato. Può eseguire le seguenti azioni (in base al tipo di conferenza):

- Aggiunta o eliminazione di partecipanti alla conferenza: (conferenza controllata da applicazioni):

  I partecipanti eliminati non restano nella conferenza.

- Disconnettere o riconnettere i partecipanti:

  Gli utenti disconnessi possono restare nella conferenza. Quando il supervisore conferenza connette un partecipante, gli altri partecipanti restano connessi gli uni agli altri; se è presente solo un altro partecipante, questo sentirà la musica su attesa.
- registrazione della conferenza

  Le conferenze registrate vengono visualizzate nella casella vocale contrassegnate da un punto rosso. Non è possibile registrare conferenze in cui è presente un utente in attesa.
- Impostare un altro utente interno dello stesso nodo come supervisore conferenza
- Prolungare la conferenza
- Lasciare la conferenza senza concluderla:

  Il partecipante interno che è stato più a lungo connesso alla conferenza diventa automaticamente il supervisore conferenza.
- Concludere la conferenza

Partecipante alla conferenza

I partecipanti alla conferenza possono lasciare la conferenza o accedervi di nuovo (conferenza pianificata e conferenza permanente). Finché nella conferenza vi è un solo partecipante, verrà riprodotta musica su attesa. Accedendo come amministratore, è possibile definire se consentire l'accesso alla conferenza a più partecipanti esterni.. Il numero massimo di partecipanti esterni alla conferenza è limitato, tra l'altro, dal numero di linee urbane disponibili.

Tono di conferenza

Al momento della connessione o disconnessione di un partecipante, gli altri partecipanti sentiranno un tono di conferenza. Accendendo come amministratore, è possibile attivare o disattivare il tono di conferenza.

Conclusione automatica senza supervisore conferenza

Se nella conferenza rimangono solo partecipanti esterni, dopo un tempo predefinito questi sentiranno un tono di avviso. Una volta trascorso un ulteriore periodo di tempo, il sistema di comunicazione concluderà automaticamente la conferenza. L'amministratore può modificare tali tempi.

Avviso tramite e-mail e appuntamento Outlook

Il sistema può avvisare i partecipanti alla conferenza automaticamente tramite e-mail e nelle conferenze pianificate anche tramite appuntamenti di Outlook come allegati (.ics):

Evento	Partecipanti avvisati	Appuntamento Outlook
Nuova conferenza	tutti	Creazione automatica
Eliminazione della conferenza		Eliminazione automatica
Sposta la conferenza		Aggiornamento automatico
Aggiunta di partecipanti alla conferenza	solo selezione	Creazione automatica (solo selezione)

Evento	Partecipanti avvisati	Appuntamento Outlook
Eliminazione dei partecipanti dalla conferenza		Eliminazione automatica (solo selezione)

Per l'uso di questa funzione è necessario che l'amministratore abbia configurato l'invio di e-mail. Inoltre, è necessario che i singoli partecipanti interni alla conferenza abbiano configurato il proprio indirizzo e-mail. Per i partecipanti esterni, il convocante della conferenza deve inserire i relativi indirizzi e-mail nel sistema.

Nota: Per le notifiche tramite e-mail, non viene fornita alcuna conferma di ricezione per le consegne mancate o per gli eventuali messaggi di assenza, in quanto le e-mail vengono inviate direttamente dal sistema a causa dell'integrazione di Web Collaboration.

Ulteriori chiamate

Se un utente esegue o accetta un'altra chiamata mentre è in conferenza, ciò comporterà l'esclusione dalla conferenza.

Parcheggio, richiamata alternata

In una conferenza non sono disponibili i servizi di parcheggio delle chiamate e richiamata alternata.

Addebiti

La conferenza viene addebitata all'utente che ha effettuato la chiamata che genera i costi. Con il cambio di supervisore conferenza, gli ulteriori costi generati verranno addebitati al nuovo supervisore.

Risorse di sistema

L'amministratore può visualizzare sia le conferenze attive che quelle memorizzate. Le conferenze inattive possono essere cancellate.

Suggerimento: Le conferenze permanenti impegnano a lungo le risorse del sistema. Siccome ogni utente con myPortal for Desktop o myPortal for Outlook può configurare conferenze permanenti, è consigliabile che l'amministratore verifichi regolarmente le conferenze memorizzate per evitare colli di bottiglia nel sistema.

Trasmissione video

Se è in corso una trasmissione video, questa deve essere conclusa prima che l'utente possa partecipare a una conferenza.

13.7.1.1 Come modificare il numero di accesso per sala conferenze virtuale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Nella struttura dei menu, selezionare **Utente** > **Applicazioni UC** > **Conferenze**.

   Nello spazio di lavoro vengono visualizzati i numeri di telefono delle sale conferenze virtuali. L'ultima si riferisce alle conferenze pianificate e permanenti.
4) Nella struttura dei menu fare clic sulla relativa voce (Indice - Numero di telefono).
5) Fare clic sulla scheda **Modifica parametri dell'utente**.
6) Nel campo **Numero di telefono** immettere il numero di accesso. Il numero di accesso può contenere solo le cifre 0-9.
7) Fare clic su **Applica**, quindi su **OK**.

13.7.1.2 Come consentire o impedire la presenza di più partecipanti esterni alla conferenza

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu selezionare **Sistema** > **Flag di sistema**.
4) Selezionare una delle seguenti opzioni:
   - Se si desidera consentire a più partecipanti esterni di prendere parte alla conferenza, selezionare la casella di controllo **Più di un partecipante esterno alla conferenza**.
   - Se si desidera impedire a più partecipanti esterni di prendere parte alla conferenza, deselezionare la casella di controllo **Più di un partecipante esterno alla conferenza**.
5) Fare clic su **Applica**, quindi su **OK**.

13.7.1.3 Come attivare/disattivare il tono di conferenza

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu selezionare **Sistema** > **Flag di sistema**.
4) Selezionare una delle seguenti opzioni:
   - Per attivare il tono di conferenza, selezionare la casella di controllo **Tono di conferenza**.
   - Per disattivare il tono di conferenza, deselezionare la casella di controllo **Tono di conferenza**.
5) Fare clic su **Applica**, quindi su **OK**.

13.7.1.4 Come modificare gli intervalli di tempo per la conclusione automatica delle conferenze

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu selezionare **Sistema** > **Temporizzazioni**.
4) Nella riga, in corrispondenza di **Tempo fino al tono di avviso nel transito con linee anal.**, in **Base** e **Fattore**, selezionare l'intervallo di tempo desiderato dall'uscita dalla conferenza del supervisore conferenza al tono di avviso.
5) Nella riga in corrispondenza di **Tempo del segnale di avviso fino al rilascio...** selezionare l'intervallo di tempo desiderato dal tono di avviso alla conclusione automatica della conferenza.
6) Fare clic su **Applica**, quindi su **OK**.

13.7.1.5 Come richiedere i dettagli di una conferenza memorizzata

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Conferenza in corso**.
4) Fare clic sulla conferenza in oggetto.
5) Fare clic su **Visualizza**.

13.7.1.6 Come eliminare una conferenza memorizzata

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Conferenza in corso**.
4) Fare clic sulla conferenza in oggetto.
5) Fare clic su **Cancella** e confermare il prompt di sicurezza.

13.7.1.7 Come configurare la registrazione di conferenze

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**.
4) Click on **Live Record**.
5) Selezionare una delle seguenti opzioni:
   - If you want to enable the recording of conferences, select the **Conference Live Recording availability** check box.
   - If you want to prevent the recording of conferences, clear the **Conference Live Recording availability** check box.
6) Fare clic su **Salva**.

Nota: Conferences that have this functionality activated cannot be transferred or held.

13.7.2 Conferenza AdHoc

Una conferenza AdHoc avviene spontaneamente e viene avviata manualmente dal supervisore conferenza. eventualmente salvarla per poterla richiamare in un momento successivo.

Avvio della conferenza

Nel terminale di tutti i partecipanti alla conferenza interni, il sistema apre automaticamente la finestra che mostra la sala conferenze virtuale, a condizione che in tale terminale il partecipante abbia avviato myPortal for Desktop con l'interfaccia classica o myPortal for Outlook. Il sistema convoca contemporaneamente tutti i partecipanti alla conferenza. Entrando in

conferenza, i partecipanti ricevono un annuncio di benvenuto che indica il nome del supervisore conferenza.

Registrazione della conferenza

Il supervisore conferenza può registrare manualmente una conferenza per sé stesso e per tutti i partecipanti interni collegati, a condizione che nel sistema sia attivata la registrazione di conversazioni. I partecipanti ubicati nei rispettivi nodi ricevono la registrazione nella casella vocale, i partecipanti di altri nodi la ricevono tramite e-mail. La durata della registrazione dipende dalla capacità di memoria del sistema.

Uscita dalla conferenza

Il supervisore conferenza può concludere la conferenza nel client oppure semplicemente riagganciando. La conferenza verrà inoltre conclusa quando tutti i partecipanti si saranno disconnessi da essa.

Espandere una chiamata in una conferenza

Un utente interno in conversazione può trasformare una chiamata in una conferenza ad hoc aggiungendo altri utenti. A tal fine l'utente deve disporre di una licenza per UC Suite Conference. Questa funzionalità non è disponibile con CallMe.

13.7.3 Conferenza pianificata

Una conferenza pianificata (conferenza incontro) si svolge in un momento predefinito del futuro, ha una durata specificata e può essere configurata per ripetersi più volte alla stessa ora.

Una conferenza pianificata rimane attiva per il periodo pianificato, indipendentemente dal fatto che siano presenti utenti o meno. Il supervisore conferenza salva una conferenza pianificata con un proprio nome.

Opzioni di configurazione di una conferenza permanente

Chi avvia la conferenza può definire le seguenti proprietà:

- Data e ora di inizio e di fine
- Ripetizione
- Necessità della presenza del supervisore conferenza
- Necessità dell'autenticazione dei partecipanti al momento di prendere parte alla conferenza (immettendo un ID conferenza o una password da tastiera).

  Nota: Gli utenti Mobility Entry dovranno immettere il proprio codice per la selezione DTMF prima dell'autenticazione.

  La password predefinita per le conferenze è 123456. Il supervisore conferenza può modificare tale password per i singoli partecipanti.
- Lingua degli annunci per l'inizio della conferenza
- Direzione della connessione per ciascun utente (predefinita: **In uscita**)

Avviare la conferenza

Alla data e all'ora impostate, nel terminale di tutti i partecipanti alla conferenza interni, il sistema apre automaticamente la finestra che mostra la sala conferenze virtuale, a condizione che in tale terminale il partecipante abbia avviato myPortal for Desktop con l'interfaccia classica o myPortal for Outlook. Se è richiesta la presenza del supervisore conferenza, il sistema lo contatta e dopo la sua autenticazione convocherà tutti gli altri partecipanti contemporaneamente. I partecipanti che hanno impostato la deviazione di chiamata sulla rispettiva casella vocale o il cui stato è assente non verranno contattati. In base a come è stata configurata la connessione, il sistema convoca i partecipanti alla conferenza oppure i partecipanti possono essi stessi effettuare la chiamata. Il sistema comunica il nome di ogni partecipante che si connette alla conferenza mediante un annuncio del tipo: "`... partecipa alla conferenza`", a condizione che il convocante abbia registrato l'annuncio del proprio nome.

Nota: Per consentire ai partecipanti di una conferenza pianificata senza autenticazione all'inizio della conferenza di sentire annunciare il nome del supervisore conferenza, è necessario che questo abbia già avviato in precedenza una conferenza con autenticazione.

Accesso

Tutti i partecipanti possono connettersi alla conferenza pianificata componendo un numero di accesso entro il periodo stabilito, indipendentemente dalla direzione configurata per ogni singolo partecipante. Se si tenta di digitare tale numero al di fuori del periodo stabilito, viene riprodotto il messaggio corrispondente. Per l'accesso tramite ITSP, è necessario il supporto per RFC 2833 (caratteri DTMF).

Forzare l'autenticazione con il tasto *

Il Supervisore conferenza può configurare una conferenza in modo che i partecipanti debbano autenticarsi premendo almeno il tasto *. Ciò garantisce la connessione alla conferenza solo da parte di utenti presenti, e non da casella vocale.

Estensione della conferenza

Dieci minuti prima del termine della conferenza pianificata, i partecipanti sentiranno un messaggio che segnala la prossima conclusione della conferenza e offre la possibilità di estendere la conferenza digitando una cifra specifica. Qualsiasi partecipante alla conferenza può quindi estendere la conferenza digitando tale cifra. Il supervisore conferenza può estendere la conferenza in qualsiasi momento tramite myPortal for Outlook.

Registrazione della conferenza

Il supervisore conferenza può registrare automaticamente o manualmente una conferenza per sé stesso e per tutti i partecipanti interni collegati, a condizione che nel sistema sia attivata la registrazione di conversazioni. I partecipanti ubicati nei rispettivi nodi ricevono la registrazione nella casella vocale, i partecipanti di altri nodi la ricevono tramite e-mail. La durata della registrazione dipende dalla capacità di memoria del sistema.

Uscita dalla conferenza

La conferenza può concludersi al momento previsto oppure anticipatamente, se il supervisore conferenza la termina.

13.7.4 Conferenza permanente

Una conferenza permanente non presenta limiti di tempo. I partecipanti possono accedervi in qualsiasi momento.

Il supervisore conferenza salva una conferenza permanente con un proprio nome. La conferenza rimane attiva finché non viene eliminata.

Opzioni di configurazione di una conferenza permanente

Il convocante della conferenza può definire quanto segue:

- Necessità dell'autenticazione dei partecipanti al momento di prendere parte alla conferenza (immettendo un ID conferenza e una password da tastiera).

  Nota: Gli utenti Mobility Entry dovranno immettere il proprio codice per la selezione DTMF prima dell'autenticazione.

  La password predefinita per le conferenze è 123456. Il supervisore conferenza può modificare tale password per i singoli partecipanti.
- Lingua utilizzata per gli annunci all'inizio della conferenza.

Avviare la conferenza

Quando il primo partecipante accede alla conferenza, il sistema apre, nel terminale di tutti i partecipanti alla conferenza interni, la finestra che mostra la sala conferenze virtuale, a condizione che nel terminale del partecipante sia stato avviato myPortal xA0;for xA0;Desktop o myPortal xA0;for xA0;Outlook. Tutti i partecipanti accedono alla conferenza componendo un numero. Il sistema annuncia tutti i partecipanti che accedono alla conferenza con un messaggio del tipo: "… partecipa alla conferenza."

Accesso

Ogni partecipante può accedere alla conferenza mediante un numero di accesso. Per l'accesso tramite ITSP, è necessario il supporto per RFC 2833 (caratteri DTMF).

Registrazione della conferenza

Il supervisore conferenza può registrare una conferenza per sé stesso e per tutti i partecipanti interni collegati, a condizione che nel sistema sia attivata la registrazione di conversazioni. I partecipanti ubicati nei rispettivi nodi ricevono la registrazione nella casella vocale, i partecipanti di altri nodi la ricevono tramite e-mail. La durata della registrazione dipende dalla capacità di memoria del sistema.

La registrazione automatica di una conferenza permanente si avvia in presenza di due o più partecipanti alla conferenza e termina quando sono presenti meno di due partecipanti. Terminata la registrazione, tutti i partecipanti ricevono lo stesso file con la registrazione dell'intera conferenza.

13.7.5 Apri conferenza

Una conferenza aperta è intesa per un numero di partecipanti specifico. Ogni utente che dispone di dati di accesso può connettersi.

Il supervisore conferenza salva una conferenza aperta con un proprio nome. La conferenza rimane attiva finché non viene eliminata.

Opzioni di configurazione di una conferenza aperta

Il convocante della conferenza può definire quanto segue:

- Numero di partecipanti alla conferenza (max. 16).
- Necessità dell'autenticazione dei partecipanti al momento di prendere parte alla conferenza (immettendo un ID conferenza e una password da tastiera).

  Nota: Gli utenti Mobility Entry dovranno immettere il proprio codice per la selezione DTMF prima dell'autenticazione.

  La password predefinita per le conferenze è 123456. Il supervisore conferenza può modificare tale password per i singoli partecipanti.
- Quale ID conferenza comune è valido per tutti i partecipanti alla conferenza.
- Lingua utilizzata per gli annunci all'inizio della conferenza.

Avviare la conferenza

Tutti i partecipanti accedono alla conferenza componendo un numero. Il sistema annuncia tutti i partecipanti interni che accedono alla conferenza con un messaggio del tipo: "`... partecipa alla conferenza.`"

Composizione di un numero

Ogni partecipante può accedere alla conferenza mediante un numero di accesso. Per l'accesso tramite ITSP, è necessario il supporto per RFC 2833 (caratteri DTMF).

Registrazione della conferenza

Il supervisore conferenza può registrare automaticamente o manualmente una conferenza per sé stesso e per tutti i partecipanti interni collegati, a condizione che nel sistema sia attivata la registrazione di conversazioni. I partecipanti ubicati nei rispettivi nodi ricevono la registrazione nella casella vocale, i partecipanti di altri nodi la ricevono tramite e-mail. La durata della registrazione dipende dalla capacità di memoria del sistema.

13.8 Web Collaboration

Per conversazioni telefoniche e conferenze, i client PC UC myPortal for Desktop (Windows) e myPortal for Outlook supportano l'integrazione del prodotto separato Web Collaboration, che offre pratiche funzioni di collaborazione simultanea e multimediale. Ciò offre un accesso rapido a funzioni quali condivisione desktop e applicazioni, condivisione di file, co-browsing, whiteboarding, URL Push, chat con IM e chat video con più utenti.

Web Collaboration può essere avviato da un utente durante una telefonata tramite la finestra popup del client PC UC o dal supervisore conferenza durante una conferenza attiva. In questo modo Web Collaboration avvia la sessione. Non è necessari installare in locale Web Collaboration sul client PC UC. Se sul client PC UC è stato salvato il programma di posta elettronica, gli interlocutori possono inviare un'e-mail con il collegamento al client Web Collaboration. Per informazioni su Web Collaboration, consultare la documentazione del prodotto Web Collaboration.

Quando si crea o si modifica una conferenza, il supervisore conferenza può pianificare una sessione di Web Collaboration. Quando si elimina o si conclude una conferenza, la relativa sessione di Web Collaboration viene automaticamente eliminata.

Nota: Per consentire l'avvio automatico dei client PC UC di Web Collaboration, è necessario che l'autenticazione proxy per l'accesso a Internet dei client PC UC tramite un server proxy sia disattivata.

Tipi di connessione supportati

L'integrazione di Web Collaboration offre supporto per conversazioni telefoniche, conferenze telefoniche e per i seguenti tipi di conferenze controllate dalle applicazioni:

- Conferenza AdHoc
- conferenza pianificata
- conferenza permanente

Integrazione di Web Collaboration

Per l'integrazione di Web Collaboration è necessario che al sistema di comunicazione sia noto l'indirizzo del relativo server. Il produttore offre il server di Web Collaboration su Internet sotto forma di servizio (server pubblico). In alternativa, il server può essere ubicato anche nella rete del cliente o presso un partner (server personalizzato). Se il server si trova nella rete del cliente, in genere questo viene indirizzato dal sistema di comunicazione tramite http sulla porta TCP 5004. In caso di soluzione residente in Internet (server pubblico), viene utilizzata una connessione sicura HTTPS perché tramite questa connessione vengono trasmessi numeri di licenza e password. Per impostazione predefinita, viene utilizzata la porta TCP 5100.

Nota: Per utilizzare Web Collaboration, il sistema di comunicazione richiede una connessione Internet (router predefinito e server DNS). Le connessioni tramite proxy non sono supportate.

I partecipanti interni a una conferenza con client PC UC vengono collegati automaticamente con la sessione di Web Collaboration all'avvio della conferenza. A tal fine, viene automaticamente scaricato FastViewer e aperto in background; tale operazione può richiedere alcuni secondi. I partecipanti alla conferenza esterni con un indirizzo e-mail noto ricevono tramite e-mail il collegamento corrispondente per la sessione di Web Collaboration.

Nota: Con Mac OS, al termine di una seduta di Web Collaboration, è necessario chiudere manualmente la finestra di dialogo che avvisa della sessione terminata.

Con una conferenza pianificata, la connessione con la sessione di Web Collaboration è possibile già 5 minuti prima dell'inizio pianificato della conferenza.

Instant Messaging e Web Collaboration

Le funzioni di instant messaging del sistema e di una sessione di Web Collaboration sono indipendenti una dall'altra: i messaggi istantanei di un client UC non vengono visualizzati in una sessione di Web Collaboration dello stesso partecipante e viceversa.

13.8.1 Come configurare la connessione al server di Web Collaboration (server personalizzato)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È disponibile un accesso a Internet.

Per una connessione sicura al server di Web Collaboration (server personalizzato) è necessaria una chiave di licenza e una password.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Web Services**.
3) Nella struttura dei menu selezionare **Web Services** > **Web Collaboration**.
4) Selezionare il pulsante di opzione **Server personalizzato**.
5) Se si desidera stabilire una connessione sicura al server di Web Collaboration (server personalizzato), procedere come segue:
   a) Nel campo **URL/Indirizzo IP** immettere l'indirizzo del server di Web Collaboration (server personalizzato) secondo il seguente modello:

      `https://<URL del server Web Collaboration>:5100/xmlrpcsecure`

      o

      `https://<Indirizzo IP del server Web Collaboration>:5100/xmlrpcsecure`
   b) Nel campo **Numero licenza**immettere il numero di licenza per la connessione sicura al server di Web Collaboration (server personalizzato).
   c) Nel campo **Password**immettere la password per la connessione sicura al server di Web Collaboration (server personalizzato).

6) Se si desidera stabilire una connessione non sicura al server di Web Collaboration (server personalizzato), procedere come segue:
   a) Nel campo **URL/Indirizzo IP** immettere l'indirizzo del server di Web Collaboration (server personalizzato) secondo il seguente modello:

   ```
   http://<URL del server Web Collaboration>:5004/
   OscInterface
   ```

   o

   ```
   http://<Indirizzo IP del server
   Web Collaboration>:5004/OscInterface
   ```

7) Fare clic su **Applica**, quindi su **OK**.

13.8.2 Come configurare la connessione al server di Web Collaboration (server pubblico)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È disponibile un accesso a Internet.

Per una connessione sicura al server di Web Collaboration (server pubblico) è necessaria una chiave di licenza e una password.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Web Services**.
3) Nella struttura dei menu selezionare **Web Services** > **Web Collaboration**.
4) Selezionare il pulsante di opzione **Server pubblico**.
5) Nel campo **Numero licenza** immettere il numero di licenza per la connessione sicura al server di Web Collaboration (server pubblico).
6) Nel campo **Password** immettere la password per la connessione sicura al server di Web Collaboration (server pubblico).

   Nota: Se si desidera testare la funzione Web Collaboration per 5 minuti, utilizzare il pulsante di opzione **Server pubblico (modalità demo/valutazione)**. A tal fine è necessario un numero di licenza e una password.

7) Fare clic su **Applica**, quindi su **OK**.

13.8.3 Come disattivare la connessione al server di Web Collaboration

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Web Services**.

3) Nella struttura dei menu selezionare **Web Services** > **Web Collaboration**.
4) Selezionare il pulsante di opzione **Nessun server di Web Collaboration**.
5) Fare clic su **Applica**, quindi su **OK**. L'opzione per l'avvio di una sessione di Web Collaboration nel client UC è disattivata.

13.9 Invio messaggi immediato

Per Invio messaggi immediato si intende la comunicazione mediante messaggi istantanei (chat).

13.9.1 Invio messaggi immediato

Con i messaggi istantanei, è possibile chattare con un interlocutore. Il sistema supporta sia utenti di UC Smart che interlocutori esterni e Multi User Chat o una combinazione di entrambi.

I seguenti client supportano i messaggi istantanei:

- myPortal for Desktop
- myPortal for Outlook
- myAgent
- myAttendant

Accendendo come amministratore, è possibile attivare o disattivare la visualizzazione di messaggi istantanei a livello di sistema. I messaggi istantanei inviati e ricevuti vengono visualizzati dall'utente e dai suoi interlocutori in una finestra di dialogo. Selezionando un destinatario, il client mostra se questo è attualmente online. Nel caso di un interlocutore non in linea, in funzione del tipo di destinatario scelto per il messaggio vocale, si verifica quanto segue:

Destinatari	Comportamento
Singoli utenti	Il messaggio istantaneo viene visualizzato al successivo accesso.
Gruppo nei Preferiti	Il messaggio istantaneo viene visualizzato per ogni utente non in linea.

Messaggi istantanei esterni

Gli utenti possono chattare con *un* interlocutore esterno (ad esempio, un utente di Google Talk).

Multi User Chat

Multi User Chat è un formato di scambio per messaggi istantanei che consente la partecipazione di più interlocutori. In questo caso, il sistema supporta un massimo di un interlocutore esterno.

Instant Messaging e Web Collaboration

Le funzioni di invio messaggi istantanei del sistema e di una sessione di Web Collaboration sono indipendenti una dall'altra: i messaggi istantanei di un client

PC UC non vengono visualizzati in una sessione di Web Collaboration dello stesso partecipante e viceversa.

13.9.1.1 Come attivare o disattivare i messaggi istantanei

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**.
4) Fare clic su**Impostazioni generali**.
5) Select one of the following options, under the **Instant Message** area:
   - If you want to enable system-wide instant messaging, clear the **Disable instant messaging** check box.
   - If you want to disable system-wide instant messaging, select the **Disable instant messaging** check box.

   Nota: La disattivazione dei messaggi istantanei non si applica per la finestra dei messaggi istantanei esistenti.
6) Fare clic su **Salva**.

13.10 AutoAttendant

AutoAttendant offre ai chiamanti la possibilità di inoltrare le chiamate vocali alla casella vocale di numeri di telefoni predefiniti, in base allo stato presenza dell'utente chiamato. I chiamanti scelgono l'opzione desiderata componendo cifre specifiche sul telefono.

13.10.1 AutoAttendant personale

AutoAttendant personale è l'istanza di AutoAttendant configurabile dall'utente.

AutoAttendant personale

Gli utenti possono eseguire le seguenti operazioni tramite myPortal for Desktop o myPortal for Outlook:

- Registrare o importare annunci per AutoAttendant personale
- Configurare i profili per AutoAttendant personale

Le relative chiamate verranno prima gestite da AutoAttendant centralizzato.

13.11 Messaggi vocali e fax

I servizi integrati nel sistema di messaggistica vocale e fax consentono agli utenti di ricevere e gestire i messaggi vocali e fax tramite myPortal for Desktop e myPortal for Outlook. Con Fax Printer, l'utente può inviare messaggi fax.

13.11.1 Casella vocale

La casella vocale registra i messaggi vocali e le chiamate centralmente. Gli utenti possono accedere telefonicamente o tramite client UC Smart.

Nota: La password Voicemail predefinita può essere modificata solo tramite un numero di telefono interno.

Vengono registrati solo i messaggi vocali più lunghi di due secondi.

Gestione dei messaggi vocali

Gli utenti possono ascoltare i propri messaggi vocali:

- tramite PC con myPortal for Desktop o myPortal for Outlook
- tramite il telefono, se il proprio stato presenza è **Ufficio** o **CallMe**
- tramite un qualsiasi telefono esterno

Tramite myAttendant, il posto operatore può accedere ai messaggi vocali degli utenti che ne hanno consentito l'accesso.

L'utente gestisce i messaggi vocali ricevuti in una cartella, ad esempio Posta in arrivo, riproducendoli, memorizzandoli o eliminandoli.

I messaggi vocali possono essere anche ascoltati, conservati e inoltrati a un altro utente. L'utente può inoltre salvare i messaggi vocali in formato .wav e inoltrarli a un account e-mail di preferenza.

Tramite la casella vocale, l'utente può gestire anche le conversazioni registrate. Le conversazioni registrate vengono contrassegnate con un'icona speciale nella casella vocale.

Nota: Per informazioni sul menu telefonico, consultare la Guida rapida nella documentazione dell'interfaccia utente del telefono UC Suite (TUI).

Come richiamare il mittente di un messaggio vocale

Ascoltando il messaggio vocale, l'utente può richiamare immediatamente la persona che ha lasciato il messaggio.

L'amministratore può configurare a livello di sistema se è possibile effettuare le richiamate

- dalla casella vocale di qualsiasi numero desiderato
- può essere eseguito solo dai numeri di telefono propri dell'utente configurati nei client myPortal for Desktop, myPortal for Outlook, myAttendant o myAgent in I miei dati personali (**Interno**, **Numero cellulare**, **Numero esterno 1**, **Numero esterno 2**, **Numero casa** e **Numero assistente**).

Tempo di conservazione

L'amministratore può configurare il Tempo di conservazione per messaggi vocali.

Assegnazione delle priorità ai messaggi vocali

Il chiamante può assegnare ai messaggi vocali la priorità normale, urgente o riservato.

In myPortal for Desktop e myPortal for Outlook, per l'assegnazione delle priorità vengono utilizzati diversi colori con cui vengono contrassegnati i messaggi vocali.

All'utente che ascolta i propri messaggi vocali tramite telefono, viene innanzitutto comunicato quanti messaggi urgenti, riservati e normali sono presenti, quindi, vengono riprodotti per primi i messaggi urgenti.

Se i messaggi vocali vengono spediti in allegato a messaggi di posta elettronica, i messaggi contrassegnati come urgenti verranno inviati come e-mail ad elevata priorità.

Selezione delle funzioni della casella vocale

L'amministratore può definire le funzioni della casella vocale da rendere disponibili selezionando una delle seguenti opzioni:

- **Completo**

  È disponibile l'intera gamma di funzioni per la propria casella vocale (valore predefinito)
- **Menu abbreviato**
- Dopo l'annuncio basato sullo stato o personale, la connessione viene segnalata alla destinazione.
- **Nessun menu**
- Dopo l'annuncio di benvenuto, il chiamante viene inoltrato direttamente alla registrazione messaggi.

Visualizzazione dei nuovi messaggi sul telefono

L'arrivo di nuovi messaggi vocali viene segnalato tramite telefono. Non appena il messaggio vocale verrà riprodotto, le informazioni visualizzate verranno cancellate.

Il tipo di segnalazione utilizzata per i nuovi messaggi vocali dipende dal terminale:

- In tutti i telefoni avviene una segnalazione acustica tramite un tono di selezione speciale.
- Nei telefoni di sistema senza display, inoltre, lampeggia il tasto Notifica messaggio (se configurato).
- Nei telefoni di sistema dotati di display lampeggia il tasto Notifica messaggio (se configurato) e sul display appare un messaggio.

Servizio informativo

Qualora l'utente utilizzi myPortal for Desktop o myPortal for Outlook, potrà definire se la notifica di un nuovo messaggio vocale ricevuto vada inoltrata e quale sia la destinazione dell'inoltro.

L'utente può specificare se l'inoltro debba avvenire tramite e-mail e se desidera venire informato sulla ricezione di un nuovo messaggio vocale tramite una chiamata telefonica o un SMS.

Lingua della casella vocale

L'amministratore può definire se applicare la lingua predefinita della casella vocale anche a menu e annunci a livello di sistema.

Dipendenze

Argomento	Dipendenza
Riproduzione del messaggio tramite telefono	L'utente può riprodurre i messaggi vocali tramite telefono solo con lo stato presenza **Ufficio** o **CallMe**. Con tutte le altre impostazioni, i messaggi possono essere riprodotti solo tramite PC.

13.11.1.1 Come configurare il numero di telefono per la casella vocale

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Posta vocale**.
4) Immettere il **Numero casella vocale**.
5) Fare clic su **OK & Avanti**, quindi su **Fine**.

13.11.1.2 Come configurare dell'inoltro chiamata alla casella vocale

La procedura guidata **Inoltro chiamata** può essere utilizzata per configurare tale funzione per la casella vocale di un utente.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Inoltro chiamate**. Viene visualizzata la finestra **Configurare il numero di inoltro**.
4) Nel campo **Seleziona utente / gruppo** selezionare l'utente desiderato.
5) Trascinare col mouse la **Casella vocale** e rilasciarla nell'area della finestra **Modifica inoltro chiamate**.
6) Modificare eventualmente il tempo che trascorrerà prima dell'inoltro di chiamata (predefinito: 15 secondi).

7) Fare clic su **OK & Avanti**, quindi su **Fine**.

13.11.1.3 Come configurare i parametri della casella vocale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**.
4) Click on the **VoiceMail** tab.
5) Nell'elenco a discesa **Lingua della casella vocale** selezionare la lingua da utilizzare per i comandi dei menu e per gli annunci personalizzati della propria casella vocale.
6) Nel campo **Ordine di riproduzione dei messaggi vocali**, specificare in quale ordine si desidera riprodurre i messaggi.
7) Enter the duration in seconds in the **Voicemail Message Recording Time** field.
8) Nel campo **Modalità casella vocale** specificare la capacità della propria casella vocale.
9) Se si desidera che le richiamate dalla casella vocale vengano eseguite solo ai numeri di telefono inseriti nei client UC come **I miei dati personali**, selezionare la casella di controllo **Consenti richiamata da casella vocale solo a numeri noti**.
10) Se si desidera disattivare l'ultimo annuncio riprodotto dal sistema, selezionare la casella di controllo **Ignora il prompt "Lasciare un messaggio dopo il segnale"**. L'annuncio del sistema non verrà ascoltato anche se viene utilizzato un annuncio di registrazione professionale.
11) Fare clic su **Salva**.

13.11.1.4 Come configurare la durata di conservazione per messaggi vocali

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**.
4) Fare clic su **Manutenzione**.
5) Nei campi sotto **Messaggio**, inserire il relativo periodo di conservazione espresso in giorni.
6) Fare clic su **Salva**.

13.11.1.5 Come attivare o disattivare la richiesta di immissione della password per la casella vocale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) In the navigation bar, click on **Expert Mode**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Rubrica utente**.
4) Click on the relevant entry and then click on **Edit** > **Sensitivity**.
5) Fare clic su **Protezione e accesso**.
6) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare la richiesta di immissione della password quando si chiama la propria casella vocale, deselezionare la casella di controllo **Ignora password in caso di chiamate a casella vocale**.
   - Se si desidera disattivare la richiesta di immissione della password quando si chiama la propria casella vocale, selezionare la casella di controllo **Ignora password in caso di chiamate a casella vocale**.
7) Fare clic su **Salva**.

13.11.1.6 Come configurare le informazioni per i messaggi vocali ricevuti

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Server telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema**.
4) Nella struttura dei menu fare clic su **Display**.
5) Nell'area **Interruttore** selezionare la casella di controllo **Indic. stato display per mess. inform**.
6) Fare clic su **Applica**, quindi su **OK**.

13.11.1.7 Come configurare del tasto "Mailbox" per richiamare messaggi vocali

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.

2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefoni / utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Programmazione dei tasti**.
4) Selezionare l'utente corrispondente.
5) Nella prima colonna, selezionare il tasto corrispondente.
6) Nella colonna **Funzioni dei tasti** selezionare la funzione **Notifica messaggio**.
7) Fare clic su **Applica**, quindi su **OK**.

13.11.2 Annunci della casella vocale

Gli annunci della casella vocale informano il chiamante ad esempio dello stato presenza di un utente.

Gli annunci predefiniti sono disponibili in tutte le lingue. Gli utenti hanno la possibilità di registrare o importare annunci per casella vocale personali. I relativi annunci predefiniti verranno quindi sovrascritti dagli annunci personali. Gli amministratori possono modificare gli annunci predefiniti mediante l'importazione di annunci. Gli annunci personali degli utenti verranno quindi sovrascritti. In caso di importazione di annunci, il sistema opera una limitazione di livello e una normalizzazione automatiche, per soddisfare i requisiti dello standard "USA / TIA 968 Signal Power Limitations".

Nota: Prima dell'uso di annunci o musica di altra origine, assicurarsi di non violare alcun copyright.

Lingua di sistema per gli annunci della casella vocale

La lingua di sistema della casella vocale viene impostata sull'inizializzazione specifica nazionale. Tuttavia, ogni utente può impostare autonomamente la lingua della propria casella vocale. Il chiamante sentirà quindi gli annunci che si riferiscono all'utente nella lingua configurata dall'utente e gli annunci che si riferiscono al sistema nella lingua di sistema.

Annunci in base allo stato presenza e al profilo

L'annuncio riprodotto nella casella vocale varia in base allo stato presenza, ad esempio, se lo stato è **Riunione**, l'annuncio informerà che l'utente è in riunione fino alle 15.00. Se, una volta trascorso il tempo previsto per la riunione, l'utente non ha aggiornato il suo stato presenza in "Ufficio", l'annuncio della casella vocale viene automaticamente modificato oppure lo stato presenza viene automaticamente impostato su Ufficio (opzione configurabile dall'utente).

La seguente tabella descrive quale saluto verrà riprodotto per il chiamante in base allo stato presenza e al profilo impostati. Il menu chiamante qui riprodotto si riferisce ad AutoAttendant centralizzato. Il profilo si riferisce all'AutoAttendant personale dell'utente. L'annuncio predefinito, il nome e il saluto definito dall'utente per il profilo devono essere registrati dall'utente. In base alla configurazione, il menu chiamante può contenere numerose opzioni oppure non essere disponibile.

	Occupato Non rispondere Non disturbare	Riunione Malattia Pausa Fuori sede ...
Casella vocale con stato presenza	Annuncio predefinito + Menu chiamante	Nome + Presenza + Menu chiamante
Casella vocale con stato presenza memorizzato	Annuncio predefinito + Menu chiamante (se attivato)	
Profilo con annuncio dinamico	Saluto definito dall'utente per profilo	Nome + Presenza + Saluto definito dall'utente per profilo
Profilo per i casi in cui l'annuncio dinamico deve essere ignorato	Saluto definito dall'utente per profilo	

Se un utente ha definito che il suo stato presenza non deve essere trasmesso a un chiamante esterno, in caso di stato presenza diverso da "Ufficio", per il chiamante esterno viene riprodotto l'annuncio di benvenuto "Occupato", anche se l'utente chiamato non è allo stato occupato. In questo caso, l'utente deve quindi definire un annuncio di benvenuto per "Occupato", indicante che non si riesce a rispondere alla chiamata.

13.11.2.1 Come importare gli annunci per la casella vocale

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

The audio files to be loaded are available as PCM files with the following properties: 8 kHz, 16 bit, Mono. Il nome del file audio può avere una lunghezza massima di 30 caratteri.

Nota: Con la procedura guidata Audio, è possibile creare file audio adatti e quindi unire due sorgenti, ovvero sottofondo musicale e annuncio.

Suggerimento: Prima dell'uso assicurarsi di non violare alcun copyright.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.

2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Click on **Edit** to start the **File Upload** wizard.
4) On the **Audio File Manager** tab, select the entry **VoiceMail Greeting** as the **Upload Destination**.
5) Se si desidera riprodurre un file audio, procedere come segue:
   a) Select the **Uploader** radio button and click on **Choose File** to select an appropriate audio file.
   b) In the **Audio File Details** area, you will see the properties of the audio file such as the file name, file size, bit rate, etc.
   c) Click **Upload**.
6) Se si desidera registrare un annuncio tramite un telefono, procedere come segue:
   a) Select the **Recorder** radio button and under **Extension** field, select the phone with which the announcement is to be recorded.
   b) Under the **Filename** field enter the name of the recording's file .
   c) Click on **Make Call**. Il telefono selezionato squilla.
   d) Lift the telephone handset and click **Record**.
   e) Speak into the handset to record your announcement and click **Finish** at the end.
   f) You can then listen to your recording again with **Play**.

13.11.2.2 Come modificare la lingua per gli annunci della casella vocale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**.
4) Click on **VoiceMail**.
5) Select the **VoiceMail Language** from the drop-down list.
6) Fare clic su **Salva**.

13.11.3 Casella fax

La casella fax consente agli utenti di ricevere e gestire i messaggi fax senza dispositivo fax tramite myPortal for Desktop o myPortal for Outlook.

L'amministratore può configurare una casella fax per gli utenti con licenza. È inoltre possibile collegare dispositivi fax o server fax tramite interfaccia ISDN o a/b.

Tramite myPortal for Desktop o myPortal for Outlook, un utente può accedere ai propri messaggi fax. Con myAttendant è anche possibile accedere ai messaggi fax degli utenti che hanno espressamente autorizzato tale accesso.

Gestione dei messaggi fax

I messaggi fax ricevuti possono essere gestiti spostandoli in una cartella (ad esempio Salvati o Eliminati). I messaggi fax si possono anche inoltrare a un altro utente. L'utente può inoltre salvare i messaggi fax in formato PDF o TIFF e inoltrarli a un account e-mail di preferenza.

L'amministratore può definire a livello di sistema se i messaggi fax devono essere salvati come file TIFF (predefinito) o PDF.

Nota: Per convertire un file TIFF in un file PDF, la dimensione della pagina deve essere A4.

Tempo di conservazione per messaggi fax

Il sistema cancella automaticamente i messaggi fax più vecchi rispetto al seguente tempo di conservazione:

Messaggio fax	Tempo di conservazione (giorni)
Nuovo	120
Leggi	365
Inviato	365
Eliminati	60

13.11.3.1 Come aggiungere una casella fax per gli utenti

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefoni / utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Terminali IP**.
4) Fare clic nel campo **N° fax** dell'utente e inserire il numero di fax al quale l'utente potrà ricevere i messaggi fax (il trattino preinserito deve essere eliminato).
5) Se per la casella fax deve essere configurato un numero di selezione passante, fare clic nel campo **Selezione passante fax** e inserire il numero di selezione passante del fax (il trattino preinserito deve essere eliminato).
6) Fare clic su **OK & Avanti**. Se necessario, è possibile stampare un elenco degli utenti con il numero di fax configurato premendo **Stampa**.
7) Fare clic su **OK & Avanti**, quindi su **Esci**, per uscire dalla procedura guidata.

13.11.3.2 Come configurare il tipo dati per i messaggi fax salvati (UC Suite)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**.
4) Fare clic su**Impostazioni generali**.
5) Se si desidera che i messaggi fax vengano salvati come file PDF, nell'area **Formato fax**, selezionare la casella di controllo **Usa PDF come formato fax**.
6) Se si desidera che i messaggi fax vengano salvati come file TIFF, nell'area **Formato fax**, deselezionare la casella di controllo **Usa PDF come formato fax**.
7) Fare clic su **Salva**.

13.11.4 Invio di messaggi fax con Fax Printer

Fax Printer è un'applicazione per l'invio di messaggi fax da applicazioni Windows, quali ad esempio, Microsoft Word, con gestione centralizzata delle singole copertine fax.

Fax Printer è costituita dai seguenti componenti:

- Fax Printer Cover Editor
- Fax Printer Driver

Fax Printer può essere utilizzata da tutte le applicazioni Windows correnti. I gruppi fax semplificano la distribuzione. I messaggi fax vengono inviati come e-mail o direttamente sul desktop. Una finestra popup conferma che l'invio è stato eseguito.

Righe intestazione

L'amministratore può configurare diverse righe d'intestazione per l'utente di Fax Printer. È possibile definire una riga d'intestazione come predefinita. Le righe d'intestazione possono contenere i seguenti elementi:

Dettaglio	Segnaposto
Data / Ora	`{{date_time}}`
Nome società	`{{company_name}}`
Nome utente	`{{user_name}}`
Num. società	`{{company_number}}`
Numero pagine	`{{page_number}}`
Conteggio pagine	`{{page_count}}`

Le righe di intestazione dei messaggi fax inviati con Fax Printer possono contenere solo caratteri ANSI. In altri termini, non sono consentiti caratteri speciali o diacritici come le umlaut. Siccome tali righe solitamente contengono il nome del mittente, questo non può contenere caratteri speciali o umlaut.

13.11.4.1 Come aggiungere una copertina centralizzata

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

È disponibile una copertina fax sotto forma di file .ocp.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Click on **Edit** to start the **File Upload** wizard.
4) Click on the **Central Fax Cover Page Upload** tab.
5) Click on **Choose File**.
6) Selezionare un file .ocp.
7) Fare clic su **Apri**.
8) Under **Name**, enter a name for the fax cover page.
9) Enter a **Description** for the fax cover page.
10) Click on **Upload**.
11) Click **OK** once the upload has been completed.
12) If you want to use this fax cover page as default, click on it in the list of fax cover pages and then click on **Set To Default**.
13) Fare clic su **Salva**.

13.11.4.2 Come modificare la copertina centralizzata

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Click on **Edit** to start the **File Upload** wizard.
4) Click on the **Central Fax Cover Page Upload** tab.
5) Nell'elenco di copertine fax, fare clic sulla copertina corrispondente.
6) Clic su **Modifica**.
7) Under **Name**, enter a name for the fax cover page.
8) Enter a **Description** for the fax cover page.
9) Fare clic su **Salva**.

13.11.4.3 Come aggiungere la riga di intestazione di Fax Printer

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Intestazione fax**.
4) Fare clic su **Aggiungi**.
5) Enter the **Template Name** for the fax headline.
6) To add details to the header line, click on the **Date / Time**, **Company Name**, **User name**, **Company Ph.**, **Page number** and **Page count** buttons in the desired sequence. Per ogni dettaglio viene visualizzato un segnaposto nel campo **Testo**.
7) Per rimuovere informazioni dalla riga d'intestazione, nel campo **Corpo** selezionare il relativo segnaposto, ad esempio, `{{page_count}}` (**Conteggio pagine**) e premere il tasto `Canc`.
8) Ove necessario, nel campo **Corpo** inserire testo aggiuntivo, ad esempio "di" tra i segnaposto `{{page_number}}` (**Numero pagine**) e `{{page_count}}` (**Conteggio pagine**).
9) Fare clic su **Salva**.

13.11.4.4 Come modificare la riga di intestazione di Fax Printer

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **UC Suite**.
3) Fare clic su **Intestazione fax**.
4) Nell'elenco di intestazioni fax, fare clic sull'intestazione desiderata.
5) Clic su **Modifica**.
6) Enter the **Template Name** for the fax headline.
7) To add details to the header line, click on the **Date / Time**, **Company Name**, **User name**, **Company Ph.**, **Page number** and **Page count** buttons in the desired sequence. Per ogni dettaglio viene visualizzato un segnaposto nel campo **Testo**.
8) Per rimuovere informazioni dalla riga d'intestazione, nel campo **Corpo** selezionare il relativo segnaposto, ad esempio, `{{page_count}}` (**Conteggio pagine**) e premere il tasto `Canc`.
9) Ove necessario, nel campo **Corpo** inserire testo aggiuntivo, ad esempio "di" tra i segnaposto `{{page_number}}` (**Numero pagine**) e `{{page_count}}` (**Conteggio pagine**).
10) Fare clic su **Salva**.

13.11.4.5 Come cancellare la riga di intestazione di Fax Printer

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Intestazione fax**.
4) Nell'elenco di intestazioni fax, fare clic sull'intestazione desiderata.
5) Fare clic su **Rimuovi**.

13.11.5 Servizio informativo per nuovi messaggi (UC Suite)

Se lo si desidera, il sistema può informare l'utente dell'arrivo di un nuovo messaggio tramite e-mail, telefono o messaggio SMS.

Il servizio informativo funziona nel modo seguente:

Avviso	per messaggi vocale	per messaggi fax	Requisiti
E-mail	L'utente riceve un'e-mail con allegato un file WAV, contenente data e ora del ricevimento, durata del messaggio e, se disponibile, numero di telefono e nome del mittente. Se la dimensione del file WAV supera 10 MB (in media 1 MB/min), questo non potrà essere allegato al messaggio e-mail. I messaggi vocali con priorità "Urgente" vengono inviati per e-mail con priorità "Alta". Le e-mail con un messaggio vocale hanno una propria icona in Outlook. Se viene utilizzata la propria casella IMAP, che mostra solo l'intestazione dell'e-mail, viene visualizzato al suo posto l'icona caratteristica delle e-mail.	L'utente riceve un'e-mail con allegato un file PDF o TIFF, contenente data e ora del ricevimento, numero di pagine e, se disponibile, numero di telefono e nome del mittente. Se la dimensione del file PDF o TIFF supera 10 MB, questo non potrà essere allegato al messaggio e-mail. Le e-mail con un messaggio fax hanno una propria icona in Outlook. Se viene utilizzata la propria casella IMAP, che mostra solo l'intestazione dell'e-mail, viene visualizzato al suo posto l'icona caratteristica delle e-mail.	Nel sistema è stato configurato l'invio di e-mail. L'indirizzo corrispondente viene utilizzato come mittente.
SMS	Si riceve un SMS al numero di telefono definito, che informa dell'arrivo del messaggio		È stato configurato un modello SMS
Telefonicamente	La casella vocale chiama il relativo utente al numero di telefono da questi impostato e riproduce il messaggio.	-	

L'utente può attivare o disattivare separatamente ogni tipo di avviso per ciascuno stato presenza. L'avviso telefonico può essere limitato agli orari di ufficio definiti dall'amministratore. È possibile definire il numero e l'intervallo tra i tentativi di invio dell'avviso telefonico.

13.11.6 Invio per e-mail

L'invio ei e-mail consente di avvisare gli utenti dell'arrivo di nuovi messaggi vocali e fax nonché di notificare i messaggi di sistema agli amministratori.

13.11.6.1 Come configurare l'invio di e-mail

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

È stato configurato un account e-mail con una password presso un provider di posta elettronica e si conoscono i dati di accesso.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione, fare clic su **Centro assistenza** > **Inoltro e-mail**.
3) Inserire il **Server della posta in uscita (SMTP)** per il server di posta elettronica, da utilizzare per l'invio delle e-mail, ad esempio, `smtp.web.de`. Eventualmente richiedere il server della posta in uscita al proprio provider di posta elettronica.

   Nota: In alcuni casi l'invio di e-mail non funziona poiché il nome del server della posta in uscita non viene risolto. Per la risoluzione del problema, è necessario indicare al posto del nome, l'indirizzo IP del server.

4) Se è necessario stabilire una connessione sicura, selezionare la casella di controllo. Chiedere al proprio provider di posta elettronica se questa opzione deve essere selezionata.
5) Immettere il **Nome utente** dell'account di posta elettronica.
6) In **Nuova password** e **Ripeti password** immettere la password dell'account di posta elettronica.
7) Inserire **l'Indirizzo di posta elettronica**, ad esempio `bruno.rossi@web.it`.
8) Per testare immediatamente l'invio di e-mail configurato, procedere come segue:
   a) Fare clic su **Test connessione**.
   b) Nel campo **Invia a un indirizzo e-mail** inserire l'indirizzo di posta elettronica del servizio a cui si ha accesso.
   c) Inserire l'**Oggetto** nell'e-mail.
   d) Fare clic su **Invia e-mail di prova**.
   e) Verificare se si è ricevuto l'e-mail.
   f) Se l'invio dell'e-mail non ha avuto esito positivo, fare clic su **Indietro** e verificare le impostazioni di posta elettronica (dal passo 3).
9) Inserire l'**Indirizzo e-mail 1** per ricevere un'e-mail di notifica quando viene utilizzata la tolleranza ALI. È anche possibile inserire un secondo indirizzo e-mail.
10) Fare clic su **OK & Avanti**, quindi su **Fine**.

Esempio

Nota: Se si apportano modifiche alla configurazione in Inoltro e-mail in un sistema OpenScape Business X con Booster Server, è necessario riavviare Booster Server per implementare le modifiche.

13.11.7 Modello SMS

Un modello SMS consente di avvisare gli utenti tramite SMS dell'arrivo di nuovi messaggi vocali.

Per ricevere comunicazioni via SMS è necessario innanzitutto attivare un indirizzo personale di posta elettronica mobile presso il proprio provider. L'utente invia a tale scopo un SMS di attivazione ad un numero di selezione breve. L'utente riceverà quindi via SMS il proprio indirizzo personale di posta elettronica che, di norma, è composto dal numero di telefono e dal nome del gateway. Quindi, per esempio, l'indirizzo di posta elettronica mobile di un cliente T-Mobile con numero di telefono 0171/1234 567 sarà: 01711234567@t-mobile-sms.de. Se analogico, vale anche per le altre reti.

Un modello SMS è composto dalle sezioni Dettagli modello e Dettagli SMS. L'amministratore deve immettere nell'area Dettagli modello il nome del modello che solitamente corrisponde al nome del provider E-mail a SMS.

Le informazioni fornite nel campo Dettagli SMS dipendono dal provider. Come Destinatario l'amministratore dovrà indicare l'indirizzo e-mail a cui deve essere inviato l'SMS. Il testo dell'oggetto può essere scelto liberamente o altrimenti l'amministratore deve immettere il numero cliente.

Nota: Ogni provider necessita di un modello specifico. Per i dati necessari, fare riferimento al rispettivo provider dei servizi mobili.

Segnaposto

I modelli SMS possono contenere i seguenti segnaposto nei campi **Destinatario**, **Oggetto** o **Corpo**:

Dettaglio	Segnaposto
Numero di cellulare per l'invio	`{{Cellulare}}`
Nome o numero di telefono del mittente	`{{Mittente}}`
Data e ora di ricezione messaggio	`{{DataOra}}`
Numero del chiamante	`{{NumeroChiamante}}`
Priorità del messaggio	`{{Priorità}}`

Informazioni specifiche del sistema

La lunghezza del messaggio è limitata a 160 caratteri.

13.11.7.1 Come aggiungere un modello SMS

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Modelli**.
4) Fare clic su **Aggiungi**.
5) Inserire il **Nome modello**.

   Nota: Il nome del modello non deve contenere spazi.

6) Inserire il nome dell'autore in **Nome autore**.
7) Se si desidera aggiungere un segnaposto, procedere come segue:
   a) Click in the field in which you want to insert the placeholder: **Recipients**, **Subject** or **Text**.
   b) Nell'elenco a discesa **Campi VSL** selezionare il segnaposto desiderato.
   c) Click on **Insert**.
   d) Se si desidera inserire altri segnaposto, ripetere il corrispondente passo 7a-c.
8) Inserire il **Destinatario**.
9) Inserire l'**Oggetto**.
10) Inserire il **Testo**.
11) Fare clic su **Crea**.

13.11.7.2 Come modificare un modello SMS

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Modelli**.
4) Select the desired SMS template from the **SMS Provider** table.
5) Clic su **Modifica**.
6) Inserire il **Nome modello**.

   Nota: Il nome del modello non deve contenere spazi.

7) Inserire il nome dell'autore in **Nome autore**.

8) Se si desidera aggiungere un segnaposto, procedere come segue:
   a) Click in the field in which you want to insert the placeholder: **Recipients**, **Subject** or **Text**.
   b) Nell'elenco a discesa **Campi VSL** selezionare il segnaposto desiderato.
   c) Click on **Insert**.
   d) Se si desidera inserire altri segnaposto, ripetere il corrispondente passo 8a-c.
9) Inserire il **Destinatario**.
10) Inserire l'**Oggetto**.
11) Inserire il **Testo**.
12) Fare clic su **Crea**.

13.11.7.3 Come eliminare un modello SMS

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Modelli**.
4) Select the desired SMS template from the **SMS Provider** table.
5) Click on **Remove**.
6) Fare clic su **OK**.

13.11.8 Fax over IP (Fax T.38 / G.711)

Fax over IP consente la trasmissione di messaggi fax conformi allo standard G2 e G3 tramite Internet con il protocollo di rete IFP (Internet Facsimile Protocol).

Generalmente, la UC Suite è in grado di gestire fino a 8 connessioni fax simultanee. Come gateway ISDN, OpenScape Business X3/X5/X8 può gestire da 3 a 12 fax simultanei, in funzione del modulo DSP. Entrambi i parametri determinano il numero di connessioni fax T.38 o G.711 simultanee.

Nota: Si consiglia vivamente di usare il fax T.38, se possibile.

Per T.38 o G.711, il sistema supporta i seguenti scenari:

- Un utente riceve fax tramite un ITSP (Internet Telephony Service Provider) nella sua casella fax e invia fax con Fax Printer sempre tramite ITSP.
- L'utente riceve fax tramite Mediatrix 4102S (SIP) nella sua casella fax e invia fax con Fax Printer sempre tramite Mediatrix 4102S (SIP).
- L'utente riceve un fax tramite un ITSP (Internet Telephonie Service Provider) su un dispositivo fax collegato direttamente a un'interfaccia ISDN o analogica e invia fax all'esterno del sistema da tale dispositivo, sempre tramite ITSP.

- L'utente riceve fax tramite un ITSP su un dispositivo fax collegato a Mediatrix 4102S e invia fax all'esterno del sistema da tale dispositivo tramite Mediatrix 4102S e ITSP.
- L'utente riceve fax tramite ISDN su un dispositivo fax collegato a Mediatrix 4102S e invia fax all'esterno del sistema da tale dispositivo tramite Mediatrix 4102S e ISDN.
- L'utente invia fax da un dispositivo fax, collegato a Mediatrix 4102S, a un altro dispositivo fax, anch'esso collegato a Mediatrix 4102S.
- Fax interno da un dispositivo fax collegato a un'interfaccia ISDN inviato a un dispositivo fax collegato a un Mediatrix 4102S e viceversa.
- Fax interno da un dispositivo fax collegato a un'interfaccia ISDN inviato a una casella fax e viceversa.

Nota: Per la casella fax è necessario attivare T.38 nel sistema. Per l'invio di fax dal sistema di comunicazione tramite ITSP, è necessario il supporto per T.38. Se l'ITSP non può essere commutato su T.38, il fax verrà gestito come G.711.

13.11.8.1 Come attivare o disattivare Fax over IP (fax T.38)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Server telefonia** > **Gateway voce**.
3) Nella struttura dei menu fare clic su **Gateway voce**.
4) Nella struttura dei menu fare clic su **Parametri Codec**.
5) Nell'area **Fax T.38**, selezionare una delle seguenti possibilità:
   - Se si desidera attivare la funzione Fax over IP (fax T.38), selezionare la casella di controllo **Fax T.38**.
   - Se si desidera disattivare la funzione Fax over IP (fax T.38), deselezionare la casella di controllo **Fax T.38**.
6) Fare clic su **Applica**, quindi su **OK**.

13.12 Panoramica sull'integrazione di Microsoft Office 365

Si può collaborare facilmente con l'accesso ovunque a e-mail, conferenze Web, documenti e calendari. Include sicurezza aziendale ed è supportato da Microsoft. Che si tratti di una piccola impresa o una multinazionale, Office 365 offre piani progettati per soddisfare le esigenze specifiche della propria organizzazione. Per maggiori dettagli o per un account di 30 giorni, visitare il sito

OpenScape Business con Microsoft Office 365

Quando un utente imposta un appuntamento nel proprio calendario di Microsoft Outlook, il sistema OpenScape Business controlla automaticamente parole chiave negli oggetti dell'appuntamento del calendario, come: "riunione",

"malato", "pausa", "fuori sede". Se viene trovata una parola chiave, il sistema imposta automaticamente lo stato di presenza dell'utente al raggiungimento dell'orario dell'appuntamento, anche se la sessione di Microsoft Outlook dell'utente interessato non è più attiva.

L'utente configura gli appuntamenti con queste parole chiave e OpenScape Business imposta automaticamente lo stato di presenza telefonica dell'utente e inoltra le chiamate alla casella vocale o, ad esempio, al cellulare, a seconda delle impostazioni. L'utente può anche configurare in uno stato client generico, se lo stato di presenza deve tornare allo stato di presenza di Office al termine dell'orario dell'appuntamento.

Funziona anche se l'utente non utilizza il client Outlook locale e fisserà un appuntamento con le parole chiave sopra indicate direttamente dalla pagina Web di Outlook nel cloud.

Inoltro e-mail:

OpenScape Business è in grado di inviare e-mail a Microsoft Office 365 incluso Microsoft Exchange Server.

Ciò consente agli utenti di ricevere e-mail per nuovi messaggi vocali, fax o chiamate in conferenza con la possibilità di eseguire automaticamente sessioni di Web Collaboration da OpenScape Business.

OpenScape Business genera e-mail per tali azioni e tiene aggiornati gli utenti anche tramite e-mail, se tale nuova notifica arriva nella casella dei messaggi di OpenScape Business.

13.12.1 Come connettere il sistema OpenScape Business a Microsoft Office 365 tramite l'autenticazione base

È possibile connettere il sistema OpenScape Business a Microsoft Office 365 nel cloud, tramite l'autenticazione base, per utilizzare l'integrazione del calendario di OpenScape Business Exchange e l'inoltro e-mail del server Microsoft Exchange integrato in Microsoft Office 365.

Prerequisiti

- Microsoft Office 365- Office 365 Enterprise E3 con la suite "Microsoft Office Professional Plus" installata in locale e l'utilizzo di Office Web Apps.
- Gli utenti sono disponibili in Microsoft Office 365 e connessi con il Microsoft Outlook locale con l'e-mail assegnata; indirizzato in Microsoft Exchange di Microsoft Office 365.
- Tutti gli aggiornamenti e i Service Pack di Microsoft disponibili sono installati.
- Verificare le licenze Microsoft Enterprise giuste necessarie.
- Consultare la nota sulla versione di OpenScape Business per le versioni rilasciate di Microsoft Office.
- Microsoft Office e Office Web Apps devono essere installati in locale.

Informazioni importanti:

- Modificare il valore del dominio Microsoft Office 365 (ad esempio: test.onmicrosoft.com) in modo che corrisponda alle impostazioni dell'ambiente.
- In questo esempio, l'utente "oso" viene utilizzato come account di servizio con il privilegio di ruolo per "ApplicationImpersonation", utilizzato per dare a

OpenScape Business accesso al database delle cassette postali di Microsoft Exchange Server. Questo utente deve essere aggiunto nella directory degli utenti di Microsoft Office 365 come illustrato di seguito. È richiesto anche un indirizzo e-mail configurato.

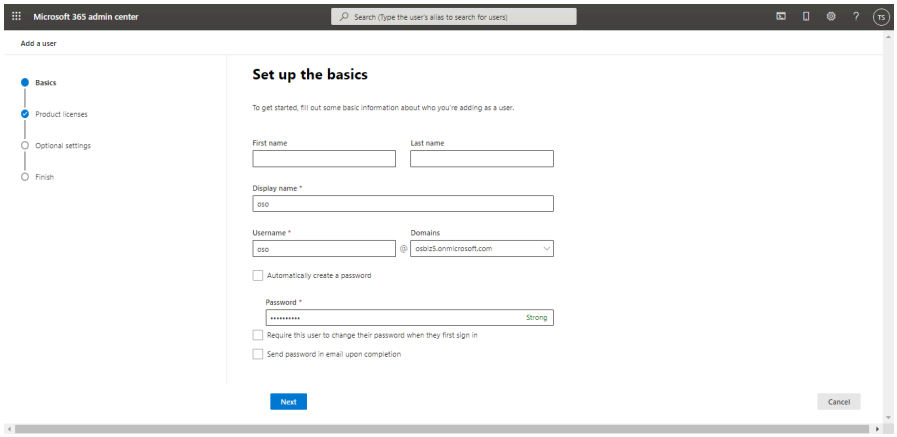
- La nota funzione "Ricerca dei contatti nelle cartelle pubbliche di Microsoft Exchange" del client Openscape Business è disponibile, dato che Microsoft Office 365 offre questa funzionalità.

Passo a passo

1) Eseguire la registrazione di **Microsoft Office 365 Enterprise E3** sul pagina Web ufficiale di Microsoft.
   a) Assegnare i diritti di amministratore globale all'utente "oso".
2) Accedere al Centro di amministrazione di Microsoft 365 e andare su **Utenti > Utenti attivi**, aggiungere l'utente "oso", testare gli utenti "utente1-utente3" e assegnare indirizzi e-mail validi.

   Seguire la configurazione guidata per configurare gli utenti.

   Aggiungere i diritti di amministratore globale all'utente "oso".



3) Uscire dall'interfaccia di amministrazione di Microsoft 365 e accedere con il nuovo utente "oso" creato per modificare la password temporanea.

   Verificare che l'utente "oso" abbia accesso alla pagina di amministrazione: **Integrità > Integrità dei servizi**. Dopo che il controllo dell'integrità dei servizi è stato completato senza problemi importanti, disconnettersi e accedere nuovamente con l'amministratore di Microsoft 365.

   Verificare che gli utenti siano disponibili nella directory degli utenti di Microsoft Office 365, abbiano già effettuato l'accesso al proprio profilo una volta per modificare le password temporanee e possano accedere alla propria casella di posta di Microsoft Office 365 con il Microsoft Outlook installato in locale. Questa installazione locale di Microsoft Office 365 deve essere connessa al portale Microsoft Office 365; installarla e aggiornarla con tutti gli aggiornamenti Microsoft disponibili.
4) Scaricare Microsoft Office dal portale di Microsoft Office 365, se non è già stato fatto. Installarlo e aggiornarlo con gli ultimi aggiornamenti Microsoft disponibili.

5) Impostare l'utente "oso" come utente con privilegi per poter accedere ai calendari degli utenti di **Integrazione del calendario di Exchange**.

a) Su un computer Microsoft Windows 10, aprire PowerShell in modalità con privilegi elevati:

- Aprire il menu di avvio e digitare "Power". Viene contrassegnato il comando "Windows PowerShell".
- Tenere premuti i tasti Maiusc + Ctrl e usare il tasto Invio per avviare PowerShell.
- Applicare il messaggio UAC imminente con Sì per avviare PowerShell.

b) Verificare se il criterio di esecuzione locale consente l'utilizzo degli script nel computer: `Get-ExecutionPolicy`

c) Se il risultato non è "RemoteSigned", eseguire il comando: `Set-ExecutionPolicy RemoteSigned`. Se l'esecuzione del comando non riesce, controllare che i privilegi sul questo computer in uso consentano tale modifica e di aver avviato PowerShell in modalità con privilegi elevati.

d) Eseguire le righe di comando per accedere a Microsoft Exchange Server online e accedere con il proprio account amministratore principale di Microsoft Office 365:

```
$LiveCred=Get-Credential Import-PSSession $Session -
AllowClobber
```

```
$Session = New-PSSession -ConfigurationName
Microsoft.Exchange -ConnextionUri https://
ps.outlook.com/powershell/-Credential $LiveCred -
Authentication Basic -AllowRedirection
```

```
Import-PSSession $Session -AllowClobber
```

e) Configurare Microsoft Office 365: `Enable-OrganizationCustomization`

f) Modificare il valore dell'utente con privilegi in modo che corrisponda alle impostazioni dell'ambiente in uso: `New-ManagementRoleAssignment -Name "Impersonatipon-`

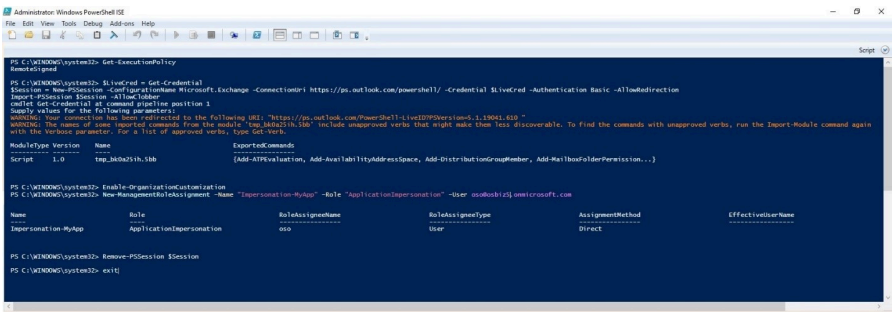
```
MyApp" -Role "ApplicationImpersonation" -User
oso@osbiz5.onmicrosoft.com
```

g) Controllare il valore impostato: `Get-ManagementRoleAssignment "Impersonatipon-MyApp"`

h) Uscire dalla sessione attuale: `Remove-PSSession $Session exit`

PoweShell si chiude dopo il comando Exit. Se PowerShell si chiude prima di inserire `Remove-PSSession $Session`, un nuovo accesso potrebbe essere bloccato per 15 minuti.

Nota: Verificare che i comandi funzionino e che non vengano visualizzati messaggi di errore rossi durante l'esecuzione.



Nota: Per ulteriori dettagli sull'utilizzo di PowerShell, vedere la guida di Microsoft Office 365.

---

6) Accedere al portale di Microsoft Office 365 www.office.com con l'utente "oso" per ottenere le informazioni e selezionare **Outlook** dalla struttura ad albero a sinistra. Quindi andare su **Impostazioni > Visualizza tutte le impostazioni di Outlook > Posta > Sincronizza posta**.

Annotare il nome del server e la porta dell'impostazione SMTP. Ad esempio, smtp.office365.com e 587. Si avrà bisogno di queste informazioni per i passaggi successivi.

7) Andare su **WBM > Configurazione > UC Suite > Configurazione provider esterni > Integrazione del calendario di Exchange** e applicare le seguenti impostazioni per connettersi al server di Microsoft Office 365:
   a) Fare clic sulla casella di controllo **Attiva integrazione del calendario di Exchange**.
   b) Dall'elenco a discesa **Metodo di autenticazione**, selezionare **Base**.
   c) Inserire l'**URL server**. Ad esempio, https://outlook.office365.com/ews/exchange.asmx
   d) Inserire il **Nome utente** dell'utente con privilegi impostato nella directory di Microsoft Office 365.
   e) Inserire la **Password** dell'utente con privilegi impostata nella directory di Microsoft Office 365.
   f) Fare clic su **Salva**.

   Queste modifiche garantiranno l'accesso di OpenScape Business a Microsoft Exchange Server all'interno di Microsoft Office 365 per l'integrazione del calendario di Exchange.

   Nota: I campi per **Provider contatti > Scambio** deve essere compilato con l'indirizzo Exchange online: https://outlook.office365.com/ews/exchange.asmx e l'indirizzo e-mail dell'amministratore globale (in questo esempio: oso@osbiz5.onmicrosoft.com), per poter cercare i contatti dalle cartelle pubbliche.

   ---

8) Navigare verso **Centro assistenza > Inoltro e-mail** per attivare l'accesso alla posta da OpenScape Business a Microsoft Office 365
   a) Inserire l'indirizzo del server di Microsoft Office 365 nel campo **Server della posta in uscita (SMTP)**, **Porta server posta in uscita** e attivare **Questo server richiede una connessione criptata (TLS/SSL)** nell'area **Informazioni server**.
   b) Dall'elenco a discesa **Metodo di autenticazione**, selezionare **Base**.
   c) Inserire **Nome utente, Password** e **Conferma password** dell'utente con privilegi in Microsoft Office 365 nell'area **Informazioni di accesso**.
   d) Inserire l'**Indirizzo email** dell'utente con privilegi in Microsoft Office 365 nell'area **Dati utente (Mittente)**.
   e) Immettere l'**Indirizzo e-mail 1** e l'**Indirizzo e-mail 2** nell'area dei destinatari della notifica di modifica ALI.
   f) Fare clic su **OK&Avanti**.
   g) Fare clic su **Test inoltro posta elettronica** per verificare che la funzione funzioni.

9) Configurare le impostazioni del client OpenScape Business:

   A partire da febbraio 2020, l'autenticazione OAuth è disponibile per le connessioni POP3, IMAP4 e SMTP AUTH a Exchange Online. Pertanto, è necessario attivare l'invio SMTP del client autenticato (SMTP AUTH) in Exchange Online. Seguire: https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission

   È necessaria anche la rappresentazione degli utenti. Accedere con admin@osbiz5.onmicrosoft.com a Office 365 e vai alla pagina di amministrazione nella struttura ad albero a sinistra. Si aprirà una nuova scheda della finestra. Nella nuova finestra, in "Interfacce di amministrazione" andare su "Exchange". La nuova scheda della finestra

si apre di nuovo e in "Ruoli" nella struttura ad albero a sinistra, andare di nuovo alla scheda "Ruoli amministratore" e fare clic su "Aggiungi gruppo di ruoli". Dare un nome e premere Avanti. Fare clic sul punto elenco "ApplicationImpersonation" e quindi su "Avanti". Infine, aggiungere gli utenti al gruppo e finalizzare.

Verificare che la suite Microsoft Office sia installata sul computer dell'utente e connessa a Microsoft Office 365 e, se non è già stato fatto, installare CommunicationsClients con almeno l'opzione myPortal for Outlook.

a) Aprire il seguente percorso in Esplora risorse: \ \198.6.127.12\applications\install-common\CommunicationsClients.exe

   Sintassi: \\<Openscape Business ip-address>\applications\install-common\CommunicationsClients.exe

b) Accedere con le credenziali WBM e seguire l'installazione guidata per installare almeno l'opzione myPortal for Outlook.

10) Aprire Microsoft Outlook e accedere con le credenziali dell'utente al sistema OpenScape Business con i client OpenScape Business. Per maggiori dettagli, vedere il manuale d'uso di myPortal for Outlook.

Nota: Si può anche usare l'opzione **Installazione Silent** per installare i CommunicationsClients non presidiati sui computer degli utenti. Per ulteriori informazioni, vedere Installazione/disinstallazione Silent per client PC UC Suite alla pagina 538.

---

11) Navigare verso **WBM > Configurazione > UC Suite > Rubrica utente** per aggiungere l'indirizzo e-mail dell'utente.

OpenScape Business invierà automaticamente un messaggio di "Benvenuto" a tutti i nuovi indirizzi di posta inseriti con questa configurazione.

Nota: Si può eseguire questo passaggio anche in **WBM > Configurazione > UC Suite > Rubrica utente**.

Nota: È necessario un indirizzo di posta valido configurato per l'utilizzo dell'integrazione del calendario di Exchange e anche per la notifica di posta facoltativa quando l'utente riceve un messaggio da OpenScape Business.

Ripetere questo passaggio per tutti gli utenti.

12) Navigare verso **WBM > Configurazione > UC Suite > Profili** per configurare la funzione **Integrazione del calendario di Exchange**.

a) Selezionare l'utente per cui si desidera attivare la funzione, fare clic su **Modifica** e poi su **Preferenze > Connettività Outlook**.

b) Selezionare l'opzione **Integrazione del calendario di Exchange** in **Integrazione del calendario**

c) Fare clic sull'opzione **Genera automaticamente gli appuntamenti del calendario dalle modifiche della mia presenza**

d) Selezionare **PST scambio** dall'elenco a discesa.

Ripetere questo passaggio per tutti gli utenti.

13) Navigare verso **WBM > Configurazione > UC Suite > Profili**. Selezionare l'utente che si desidera configurare e fare clic su **Avviso VM** per configurare se le notifiche di posta per i messaggi vocali verranno inviate in stati di presenza specifici, quando un nuovo messaggio vocale viene salvato nella casella postale dell'utente.

    Ripetere questo passaggio per tutti gli utenti. Questo passaggio è facoltativo.

14) Navigare verso **WBM > Configurazione > UC Suite > Profili**. Selezionare l'utente che si desidera configurare e fare clic su **Avviso Fax** per configurare se le notifiche fax per i messaggi vocali verranno inviate in stati di presenza specifici, quando un nuovo fax viene salvato nella casella postale dell'utente

    Ripetere questo passaggio per tutti gli utenti. Questo passaggio è facoltativo.

13.12.2 How to connect OpenScape Business system to Microsoft Office 365 using Modern Authentication

You can connect your OpenScape Business system to Microsoft Exchange Online / Office 365 using modern authentication (Microsoft OAuth 2.0 token-based authorization) in order to use the E-mail forwarding, Exchange Calendar Integration, Exchange directory integration and E-mail Queues features.

Detailed instructions on how to setup the connection can be found in the Unify Experts Wiki at `https://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Office_365`.

13.12.3 Come verificare che le funzionalità di integrazione di Microsoft Office 365 siano configurate

E-mail:

Puoi controllare la funzione E-mail con il pulsante **Test inoltro posta elettronica** dall'area **Centro assistenza > Inoltro e-mail** in WBM. Inserire un indirizzo di posta valido come destinatario e controllare la ricezione dell'e-mail di prova nella posta in arrivo dell'account di posta interessato.

Integrazione del calendario di Exchange:

Quando gli utenti impostano appuntamenti nel proprio calendario di Microsoft Outlook, il sistema OpenScape Business controlla automaticamente parole chiave negli oggetti dell'appuntamento del calendario, come: "Riunione", "Malattia", "Pausa", "Fuori sede", "Vacanze", "Pranzo" o "Casa". Se viene trovata tale parola chiave, il sistema imposta automaticamente lo stato di presenza dell'utente al raggiungimento dell'orario dell'appuntamento, anche se la sessione di Microsoft Outlook dell'utente non è più attiva. L'utente configura semplicemente gli appuntamenti con queste parole chiave e OpenScape Business imposterà automaticamente lo stato di presenza del telefono e inoltrerà le chiamate alla casella vocale o, ad esempio, al cellulare, a seconda dello stato di presenza impostato e della destinazione di inoltro

desiderata dall'utente. L'utente può anche configurare in un'impostazione client generale, se lo stato di presenza deve essere riportato su "Ufficio" al termine dell'appuntamento. Funziona anche se l'utente non utilizza il client Outlook locale e imposta l'appuntamento con le parole chiave dell'oggetto summenzionate direttamente nella pagina Web di Outlook in Outlook Web Access (OWA).

L'utente che utilizza l'integrazione di Exchange o del calendario di Outlook locale deve disporre di un indirizzo e-mail valido nella configurazione del client UC Suite e della configurazione delle impostazioni di Outlook del client UC Suite definita nel manuale precedente. È obbligatorio che la combinazione utente di UC Suite-utente di Exchange venga eseguita dall'indirizzo di posta inserito,

L'impostazione della lingua della casella vocale degli utenti di UC Suite viene utilizzata per combinare parole chiave come: "Riunione", "Malattia", "Pausa", "Fuori sede", "Vacanza", "Pranzo" o "Casa" all'impostazione della lingua dell'utente, quindi ad esempio se in Casella vocale è selezionata la lingua tedesca, nella riga dell'oggetto degli appuntamenti verranno controllate parole chiave tedesche come "Besprechung", "Krank", "Pause", "Außer Haus", "Urlaub", "Mittag" o "Zu Hause".

Se l'opzione "Ritorno autom. in ufficio" non viene utilizzata, lo stato di presenza dell'utente verrà mantenuto allo stato impostato dopo la fine dell'orario dell'appuntamento e l'orario di ritorno mostrato ad altri utenti o chiamanti verrà aumentato ogni 15 minuti. Se viene utilizzata l'opzione "Ritorno autom. in ufficio" e l'orario dell'appuntamento termina, la presenza dell'utente viene automaticamente impostata nuovamente su "Ufficio".

Gli appuntamenti fissati nel futuro con meno di 3 minuti vengono ignorati, perché il sistema si aspetta che l'utente stia solo creando un nuovo appuntamento e tutto può cambiare in questi 3 minuti. Il sistema di comunicazione verifica la presenza di appuntamenti nei calendari degli utenti ogni 30 secondi. Per questo motivo e per eventuali ritardi tra il sistema di comunicazione ed Exchange Server, provare ad utilizzare appuntamenti di prova con più di 3,5 minuti. Nei test gli appuntamenti fissati nel futuro con più di 5 minuti funzionano perfettamente per evitare i piccoli ritardi tra il sistema di comunicazione e il server Exchange e il ritardo di 30 secondi di lettura delle richieste di lettura del calendario.

I nuovi valori degli appuntamenti vengono letti completamente entro il minuto in cui l'ora di inizio dell'appuntamento è impostata entro le query di 30 secondi precedentemente indicate. Quindi, nel caso in cui l'ora di inizio sia stata appena raggiunta, tenere presente che la query di 30 secondi deve essere eseguita entro questo minuto, dopo di che viene impostato lo stato di presenza. La query imposta anche l'ora di ritorno degli utenti in base all'ora di fine dell'appuntamento.

Se si desidera testare la funzionalità quando myPortal for Outlook o myPortal for Desktop è chiuso per l'utente, è sufficiente utilizzare la pagina Web di Outlook in Outlook Web Access (OWA). Accedere con le credenziali degli utenti e aggiungere l'appuntamento con la parola chiave al calendario. Controllare nel client di un altro utente di UC Suite che la presenza cambi quando viene raggiunto l'orario dell'appuntamento.

14 Funzioni del telefono

Il sistema di comunicazione offre diversi servizi di telefonia, quali ad esempio messa in attesa, richiamata alternata e consultazione, diversi tipi di segnalazione delle chiamate, inoltro di chiamata e deviazione di chiamata.

14.1 Esegui chiamata

Il sistema di comunicazione offre diverse possibilità di eseguire chiamate dirette, tra cui Chiamata diretta o Selezione breve.

14.1.1 Composizione a cifre

Se si seleziona la composizione a cifre, ciascuna cifra selezionata viene inviata direttamente dopo l'immissione.

La connessione viene attivata immediatamente alla digitazione della prima cifra. L'utente quindi non ha alcuna possibilità di modificare le cifre composte.

14.1.2 Selezione in blocco

In caso di selezione in blocco, la connessione viene stabilita solo dopo aver immesso l'intero numero di telefono. Il numero di telefono viene trasmesso in un unico blocco.

La trasmissione della selezione può essere avviata digitando il codice di fine selezione #.

La chiamata in preselezione è obbligatoriamente utilizzata per:

- Collegamento di linea urbana ITSP
- Collegamento ISDN primario multiplex negli USA

Se entro 5 secondi non vengono più digitate cifre, il sistema interpreta l'ultima cifra digitata come cifra finale del numero.

14.1.3 Selez. blocco tasti

In diversi paesi, i servizi delle linee urbane digitali vengono controllati tramite selezione keypad e non tramite funzioni. Per attivare questi servizi nella PSTN, è possibile utilizzare la cosiddetta interfaccia Stimulus.

La funzione deve essere configurata in Manager E.

Gli utenti confermano il traffico di messaggi tramite il display. Di conseguenza, la composizione di numeri con il tastierino è possibile solo sui telefoni con display (optiPoint, OpenStage), sui telefoni cordless con menu optiPoint e telefoni IP con interfaccia Stimulus. I telefoni ISDN non sono supportati. L'operatore di rete determina quali servizi possono essere utilizzati con il tastierino di selezione.

Un utente autorizzato può attivare la selezione blocco tasti tramite il menu di servizio o il codice *503. Questo è possibile solo nello stato di inattività. Successivamente è necessario selezionare una linea esterna ISDN che tale funzione potrà usare.

A seconda dei messaggi inviati dal centralino (ad esempio in caso di connessione), la composizione mediante il tastierino può determinare la registrazione dei dettagli chiamata. Vengono registrati i numeri degli utenti che utilizzano la composizione mediante tastiera, le linee usate e la durata di utilizzo della funzione.

Nota: Tramite la selezione blocco tasti, le azioni avviate mediante selezione da tastiera non vengono monitorate dal sistema. Il sistema non può impedire l'uso improprio, quale ad esempio addebiti fraudolenti o blocchi delle linee.

Il cliente deve essere consapevole che esso stesso è tenuto a rispondere dei danni eventualmente causati da un uso improprio di questa funzione.

14.1.4 Identificazione della fine della selezione

La parte finale della selezione viene identificata automaticamente dopo 5 secondi o contrassegnata manualmente dall'utente mediante il codice di fine selezione "#".

14.1.5 Modifica d.selez.

Con Modifica d.selez. l'utente può modificare le cifre immesse del numero di telefono. Questa funzione è comune per i telefoni mobili. Il numero di telefono può essere corretto soltanto mentre lo si compone.

Se necessario, il numero inserito può essere corretto cancellando le rispettive cifre da destra a sinistra con l’apposito tasto. Una volta composto il numero corretto, la selezione può essere avviata premendo il tasto di conferma o sollevando il ricevitore.

I numeri di telefono memorizzati, ad esempio per la ripetizione della selezione, non possono essere modificati.

Suggerimento: Modifica d.selez. può essere attivata singolarmente per ciascun utente.

Dipendenze

Argomento	Dipendenza
Avviso di chiamata in attesa	Le chiamate in attesa vengono segnalate poiché il telefono è in stato di registrazione della selezione e risulta quindi occupato per il traffico in entrata.
Consultazione	Dopo la consultazione, il telefono è in stato di registrazione della selezione ed è quindi possibile modificare le cifre del numero.

14.1.5.1 Come attivare o disattivare Modifica d.selez.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Nella struttura dei menu fare clic su **Utente**.
4) Nella struttura dei menu fare clic sull'utente (Indice - Numero di telefono - Nome).
5) Fare clic sulla scheda **Modifica i flag dell'utente**.
6) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Modifica d.selez.**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Modifica d.selez**.
7) Fare clic su **Applica**, quindi su **OK**.

14.1.6 Ripetizione della selezione

Quando viene instaurata una chiamata il numero di telefono selezionato viene memorizzato. Se la destinazione chiamata è occupato o non raggiungibile, l'utente potrà premere il pulsante ripetizione per richiamare lo stesso numero.

I numeri di selezione breve composti vengono trascritti nella memoria di ripetizione della selezione.

La composizione di numeri di telefono interni non influisce sulla memoria di ripetizione della selezione.

Eventuali cifre di post-selezione (denominate anche cifre DTMF) non vengono considerate informazioni di selezioni pertanto non vengono salvate (ad es. cifre che vengono inviate a una casella vocale).

La funzione di ripetizione della selezione può essere utilizzata solo tramite il tasto, non con un codice di accesso.

Premendo il tasto di ripetizione della selezione, sarà quindi possibile scegliere e selezionare uno dei tre numeri contenuti nella memoria. Premendo una volta il tasto, viene selezionato l'ultimo numero composto. Premendolo due volte viene selezionato il penultimo numero composto. Premendolo tre volte viene selezionato il numero presente da più tempo in memoria.

Dopo aver premuto il tasto di ripetizione della selezione, il numero di telefono memorizzato viene selezionato automaticamente entro 2 secondi. Se è necessario più tempo per leggere il numero telefonico visualizzato, utilizzare il tasto di conferma "Scorri". Ogni volta che si preme il tasto "Avanti" vengono visualizzati i numeri di telefono memorizzati in sequenza. Solo selezionando il comando "Chiama" viene composto il numero di telefono. In questo modo è disponibile più tempo per verificare se è stato selezionato il numero di telefono corretto.

All'arrivo di una chiamata tramite LCR vengono salvati solo i numeri composti dall'utente.

I codici di addebito vengono memorizzati anche nella memoria di ripetizione della selezione. La premessa al riguardo è che sia impostato il flag corrispondente su tutto il sistema.

14.1.6.1 Come attivare o disattivare la ripetizione automatica dell'ultimo nr. selez.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema**.
4) Fare clic su **Flag di sistema**.
5) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Ripetizione automatica dell'ultimo nr. selez.**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Ripetizione automatica dell'ultimo nr. selez.**.
6) Fare clic su **Applica**, quindi su **OK**.

14.1.7 Selezione breve del sistema

I numeri di telefono esterni più utilizzati possono essere memorizzati nel sistema di comunicazione. Ogni numero sarà quindi rappresentato da un numero di selezione breve che verrà utilizzato al posto del numero di telefono completo.

I numeri di selezione breve sono costituiti da 4 cifre.

Per impostazione predefinita, ogni utente si trova in un gruppo a cui sono assegnati tutti i numeri di selezione breve. Ogni utente può quindi utilizzarli tutti.

La selezione breve del sistema non è sottoposta alle regole dell'abilitazione alla linea urbana. Si noti che la composizione di una destinazione di selezione breve trovata durante una ricerca nella rubrica interna non annullerà le regole di limitazione delle chiamate a pagamento.

I numeri di selezione breve del sistema vengono configurati in gruppi dall'amministratore. Gli utenti possono essere assegnati ad uno di questi gruppi. L'utente può utilizzare solo i numeri di selezione breve del gruppo a lui assegnato. Ad un gruppo può essere assegnato solo un intervallo di selezioni brevi del sistema.

Le voci di selezione breve supportano le ricerche basate su nome e cognome se il nome è configurato nel formato <Cognome>, <Nome> o <Nome>, <Cognome>.

I numeri di selezione breve composti vengono trascritti nella memoria di ripetizione della selezione.

Per programmare una pausa di selezione e una commutazione DTMF per la post-selezione di caratteri DTMF (ad esempio per il controllo delle caselle vocali) deve essere utilizzato il "tasto P" o il "tasto #".

Il tasto di ripetizione della chiamata per il cliente deve essere impostato come segue: <numero><numero_dtmf><numero_pausa><codice_accesso> Ad esempio: 008007728477#P2210344

Conversione dei numeri in nomi

Ad ogni numero può essere assegnato un nome Se si riceve una chiamata da un numero memorizzato ed è impostato CLIP, il sistema visualizza automaticamente il nome associato a quel numero telefonico anziché il numero stesso.

Post-selezione

La post-selezione non è supportata per la trasmissione di cifre "in preselezione" (ad esempio, una configurazione ITSP). È supportata per la trasmissione di cifre "sincrona".

Nota: Il campo di trasmissione delle cifre può essere modificato in WBM tramite **Modalità esperti > Linee/Rete > Fascio**

Possibilità di post-selezione:

- Post-selezione manuale

  Dopo aver selezionato il codice di accesso e specificato il numero di indice (numero di selezione rapida), l'utente può digitare altre cifre che verranno aggiunte al numero di telefono dell'indice e composte.
- Post-selezione automatica

  Nella configurazione di una selezione breve del sistema è possibile suddividere il numero immesso in due parti. Utilizzare "-" come carattere separatore. La prima parte viene sempre inviata. Quindi viene avviato un timer. Se l'utente non seleziona altre cifre prima dello scadere del timer, la seconda parte del numero immesso viene selezionata automaticamente; in caso contrario vengono inviate le cifre selezionate manualmente.

  Ad esempio: SSD = 7007–0

  Se dopo aver selezionato la destinazione, l'utente non compone un DID (post-selezione manuale) prima dello scadere del timer, viene post-selezionato automaticamente lo 0 (post-selezione automatica).

Importazione dei numeri di selezione breve

È possibile importare i numeri di selezione breve da un file XML nel formato UTF-8. I numeri di selezione breve già esistenti vengono eliminati prima dell'importazione.

Nel WBM, disponibile in **Centro assistenza** > **Documenti** > **Modelli CSV**, è disponibile un modello XML con relativa spiegazione. In questo modello è ad esempio possibile inserire con Microsoft Excel i propri numeri di selezione breve.

Nota: L'importazione di numeri di selezione breve da file CSV non è più raccomandata ed è supportata solo in casi particolari.

Esportazione dei numeri di selezione breve

Un amministratore con il profilo **Expert** può esportare i numeri di selezione breve in un file XML con la codifica UTF-8 utilizzando la **Modalità esperti**. Vengono sempre esportati tutti i record dati.

14.1.7.1 Come aggiungere una destinazione di selezione breve

La procedura guidata **Rubrica/Selezione breve** consente di aggiungere nel sistema centrale destinazioni di selezione breve utilizzabili per la medesima funzione.

Prerequisiti

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Rubrica/Selezione breve**.
4) Nella riga libera della tabella inserire **Il numero di** selezione breve e il relativo **Numero di telefono** e **Nome**.
5) Se si desidera aggiungere altre destinazioni di selezione breve, fare clic su **Salva i dati**, quindi ripetere il passo precedente.
6) Fare clic su **OK & Avanti**.
7) Fare clic su **Fine**.

14.1.7.2 Come importare destinazioni di selezione breve da un file XML

Con la procedura guidata **Elenco telefonico/Selezione breve** è possibile importare i numeri di selezione breve e i numeri di telefono da un file XML. I numeri di selezione breve già esistenti vengono eliminati prima dell'importazione.

Prerequisiti

Si è connessi al WBM.

È disponibile un file XML in formato UTF-8 con i numeri di selezione breve registrati. Un modello XML per l'importazione dei numeri di selezione breve è disponibile in **Centro assistenza** > **Documenti** > **Modelli CSV**.

Nota: L'importazione di numeri di selezione breve da file CSV non è più raccomandata ed è supportata solo in casi particolari.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su > **Procedure guidate**Telefonia centrale.

3) Fare clic su **Modifica**, per avviare la procedura guidata **Rubrica/Selezione breve**. Viene visualizzata la finestra **Modifica voce della rubrica centrale**.
4) Fare clic su **Importa/esporta dati CSV/XML**.
5) Nell'area **Importa file CSV/XML via HTTP**, fare clic su **Sfoglia** per selezionare il file desiderato.
6) Fare clic su **OK**. I numeri di selezione breve disponibili vengono eliminati mentre quelli contenuti nel file XML vengono importati nel sistema.
7) Fare clic su **Fine**.

14.1.7.3 Come esportare le destinazioni di selezione breve in un file XML

È possibile esportare i numeri di selezione breve in un file XML. Vengono sempre esportati tutti i dati.

Prerequisiti

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Rubrica/Selezione breve**. Viene visualizzata la finestra **Modifica voce della rubrica centrale**.
4) Fare clic su **Importa/esporta dati CSV/XML**.
5) Nell'area **Esporta file XML via HTTP** fare clic su **Download**. L'elenco dei numeri di selezione breve viene preparato per il download.
6) Selezionare il percorso di memorizzazione per il file e fare clic su **Salva**.

14.1.7.4 Come modificare le destinazioni di selezione breve

La procedura guidata **Rubrica/Selezione breve** consente di modificare le destinazioni di selezione breve.

Prerequisiti

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Rubrica/Selezione breve**.
4) È possibile cercare una voce inserendo nei campi di ricerca **Selezione breve**, **Numero di telefono** o **Nome** un termine di ricerca e quindi facendo clic sul tasto Return. Vengono visualizzate tutte le voci che contengono il termine di ricerca. Immettendo `521` come numero di telefono verranno

ad esempio trovati i numeri `+495213535` e `+498967521` oppure con `co` inserito come nome, verranno trovate le voci `Collins`, `Mcoin` e `Branco`.

Nota: Se non si inserisce nulla in nessun campo di ricerca e si preme il tasto Return, vengono visualizzate tutte le voci.

5) Nella voce della tabella desiderata, modificare il valore nel campo **Selezione breve**, **Numero di telefono** o **Nome**.
6) Se si desidera modificare altre destinazioni di selezione breve, fare clic su **Salva i dati**, quindi ripetere il passo precedente.
7) Fare clic su **OK & Avanti**.
8) Fare clic su **Fine**.

14.1.8 Selezione breve individuale (KWI)

Selezione breve individuale consente agli utenti di salvare nel sistema centrale 10 selezioni brevi individuali esterne come singoli numeri di selezione breve.

Nei telefoni senza display, dopo aver inserito il numero l'utente deve attendere il tono di conferma.

Nel pool di selezione breve personale è possibile programmare numeri esterni. L'accesso al servizio è legato all'abilitazione alla selezione assegnata all'utente. Prima di immettere il numero di telefono, l'utente deve inserire il codice di accesso linea urbana (ad esempio 0).

Per programmare una pausa nella selezione o una commutazione DTMF si utilizza il tasto di ripetizione della selezione o il tasto cancelletto (#).

14.1.9 Chiamata diretta

I tasti funzione di un telefono o di un modulo aggiuntivo possono essere configurati come tasti per la chiamata diretta. A tale scopo i tasti vengono programmati con il numero di telefono di un utente interno o di un gruppo. Premendo un tasto di quel tipo viene effettuata immediatamente una chiamata alla destinazione programmata (chiamata diretta). Lo stato corrente dell'utente o del gruppo è visibile grazie al LED del tasto di chiamata diretta.

Un tasto di chiamata diretta (anche DSS, Direct Station Selection) può inoltre essere utilizzato per trasferire rapidamente una chiamata all'utente o al gruppo desiderato. Premendo un tasto di chiamata diretta durante una conversazione con un chiamante esterno, la chiamata viene messa in consultazione. L'utente che trasferisce può inoltrare la chiamata alla destinazione semplicemente abbassando il ricevitore (Trasferta rapida). È anche possibile attendere finché il destinatario non risponde quindi trasferire la chiamata (Trasferimento consultazione). Se la destinazione del trasferimento non risponde alla chiamata, viene rilasciata una richiamata.

Stato del LED associato a un tasto di chiamata diretta

Il LED associato a un tasto di chiamata diretta visualizza lo stato corrente dell'utente programmato:

- spento: l'utente corrispondente non sta telefonando.

- acceso: l'utente corrispondente sta telefonando o ha attivato la funzione Non disturbare.
- lampeggio veloce: l'utente corrispondente chiama. È possibile rispondere alla chiamata premendo il tasto di chiamata diretta.
- lampeggio lento: l'utente corrispondente viene chiamato e non sta rispondendo alla chiamata. È possibile rispondere alla chiamata premendo il tasto di chiamata diretta.

Dipendenze

Argomento	Dipendenza
Telefoni ISDN, SIP	Non è possibile programmare tasti di chiamata diretta su telefoni ISDN o SIP.

Concetti correlati

Configurazione team / gruppo Team alla pagina 701
Direttore/Segretaria / Gruppo Top alla pagina 705

14.1.10 Chiamata diretta / Risposta tramite altoparlante

La chiamata diretta permette di collegarsi con un utente interno senza che questi sollevi il ricevitore. L'altoparlante dell'utente chiamato viene quindi attivato automaticamente.

Nei telefoni con dispositivo vivavoce (microfono) è possibile rispondere direttamente all'utente che chiama tramite il microfono. Sollevando il ricevitore si passa alla normale conversazione a due.

La chiamata diretta può essere utilizzata tramite un tasto funzione appositamente programmato, la voce di menu corrispondente, il codice e la successiva selezione del numero dell'utente o del gruppo di destinazione. Un tasto funzione può essere programmato anche per un numero telefonico di un utente. Utilizzando questo tasto funzione viene stabilita immediatamente la connessione alla destinazione programmata.

La funzione di chiamata diretta consente l'uso del paging per tutti gli utenti interni di un gruppo.

La risposta tramite altoparlante può essere attivata mediante la voce di menu disponibile sul display o un tasto funzione appositamente programmato.

È possibile impedire la chiamata diretta di un utente attivando il rifiuto chiamata su altoparlante. In questo caso la chiamata diretta viene segnalata come una normale chiamata.

Dipendenze

Argomento	Dipendenza
Non disturbare, Interrompi non disturbare	Gli utenti con la funzione Non disturbare attivata non possono usufruire di/ricevere chiamate dirette. Se l'utente che desidera utilizzare il servizio di chiamata diretta dispone dell'autorizzazione per interrompere la funzione Non disturbare, riceve per cinque secondi il segnale di occupato. Infine viene chiamato l'utente di destinazione.

Argomento	Dipendenza
Richiamata alternata, Consultazione, Trasferimento	Questi servizi non possono essere utilizzati in una Chiamata diretta/Risposta tramite altoparlante.
Telefoni ISDN, SIP	I servizi "Chiamata diretta" e "Risposta tramite altoparlante" non possono essere utilizzati su telefoni ISDN o SIP.

14.1.10.1 Come attivare/disattivare il rifiuto chiamata su altoparlante per utenti

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Navigare nella struttura dei menu in **Utente** > **Utente** > **…** fino all'utente desiderato (Indice - Numero di telefono - Nome).
4) Fare clic sulla scheda **Modifica i flag dell'utente**.
5) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare l'opzione Rifiuto chiamata su altoparlante per utenti, deselezionare la casella di controllo **Rifiuto chiamata su altoparlante Off**.
   - Se si desidera disattivare l'opzione Rifiuto chiamata su altoparlante per utenti, selezionare la casella di controllo **Rifiuto chiamata su altoparlante Off**.
6) Fare clic su **Applica**, quindi su **OK**.

14.1.11 Composizione associata

Selezione associata consente a un utente autorizzato di comporre un numero al posto di un altro utente. L'effetto è lo stesso che si otterrebbe se il numero di telefono fosse stato composto dall'altro utente.

Per accedere alla funzione occorre specificare un codice e l’utente per il quale deve essere selezionato il numero. Le cifre successive risultano come selezionate dall’utente per il quale è stato composto il numero.

14.1.12 Prenotazione linea

Un utente può prenotare una linea esterna se al momento non è disponibile alcuna linea esterna libera. Non appena si libera una linea esterna, l'utente ne ottiene la disponibilità mediante richiamata.

Se al momento della richiamata l'apparecchio è occupato, viene emesso l'avviso di chiamata in attesa. Se questo avviso non ottiene risposta la prenotazione viene annullata e la linea può essere impegnata dall'utente successivo nell'elenco della coda di attesa. Se prima della richiamata l'utente

ha attivato la funzione Non disturbare da una linea urbana contenuta nella coda di attesa, viene annullata la prenotazione e la linea potrà essere impegnata dall'utente successivo nel relativo elenco.

Se più utenti prenotano una linea, questa viene assegnata in base alla rispettiva sequenza.

Da un telefono può essere eseguita una sola prenotazione/lista di attesa. Qualora l'utente ne attivi una seconda, viene cancellata la prima.

Il servizio "Prenotare la linea" non può essere attivato se l'utente intende effettuare la chiamata tramite LCR.

Il servizio di prenotazione della linea ignora un inoltro chiamata disponibile. Se la chiamata non ottiene risposta entro 20 secondi, la prenotazione viene annullata.

Alla richiamata non è possibile rispondere – né tramite "Risposta per assente, selettiva" né tramite "Gruppo di risposta per assente".

La prenotazione delle linee può essere attivata in uno dei modi seguenti:

- prenotazioni manuali solo per i telefoni con display.
- prenotazione automatica (in tutti gli altri telefoni)

  Se questo flag è selezionato e le linee sono tutte impegnate, l'utente riceve il segnale di occupato. Dopo 5 secondi viene emesso un tono di conferma atto a segnalare che la linea è prenotata - ammesso che l'utente disponga dell'abilitazione richiesta.

Nota: I telefoni S_0 non supportano la prenotazione della linea.

14.1.12.1 Come attivare/disattivare la prenotazione della linea

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema**.
4) Fare clic su **Flag di sistema**.
5) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Prenotazione automatica della linea**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Prenotazione automatica della linea**.
6) Fare clic su **Applica**, quindi su **OK**.

14.1.13 Linea privata

Una linea privata è una linea esterna a disposizione di un utente specifico in modo esclusivo.

14.2 Segnalazione della chiamata, visualizzazione del numero di telefono

Il sistema di comunicazione offre diverse opzioni per la segnalazione delle chiamate e per la visualizzazione del numero di telefono, ad es. CLIP, CLIR, COLP e COLR.

14.2.1 Segnalazione delle chiamate diversificata

La segnalazione delle chiamate diversificata consente di distinguere tra chiamate interne ed esterne all'arrivo di una chiamata.

Tali chiamate vengono segnalate acusticamente e visivamente sul telefono. Sul display viene visualizzato quanto segue:

- Numero del chiamante
- Per le deviazioni di chiamata interne: anche il numero di telefono composto

La chiamata in entrata può essere inoltre segnalata da un LED. Per le chiamate interne ed esterne sono previsti segnali acustici diversi.

Segnalazione di chiamate interne

Ciascun utente può scegliere una fra otto segnalazioni acustiche da assegnare alle chiamate interne. In questo modo l'utente invia agli altri utenti interni un tono di chiamata modificato, che lo rende riconoscibile. Ad esempio, il direttore dell'azienda può scegliere un tono di chiamata speciale ed essere quindi immediatamente identificato dai collaboratori in caso effettui una chiamata interna.

Segnalazione di chiamate esterne

Per una chiamata esterna sono disponibili tre tipi diversi di suoneria. In questo modo è possibile differenziare acusticamente le chiamate per due gruppi, come Vendite e Magazzino.

- In Germania l'amministratore può configurare tre tipi diversi di chiamata per telefoni analogici, ISDN e di sistema.
- In altri paesi i tipi di chiamata da telefoni analogici vengono segnalati allo stesso modo.

14.2.2 Trasmissione del numero di telefono (CLIP = Calling Line Identification Presentation)

La trasmissione del numero di telefono del chiamante mostra il numero del chiamante all'utente chiamato.

La funzione CLIP (Calling Line Identification Presentation) si applica alla chiamate in entrata e deve essere supportata dal gestore di rete.

Se il nome e il numero di telefono del chiamante sono memorizzati nella selezione breve del sistema di comunicazione, a display verrà visualizzato il nome.

Il servizio di trasmissione del numero di telefono del chiamante (CLIP) e la funzione di disattivazione della visualizzazione del numero di telefono del chiamante (CLIR) si escludono vicendevolmente, ovvero se viene attivata la funzione CLIP, la funzione CLIR viene disattivata e viceversa.

CLIP impostabile

La funzione CLIP impostabile trasmette all'esterno, al posto del numero di telefono del chiamante (ad esempio un membro di un gruppo di ricerca), un numero di telefono preimpostato (ad esempio, il numero di telefono del gruppo di ricerca).

Informazioni specifiche del sistema

Paese	Attivato per impostazione predefinita
USA	LIN (Location Identification Number). Se CLIP viene attivato per gli USA; LIN viene automaticamente disattivato.
Resto del mondo	CLIP

14.2.2.1 Come attivare o disattivare la funzione CLIP impostabile

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema**.
4) Fare clic su **Flag di sistema**.
5) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare la funzione CLIP impostabile, selezionare la casella di controllo **CLIP impostabile**.
   - Se si desidera disattivare la funzione CLIP impostabile, deselezionare la casella di controllo **CLIP impostabile**.
6) Fare clic su **Applica**, quindi su **OK**.

14.2.3 Disattivazione della visualizzazione del numero di telefono (CLIR = Calling Line Identification Restriction)

La funzione di disattivazione della visualizzazione del numero del chiamante nasconde la visualizzazione del numero di telefono del chiamante all'utente chiamato.

La disattivazione della visualizzazione del numero di telefono del chiamante (CLIR, Calling Line Identification Restriction) si riferisce alle chiamate in uscita. È necessario che la linea PSTN supporti tale servizio. La disattivazione della visualizzazione del numero di telefono ha priorità sulla trasmissione del numero di telefono.

Il servizio di trasmissione del numero di telefono del chiamante (CLIP) e la funzione di disattivazione della visualizzazione del numero di telefono del chiamante (CLIR) si escludono vicendevolmente, ovvero se viene attivata la funzione CLIP, la funzione CLIR viene disattivata e viceversa.

CLIR e COLR possono essere attivati o disattivati solo congiuntamente.

La disattivazione della visualizzazione del numero di telefono del chiamante non è attiva per alcune destinazioni di chiamata (ad esempio, i numeri di emergenza della polizia e dei vigili del fuoco).

Disattivazione della visualizzazione del numero di telefono per tutto il sistema

Accendendo come amministratore, è possibile attivare o disattivare la visualizzazione del chiamante CLIR a livello di sistema.

Suggerimento: Il flag "Disattivazione della visualizzazione del numero di telefono su tutto il sistema" non è attivo per gli USA.

Disattivazione temporanea della visualizzazione del numero di telefono

Accendendo come utente, è possibile attivare o disattivare temporaneamente il mascheramento del numero chiamante. La disattivazione temporanea della visualizzazione del numero di telefono è possibile solo se tale funzione è disattivata a livello di sistema.

Mascheramento del numero di telefono dell'utente

Per ogni fascio, l'amministratore può configurare il sistema in modo che al posto del numero di telefono dell'utente venga trasmesso solo il numero di sistema.

14.2.3.1 Come attivare o disattivare la visualizzazione del numero di telefono

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Fascio**.
4) Selezionare il **Fascio** corrispondente.
5) In **Numero del sistema in uscita**, selezionare la casella di controllo **Disattiva nr. di tel. utente**.
6) Fare clic su **Applica**, quindi su **OK**.

14.2.4 Presentazione dell'identificazione delle linee collegate (COLP)

La funzione Presentazione dell'identificazione delle linee collegate (COLP) trasmette il numero di telefono dell'utente chiamato al chiamante non appena i due vengono collegati.

La funzione COLP è utile, ad esempio, con l'inoltro di chiamata, in quanto il chiamante può vedere il numero di telefono dell'effettivo interlocutore invece del numero di telefono originariamente composto.

Le funzioni Presentazione dell'identificazione della linea collegata (COLP) e Restrizione dell'identificazione della linea collegata (COLR) sono mutuamente esclusive, ovvero non appena viene attivata la funzione COLP, la funzione COLR viene disattivata e viceversa.

14.2.4.1 Come attivare o disattivare la trasmissione del numero di telefono del chiamante

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Fascio**.
4) Selezionare il **Fascio** corrispondente.
5) Fare clic sulla scheda **Cambia parametri Special**.
6) Selezionare la casella di controllo **COLP**.
7) Fare clic su **Applica**, quindi su **OK**.

14.2.5 Disattivazione della visualizzazione del numero di telefono del chiamato (COLR)

La funzione di disattivazione della visualizzazione del numero del chiamato nasconde al chiamante la visualizzazione del numero di telefono degli utenti chiamati.

La disattivazione della visualizzazione del numero di telefono dell'utente chiamato (COLR, Connected Line Identification Restriction) si riferisce alle chiamate in entrata.

La disattivazione della visualizzazione del numero di telefono del chiamato (COLR) ha priorità rispetto all'identificazione del numero chiamato presso il dispositivo del chiamante.

Il servizio di trasmissione del numero di telefono del chiamato (COLP) e la funzione di disattivazione della visualizzazione del numero di telefono del chiamato (COLR) si escludono vicendevolmente, ovvero se viene attivata la funzione COLP, la funzione COLR viene disattivata e viceversa.

CLIR e COLR possono essere attivati o disattivati solo congiuntamente.

14.2.6 CLIP no screening (trasmissione di informazioni sul numero di telefono specifiche del cliente)

CLIP no screening trasmette uno dei numeri di telefono predefiniti dal chiamante al posto del numero di telefono del chiamante.

Il numero del sistema in uscita non deve essere identico a quello del sistema in entrata.

Per speciali applicazioni del cliente è possibile attivare il flag "Nascondi numero di telefono utente". per impedire che con il "Numero di telefono del sistema in uscita" venga trasmesso il numero di telefono dell'utente.

Esempio: si desidera impedire che un addetto all'assistenza, raggiungibile ad un numero di telefono di servizio generale, possa essere contattato direttamente dai clienti. Per evitare la visualizzazione del proprio numero di selezione passante, come numero di telefono del sistema in uscita deve essere registrato il numero di telefono di servizio generale e inoltre va attivato il flag di disattivazione della visualizzazione del numero di telefono dell'utente" Sul display dell'utente esterno chiamato, viene visualizzato soltanto il numero di telefono di servizio come CLIP.

Di regola, per le chiamate in entrata e in uscita viene utilizzato lo stesso numero di telefono del sistema. In questo caso, la voce contenuta in "Numero di telefono del sistema in uscita" è vuota o uguale a quella contenuta in "Numero di telefono del sistema in entrata". In caso contrario,

- in "Numero di telefono del sistema in uscita" può essere specificato un altro numero;
- tramite il parametro del fascio "Tipo nr. in uscita" è possibile definire se il "Numero di telefono del sistema in uscita" specificato debba contenere il numero di telefono dell'utente senza indicativo della località, con indicativo della località (nazionale) o con l'indicativo internazionale (internazionale)

Suggerimento: CLIP no screening deve essere supportato e attivato dal gestore di rete.

14.2.6.1 Come configurare CLIP no screening

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Fascio**.
4) Selezionare il **Fascio** corrispondente.
5) Come **numero del sistema in uscita**, immettere il **Numero del sistema** desiderato.
6) Fare clic su **Applica**, quindi su **OK**.

14.2.7 CLIP per dispositivi analogici

La funzione CLIP per dispositivi analogici trasmette il numero di telefono di un terminale analogico del chiamante al chiamato e la visualizzazione locale su terminali idonei CLIP (Calling Line Identification Presentation) analogici.

La trasmissione delle informazioni sul nome, chiamata CNIP (Calling Name Identification Presentation), è configurabile.

Suggerimento: La funzione CNIP è disponibile se supportata dal terminale. Verificare le indicazioni del costruttore.

14.2.8 Chiamata senza suoneria / Silenzio

Il servizio Chiamata senza suoneria / Silenzio segnala le chiamate in arrivo sia a display che acusticamente, solo con un breve tono di avviso.

Il servizio Chiamata senza suoneria / Silenzio è disponibile solo con i telefoni dotati di display e non ha alcun effetto sulla segnalazione di appuntamenti.

14.2.9 Conversione del numero in nome nella selezione breve del sistema

Con le chiamate eseguite mediante la funzione di selezione breve del sistema nonché con le chiamate in arrivo da destinazioni configurate in tale funzione, dopo la composizione viene visualizzato il nome anziché il numero di telefono composto.

14.3 Funzioni disponibili durante la chiamata

Durante una connessione, il sistema di comunicazione offre diverse funzioni, quali ad esempio messa in attesa, inoltro o trasferimento di chiamata.

14.3.1 Metti in attesa

Con Metti in attesa, una chiamata passa in stato di attesa. Mentre si trova in attesa, per il chiamante viene riprodotta la musica su attesa.

L'attesa si conclude quando la conversazione viene ripresa.

Esistono diversi tipi di messa in attesa:

- Messa in attesa generale:

  Qualsiasi utente può riprendere la conversazione premendo il tasto relativo a una linea o a una chiamata.
- Messa in attesa esclusiva: (solo con funzione Team o Top e Posto operatore)

  Solo l'utente che ha messo in attesa la conversazione può riprenderla.

In attesa e richiamata

Allo scadere del timer **Tempo per parcheggio + passaggio a messa in attesa** (predefinito: 160 s), una conversazione parcheggiata attiva una richiamata.

14.3.2 Parcheggio

Con la funzione Parcheggio, un utente mette una conversazione in attesa. Mentre si trova in attesa, per il chiamante viene riprodotta la musica su attesa. Una conversazione parcheggiata può essere ripresa da qualsiasi altro telefono.

Nel caso sia necessario parcheggiare una connessione, gli utenti possono assegnare a questa le posizioni di parcheggio (0-9) nel sistema di comunicazione. Se la posizione di parcheggio selezionata è già occupata, viene emesso un tono di conferma negativo, il numero non viene rappresentato ed è possibile selezionare altre posizioni di parcheggio. Per la ripresa di una conversazione parcheggiata, è necessario indicare la posizione di parcheggio.

Per la ripresa di una conversazione parcheggiata può essere utilizzato un codice o un tasto programmato. La ripresa è inoltre consentita anche durante una chiamata in corso.

Parcheggio e richiamata

Allo scadere del timer **Tempo per parcheggio + passaggio a messa in attesa** (predefinito: 160 s), una conversazione parcheggiata attiva una richiamata.

Parcheggio e deviazione di chiamata

In caso di richiamata, la richiamata parcheggiata non segue la deviazione.

Parcheggio e DISA

In modalità DISA, non è possibile attivare la funzione parcheggio.

Parcheggio e conferenza

Una conferenza non può essere parcheggiata.

Parcheggio e collegamento in rete

Una chiamata parcheggiata può essere ripresa solo nell'ambito dello stesso nodo. Le chiamate in entrata dalla rete possono essere parcheggiate soltanto sul nodo di destinazione.

Parcheggio e funzione Non disturbare

Un utente che ha attivato la funzione Non disturbare, può assegnare ad una chiamata una posizione di parcheggio. Se giunge una richiamata originata dalla chiamata parcheggiata e nel Call Management non sono state specificate altre destinazioni, una volta scaduto il tempo impostato, viene automaticamente conclusa la chiamata.

Nota: Per istruzioni dettagliate su come parcheggiare una chiamata e su come recuperare una chiamata parcheggiata consultare il relativo capitolo del manuale d'uso del dispositivo

corrispondente (Guida per l'utente OpenStage X, HiPath/ OpenScape 3000/4000).

14.3.3 Consultazione

Con la funzione Consultazione, durante una chiamata l'utente ha la possibilità di stabilire un'altra connessione dallo stesso telefono o di rispondere a un avviso di chiamata. La prima chiamata viene messa in attesa.

Una consultazione può essere conclusa nei seguenti modi:

- Ripresa della conversazione messa in attesa
- Disconnetti

  Si verifica quindi uno dei seguenti eventi:

  – Trasferimento della conversazione in attesa o
  – Richiamata immediata dell'utente in attesa da parte dell'utente che ha disconnesso la chiamata

Consultazione mediante tasto chiamata diretta

La pressione di un tasto chiamata diretta mentre è in corso una conversazione attiva una consultazione alla corrispondente destinazione.

Collegamento di un secondo interlocutore esterno

Durante una conversazione esterna, con una consultazione si effettua una connessione a una destinazione esterna con successiva trasferta di entrambi gli interlocutori. È possibile che vengano generati addebiti.

14.3.4 Richiamata alternata

Con la funzione Richiamata alternata un utente può condurre due conversazioni passando da una all'altra. Mentre l'utente è in conversazione con un interlocutore, l'altro rimane in attesa.

Mediante la pressione dei tasti di linea corrispondenti, gli utenti possono passare da una conversazione a un'altra.

Richiamata alternata e messa in attesa

Un utente in attesa non può eseguire una richiamata alternata.

14.3.5 Trasferisci

Con il comando trasferisci, un utente può trasferire la propria conversazione in un'altra destinazione. Non appena un utente attiva la trasferta, l'utente resta provvisoriamente in attesa.

Esistono diversi tipi di trasferimento:

- Trasferta rapida:

  È possibile trasferire la chiamata senza che l'utente presso la destinazione risponda. Nel caso in cui l'utente alla destinazione sia occupato, viene

generato un avviso di chiamata. Se un terzo utente prova a trasferire una chiamata a questo utente occupato o se è attivato l'avviso di chiamata su occupato viene eseguita immediatamente una richiamata. Se l'utente presso la destinazione di trasferimento non accetta la chiamata trasferita entro un determinato intervallo di tempo (timer Tempo di segnalazione durante la trasferta prima della risposta), viene eseguita una richiamata. Non è possibile eseguire una trasferta rapida a un agente in un altro Contact Center multimediale.

- Trasferimento consultazione:

  È possibile trasferire la chiamata se l'utente presso la destinazione risponde. Per trasferire la chiamata occorre riagganciare.

Trasferisci con deviazione di chiamata

Viene eseguita una deviazione di chiamata alla destinazione della trasferta. Il display mostra la destinazione finale della trasferta.

Trasferisci con Non disturbare

Se la chiamata viene trasferita a un utente sul cui telefono è attivata la funzione Non disturbare, viene segnalata immediatamente una richiamata a colui che esegue la trasferta, indipendentemente dal fatto che quest'ultimo abbia anch'esso attiva la funzione Non disturbare.

Informazioni specifiche del sistema

Timer "Tempo di chiamata durante la trasferta prima della risposta": 45 secondi per impostazione predefinita

A un utente occupato possono essere trasferite contemporaneamente fino a 5 chiamate.

Nota: Durante una trasferta, l'aggiornamento delle informazioni visualizzate tramite l'interfaccia ITSP/NATIVE-SIP non è supportato.

14.3.6 Richiamata

Con la richiamata, l'utente che ha attivato la funzione riceve automaticamente di nuovo una chiamata messa in attesa o parcheggiata da troppo tempo oppure una chiamata trasferita senza successo.

La richiamata avviene nei seguenti casi:

- Una chiamata messa in attesa o parcheggiata non viene ripresa entro un determinato lasso di tempo (Tempo per parcheggio + passaggio a messa in attesa).
- Con "Trasferta prima della risposta" nei seguenti casi:
  - nessuna risposta prima che sia trascorso un tempo definito (Tempo di chiamata durante la trasferta prima della risposta)
  - La destinazione non esiste
  - La destinazione è occupata in secondo grado
  - il telefono digitale alla destinazione è guasto
  - La trasferta non è consentita

Se l'utente cha ha attivato la funzione è occupato durante la richiamata, questa viene segnalata come un avviso di chiamata. Appena la linea si libera viene segnalata la richiamata. Sul display dell'utente cha ha attivato la funzione può essere visualizzato il numero di telefono del chiamante oppure dell'utente di destinazione. Se l'utente non risponde alla richiamata entro il Tempo di rinvio per la richiamata, viene eseguito il rinvio sul posto di rinvio se è impostato il flag "in caso di richiamata senza risposta". Se il posto di rinvio non risponde alla richiamata entro il Tempo per il rilascio di una richiamata dal PO, la richiamata viene disconnessa automaticamente.

Richiamata e Risposta per assente

Ogni utente appartenente a un gruppo di risposta dell'utente che ha attivato la funzione può ricevere una richiamata se è stato attivato a livello globale il flag AUN dopo richiamata.

Richiamata e Non disturbare

Una Richiamata ignora la funzione Non disturbare.

Informazioni specifiche del sistema

Tempo di rinvio per la richiamata: per impostazione predefinita 30 s

Tempo per il rilascio di una richiamata dal PO: impostazione predefinita 60 s

14.3.7 Ascolto di una chiamata

La funzione Ascolto chiamate consente agli utenti autorizzati di ascoltare la conversazione di un qualsiasi utente interno. Al microfono dell'utente in ascolto viene tolto l'audio automaticamente. Gli utenti della conversazione in ascolto non vengono avvisati in nessun modo, né mediante un tono, né mediante la visualizzazione sul display.

La funzione è disattivata nella configurazione predefinita. Può essere attivata solo se consentito dalla legislazione specifica del paese. A seconda dei casi, deve sempre essere verificata la legislazione specifica in vigore nel paese prima di attivare la funzione.

Gli utenti autorizzati necessitano di un telefono di sistema e dell'abilitazione necessaria per l'inclusione.

L'utente che si desidera porre sotto ascolto deve trovarsi in uno stato di conversazione attivo. All'inizio e alla fine dell'ascolto della chiamata possono verificarsi salti nelle conversazioni, di durata fino a due secondi. Non appena uno degli interlocutori della chiamata sotto ascolto viene messo in attesa, trasferito o termina la conversazione telefonica, la funzione di ascolto si disattiva e può essere ripristinata quando l'utente da ascoltare è di nuovo in conversazione.

Dipendenze

Argomento	Dipendenza
Telefoni cordless	La funzione di ascolto delle chiamate non può essere utilizzata con telefoni wireless, in quanto questi non supportano la funzione di silenziamento automatico del microfono.

Argomento	Dipendenza
Conferenze	La funzione Ascolto chiamate limita il numero di conferenze possibili. Numero massimo di conferenze nel sistema = numero massimo di utenti contemporanei con la funzione Ascolto chiamate attiva.
Ascolto di una chiamata	La chiamata può essere cancellata solo utilizzando il codice *944 + il numero utente (non a partire da un menu).
Ascolto di una chiamata	Per attivare l'uso delle funzioni per un utente, devono essere attivati i flag **Ascolto chiamate** e il flag **Autorizzazione inclusione**. (La funzione non può essere utilizzata con il monitoraggio CSTA.)

14.3.7.1 Come attivare/disattivare l'ascolto chiamate per un utente

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Per l'utente in questione è attivata la funzione Autorizzazione ad includersi.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utenti**.
3) Nella struttura dei menu fare clic su **Utenti**.
4) Navigare nella struttura dei menu in **Utenti** > **Utente** > **…** fino all'utente desiderato (Indice - Numero Utente - Nome).
5) Fare clic sulla scheda **Modifica i flag dell'utente**.
6) Selezionare una delle seguenti opzioni:
   - Per concedere a un utente l'autorizzazione per questa funzione, selezionare la casella **Ascolto chiamate**.
   - Per revocare a un utente l'autorizzazione per questa funzione, deselezionare la casella **Ascolto chiamate**.
7) Fare clic su **Applica**, quindi su **OK**.

14.3.8 Chiamata altoparlante discreta

La funzione Chiamata altoparlante discreta consente a un utente (ad esempio Utente C) di monitorare una connessione semplice tra i due utenti A e B e di passare informazioni all'utente A senza che l'utente B possa sentirle, come avviene solitamente nei Call Center o nei sistemi Direttore/Segretaria.

La funzione deve essere configurata in Manager E.

Nota: Anche se non vi è alcuna connessione tra gli utenti B e C, a causa del feedback sul telefono dell'utente A, l'utente B può sentire parlare l'utente C, anche se in modo attutito.

I terminali di destinazione per la risposta discreta (utente A) possono essere solo telefoni di sistema con display. Gli utenti A e C devono essere nello stesso nodo.

Nello stato Inattività/Pronto, la funzione viene attivata dall'utente C componendo un codice. Sul telefono è presente un tasto parzialmente programmato (sul pulsante è impostato solo il codice, il numero di telefono deve essere selezionato). Nel menu di servizio viene inserito un punto, il menu Idle/ Chiamata rimane invariato.

La possibilità di attivare le funzionalità è legata a un'abilitazione specifica dell'utente. Con una seconda abilitazione l'utente A può proteggersi dalla funzione Suggerimento discreto.

La disattivazione può avvenire per azione dell'utente C che l'ha attivata o come conseguenza di altre funzioni.

Nota: Se nessuno degli utenti coinvolti nella chiamata originaria è un utente TDM, al momento dell'attivazione la rete non è coinvolta, quindi la commutazione non può avvenire senza una breve interruzione della connessione esistente.

Nota: Le funzionalità di trasferimento chiamata e conferenza non sono disponibili nei prodotti di UC Suite se è attiva la Chiamata discreta.

Se la funzione Chiamata altoparlante discreta è attiva e l'utente A o B avvia una funzione che richiede una connessione, la funzione Chiamata altoparlante discreta viene disattivata. Per i dettagli sullo svolgimento di determinati servizi, vedere la seguente tabella:

Servizio	Utente A		Utente B		Utente C	
	Possibile	Azione	Possibile	Azione	Possibile	Azione
Consultazione, Messa in attesa, Parcheggio, Messa in attesa comune	Sì	Concludere la "Chiamata discreta"	Sì	Concludere la "Chiamata discreta"	No	Confermare negativamente
Trasferisci	--	--	--	--	--	--
Conferenza	--	--	--	--	--	--
Avviso di chiamata in attesa	Sì	--	Sì	--	Sì	--
Rispondi ad avv.chiamata	Sì	Concludere la "Chiamata discreta"	Sì	Concludere la "Chiamata discreta"	Sì	Confermare negativamente
Inclusione	No	--	No	--	No	--
Trasmissione DTMF	Sì	--	Sì	--	No	--
Contatore LM	--	--	--	--	--	--
Servizi associati	--	--	--	--	--	--

Servizio	Utente A		Utente B		Utente C	
DISA / DISI	--	--	--	--	--	--

14.3.9 Registrazione delle chiamate (Voice Recording, registrazione vocale)

Questa funzione viene utilizzata per registrare dati da una connessione vocale attiva tra due utenti (un utente deve essere interno, l'altro può essere esterno), ovvero, in altre parole, per registrare le chiamate. Per la registrazione è necessario un dispositivo separato.

La registrazione può essere avviata/interrotta premendo un tasto funzione o immettendo un codice (telefoni analogici). A seconda della configurazione, la registrazione può anche essere interrotta mediante il dispositivo di registrazione.

Il dispositivo di registrazione può essere utilizzato da tutti i telefoni supportati all'interno di una rete CorNet-NQ. Le connessioni a CorNet-N e QSIG (ECMA, ISO) non sono supportate. Il segnale di registrazione può essere disattivato durante la registrazione.

I telefoni TDM e CorNet-IP (HFA) (inclusi i dispositivi senza display), OpenScape Personal Edition (HFA) e optiClient Attendant sono supportati. I telefoni standard H.323, i telefoni SIP e gli utenti EDSS1 non sono supportati.

Nota: La registrazione vocale attivata è indicata da un LED o da un segnale di registrazione durante la chiamata.

È possibile configurare singolarmente per ciascun utente l'autorizzazione all'utilizzo della registrazione vocale.

Dipendenze/imitazioni

Oggetto	Correlazione/limite
Consultazione, richiamata alternata, trasferimento, conferenza	L'avvio di una di queste funzioni durante la registrazione di una chiamata interrompe automaticamente la registrazione vocale.
In attesa (Call Hold)	La registrazione in corso viene interrotta attivando In attesa (Call Hold). La registrazione non può essere attivata quando un utente è in attesa.
Inclusione	La registrazione vocale non è consentita. Quando una chiamata viene registrata non è possibile inserirsi. Allo stesso modo, non è possibile attivare la registrazione dopo essersi inseriti in una chiamata.

Oggetto	Correlazione/limite
Ascolto di una chiamata	La registrazione vocale non è consentita. Quando una chiamata viene registrata non è possibile ascoltarla. Analogamente, non è possibile effettuare la registrazione dopo aver attivato l'ascolto di una chiamata.

Nota: La registrazione vocale può essere utilizzata solo per conversazioni fra due utenti, non per conferenze o conversazioni con un utente in attesa.

Nota: Note aggiuntive:

-) Il dispositivo di registrazione può essere indirizzato a un nodo casuale in una rete CorNet NQ.

-) L'autorizzazione alla registrazione vocale può essere concessa solo a un numero limitato di utenti in un nodo (attualmente solo 50 utenti).

-) Le risorse della conferenza vengono assegnate durante la registrazione.

-) Il codice di servizio predefinito per attivare la registrazione delle chiamate è * 493.

14.4 Controllo della reperibilità

Per controllare l'accessibilità il sistema offre funzioni quali Deviazione di chiamata, Non disturbare e Rifiuto di chiamate.

I diversi tipi di deviazione di chiamata richiedono l'uso di elenchi destinazioni chiamata. Gli elenchi destinazioni chiamata definiscono come vengono trattate le chiamate per gli utenti o i gruppi assegnati. Le singole destinazioni in una lista destinazioni chiamata vengono elaborate una dopo l'altra. Sono disponibili diverse voci per le chiamate interne ed esterne (servizio giorno o notte).

14.4.1 Inoltro di chiamata

L'inoltro di chiamata consente di inoltrare le chiamate se queste non ricevono risposta entro un tempo predefinito.

Questo tipo di inoltro è noto anche come inoltro di chiamata fisso, in quanto è configurabile da parte dell'amministratore.

Per ogni inoltro di chiamata, sono presenti una o più liste destinazioni chiamata a cui possono essere assegnati gli utenti per i seguenti tipi di chiamate:

- Chiamate esterne di giorno (mentre non è attivo il servizio notturno)
- Chiamate esterne di notte (mentre è attivo il servizio notturno)
- Chiamate interne

Per ogni lista destinazioni chiamata, è possibile indicare fino a 4 destinazioni chiamata alle quali la chiamata verrà inoltrata.

Normalmente, il numero di telefono o il nome dell'utente chiamato e del chiamante vengono visualizzati presso la destinazione chiamata. La visualizzazione aggiuntiva del numero di telefono o del nome del chiamante può essere disattivata dall'amministratore.

Inoltro di chiamata su occupato

La funzione di inoltro chiamata consente di inoltrare immediatamente la chiamata alla destinazione di chiamata successiva in caso di interno occupato.

Se anche la destinazione chiamata è occupata, al chiamante viene trasmesso il segnale di occupato. Nel caso di una chiamata interna, la chiamata rimane sulla destinazione chiamata che viene controllata ciclicamente finché non passa nuovamente allo stato di libero. L'amministratore può definire il ciclo.

Se la destinazione di inoltro della chiamata non è disponibile e se non è stato configurato nessun altro inoltro, la chiamata non viene inoltrata.

Dipendenze

Argomento	Dipendenza
Telefoni analogici	Questi telefoni non consentono di riconoscere se le chiamate in entrata sono inoltrate.
Avviso di chiamata in attesa	Qualora un utente abbia attivato l'avviso di chiamata in attesa, riceverà un avviso di chiamata in attesa anche nel caso in cui abbia configurato l'inoltro di chiamata su occupato.
Non disturbare	Una destinazione chiamata, su cui è attivata la protezione dall'avviso di chiamata in attesa, viene ignorata.
Inoltro di chiamata	L'inoltro di chiamata viene eseguito solo se, trascorso il tempo impostato dall'amministratore, la destinazione di deviazione della chiamata non risponde.
Servizio notturno	Se per un utente viene utilizzata l'opzione "di giorno / di notte" nella deviazione di chiamata e se il servizio notturno è attivato, durante tale servizio, le chiamate esterne vengono deviate come previsto nelle relative impostazioni. Le chiamate interne continuano a essere gestite in base all'impostazione "di giorno".
Inoltro di chiamata nella linea urbana	Se la funzione Inoltro di chiamata nella linea urbana è attiva, ha priorità rispetto alle altre istruzioni di inoltro di chiamata.

Argomento	Dipendenza
Gruppo di ricerca/ Chiamata di gruppo	Se la destinazione di un inoltro di chiamata è rappresentata da un gruppo o da un gruppo di ricerca, prima di prendere in considerazione la destinazione di inoltro successiva il sistema chiamerà tutti i membri del gruppo uno dopo l'altro. La chiamata di gruppo e il gruppo di ricerca devono essere considerati come un'inoltro di chiamata dell'inoltro di chiamata. Un gruppo di ricerca risulta occupato quando tutti i membri sono in questo stato o hanno abbandonato il gruppo di ricerca. Un gruppo risulta occupato, quando tutti i membri del gruppo sono in questo stato.

14.4.1.1 Come configurare un inoltro di chiamata

La procedura guidata **Inoltro di chiamata** può essere utilizzata per configurare, per un utente interno l'inoltro all'arrivo delle chiamate.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Inoltro di chiamata**. Viene visualizzata la finestra **Elenchi destinazioni chiamata - Definizione**.
4) In primo luogo, definire una lista destinazioni chiamata facendo clic, nella riga della lista da modificare, sull'icona **Modifica**.
5) Negli elenchi a discesa da **1ª dest.** a **4ª dest.**, selezionare la destinazione desiderata. Sono disponibili le seguenti opzioni:
   - **Nessuna voce**: La destinazione viene saltata
   - **Destinazione esterna**: Fascio e numero di telefono esterno con il codice di accesso linea urbana
   - *** Utente selezionato**: l'utente chiamato
   - **** Definito dall'utente**: destinazione del trasferimento di chiamata a tempo (se configurato).
   - **#9 Ricerca sistema**: Utente disponibile successivo (eccetto interno del direttore)
   - **#201 - #260**: Distribuzione delle chiamate (gruppo UCD)
   - **#801 - #817**: Risponditore
   - **100, 101, ...**: Numero di telefono di un utente interno o di un gruppo (ad esempio casella vocale)

Nota: Per trovare una destinazione di chiamata più velocemente, è anche possibile inserire nei campi **1ª**

- 4ª dest. una o più cifre. Successivamente si passa direttamente alla voce del menu che inizia con la serie di cifre inserita. È anche possibile immettere una sequenza di lettere.

---

6) Dal menu a discesa, **L'inoltro chiamate inizia dopo** selezionare il tempo in secondi trascorso il quale la chiamata verrà inoltrata alla destinazione successiva.

7) Selezionare la casella di controllo **Inoltro di chiamata** se su occupato la chiamata deve essere immediatamente inoltrata alla destinazione della chiamata successiva.

8) Se la chiamata deve essere segnalata a un ulteriore utente interno o a un relè (attuatore) di una suoneria centrale, dall'elenco a discesa **Seconda suoneria^Destinazione**, selezionare il numero di telefono desiderato. In **Seconda suoneria Tipo**, selezionare se la chiamata viene segnalata all'utente immediatamente o solo una volta trascorso l'intero tempo di inoltro della chiamata.

9) Fare clic su **OK & Avanti**. Si ritorna di nuovo nella finestra **Elenchi destinazioni chiamata - Definizione**.

10) Se si desidera definire un'ulteriore lista destinazioni chiamata, ripetere il passo precedente.

11) Fare clic su **OK & Avanti**.

12) Assegnare ora agli utenti le liste destinazioni chiamata.

13) È possibile cercare un utente inserendo nei campi di ricerca **N° tel** o **Nome** un termine di ricerca e quindi facendo clic sul tasto Return. Vengono visualizzate tutte le voci che contengono il termine di ricerca. Immettendo `521` come numero di telefono verranno ad esempio trovati i numeri `+495213535` e `+498967521` oppure con `co` inserito come nome, verranno trovate le voci `Collins`, `Mcoin` e `Branco`.

Nota: Se non si inserisce nulla in nessun campo di ricerca e si preme il tasto Return, vengono visualizzate tutte le voci.

---

14) Nella riga dell'utente desiderato, selezionare dall'elenco a discesa la lista destinazioni chiamata per i seguenti casi:

- **Giorno**: Lista destinazioni chiamata per le chiamate esterne in entrata durante l'orario d'ufficio (servizio giorno)
- **Notte**: Lista destinazioni chiamata per le chiamate esterne in entrata con servizio notte attivato
- **Interno**: lista destinazioni chiamata per chiamate interne in entrata

15) Salvare le voci con **Salva**prima di passare a un utente in un'altra pagina.

16) Per assegnare in modo pratico più utenti a una lista destinazioni chiamata, fare clic su **Copia**.

a) In **Lista destinazioni chiamata** selezionare la lista a cui devono essere assegnati gli utenti.

b) Nella finestra **Scelta** selezionare uno o più utenti e copiarli con **Aggiungi** nella finestra **Membri**.

c) Con le caselle di controllo **Giorno**, **Notte** e **Interno** definire se la lista destinazioni chiamata deve essere applicata per le chiamate esterne

in entrata durante l'orario di lavoro (giorno), durante il servizio notturno attivo o solo per le chiamate interne.

d) Fare clic su **OK & Avanti**.

17) Fare clic di nuovo su **OK & Avanti**.

18) Qui è possibile visualizzare tutti gli utenti di una lista destinazioni chiamata. In **Mostra tutti i membri con l'elenco destinazioni di chiamata** selezionare la lista destinazioni chiamata desiderata.

19) Fare clic su **OK & Avanti**. L'inoltro di chiamata per gli utenti interni è configurato.

20) Fare clic su **Fine**.

14.4.2 Come attivare la deviazione di chiamata (AUL)

La funzione di deviazione di chiamata consente all'utente di trasferire le chiamate in arrivo a una destinazione di propria scelta.

La deviazione di chiamata può anche essere configurata per una linea (o linea MULAP) specifica) in riferimento a singoli tasti di linea (anche i tasti di linea MULAP) - qualora disponibili.

È possibile deviare le seguenti chiamate:

- Tutte le chiamate
- solo esterne
- solo interne

È possibile utilizzare le seguenti destinazioni di deviazione delle chiamate:

- Altro telefono (interno o esterno)
- Posto operatore
- Casella vocale
- Gruppo di ricerca
- Gruppo UCD (distribuzione universale delle chiamate)

Le chiamate in uscita possono essere sempre effettuate.

Destinazione esterna

In caso di destinazione esterna di deviazione delle chiamate, è necessario immettere il codice di linea urbana seguito dal numero di telefono esterno di destinazione della deviazione.

Deviazione di chiamata verso destinazioni esterne

Se nella Lista destinazioni chiamata dell'utente è presente una deviazione di chiamata verso una destinazione esterna, l'inoltro di chiamata termina presso questa destinazione. Eventuali altre destinazioni inserite nella Lista destinazioni chiamata verranno ignorate.

Se si richiede l'inoltro ad altre destinazioni, è necessaria l'attivazione del flag di sistema **Inoltro chiamata dopo DEV alla destinazione esterna**. Questa operazione può essere eseguita solo da un tecnico dell'assistenza.

Per consentire una deviazione di chiamata a una destinazione esterna anche in caso di chiamata su una linea urbana analogica, è necessario che un tecnico dell'assistenza attivi il flag di sistema **DEV su linea analogica permessa**.

Nota: Quando una chiamata viene instradata tramite Smart AA e inoltrata all'utente A con inoltro esterno attivato (*11) all'utente B, all'utente B non verrà presentata la CLI della parte chiamante, ma il DID dell'utente A.

Dipendenze

Argomento	Dipendenza
Non disturbare	Non è possibile programmare la deviazione di chiamata sui telefoni in cui il servizio Non disturbare è attivo.
Appuntamento, promemoria	Se l'utente ha programmato un appuntamento, all'ora impostata il sistema segnala tale appuntamento sul telefono deviato indipendentemente dalle eventuali deviazioni impostate.
Gruppo UCD come destinazione di inoltro	La deviazione di chiamata verso un gruppo ACD/ UCD non viene seguita nei seguenti casi: • Se si chiama un gruppo di ricerca linea libera e un utente con una deviazione di chiamata a un gruppo UCD è nella serie, la deviazione di chiamata non avviene. In questo caso viene chiamato direttamente l'utente successivo del gruppo di ricerca. • Un utente è membro di una chiamata a gruppo con proprietà "Gruppo" e presenta una deviazione di chiamata a un gruppo UCD • Un utente è membro di un gruppo in caso di libero. Se viene chiamato il gruppo, la deviazione di chiamata al gruppo UCD non avviene. Eccezione: il primo utente immesso presenta la deviazione di chiamata a un gruppo UCD. Questa deviazione di chiamata viene eseguita.

14.4.2.1 Come attivare o disattivare la deviazione di chiamata tramite linea urbana analogica

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu selezionare **Sistema** > **Flag di sistema**.

4) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare la deviazione di chiamata tramite linea urbana analogica, selezionare la casella di controllo **DEV su linea analogica permessa**.
   - Se si desidera disattivare la deviazione di chiamata tramite linea urbana analogica, deselezionare la casella di controllo **DEV su linea analogica permessa**.
5) Fare clic su **Applica**, quindi su **OK**.

14.4.2.2 Come attivare o disattivare la deviazione di chiamata dopo una deviazione verso una destinazione esterna

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu selezionare **Sistema** > **Flag di sistema**.
4) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare una deviazione di chiamata dopo una precedente deviazione verso una destinazione esterna, selezionare la casella di controllo **Inoltro chiamata dopo DEV alla destinazione esterna**.
   - Se si desidera disattivare la deviazione di chiamata dopo una precedente deviazione verso una destinazione esterna, deselezionare la casella di controllo **Inoltro chiamata dopo DEV alla destinazione esterna**.
5) Fare clic su **Applica**, quindi su **OK**.

14.4.3 Deviazione di chiamata a tempo

La deviazione di chiamata a tempo devia la chiamate che non hanno ottenuto risposta entro un tempo predefinito. La deviazione di chiamata a tempo è simile all'inoltro di chiamata a tempo, con l'unica differenza che l'utente può impostare autonomamente la deviazione.

L'utente può impostare la deviazione di chiamata a tempo per il proprio telefono; possono essere inseriti anche gruppi e destinazioni esterne.

La destinazione di deviazione non viene salvata in modo permanente, ma viene cancellata dopo la disattivazione del servizio.

Se la linea è occupata si applicano le regole di inoltro di chiamata, vale a dire che il sistema passa alla destinazione successiva.

Informazioni specifiche del sistema

Per ogni utente possono essere impostate tre destinazioni. Inoltre è disponibile lo speciale identificativo "Definito dall'utente" mediante il quale l'amministratore può attivare o bloccare il servizio Deviazione di chiamata a tempo per un determinato utente. Per impostazione predefinita il servizio è abilitato.

Se una chiamata non ottiene risposta entro il tempo preimpostato, il sistema cerca e chiama la destinazione di deviazione salvata dall'utente. In caso l'utente non abbia inserito nessuna destinazione di deviazione, il sistema passa alla destinazione successiva della lista delle destinazioni di chiamata.

L'amministratore deve abilitare la deviazione di chiamata per i singoli utenti tramite le liste destinazioni chiamata.

14.4.4 Inoltro di chiamata nella linea urbana (Stati Uniti esclusi)

Tutti gli utenti a cui è assegnato un MSN (Multiple Subscriber Number in una connessione ISDN punto-multipunto o in una connessione ISDN) come numero di selezione passante possono attivare o disattivare la funzione di inoltro di chiamata nella linea urbana per tale MSN. La premessa al riguardo è che all'utente sia assegnata l'abilitazione per l'inoltro sulla linea esterna.

Se ad un gruppo è assegnato un MSN, ogni utente può attivare o disattivare l'inoltro di detto MSN.

Il servizio viene distinto in tre varianti:

- Deviazione di chiamata incondizionata (CFU = Call Forwarding Unconditional): Il gestore di rete inoltra direttamente tutte le chiamate destinate a questo numero MSN, indipendentemente dal suo stato.
- Deviazione di chiamata su occupato (CFB = Call Forwarding Busy): Le chiamate vengono inoltrate se il numero MSN chiamato è occupato.
- Deviazione di chiamata su mancata risposta (CFNR = Call Forwarding No Reply): Le chiamate vengono inoltrate se non ottengono risposta entro un determinato lasso di tempo (impostabile).

Nota: Per gli scenari di inoltro di chiamata sopra descritti, gli utenti possono acquisire solo una destinazione di inoltro per MSN. Possono essere inoltrati fino a 10 MSN.

In caso di connessione ITSP o ISDN configurata con numero di selezione passante, tale numero è 249.

Dipendenze

Argomento	Dipendenza
Servizio notte	L’inoltro di chiamata nella linea pubblica ha la priorità sul servizio notte.

14.4.5 Assegnazione delle chiamate

L'assegnazione delle chiamate consente l'inoltro di chiamate in arrivo di una linea analogica o S_0 a un utente o a un gruppo, in base al numero composto e all'attivazione o meno della funzione Servizio notturno.

Per le chiamate diurne e notturne sono possibili destinazioni diverse. Una chiamata in arrivo non viene segnalata all'utente: la segnalazione avverrà in base alle liste destinazioni chiamata (per l'utente).

14.4.5.1 Come configurare l'assegnazione delle chiamate

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Linee/Routing** > **Linee**.
4) Navigare nella struttura dei menu in **Linee** > **…** (codice porta box) fino alla linea analogica o S_0 desiderata.
5) Nell'elenco a discesa **Nr. tel Giorno**, selezionare il numero di telefono desiderato.
6) Nell'elenco a discesa **Nr. tel Notte**, selezionare il numero di telefono desiderato.
7) Fare clic su **Applica**, quindi su **OK**.

14.4.6 Segnalazione delle chiamate

La funzione Segnalazione di chiamata consente a un utente interno di gestire un elenco personale di numeri interni che possono essere chiamati in caso di chiamata al suo numero di telefono.

Un utente può inserire anche il proprio numero di telefono, ad esempio se il numero viene permanentemente deviato su un altro utente (Direttore-Segretaria).

Per l'attivazione/disattivazione di questa funzione, è possibile programmare un tasto nei telefoni IP di sistema, nei telefoni TDM OpenStage o nei telefoni optiPoint 500. Per consentire variazioni, è possibile programmare più tasti segnalazione chiamate su un telefono. È possibile attivare più tasti contemporaneamente, tuttavia il numero massimo di telefoni con segnalazione di chiamata non può essere superiore a cinque.

Il sistema consente agli utenti di attivare o disattivare questo servizio per il proprio telefono tramite una connessione DISA o per un altro utente, tramite la funzione "Servizi associati".

La finestra Inoltro... è una delle tre visualizzazioni nel menu di sistema di Manager E che forniscono informazioni di stato specifiche del terminale (e non del sistema). Nella finestra Inoltro, è possibile determinare se in un telefono è attiva la segnalazione di chiamata o se il telefono fa parte di un gruppo di chiamata.

Se questa funzione viene utilizzata spesso, l'utente può assegnarle un tasto libero sul proprio telefono. Il nome del tasto è Segnalazione delle chiamate on nella programmazione dei tasti. Se la funzione è attiva, il LED si accende.

Con il flag utente "No segnalaz. chiamata su occupato" è possibile controllare quale utente del gruppo riceve una chiamata quando il "master" è occupato (= utente che attiva il servizio) e quale no. Se a più "master" è assegnato lo stesso utente, il flag si applica a tutte le segnalazioni chiamata di questo utente.

Se il flag non è attivato, viene comunque eseguita la segnalazione delle chiamate a condizione che l'utente incluso nella segnalazione delle chiamate sia raggiungibile (comportamento predefinito).

Se il flag è attivato, la segnalazione delle chiamate dipende dalla raggiungibilità del master:

- Il "Master" è libero, la segnalazione della chiamata ha luogo immediatamente.

  Il master può ricevere la segnalazione di chiamata in attesa - la segnalazione della chiamata avviene dopo 5 sec.

  Con il master non si può ricevere chiamate e l'attesa chiamata non è attiva: non avviene alcuna segnalazione delle chiamate.

Argomento	Correlazione/limite
Richiamata Ricerca sistema Richiamata	Nel caso il numero venga immediatamente richiamato (ad esempio, per un errore dell'operatore) o in caso di ricerca sistema o di richiamata, la segnalazione delle chiamate non viene eseguita.
Deviazione di chiamata	Se l'utente che ha attivato la segnalazione della chiamata, ha attivato anche l'inoltro chiamata (AUL), non verrà segnalata alcuna chiamata.
Non disturbare (DND)	Se l'utente di un gruppo segnalazione chiamata ha attivato la funzione Non disturbare, non verrà chiamato.
Appuntamento	Un appuntamento attivo non segue la segnalazione di chiamata.
No segnalaz. chiamata su occupato	Se il flag è attivato, la segnalazione di chiamata non viene eseguita quando l'utente è occupato.

14.4.7 Rifiuto di chiamate

L'utente ha la facoltà di respingere le chiamate iniziali in entrata interne o esterne. Per respingere le chiamate, premere il tasto di fine chiamata.

La chiamata respinta segue quindi l'inoltro di chiamata. Se non è disponibile nessuna destinazione di inoltro di chiamata, la chiamata esterna viene rinviata al posto operatore a condizione che siano stati configurati i relativi criteri di rinvio. Nel caso in cui non sia possibile chiamare nessuna destinazione, al chiamante viene trasmesso il segnale di occupato.

Richiamate, chiamate trasferite, prenotazioni, chiamate in attesa o parcheggiate non possono essere respinte. Quando una chiamata viene rinviata al posto di rinvio, non può essere respinta.

Dipendenze

Argomento	Dipendenza
Chiamata di gruppo, gruppo di ricerca, MULAP	In questi casi l'intera chiamata di gruppo viene terminata e la chiamata segue l'inoltro di chiamata configurato. Se non è programmata un’ulteriore destinazione, la chiamata viene rilasciata.

14.4.8 Rinvio di una chiamata

Un utente ha la possibilità di differire una chiamata in entrata. L'utente chiamato può creare la connessione senza accettare la chiamata in entrata.

La prima viene poi segnalata come "Avviso di chiamata in attesa".

Quando una chiamata in entrata viene segnalata, l'utente preme un tasto di linea o di conversazione ed esegue una chiamata esterna. A questo scopo devono essere programmati due tasti di chiamata e uno di linea. Uno dei tasti deve essere libero per l'esecuzione del servizio.

Se è impostata la segnalazione dell'avviso di chiamata in attesa, il chiamante non nota cambiamenti della segnalazione.

14.4.9 Non disturbare

L'opzione Non disturbare evita l'inoltro di chiamate in arrivo.

Se la funzione è attivata, quando viene sollevato il ricevitore si potrà sentire un tono di selezione speciale. Nei telefoni dotati di display il "Non disturbare" viene visualizzato fino a che la funzione è attiva. In tutti gli altri telefoni, quando il servizio Non disturbare è attivo, il LED del tasto di chiamata diretta lampeggia con una breve interruzione.

La funzione Non disturbare può essere scavalcata dal posto operatore o da un utente autorizzato. La chiamata può quindi essere inoltrata immediatamente anche ad un utente che ha attivato la funzione Non disturbare.

A coloro che chiamano un utente che ha attivato la funzione Non disturbare, viene trasmesso il segnale di occupato.

Dipendenze

Argomento	Dipendenza
Posto operatore/ destinazione notte	Il posto operatore e il posto di rinvio non possono attivare la funzione Non disturbare.
Deviazione di chiamata	Se sul terminale è attivata la deviazione di chiamata, la funzione Non disturbare non può essere utilizzata. Se sul terminale è attivata la funzione Non disturbare, non può essere attivata la deviazione di chiamata.

Argomento	Dipendenza
Richiamata	Se viene effettuata una richiamata automatica su un utente con il servizio Non disturbare attivo, la stessa non viene eseguita finché Non Disturbare non viene disattivato. Se un utente con il servizio Non disturbare attivo effettua una prenotazione, la conseguente richiamata automatica scavalca la funzione Non disturbare.
Appuntamento, promemoria	Se un utente ha programmato un appuntamento e attivato la funzione Non disturbare, all'ora impostata viene emessa una segnalazione acustica dal terminale.
DISA	La funzione DISA può essere attivata dall'utente per i propri telefoni o da un utente per un altro telefono (servizi associati).

14.5 Ottimizzazione dell'accelerazione delle comunicazioni

Il sistema di comunicazione offre diverse possibilità di esecuzione delle chiamate in modo comodo e pratico, ad esempio mediante le funzioni richiamata automatica o avviso di chiamata in attesa.

14.5.1 Richiamata

La richiamata automatica può essere attivata quando l'utente chiamato non risponde o è occupato. La richiamata automatica fa sì che la chiamata venga avviata non appena l'utente chiamato risulta nuovamente raggiungibile.

Richiamata automatica su "libero" o "occupato"

Se la chiamata non può essere eseguita perché l'utente chiamato è occupato o non risponde alla chiamata, il chiamante può attivare la richiamata automatica per eseguire la chiamata in un momento successivo. Se l'utente chiamato è occupato, la funzione di richiamata automatica monitora la chiamata per rilevarne la conclusione. Non appena l'utente è di nuovo libero, il sistema di comunicazione chiama l'utente chiamante segnalando la possibilità di eseguire la chiamata. Se l'utente accetta la chiamata il sistema compone nuovamente il numero dell'utente precedentemente occupato. In caso di mancata riuscita di una chiamata mediante la funzione di richiamata automatica, tale funzione rimane attiva. La richiamata automatica viene ripetuta dopo che l'utente desiderato ha eseguito una nuova chiamata.

Un telefono può attivare ed essere destinazione di due prenotazioni. Le ulteriori richieste in uscita vengono respinte.

Le prenotazioni vengono cancellate quando:

- la chiamata viene effettuata, altrimenti la richiamata automatica rimane attiva (nel caso di una prenotazione interna),
- la richiamata automatica viene attivata ma non ha luogo una conversazione (nel caso di una prenotazione esterna),
- viene cancellata dall'utente stesso,

- il sistema cancella tutte le prenotazioni ogni giorno alle 23:57.

Le richieste di prenotazione possono essere attivate per utenti e gruppi interni. Le richieste di prenotazione di gruppo sono memorizzate a livello del primo utente. Durante una richiamata automatica di gruppo squillano tutti i telefoni liberi.

Richiamata automatica su libero sull'interfaccia di linea urbana

Se un utente interno non raggiunge un utente esterno libero, ha la possibilità di attivare una prenotazione sulla linea urbana a seguito della quale viene avviato un monitoraggio nella linea dell'utente chiamato. Non appena l'utente chiamato effettua e conclude una chiamata, la linea urbana tenta di stabilire un connessione fra gli utenti. Questo servizio deve essere supportato dalla linea urbana.

Richiamata automatica su dispositivo occupato

La funzione consente di attivare una richiamata automatica, qualora il numero esterno chiamato sia occupato. Una volta che quest'ultimo è di nuovo libero, viene rieseguita automaticamente la chiamata. Questo servizio deve essere supportato e abilitato dalla linea urbana e dal terminale remoto.

14.5.2 Avviso di chiamata in attesa

L'avviso di chiamata in attesa segnala a un utente in conversazione l'arrivo di un'altra chiamata.

La segnalazione è visiva e viene effettuata mediante la visualizzazione di un messaggio sul display. La segnalazione può essere anche acustica, mediante la trasmissione di un breve tono di avviso di chiamata in attesa. Il tono di avviso di chiamata viene trasmesso ogni 5 secondi.

L'utente chiamato ha la possibilità di accettare o di ignorare la seconda chiamata. Per accettare la seconda chiamata, l'utente può concludere la prima e rispondere alla seconda, oppure utilizzare la funzione visualizzata sul display **Rispondere all'avviso di chiamata in attesa**. In questo caso la prima conversazione viene messa in attesa.

Se un utente ha già ricevuto un avviso di chiamata in attesa (possono mettersi in attesa un max. di 4 utenti) o ha attivato l'opzione Rifiuto dell'avviso di chiamata in attesa, non può ricevere nessun avviso di chiamata in attesa. Se non è stato configurato alcun inoltro di chiamata su occupato, al chiamante viene trasmesso il segnale di occupato.

Attivazione dell'avviso di chiamata in attesa

Avviso di chiamata in attesa tramite la console posto operatore

L'utente deve avere attivato il flag **Rifiuto dell'avviso di chiamata in attesa** per poter attivare o disattivare l'avviso di chiamata in attesa mediante il menu o il codice. Qualora l'utente abbia attivato l'avviso di chiamata in attesa, riceverà un avviso di chiamata in attesa anche nel caso in cui abbia configurato l'inoltro di chiamata su occupato.

L'impostazione predefinita è sempre Avviso di chiamata in attesa - A tempo. La console posto operatore può tuttavia anche inviare immediatamente l'avviso di chiamata in attesa.

Dipendenze

Argomento	Dipendenza
Avviso di chiam. in attesa senza segnalazione acustica	Mediante un codice, l'utente può attivare/disattivare il tono di avviso di chiamata in attesa. La chiamata in attesa viene comunque segnalata visivamente sul display del telefono. Per impostazione predefinita, il tono di avviso di chiamata in attesa è attivato.
Inclusione	Quando l'opzione Rifiuto dell'avviso di chiamata in attesa è attivata si evita l'inclusione di un'altra chiamata su una chiamata di questo utente.
Chiamata di gruppo	In un gruppo di utenti, l'avviso di chiamata in attesa viene segnalato soltanto a coloro che sono liberi. Se tutti gli utenti del gruppo sono occupati, l'avviso di chiamata in attesa viene segnalato a tutti tranne a coloro che hanno attivato l'opzione Rifiuto dell'avviso di chiamata.
Chiamata diretta	Gli utenti occupati non possono essere chiamati tramite altoparlante.

14.5.2.1 Come attivare o disattivare l'avviso di chiamata in attesa

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Nella struttura dei menu fare clic su **Utente**.
4) Fare clic ad es. su **Client IP**.
5) Fare clic ad esempio su **Client sistema**.
6) Selezionare l'utente corrispondente.
7) Fare clic sulla scheda **Modifica i flag dell'utente**.
8) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione Avviso di chiamata in attesa, deselezionare la casella di controllo Rifiuto dell'avviso di chiamata in attesa.
   - Per disattivare la funzione Avviso di chiamata, selezionare la casella di controllo **Rifiuto dell'avviso di chiamata in attesa**.
9) Fare clic su **Applica**, quindi su **OK**.

14.5.2.2 Come attivare o disattivare l'avviso di chiamata in attesa immediato tramite la console posto operatore

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema**.
4) Fare clic su **Rinvio/PO/Hotline**.
5) In **Altri criteri**, selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Attesa immediata per chiamate posto operatore**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Attesa immediata per chiamate posto operatore**.
6) Fare clic su **Applica**, quindi su **OK**.

Nota:

Per i deskphone CMI DECT - TDM, quando viene chiamata una postazione occupata ed è consentito l'avviso di chiamata in attesa, il tono di occupato è attivo per 5 secondi, quindi si verifica l'avviso di chiamata ed è possibile sentire il tono di richiamata.

Per i deskphone IP DECT - SIP, quando viene chiamata una postazione occupata ed è consentito l'avviso di chiamata in attesa, l'avviso di chiamata è immediato, quindi il tono di richiamata si sente dall'inizio.

14.5.3 Inclusione (intrusione)

Con l'inclusione, un utente abilitato può inserirsi in una conversazione di un utente interno.

Agli utenti in conversazione, l'inclusione, eseguibile mediante l'inserimento di un codice o la pressione di un tasto, viene segnalata con tono di avviso e la visualizzazione a display.

Questa prestazione può essere attivata durante la segnalazione di occupato o dell'avviso di chiamata in attesa.

L'inclusione in una conversazione telefonica dà luogo a quanto segue:

- Se l'utente chiamato riaggancia, riceve una chiamata dall'utente chiamante (che effettua la trasferta).
- se l'utente che esegue l'inclusione (che desidera effettuare la trasferta) riaggancia, la conversazione in trasferta viene connessa con l'utente di destinazione.
- Se riaggancia l'utente che è stato connesso con la persona chiamata, restano collegati l'utente che è stato incluso e colui che è stato chiamato.

L'inclusione è possibile con ogni utente interno e posto di rinvio (posto operatore). Per utilizzare questa funzione, l'utente interno e il posto di rinvio devono essere abilitati.

L'inclusione su un determinato telefono non può essere impedita.

Dipendenze

Argomento	Dipendenza
Protezione da segnalazione su canale fonia	Se l'utente chiamato o il suo interlocutore interno è registrato come terminale dati (protezione da segnalazione su canale fonia) o l'utente chiamato sta selezionando un numero, l'inclusione non è possibile.
Non disturbare	Se l'utente chiamato ha attivato l'opzione Non disturbare, durante la conversazione in corso può essere inclusa solo una chiamata.
Gruppo/Gruppo di ricerca	Se viene chiamato un gruppo o un gruppo di ricerca e tutti gli utenti sono occupati, l'inclusione non è possibile.
Apparecchio S_0	Non è possibile includersi in un apparecchio S_0.

14.5.3.1 Come autorizzare un utente interno all'inclusione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Nella struttura dei menu fare clic su **Utente**.
4) Nella struttura dei menu fare clic sull'utente (Indice - Numero di telefono - Nome).
5) Fare clic sulla scheda **Modifica i flag dell'utente**.
6) Selezionare la casella di controllo **Autorizzazione a includersi on**.
7) Fare clic su **Applica**, quindi su **OK**.

14.5.3.2 Come abilitare il posto di rinvio per l'inclusione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu, fare clic su **Sistema** > **Rinvio/PO/Hotline**.
4) Nel campo **Altri criteri** selezionare la casella di controllo **Sovrascrivi per posto operatore**.
5) Fare clic su **Applica**, quindi su **OK**.

14.5.4 Testi di assenza

Il testo di assenza di un utente viene visualizzato sul display del chiamante.

Nei testi di assenza (chiamati anche testi di risposta) possono essere specificati parametri variabili. Questi parametri (ad es. l'ora) vengono immessi durante l'attivazione. I caratteri possono essere inseriti con la tastiera telefonica del terminale. Il testo di assenza può essere attivato/disattivato mediante un codice o un tasto funzione preconfigurato del telefono.

Deviazione di chiamata

In caso di deviazione di chiamata, viene visualizzato il testo di assenza dell'utente chiamato e la chiamata viene deviata.

14.5.4.1 Come modificare il testo di assenza

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema**.
4) Fare clic su attivare **Testi**.
5) Nella colonna **Messaggi di risposta** fare clic sul campo corrispondente e digitare il Messaggio di assenza.
6) Fare clic su **Applica**, quindi su **OK**.

14.5.5 Messaggi

I messaggi sono testi di sistema che un utente può selezionare e inviare a utenti interni.

Un messaggio (testo informativo) può essere inviato a uno o più destinatari.

Qualora il messaggio debba essere inviato a tutti i membri di un gruppo interno o di un gruppo di ricerca interno, nel campo Destinatario dovrà essere specificato il numero di telefono del gruppo o del gruppo di ricerca e non quello di un singolo utente.

Nota: Solo 100 telefoni possono ricevere l'indicazione massiva di nuovi messaggi in attesa (MWI); eventuali messaggi aggiuntivi non vengono emessi.

L'invio avviene mediante il tasto o il menu Invio messaggi.

I messaggi possono essere inviati quando il telefono è in stato di quiete, di chiamata, di occupato o durante una conversazione. In stato di chiamata, non è necessario specificare il numero di telefono del destinatario.

14.5.5.1 Come modificare il testo di un messaggio

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema**.
4) Fare clic su attivare **Testi**.
5) Nella colonna **Messaggi** fare clic sul campo corrispondente e digitare il testo.
6) Fare clic su **Applica**, quindi su **OK**.

14.5.6 Servizi associati

Un utente autorizzato può controllare servizi al posto di un altro utente a scelta (ad es. attivare/disattivare Inoltro chiamata, Chiave elettronica o Gruppo di ricerca). L'effetto è lo stesso che si ottiene attivando o disattivando i servizi per se stessi.

È possibile controllare i seguenti servizi:

- Deviazione di chiamata on / off
- Chiave elettronica on / off
- Segnalazione delle chiamate on / off
- Messaggio di risposta on / off
- Gruppo di ricerca e chiamata di gruppo on / off
- Servizio notte on / off
- Attivare / disattivare appuntamenti
- Invio Info / Cancella Info inviate
- Modifica password Chiave elettronica
- Accesso / disconnessione agenti UCD
- Agente UCD disponibile / non disponibile
- Post-elaborazione agente UCD on / off
- Servizio notte agente UCD on / off
- Trasferimento MULAP on / off
- Reimpostazione dei servizi attivati

L'utilizzo avviene tramite una procedura. L'utente deve immettere quanto segue:

- il codice del servizio associato
- il numero di telefono dell'utente, per il quale eseguire l'azione
- il codice del servizio da controllare

Prima che un utente possa utilizzare servizi associati, deve disattivare il codice dell'altro utente, se attivato.

14.5.6.1 Come attivare/disattivare i vari servizi

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Nella struttura dei menu fare clic su **Utente**.
4) Nella struttura dei menu fare clic sull'utente (Indice - Numero di telefono - Nome).
5) Fare clic sulla scheda **Modifica i flag dell'utente**.
6) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Selezione associata/servizi**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Selezione associata/servizi**.
7) Fare clic su **Applica**, quindi su **OK**.

14.5.7 DISA

DISA (Direct Inward System Access) consente agli utenti autorizzati di utilizzare servizi del sistema di comunicazione dall'esterno (ad es. da un telefono cellulare tramite myPortal for Mobile (con Mobile Callback) e Mobility.

Inoltre un utente tramite DISA può instaurare chiamate interne ed esterne. Ad ogni utilizzo di DISA l'utente deve immettere la password per la Chiave elettronica. Quindi ha a disposizione specifici servizi, come se si trattasse di un utente interno.

DISA supporta i servizi seguenti:

Servizio	tramite l'utente stesso	tramite servizi associati
Deviazione di chiamata on / off	x	x
Non disturbare on / off	x	x
Gruppo di ricerca on / off	x	x
Testo di assenza on / off	x	x
Segnalazione delle chiamate on / off	x	x
Chiave elettronica on / off	x	x
Reimposta i servizi	x	x
Selezione breve del sistema	x	–
Invio Info	x	–

Servizio	tramite l'utente stesso	tramite servizi associati
Servizio notte on / off	x	–

L'amministratore specifica a quale numero di telefono devono utilizzare gli utenti per DISA. Il numero di telefono può essere diverso per l'utilizzo interno ed esterno. Interno significa verso un altro nodo in rete IP.

La password immessa dall'utente comprende il numero di telefono interno e il PIN per la Chiave elettronica. Una volta immessa la password, l'utente deve premere il tasto # oppure attendere che il sistema di comunicazione riconosca la sua immissione in base al modo di sicurezza definito dall'amministratore per DISA.

Per una nuova attività DISA l'utente deve riaccedere.

Nota: In OpenScape Business X quando viene chiamato un numero DISA, si sentirà un tono continuo. In OpenScape Business S, quando viene chiamato un numero DISA, si sentirà Musica su attesa.

14.5.7.1 Come attivare/disattivare l'abilitazione DISA per un utente

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Nella struttura dei menu fare clic su **Utente**.
4) Nella struttura dei menu fare clic sull'utente (Indice - Numero di telefono - Nome).
5) Fare clic sulla scheda **Modifica i flag dell'utente**.
6) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Autorizzazione DISA**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Autorizzazione DISA**.
7) Fare clic su **Applica**, quindi su **OK**.

14.5.7.2 Come configurare il numero DISA

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Sistema** > **DISA**.
4) Nel campo **Interno** immettere il numero di telefono tramite il quale l'utente può utilizzare DISA dall'esterno.
5) Nel campo **Numero di telefono** immettere il numero di telefono che l'utente può utilizzare internamente per DISA.
6) Fare clic su **Applica**, quindi su **OK**.

14.5.7.3 Come configurare la modalità di sicurezza DISA

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Sistema** > **DISA**.
4) Nell'elenco a discesa **Sicurezza-Modo** selezionare fra **A tempo** o **Dopo l'immissione #**.
5) Fare clic su **Applica**, quindi su **OK**.

14.5.8 Flex Call/PIN mobile

Flex Call (PIN mobile) consente l'uso temporaneo di un telefono di sistema da parte di altri utenti per la successiva chiamata in uscita, come se questo telefono fosse il proprio.

Flex Call contiene il numero di telefono, il nome, l'abilitazione alla linea urbana e la documentazione addebiti dell'utente.

Finché Flex Call è attivo, il telefono utilizzato non è raggiungibile al proprio numero di telefono. Al termine della comunicazione, questo stato verrà interrotto.

Per l'attivazione di Flex Call, è necessario assegnare all'utente mobile una chiave elettronica individuale.

Per l'attivazione di questa funzione, eseguire una delle seguenti azioni sul telefono di sistema:

- OpenStage: Menu di servizio > PIN e Autorizzazione > Flex Call + Numero telefono Mobile + Chiave elettronica dell'utente mobile
- Codice per FlexCall + Numero telefono mobile + Chiave elettronica dell'utente mobile

14.5.9 Trasferimento

La funzione Trasferimento/scambio numeri consente a un utente OpenStage TDM di cambiare l'assegnazione tra la porta fisica del telefono e i dati utente (profilo utente) logici mediante un'apposita procedura.

La funzione trasferimento può essere utile quando due utenti che utilizzano lo stesso tipo di telefono decidono di scambiare le proprie postazioni di lavoro. Il trasferimento consente quindi la realizzazione della funzione Desk sharing per gli utenti TDM. Gli utenti TDM possono eseguire lo scambio dei numeri di telefono senza l'assistenza di un amministratore.

Possono essere scambiati solo profili utente dello stesso tipo di telefono, ovvero con identico layout dei tasti. Se si scambiano i profili utente di tipi di telefono diversi, i tasti funzione singolarmente programmati del dispositivo base vengono sostituiti dai valori predefiniti. Quando si esegue la funzione, i telefoni TDM vengono messi fuori servizio/riavviati. Le funzioni attive vengono trattate di conseguenza, ovvero le richiamate correnti e le informazioni inviate vengono cancellate mentre tutte le altre funzioni vengono mantenute.

Requisito essenziale per l'uso della funzione trasferimento è l'abilitazione della funzione a livello di sistema. Per lo scambio di numeri selezionare Scambio numero nel menu di servizio del telefono con il numero da scambiare, quini inserire il numero di telefono interno dell'utente di destinazione con il codice PIN (il codice PIN non è necessario se il PIN corrisponde al numero predefinito 00000). Dopo aver inserito il numero di destinazione, il trasferimento viene bloccato per tutti gli altri utenti fino al termine della procedura. Con l’esecuzione dello scambio, viene effettuato il reset di entrambi gli apparecchi interessati. L'esito positivo dello scambio viene segnalato su entrambi i telefoni TDM visualizzando il nuovo numero di telefono (indicazione a display: Nuovo n° tel.: XXXXX).

Il trasferimento non può avere luogo in caso di telefoni di sistema con abilitazioni di programmazione (per Assistant T). Quindi normalmente non ai primi due telefoni di sistema attivi.

14.5.9.1 Come eseguire il trasferimento/scambio numero a livello di sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Impostazioni di base** > **Sistema**.
3) Nella struttura dei menu fare clic su **Flag di sistema**.
4) Selezionare la casella di controllo **Cambio di terminali permesso**.
5) Fare clic su **Applica**, quindi su **OK**.

14.5.10 Reimpostazione dei servizi attivati

Tramite codice è possibile reimpostare collettivamente servizi specifici sui terminali.

Questo è consentito per le seguenti funzioni:

- Deviazione di chiamata
- Cancellare Info ricevute
- Messaggio di risposta on / off
- Segnalazione delle chiamate on / off
- Gruppo di ricerca on / off
- Disattivazione della visualizzazione del numero di telefono on / off
- Avviso di chiamata in attesa senza tono on / off
- Non disturbare on / off
- Silenzio on / off
- Appuntamento
- Cancella tutte le prenotazioni

14.5.11 Procedure

Il sistema di comunicazione permette all'utente di memorizzare codici, numeri di telefono e ulteriori informazioni di composizione come procedure su un singolo tasto. Se l'utente preme il tasto nella post-selezione o durante una conversazione, il sistema di comunicazione invia il carattere DTMF corrispondente.

Esempi di applicazioni:

- Codice per richiamata automatica
- Codice per avviso di chiamata in attesa
- Codice per inclusione
- Sequenza di cifre per Casella vocale o Segreteria telefonica.
- codice flash sulla linea urbana + numero di destinazione
- Codice per il controllo di un servizio + numero di telefono di destinazione, ad es. codice per invio/richiesta Info (Message Waiting) + numero di telefono + numero testo
- Codice di addebito + codice fascio + numero di telefono di destinazione

Le procedure che richiedono l'immissione di un PIN non possono essere salvate.

Solo il primo livello di tasti supporta i tasti procedura.

Durante le procedure, un utente può utilizzare i seguenti servizi, in base alle situazioni:

Servizio	pronto alla composizion	su occupat	al telefono	Chiamata in uscita	chiamata entrante
Risposta per assente, selettiva	x	–	x	–	–
Deviazione di chiamata On, (non nei sistemi ad uso comune e non per singoli MSN di un attacco di linea S_0)	x	–	x	x	–
Deviazione di chiamata nella linea pubblica on / off; Commutazione; (non nei sistemi ad uso comune);	x	–	x	x	–
UCD, Accesso / Disconnessione; Commutazione	x	–	x	x	–
UCD, Destinazione notte on / off; Commutazione	x	–	x	x	–

Servizio	pronto alla composizion	su occupat	al telefono	Chiamata in uscita	chiamata entrante
Deviazione di chiamata per configurazione team	x	x	x	x	x
Messaggio di risposta on / off; Commutazione	x	–	x	x	–
Composizione associata	x	x	x	x	x
Servizi associati	x	–	x	x	–
Chiamata diretta	x	–	x	–	–
Liberare le linee (Emergency Trunk Access)	x	–	x	x	–
Inviare informazioni (Message Waiting)	x	–	x	x	–
Programmare selezione breve personale	x	–	x	x	–
Programmare selezione breve comune	x	–	x	x	–
Trasmissione DTMF	–	–	x	–	–
Trasmissione DTMF durante una conversazione con tasto di procedura	x	x	x	x	x
Servizio notte on / off; Commutazione	x	–	x	x	–
Parcheggio / Ripresa; Commutazione	–	x	x	x	–
Codice di addebito CA	x	–	x	–	–
Codice di addebito CA in preselezione	x	–	x	–	–
Visualizzare/cancellare le prenotazioni; Commutazione	x	–	–	–	–
Segnalazione delle chiamate on / off; Commutazione	x	–	x	x	–
Selezione lingua	x	x	x	x	x
Telephone Data Service TDS	x	–	x	x	–
Apriporta tramite box adattatore	x	x	x	x	x
Appuntamenti on / off; Commutazione	x	x	x	x	x
Ripresa di una chiamata esterna da messa in attesa generale	x	x	x	x	x
Chiave elettronica centrale	x	–	x	–	–

Informazioni specifiche del sistema

Un tasto procedura può memorizzare fino a 32 caratteri.

14.5.12 Promemoria e appuntamenti

Gli utenti hanno la possibilità di programmare un appuntamento sul proprio telefono, Al momento predefinito viene segnalato l'appuntamento. Tale segnalazione può avvenire una volta (una volta in un periodo di 24 ore) o più volte (ovvero quotidianamente).

L'ora dell'appuntamento è costituita da quattro cifre di cui le prime due rappresentano l'ora e le ultime due i minuti. Per gli Stati Uniti, è supportata l'indicazione dell'ora nel formato 12 ore, con immissione da parte dell'utente di

"am" (tasto 2) o "pm" (tasto 7) dopo la digitazione delle quattro cifre dell'ora. Se non viene specificato alcun dato, il sistema presume "am".

I telefoni analogici, optiPoint 500 entry o telefoni CMI possono programmare solo appuntamenti che non si ripetono.

Per impostazione predefinita, la segnalazione di un appuntamento dura 20 secondi e viene ripetuta fino a cinque volte, con una pausa di un minuto tra una ripetizione e l'altra. La cancellazione del processo avviene automaticamente sollevando il ricevitore o premendo il pulsante dell'altoparlante durante una chiamata o dopo la quinta ripetizione (numero configurabile). La memoria appuntamenti può anche essere cancellata tramite procedura. Nei terminali con display, può essere controllata l'ora che è stata impostata.

Se l'appuntamento non può essere segnalato (p.e. apparecchio occupato) viene annullato fino al ciclo successivo.

Suggerimento: I promemoria temporizzati possono essere pianificati per un massimo di 50 utenti, per sistema.

14.6 Panoramica di funzioni e codici

Codice servizio	Descrizione
*0	Ritorno all'utente in attesa
*1	Trasferimento chiamata
*2	Richiamata alternata
*3	Conferenza
*44	Servizio notte on
*51	Segnale alla rete
*52	Mute on
*53	Selezione DTMF
*55	Rispondere all'avviso di chiamata in attesa
*56	Iniziare il parcheggio
*57	Risposta per assente in gruppi RPA
*58	Iniziare la prenotazione
*59	Risposta per assente esterna ai gruppi RPA
*60	Codice d'addebito
*61	Apriporta
*62	Inclusione
*64	Deviazione di chiamata nella linea urbana (ISDN) on
*65	Visualizza addebiti
*66	Chiave elettronica on

Codice servizio	Descrizione
*67	Composizione associata
*68	Invia messaggio
*69	Messaggio di assenza on
*7	Salvare SBS/SBI
*80	Chiamata su altoparlante
*90	Attivazione dei relè
*91	Programmazione dei tasti
*92	Modificare numero breve
*93	Modifica PIN
*940	Test terminali
*95	Gestione del sistema
*97	Non disturbare on
	Babyphone on
*81	Segnalazione delle chiamate on
#1	Deviazione di chiamata off
#44	Servizio notte off
#52	Mute off
#56	Ripresa da parcheggio
#58	Controllare/cancellare prenotazioni
#64	Deviazione di chiamata nella linea urbana (ISDN) off
#66	Chiave elettronica off
#68	Leggere/cancellare informazioni (inviate)
#69	Messaggio di assenza off
#97	Non disturbare off
*96	Risposta tramite altoparlante on
#96	Risposta tramite altoparlante off
#90	Disattivazione dei relè
#81	Segnalazione delle chiamate off
#0	Reset di tutti i servizi
#3	Conferenza a cinque off
#82	Controllare la lista delle chiamate
*83	Servizi associati
*84	Identificazione di chiamate di disturbo
*85	Passo multiplo on

Codice servizio	Descrizione
#85	Passo multiplo off
*82	Descrivere la lista delle chiamate
*86	Disattivazione della visualizzaz. del nr. di telefono on
#86	Disattivazione della visualizzaz. del nr. di telefono off
*87	Segnalazione acustica dell'avviso di chiamata in attesa on
#87	Segnalazione acustica dell'avviso di chiamata in attesa off
*98	Silenzio on
#98	Silenzio off
*991	Gestione di sistema DTMF remota
*992	Rilasciare la gestione di sistema DTMF remota
*993	Rilasciare la gestione di sistema ISDN remota (obsoleto)
*994	Rilasciare il richiamo remoto dei dati del sistema
*89	Rilasciare l'apriporta tramite codice DTMF
#89	Bloccare l'apriporta tramite codice DTMF
*63	Continuare chiam. est. dopo il tasto di attesa
*41	Assegnare il nr. di telefono con MUSAP
*401	Effettuare il login degli operatori
#401	UCD - log of operatore
*402	UCD - operatore disponibile
#402	UCD - operatore non disponibile
*403	Elaborazione UCD on
#403	Elaborazione UCD off
*404	Servizio notte UCD on
#404	Servizio notte UCD off
*405	Controllo stato coda chiam.UCD
*42	Telephone Data Service (TDS)
*43	Attiva linea
*45	DCP: ricerca

Codice servizio	Descrizione
#45	DCP: risposta
*46	Dispositivo sveglia: appunt. on
#46	Dispositivo sveglia: appunt. off
*9419	Attivare cambio terminali
#9419	Disattivare cambio terminali
*942	Pronto alla registraz. (portatile)
*943	Chiave elettronica centrale
*944	Ascolto di una chiamata
	Drop Last Conference Party con linea urbana (solo USA)
*490	Rilascio avviso chiamata in attesa on
#490	Rilascio avviso chiamata in attesa off
*48	Selezione lingua
*508	Flex Call
*502	Commutazione di chiamata per MULAP on
#502	Commutazione di chiamata per MULAP on
*501	AUL per MULAP on
#501	AUL per MULAP off
*509	Congelamento del tracer
*47	DISA interno
*503	Selez. blocco tasti
*54	Elenco telefonico interno
*491	Terminale hotel analogico
#943	Chiave elettronica centrale/ Reset codice
*9411	Client per Call Forwarding in modalità Emergenza on
#9411	Client per Call Forwarding in modalità Emergenza off
*493	Registrazione vocale On
#493	Registrazione vocale Off
*495	Deviazione a tempo on
#495	Deviazione a tempo off
*945	Chiamata altoparlante discreta
*494	Data I/O

Codice servizio	Descrizione
*996	Consenti Smart Services via HTTPS per amministrazione remota
#996	Disattiva Smart Services via HTTPS per amministrazione remota
*997	Arresto controllato

15 Lavoro in team (Gruppi)

Il sistema di comunicazione mette a disposizione degli utenti diversi servizi volti ad agevolare il lavoro in team. Oltre a gruppi di risposta per assente, chiamate di gruppo e gruppi di ricerca, sono disponibili anche gruppi Team e per funzioni Direttore/Segretaria, gruppi casella vocale e gruppi fax. Grazie al servizio Uniform Call Distribution (UCD), il sistema di comunicazione consente di distribuire in modo uniforme le chiamate in arrivo a un gruppo di utenti (Gruppo UCD).

Suggerimento: Nella configurazione dei gruppi occorre notare che i primi tre gruppi sono riservati:

Per impostazione predefinita, il primo gruppo è utilizzato come gruppo di ricerca per la casella vocale esterna.

Per impostazione predefinita, il secondo gruppo è utilizzato come gruppo di ricerca per OpenScape Business Smart VoiceMail.

Per impostazione predefinita, il terzo gruppo è utilizzato gruppo di ricerca per il Company AutoAttendant di OpenScape Business Smart VoiceMail.

15.1 Gruppo di risposta per assente, chiamata di gruppo e gruppo di ricerca

Il sistema di comunicazione offre varie possibilità per riunire gli utenti in gruppi in modo che più utenti o telefoni siano raggiungibili allo stesso numero telefonico o che una chiamata per un utente venga segnalata anche ad altri.

In un gruppo di risposta per assente la chiamata destinata a un membro del gruppo viene sempre segnalata anche agli altri membri.

Con la funzione Chiamata di gruppo tutti i membri sono raggiungibili mediante un unico numero di telefono (numero di telefono del gruppo). La chiamata viene presa dal primo utente che risponde.

In un gruppo di ricerca, una chiamata in arrivo viene segnalata a uno dei membri del gruppo. Se questo membro non risponde alla chiamata, questa viene assegnata al membro successivo. Tutti i membri di un gruppo di ricerca sono raggiungibili sotto lo stesso numero.

15.1.1 Gruppo di risposta per assente

Una chiamata per un membro di un gruppo di risposta viene segnalata anche agli altri membri del gruppo. La chiamata può essere accettata da tutti gli altri membri del gruppo tramite il tasto funzione del telefono appositamente programmato, la selezione della voce di menu corrispondente o la composizione del codice.

La chiamata viene segnalata visivamente (display) e acusticamente al membro originariamente chiamato. Se programmata, la chiamata viene inoltre segnalata tramite il LED del tasto funzione.

Gli altri membri del gruppo inizialmente ricevono solo una segnalazione visiva della chiamata. Sul display vengono visualizzati il numero di telefono o il nome del destinatario originale della chiamata e il numero di telefono o il nome del chiamante. La visualizzazione del numero di telefono o del nome del chiamante può essere disattivata da un amministratore con il profilo **Expert**tramite la **Modalità esperti**. Se programmata, la chiamata viene inoltre segnalata tramite il LED del tasto funzione.

Se la chiamata non riceve una risposta entro quattro cicli di chiamata (4 x 5 secondi), gli altri membri del gruppo ricevono un tono di avviso (segnale acustico). Il tempo dall'inizio della segnalazione della chiamata fino al tono di avviso non è modificabile. Il tono di avviso può essere disattivato per tutti i membri del gruppo da un amministratore con il profilo **Expert**tramite la **Modalità esperti**.

Se vengono ricevute più chiamate per un gruppo di risposta per assente, la segnalazione avviene in base all'ordine di ingresso delle chiamate.

Perché la richiamata per i membri di un gruppo RPA possa essere ricevuta anche da altri membri, è necessario attivare tale funzione in **Modalità esperti**. Tale operazione deve essere eseguita da un amministratore con il profilo **Expert**.

Un utente può far parte di un solo gruppo di risposta per assente.

Gli eventuali addebiti per una chiamata a cui si ha risposto vengono attribuiti all'utente che ha risposto alla chiamata.

Nota: Le virgolette (") non sono supportate per il nome di un gruppo RPA.

Telefoni SIP

È possibile integrare telefoni SIP in un gruppo di risposta per assente

---

Suggerimento: Per i telefoni SIP è inoltre possibile impostare un tasto funzione per i gruppi di risposta per assente e visualizzare sul display del telefono i messaggi specifici destinati a tali gruppi. Per utilizzare questa funzione, è necessario attivare il servizio "Gruppo di risposta per assente" nel telefono SIP (vedere le istruzioni per l'uso del telefono stesso).

Risposta esterna a un gruppo Risposta per assente

Una variante del servizio è la "risposta all'esterno di un gruppo di risposta". In questo modo possono rispondere alle chiamate dirette a utenti interni anche persone che non appartengono allo stesso gruppo di risposta. La chiamata può essere risposta tramite il tasto funzione appositamente programmato, la voce di menu corrispondente o la composizione del codice specifico e successivamente l'immissione del numero di telefono dell'utente chiamato.

Dipendenze

Argomento	Dipendenza
Richiamata automatica	Le richiamate e le prenotazioni vengono segnalate agli altri membri del gruppo solo se si attiva il flag di sistema **RPA alla richiamata**.
Non disturbare	Sugli apparecchi dove è stata attivata la funzione Non disturbare, le chiamate RPA non vengono segnalate.
Telefoni ISDN	Non è possibile integrare telefoni ISDN in gruppi di risposta per assente.
MULAP	Non è possibile inserire numeri di telefono MULAP in un gruppo di risposta per assente.

Attività correlate

Come configurare un gruppo di risposta per assente alla pagina 688

Come aggiungere o cancellare un membro dal gruppo di risposta per assente alla pagina 688

Come abilitare o disabilitare la visualizzazione del numero di telefono e del nome del chiamante alla pagina 696

Come attivare o disattivare il tono di avviso alla pagina 697

Come attivare o disattivare la risposta per assente di richiamate alla pagina 697

15.1.2 Chiamata di gruppo

Una chiamata di gruppo può essere definita nei casi in cui più abbonati debbano essere raggiunti da un unico numero di telefono (numero di telefono di gruppo). Le chiamate esterne e interne in arrivo vengono segnalate contemporaneamente ai telefoni di tutti i membri del gruppo. La prima stazione che risponde alla chiamata viene collegata al chiamante.

Ogni membro di una chiamata di gruppo può essere raggiunto anche al proprio numero di stazione.

Al gruppo deve essere assegnata una delle seguenti proprietà:

- Gruppo

  Le chiamate in arrivo vengono segnalate contemporaneamente a tutti i membri del gruppo disponibili. I membri del gruppo disponibili sono gli abbonati che non sono occupati. Se tutti i membri del gruppo sono occupati, la chiamata viene segnalata dal tono di avviso di chiamata. La segnalazione della chiamata continua per tutti i membri del gruppo (tono di avviso di chiamata per i membri del gruppo occupati) anche se l'abbonato riaggancia.

  Il chiamante sente il tono di occupato se tutti i membri del gruppo sono occupati e tutti hanno attivato la funzione DND. Se per questo gruppo è stata definita una destinazione di inoltro delle chiamate, il chiamante non sente il tono di occupato, ma viene inoltrato direttamente alla destinazione di inoltro successiva.

- RNA

  Le chiamate in arrivo vengono segnalate contemporaneamente a tutti i membri del gruppo. Se un membro del gruppo è occupato, l'intera chiamata di gruppo viene contrassegnata come occupata. Gli altri chiamanti ricevono una tonalità di occupato.

  Nota: Non è possibile rilevare lo stato di presenza di una destinazione esterna appartenente al gruppo.

- Chiamata in attesa

  Le chiamate in arrivo vengono segnalate contemporaneamente a tutti i membri del gruppo disponibili. I membri del gruppo disponibili sono gli abbonati che non sono occupati. Una chiamata è segnalata da un tono di avviso di chiamata per i membri del gruppo occupati.

  Ciò richiede che tutti i membri del gruppo abbiano la funzione Non disturbare disabilitata.

Le chiamate di gruppo sono trattate come stazioni dalla funzione di inoltro delle chiamate senza risposta. In altre parole, se una chiamata non può essere accettata da nessuno dei membri di una chiamata di gruppo, viene reindirizzata a una destinazione di inoltro di chiamata in base all'elenco delle destinazioni di chiamata. È possibile specificare se il trasferimento di chiamata deve essere eseguito su RNA (chiamata senza risposta) o su occupato.

Quando una chiamata non riceve risposta da un membro di un gruppo, viene visualizzata come chiamata persa nel diario dei client UC di tutti i membri. Una chiamata accettata appare solo nel diario del membro che ha risposto alla chiamata.

Una singola stazione può appartenere a più gruppi contemporaneamente. Quanto segue si applica ai gruppi di tipo Chiamata di gruppo, Gruppo di ricerca, Configurazione team/Gruppo team e Direttore/Segretaria / Gruppo Top: La somma di tutte le adesioni degli utenti a questi gruppi non deve superare 32.

Il nome del gruppo assegnato viene visualizzato sul display del chiamante interno. Dopo l'accettazione di una chiamata, viene visualizzato il nome dell'abbonato che ha accettato la chiamata.

Se un utente ha definito delle regole con l'AutoAttendant, ad esempio per inoltrare le chiamate, queste regole si applicheranno solo alle chiamate al proprio numero di stazione. Le regole vengono ignorate per le chiamate di gruppo.

Per ogni chiamata di gruppo è possibile configurare fino a 20 abbonati.

A ciascuna chiamata di gruppo è possibile assegnare un nome contenente al massimo 16 caratteri.

Casella vocale per chiamate di gruppo

Quando si imposta una chiamata di gruppo, viene creata automaticamente una casella vocale. Il numero di chiamata di questa casella vocale per la chiamata di gruppo corrisponde sempre a quello della chiamata di gruppo. Se una chiamata di gruppo non viene accettata da nessun membro, la chiamata viene inoltrata alla casella vocale della chiamata di gruppo. Ciò richiede che la casella vocale della chiamata di gruppo sia stata definita come destinazione CFNA (deviazione di chiamata senza risposta) di questa chiamata di gruppo.

Se un membro non accetta una chiamata in arrivo al proprio numero di stazione, questa viene reindirizzata a una destinazione di inoltro di chiamata in base all'elenco delle destinazioni di chiamata.

Esempio di chiamata di gruppo di tipo RNA (senza risposta) con il numero di chiamata di gruppo 404 e i membri A (numero di chiamata 200), B (201) e C (202). Per la chiamata di gruppo è stato impostata la deviazione di chiamata senza risposta dopo il timeout alla casella vocale della chiamata di gruppo. Ogni membro ha definito la deviazione di chiamata senza risposta (CFNA) dopo il timeout alla propria casella vocale.		
Chiamata in entrata per il membro A (200)	Tutti i membri sono liberi.	Il membro A non accetta la chiamata. La deviazione di chiamata senza risposta dopo il timeout avviene verso la casella vocale dell'utente A.
	L'utente A ha definito la deviazione di chiamata incondizionata (CFU) alla propria casella vocale. I membri B e C sono liberi.	La chiamata viene deviata immediatamente (CFU) alla casella vocale del membro A.
Chiamata in entrata per la chiamata di gruppo (404)	Tutti i membri sono liberi.	La chiamata viene segnalata a tutti gli altri membri. Nessun membro accetta la chiamata. La deviazione di chiamata senza risposta dopo il timeout avviene verso la casella vocale della chiamata di gruppo.
	L'utente A ha definito la deviazione di chiamata incondizionata (CFU) alla propria casella vocale. I membri B e C sono liberi.	La chiamata viene segnalata ai membri B e C. Nessun membro accetta la chiamata. La deviazione di chiamata senza risposta dopo il timeout avviene verso la casella vocale della chiamata di gruppo.
	Il membro A ha definito la deviazione di chiamata incondizionata (CFU) verso una destinazione esterna. I membri B e C sono liberi.	La chiamata viene segnalata ai membri B e C e alla destinazione esterna. Nessun membro accetta la chiamata. La deviazione di chiamata senza risposta dopo il timeout avviene verso la casella vocale della chiamata di gruppo.
	Il membro A ha definito le regole CFNA utilizzando l'AutoAttendant. I membri B e C sono liberi.	La chiamata viene segnalata a tutti gli altri membri. Nessun membro accetta la chiamata. La deviazione di chiamata senza risposta dopo il timeout avviene verso la casella vocale della chiamata di gruppo.

Attivazione/disattivazione di una chiamata di gruppo

Se un abbonato è membro di una chiamata di gruppo, può utilizzare i codici per uscire e rientrare nella chiamata di gruppo.

Se un abbonato è membro di più gruppi di chiamata e di più gruppi di ricerca, può utilizzare i codici per uscire e rientrare in tutti i gruppi di chiamata e di ricerca. Gli abbonati vengono aggiunti o rimossi da uno specifico gruppo di chiamata o gruppo di ricerca immettendo i codici ed effettuando una selezione tra le chiamate di gruppo e i gruppi di ricerca visualizzati.

È inoltre possibile programmare i tasti funzione con una funzione di spostamento per l'ingresso e l'uscita. È possibile programmare qui un tasto funzione valido per una chiamata di gruppo e un gruppo di ricerca specifici o per tutte le chiamate di gruppo e i gruppi di ricerca. È possibile anche una programmazione variabile. Dopo aver premuto un tasto funzione di questo tipo, è necessario selezionare una delle chiamate di gruppo e dei gruppi di ricerca visualizzati per definire la chiamata di gruppo o il gruppo di ricerca che si desidera abbandonare/aggiungere.

Tipo chiam.

Per ogni chiamata di gruppo, l'amministratore con il profilo **Esperto** può definire un segnale acustico all'arrivo delle chiamate esterne impostando il tipo di suoneria. Sono disponibili le seguenti opzioni:

- Tono di chiamata doppio (Impostazione predefinita)
- Tono di chiamata triplo
- Tono di chiamata breve/lungo/breve

Nei telefoni analogici è disponibile solamente l'impostazione predefinita. Le modifiche non hanno alcun effetto.

Telefoni SIP

I telefoni SIP possono essere integrati in una chiamata di gruppo.

Nota: Nei telefoni SIP non è possibile programmare i tasti funzione. I messaggi a display specifici di un gruppo di ricerca non sono supportati.

Dipendenze

Argomento	Dipendenza
Inoltro di chiamata	Se un membro del gruppo attiva la deviazione di chiamata per tutte le chiamate, tutte le chiamate vengono segnalate al telefono di destinazione.
Non disturbare	Se un membro del gruppo attiva la funzione Non disturbare, le chiamate in arrivo sul suo telefono non vengono presentate/passate. Questo vale per le chiamate effettuate tramite il numero di telefono del gruppo e il numero della propria postazione.
Inclusione	L'inclusione non è possibile se tutti i membri di un gruppo di chiamata sono occupati.
Telefoni ISDN	Non è possibile includere i telefoni ISDN in una chiamata di gruppo.

Concetti correlati

Rubrica interna alla pagina 506

Attività correlate

Come aggiungere una chiamata di gruppo (gruppo) alla pagina 689
Come modificare una chiamata di gruppo (gruppo) alla pagina 690
Come eliminare una chiamata di gruppo (gruppo) alla pagina 691
Come aggiungere o cancellare membri dalle chiamate di gruppo (gruppo) alla pagina 692
Come aggiungere una chiamata di gruppo (Libero o Avviso di chiamata in attesa) alla pagina 697
Come visualizzare o modificare una chiamata di gruppo (Libero o Avviso di chiamata in attesa) alla pagina 698
Come cancellare una chiamata di gruppo (Libero o Avviso di chiamata in attesa) alla pagina 699
Come aggiungere o eliminare un membro di una chiamata di gruppo (Libero o Avviso di chiamata in attesa) alla pagina 699
Come disattivare o attivare il rifiuto dell'avviso di chiamata per i membri del gruppo alla pagina 700

15.1.3 Gruppo di ricerca

I gruppi di ricerca consentono di distribuire le chiamate in entrata agli abbonati associati (membri). Se un utente è occupato o non accetta una chiamata in arrivo, la chiamata viene automaticamente inoltrata al successivo membro libero del gruppo di ricerca. Tutti i membri del gruppo di ricerca sono raggiungibili allo stesso numero di telefono.

Ogni membro di un gruppo di ricerca può essere raggiunto anche al numero della propria stazione.

Al gruppo di ricerca deve essere assegnata una delle seguenti proprietà.

- Lineare

  Una chiamata in entrata viene sempre segnalata per prima al primo membro di un gruppo di ricerca. L'ulteriore segnalazione viene effettuata in base alla sequenza di inserimento dei membri nella tabella dei gruppi.
- Ciclica

  Una chiamata in entrata viene sempre segnalata per prima al membro che segue l'abbonato che ha risposto all'ultima chiamata. L'ulteriore segnalazione viene effettuata in base alla sequenza di inserimento dei membri nella tabella dei gruppi.

La chiamata viene inoltrata automaticamente al successivo membro libero del gruppo di ricerca allo scadere del tempo di deviazione, a condizione che non si risponda alla chiamata, che un membro sia occupato o che sia attivato il DND.

È possibile programmare una destinazione di deviazione delle chiamate (elenco di destinazione delle chiamate) se una chiamata non può ricevere risposta da nessuno dei membri del gruppo di ricerca.

Una singola stazione può appartenere a più gruppi contemporaneamente. Quanto segue si applica ai gruppi di tipo Chiamata di gruppo, Gruppo di ricerca,

Configurazione team/Gruppo team e Direttore/Segretaria / Gruppo Top: La somma di tutte le adesioni degli utenti a questi gruppi non deve superare 32.

Il nome assegnato al gruppo di ricerca viene visualizzato sul display del chiamante interno. Dopo l'accettazione di una chiamata, viene visualizzato il nome dell'abbonato che ha accettato la chiamata.

Se un utente ha definito delle regole con l'AutoAttendant, ad esempio per inoltrare le chiamate, queste regole si applicheranno solo alle chiamate al proprio numero di stazione. Le regole vengono ignorate per le chiamate dei gruppi di ricerca.

Per ogni gruppo di ricerca è possibile configurare fino a 20 membri.

A ciascun gruppo di ricerca è possibile assegnare un nome contenente al massimo 16 caratteri.

Casella vocale per gruppo di ricerca

Quando si configura un gruppo di ricerca, viene automaticamente creata una casella vocale. Il numero di chiamata di questa casella vocale per il gruppo di ricerca corrisponde sempre a quello del gruppo di ricerca. Se una chiamata per un gruppo di ricerca non viene accettata da nessun membro, la chiamata viene deviata alla casella vocale del gruppo di ricerca. Ciò richiede che la casella vocale del gruppo di ricerca sia stata definita come destinazione CFNA (deviazione di chiamata senza risposta) di questo gruppo di ricerca.

Se un membro non accetta una chiamata in arrivo al proprio numero di stazione, questa viene reindirizzata a una destinazione di inoltro di chiamata in base all'elenco delle destinazioni di chiamata.

Esempio di gruppo di ricerca lineare con il numero di chiamata 404 e i membri A (numero di chiamata 200), B (201) e C (202). Per il gruppo di ricerca è stata impostata la deviazione di chiamata senza risposta dopo il timeout alla casella vocale della chiamata del gruppo di ricerca. Ogni membro ha definito la deviazione di chiamata senza risposta (CFNA) dopo il timeout alla propria casella vocale.		
Chiamata in entrata per il membro A (200)	Tutti i membri sono liberi.	Il membro A non accetta la chiamata. La deviazione di chiamata senza risposta dopo il timeout avviene verso la casella vocale dell'utente A.
	L'utente A ha definito la deviazione di chiamata incondizionata (CFU) alla propria casella vocale. I membri B e C sono liberi.	La chiamata viene deviata immediatamente (CFU) alla casella vocale del membro A.
Chiamata in entrata per il gruppo di ricerca (404)	Tutti i membri sono liberi.	La chiamata viene segnalata prima al membro A, poi al membro B e infine al membro C. Nessun membro accetta la chiamata. La deviazione di chiamata senza risposta dopo il timeout avviene verso la casella vocale del gruppo di ricerca.

	L'utente A ha definito la deviazione di chiamata incondizionata (CFU) alla propria casella vocale. I membri B e C sono liberi.	La chiamata viene segnalata prima al membro B e poi al membro C. Nessun membro accetta la chiamata. La deviazione di chiamata senza risposta dopo il timeout avviene verso la casella vocale del gruppo di ricerca.
	Il membro A ha definito la deviazione di chiamata incondizionata (CFU) verso una destinazione esterna. I membri B e C sono liberi.	La chiamata viene segnalata prima al membro B e poi al membro C. Nessun membro accetta la chiamata. La deviazione di chiamata senza risposta dopo il timeout avviene verso la casella vocale del gruppo di ricerca.
	Il membro A ha definito le regole CFNA utilizzando l'AutoAttendant. I membri B e C sono liberi.	La chiamata viene segnalata prima al membro A, poi al membro B e infine al membro C. Nessun membro accetta la chiamata. La deviazione di chiamata senza risposta dopo il timeout avviene verso la casella vocale del gruppo di ricerca.

Attivazione/disattivazione del gruppo di ricerca

Se un abbonato è membro di un gruppo di ricerca, può utilizzare i codici per uscire e rientrare nel gruppo.

Se un abbonato è membro di più gruppi di ricerca e di più gruppi di chiamata, può utilizzare i codici per uscire e rientrare in tutti i gruppi. Gli abbonati vengono aggiunti o rimossi da uno specifico gruppo di ricerca o gruppo di chiamata immettendo i codici ed effettuando una selezione tra i gruppi di ricerca e le chiamate di gruppo visualizzati.

È inoltre possibile programmare i tasti funzione con una funzione di spostamento per l'ingresso e l'uscita. È possibile programmare qui un tasto funzione valido per un gruppo di ricerca o una chiamata di ricerca specifici o per tutti i gruppi di ricerca e tutte le chiamate di gruppo. È possibile anche una programmazione variabile. Dopo aver premuto un tasto funzione di questo tipo, è necessario selezionare uno dei gruppi di ricerca e delle chiamate di gruppo visualizzati per definire il gruppo di ricerca o la chiamata di gruppo che si desidera abbandonare o a cui si desidera unirsi.

Tipo chiam.

Per ogni gruppo di ricerca, l'amministratore con il profilo **Esperto** può definire un segnale acustico all'arrivo delle chiamate esterne impostando il tipo di suoneria. Sono disponibili le seguenti opzioni:

- Tono di chiamata doppio (Impostazione predefinita)
- Tono di chiamata triplo
- Tono di chiamata breve/lungo/breve

Nei telefoni analogici è disponibile solamente l'impostazione predefinita. Le modifiche non hanno alcun effetto.

Telefoni SIP

È possibile integrare telefoni SIP in un gruppo di ricerca.

Suggerimento: Nei telefoni SIP non è possibile programmare i tasti funzione. I messaggi a display specifici di un gruppo di ricerca non sono supportati.

Dipendenze

Argomento	Dipendenza
Inoltro di chiamata	Se un membro del gruppo di ricerca attiva la deviazione di chiamata per tutte le chiamate, tutte le chiamate vengono segnalate al telefono di destinazione.
Non disturbare	Se un membro del gruppo di ricerca attiva la funzione Non disturbare, le chiamate in arrivo non vengono presentate/passate. Questo vale per le chiamate del gruppo di ricerca e per il numero di stazione del membro.
Coda	Per i gruppi di ricerca ciclici e lineari non è possibile impostare una coda di chiamata.
Telefoni ISDN	Non è possibile integrare telefoni ISDN nei gruppi di ricerca.

Attività correlate

Come aggiungere un gruppo di ricerca alla pagina 692
Come modificare un gruppo di ricerca alla pagina 693
Come eliminare un gruppo di ricerca alla pagina 694
Come aggiungere o cancellare membri dal gruppo di ricerca alla pagina 695

15.1.4 Configurazione di gruppi di risposta per assente, chiamate di gruppo e gruppi di ricerca tramite procedure guidate

Diverse procedure guidate consentono di impostare in modo pratico gruppi di risposta per assente, chiamate di gruppo e gruppi di ricerca.

Con la procedura guidata **Risposta per assente** è possibile riunire gli utenti in un gruppo con il compito comune di occuparsi della risposta alle chiamate. Viene descritta la procedura nei seguenti casi configurabili tramite la procedura guidata:

- Come configurare un gruppo di risposta per assente
- Come aggiungere o cancellare un membro dal gruppo di risposta per assente

Con la procedura guidata **Chiamata di gruppo/Gruppo di ricerca** è possibile configurare le chiamate di gruppo del tipo Gruppo. Viene descritta la procedura nei seguenti casi configurabili tramite la procedura guidata:

- Come aggiungere una chiamata di gruppo (gruppo)
- Come modificare una chiamata di gruppo (gruppo)

- Come eliminare una chiamata di gruppo (gruppo)
- Come aggiungere o cancellare membri dalle chiamate di gruppo (gruppo)
- Come aggiungere un gruppo di ricerca
- Come modificare un gruppo di ricerca
- Come eliminare un gruppo di ricerca
- Come aggiungere o cancellare membri dal gruppo di ricerca

15.1.4.1 Come configurare un gruppo di risposta per assente

La procedura guidata **Risposta per assente** consente di riunire gli utenti in un gruppo con possibilità di risposta alle chiamate reciproca.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Risposta per assente**. Viene visualizzata una lista di tutti i gruppi possibili di risposta per assente.
4) Per configurare un gruppo di risposta per assente, fare clic su **Modifica** nella riga del gruppo di risposta per assente desiderato.
5) Se si desidera aggiungere un membro al gruppo di risposta per assente, selezionare la casella di controllo **Assegnazione Gruppo <Numero>** del numero di telefono/nome desiderato.
6) Se si desidera eliminare un membro da un gruppo di risposta per assente, deselezionare la casella di controllo**Assegnazione Gruppo <Numero>** del numero di telefono/nome desiderato.
7) Fare clic su **OK** per applicare le impostazioni.
8) Nel campo **Nome** indicare il nome del gruppo di risposta per assente precedentemente configurato.
9) Se si desidera configurare un altro gruppo di risposta per assente, ripetere i passi da 4 a 8.
10) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Gruppo di risposta per assente alla pagina 678

15.1.4.2 Come aggiungere o cancellare un membro dal gruppo di risposta per assente

Con la procedura guidata **Risposta per assente** è possibile aggiungere o cancellare membri dai gruppi di risposta.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Risposta per assente**.
4) Nella riga del gruppo di risposta per assente desiderato, fare clic su **Modifica**.
5) Selezionare una delle seguenti opzioni:
   - Se si desidera aggiungere un membro al gruppo di risposta per assente, selezionare la casella di controllo **Assegnazione Gruppo <Numero>** del numero di telefono/nome desiderato.
   - Se si desidera eliminare un membro da un gruppo di risposta per assente, deselezionare la casella di controllo**Assegnazione Gruppo <Numero>** del numero di telefono/nome desiderato.
6) Fare clic su **OK** per applicare le impostazioni.
7) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Gruppo di risposta per assente alla pagina 678

15.1.4.3 Come aggiungere una chiamata di gruppo (gruppo)

Con la procedura guidata **Chiamata di gruppo/Gruppo di ricerca** è possibile configurare le chiamate di gruppo del tipo Gruppo.

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Chiamata di gruppo / Gruppo di ricerca**.
4) Fare clic su **Aggiungi**, per configurare una nuova chiamata di gruppo.
5) Nel campo **Numero di telefono del gruppo**, indicare il numero di telefono della nuova chiamata a gruppo.
6) Nel campo **Interno**, indicare il numero di interno della nuova chiamata di gruppo.

   : Se si desidera utilizzare il numero di interno 879, 890 o 891, occorre configurare l'impostazione tramite Manager E e non tramite WBM.

   ---

7) Nel campo **Nome del gruppo**, indicare il nome della nuova chiamata a gruppo.
8) Nell'elenco a discesa **Tipo**, selezionare la voce **Gruppo**.

9) Selezionare una delle seguenti opzioni relativamente all'inserimento del numero di telefono della chiamata di gruppo nella rubrica interna:
   - Se il numero di telefono della chiamata di gruppo deve essere visualizzato nell'elenco, selezionare la casella di controllo **El. telef.**.
   - Se il numero di telefono della chiamata di gruppo non deve essere visualizzato nell'elenco, deselezionare la casella di controllo **El. telef.**.
10) Nell'elenco a discesa **Numero di telefono dell'utente da assegnare al gruppo**, selezionare il numero di telefono dell'utente desiderato.
11) Fare clic su **OK & Avanti**.

> **Suggerimento:** Se il numero di telefono e/o di interno (selezione passante) è già disponibile, è possibile richiamare il piano di composizione effettivo per individuare un numero di telefono e/o di interno libero.

12) Nella riga della chiamata di gruppo desiderata, fare clic su **Modifica** per assegnare la chiamata di gruppo ad altri utenti.
13) Nell'elenco a discesa **Nº tel.**, selezionare il numero di telefono dell'utente da assegnare alla chiamata di gruppo.
14) Fare clic su **Aggiungi**.
15) Se si desidera assegnare altri utenti alla chiamata di gruppo, ripetere i passi 13 e 14.
16) Fare clic su **OK** per applicare le impostazioni.
17) Se si desidera configurare un'altra chiamata di gruppo, ripetere i passi da 4 a 16.
18) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Chiamata di gruppo alla pagina 680

15.1.4.4 Come modificare una chiamata di gruppo (gruppo)

Con la Procedura guidata **Chiamata di gruppo / Gruppo di ricerca** è possibile modificare le chiamate di gruppo del tipo Gruppo.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Chiamata di gruppo / Gruppo di ricerca**.
4) Nella riga del gruppo di risposta alle chiamate da modificare, fare clic su **Modifica**.
5) Modificare i parametri di gruppo desiderati.

6) Solo con UC Smart: se necessario assegnare alla chiamata di gruppo una casella di posta:
   a) Dal menu a discesa selezionare **Tipo mailbox UC Smart** se la chiamata di gruppo deve ricevere una mailbox standard o una mailbox posto operatore (AutoAttendant).
   b) Solo con mailbox standard: se un chiamante può lasciare un messaggio nella casella vocale, selezionare la casella di controllo **Registrare**.
   c) Dall'elenco a discesa **Annuncio**, selezionare un annuncio di benvenuto.
   d) Se la password della casella vocale deve essere reimpostata, selezionare la casella di controllo **Reset password**.

   Nota: Se una casella vocale viene riconfigurata, la casella di controllo **Reset password** non deve essere selezionata. Consente di reimpostare la password per la casella vocale. In caso di riconfigurazione, l'utente deve cambiare comunque la password iniziale della casella vocale al primo accesso.

7) Se si desidera aggiungere un membro alla chiamata di gruppo, dall'elenco a discesa **N°. tel.**, selezionare il numero di telefono dell'utente desiderato, quindi fare clic su **Aggiungi**.
8) Se si desidera cancellare un membro dalla chiamata di gruppo, nella riga del membro gruppo da eliminare, fare clic su **Cancella**, quindi su **OK**.
9) Fare clic su **OK** per applicare le impostazioni.
10) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Chiamata di gruppo alla pagina 680

15.1.4.5 Come eliminare una chiamata di gruppo (gruppo)

Con la procedura guidata **Chiamata di gruppo / Gruppo di ricerca** è possibile eliminare le chiamate di gruppo del tipo Gruppo.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Chiamata di gruppo / Gruppo di ricerca**.
4) Nella riga della chiamata di gruppo da modificare, fare clic su **Modifica**.
5) Fare clic su **Cancella dati**.
6) Fare clic su **OK** per confermare la cancellazione.
7) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Chiamata di gruppo alla pagina 680

15.1.4.6 Come aggiungere o cancellare membri dalle chiamate di gruppo (gruppo)

Con la Procedura guidata **Chiamata di gruppo / Gruppo di ricerca** è possibile aggiungere o cancellare membri dalle chiamate di gruppo del tipo Gruppo.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Chiamata di gruppo / Gruppo di ricerca**.
4) Nella riga della chiamata di gruppo desiderata, fare clic su **Modifica**.
5) Selezionare una delle seguenti opzioni:
   - Se si desidera aggiungere un membro alla chiamata di gruppo, dall'elenco a discesa **N°. tel.**, selezionare il numero di telefono dell'utente desiderato, quindi fare clic su **Aggiungi**.
   - Se si desidera cancellare un membro dalla chiamata di gruppo, nella riga del membro gruppo da eliminare, fare clic su **Cancella**, quindi su **OK**.
6) Fare clic su **OK** per applicare le impostazioni.
7) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Chiamata di gruppo alla pagina 680

15.1.4.7 Come aggiungere un gruppo di ricerca

Con la procedura guidata **Chiamata di gruppo/Gruppo di ricerca** è possibile configurare i gruppi di ricerca.

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Chiamata di gruppo / Gruppo di ricerca**.
4) Fare clic su **Aggiungi** per configurare un nuovo gruppo di ricerca.
5) Nel campo **Numero di telefono del gruppo**, indicare il numero di telefono del nuovo gruppo di ricerca.

6) Nel campo **Interno**, indicare il numero di interno del nuovo gruppo di ricerca.

: Se si desidera utilizzare il numero di interno 879, 890 o 891, occorre configurare l'impostazione tramite Manager E e non tramite WBM.

---

7) Nel campo **Nome del gruppo**, indicare il nome del nuovo gruppo di ricerca.
8) Nell'elenco a discesa **Tipo**, selezionare il tipo del nuovo gruppo di ricerca. Sono disponibili le seguenti opzioni:
   - Se la chiamata deve essere segnalata sempre prima al primo membro di un gruppo di ricerca, selezionare l'opzione **Linea con ricerca lineare**.
   - Se la chiamata deve essere sempre prima segnalata al membro che segue l'utente che ha ricevuto l'ultima chiamata, selezionare l'opzione **Linea con ricerca ciclica**.
9) Selezionare una delle seguenti opzioni relativamente all'inserimento del numero di telefono del gruppo di ricerca nella rubrica interna:
   - Se il numero di telefono del gruppo di ricerca deve essere visualizzato nell'elenco, selezionare la casella di controllo **El. telef.**.
   - Se il numero di telefono del gruppo di ricerca non deve essere visualizzato nell'elenco, deselezionare la casella di controllo **El. telef.**.
10) Nell'elenco a discesa **Numero di telefono dell'utente da assegnare al gruppo**, selezionare il numero di telefono dell'utente desiderato.
11) Fare clic su **OK & Avanti**.

Suggerimento: Se il numero di telefono e/o di interno (selezione passante) è già disponibile, è possibile richiamare il piano di composizione effettivo per individuare un numero di telefono e/o di interno libero.

---

12) Nella riga del gruppo di ricerca desiderato, fare clic su **Modifica** per assegnare il gruppo di ricerca ad altri utenti.
13) Nell'elenco a discesa **Nº tel.**, selezionare il numero di telefono dell'utente da assegnare al gruppo di ricerca.
14) Fare clic su **Aggiungi**.
15) Se si desidera assegnare altri utenti al gruppo di ricerca, ripetere i passi 13 e 14.
16) Fare clic su **OK** per applicare le impostazioni.
17) Se si desidera configurare altri gruppi di ricerca, ripetere i passi da 4 a 16.
18) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Gruppo di ricerca alla pagina 684

15.1.4.8 Come modificare un gruppo di ricerca

Con la procedura guidata **Chiamata di gruppo / Gruppo di ricerca** è possibile modificare i gruppi di ricerca.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Chiamata di gruppo / Gruppo di ricerca**.
4) Nella riga del gruppo di ricerca da modificare, fare clic su **Modifica**.
5) Modificare i parametri desiderati del gruppo di ricerca.
6) Solo con UC Smart: se necessario assegnare al gruppo di ricerca una casella di posta:
   a) Dal menu a discesa selezionare **Tipo mailbox UC Smart** se il gruppo di ricerca deve ricevere una mailbox standard o una mailbox posto operatore (AutoAttendant).
   b) Solo con mailbox standard: se un chiamante può lasciare un messaggio nella casella vocale, selezionare la casella di controllo **Registrare**.
   c) Dall'elenco a discesa **Annuncio**, selezionare un annuncio di benvenuto.
   d) Se la password della casella vocale deve essere reimpostata, selezionare la casella di controllo **Reset password**.

   Nota: Se una casella vocale viene riconfigurata, la casella di controllo **Reset password** non deve essere selezionata. Consente di reimpostare la password per la casella vocale. In caso di riconfigurazione, l'utente deve cambiare comunque la password iniziale della casella vocale al primo accesso.
7) Se si desidera aggiungere un membro a un gruppo di ricerca, dall'elenco a discesa **N°. tel.**, selezionare il numero di telefono dell'utente desiderato, quindi fare clic su **Aggiungi**.
8) Se si desidera cancellare un membro dal gruppo di ricerca, nella riga del membro del gruppo da eliminare, fare clic su **Cancella**, quindi su **OK**.
9) Se si desidera modificare la posizione dei membri all'interno del gruppo di ricerca, fare clic su **Modifica ordine**. Nel campo **Posizione**, inserire il numero di posizione desiderato per ciascun membro. Fare clic su **OK & Avanti**.
10) Fare clic su **OK** per applicare le impostazioni.
11) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Gruppo di ricerca alla pagina 684

15.1.4.9 Come eliminare un gruppo di ricerca

Con la procedura guidata **Chiamata di gruppo / Gruppo di ricerca** è possibile eliminare i gruppi di ricerca.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Chiamata di gruppo / Gruppo di ricerca**.
4) Nella riga della chiamata di gruppo da eliminare, fare clic su **Elimina**.
5) Fare clic su **Cancella dati**.
6) Fare clic su **OK** per confermare la cancellazione.
7) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Gruppo di ricerca alla pagina 684

15.1.4.10 Come aggiungere o cancellare membri dal gruppo di ricerca

Con la procedura guidata **Chiamata di gruppo / Gruppo di ricerca** è possibile aggiungere o cancellare membri dai gruppi di ricerca.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Chiamata di gruppo / Gruppo di ricerca**.
4) Nella riga del gruppo di ricerca desiderato fare clic su **Modifica**.
5) Selezionare una delle seguenti opzioni:
   - Se si desidera aggiungere un membro a un gruppo di ricerca, dall'elenco a discesa **N°. tel.**, selezionare il numero di telefono dell'utente desiderato, quindi fare clic su **Aggiungi**.
   - Se si desidera cancellare un membro dal gruppo di ricerca, nella riga del membro del gruppo da eliminare, fare clic su **Cancella**, quindi su **OK**.
6) Fare clic su **OK** per applicare le impostazioni.
7) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Gruppo di ricerca alla pagina 684

15.1.5 Configurazione di gruppi di risposta per assente, chiamate di gruppo e gruppi di ricerca tramite la Modalità esperti

Oltre alle possibilità di configurazione mediante procedura guidata, sono a disposizione di un amministratore con il profilo **Expert** ulteriori opzioni di configurazione in **Modalità esperti** per l'impostazione di gruppi di risposta per assente, chiamata di gruppo, gruppi di ricerca.

Viene descritta la procedura nei seguenti casi configurabili tramite la **Modalità esperti**:

- Come abilitare o disabilitare la visualizzazione del numero di telefono e del nome del chiamante
- Come attivare o disattivare il tono di avviso
- Come attivare o disattivare la risposta per assente di richiamate
- Come aggiungere una chiamata di gruppo (Libero o Avviso di chiamata in attesa)
- Come visualizzare o modificare una chiamata di gruppo (Libero o Avviso di chiamata in attesa)
- Come cancellare una chiamata di gruppo (Libero o Avviso di chiamata in attesa)
- Come aggiungere o eliminare un membro di una chiamata di gruppo (Libero o Avviso di chiamata in attesa)
- Come disattivare o attivare il rifiuto dell'avviso di chiamata per i membri del gruppo

15.1.5.1 Come abilitare o disabilitare la visualizzazione del numero di telefono e del nome del chiamante

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema** > **Flag di sistema**.
4) Selezionare una delle seguenti opzioni:
   - Se è necessario che il numero di telefono e il nome del chiamante siano visualizzati, selezionare la casella di controllo **Numero chiamante in gruppi di risposta / gruppi di segnalazione chiamate / CFN / RNA**.
   - Se non si desidera che il numero di telefono e il nome del chiamante siano visualizzati, deselezionare la casella di controllo **Numero chiamante in gruppi di risposta / gruppi di segnalazione chiamate / CFN / RNA**.
5) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Gruppo di risposta per assente alla pagina 678

15.1.5.2 Come attivare o disattivare il tono di avviso

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema** > **Flag di sistema**.
4) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare uno squillo di avviso, selezionare la casella di controllo **Squillo di avviso in gruppi RPA**.
   - Se si desidera disattivare lo squillo di avviso, deselezionare la casella di controllo **Squillo di avviso in gruppi RPA**.
5) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Gruppo di risposta per assente alla pagina 678

15.1.5.3 Come attivare o disattivare la risposta per assente di richiamate

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema** > **Flag di sistema**.
4) Selezionare una delle seguenti opzioni:
   - Se si vuole consentire la risposta per assente di richiamate, selezionare la casella di controllo **RPA alla richiamata**.
   - Se non si vuole consentire la risposta per assente di richiamate, deselezionare la casella di controllo **RPA alla richiamata**.
5) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Gruppo di risposta per assente alla pagina 678

15.1.5.4 Come aggiungere una chiamata di gruppo (Libero o Avviso di chiamata in attesa)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Nella struttura dei menu, fare clic su **Chiamate in entrata** > **Linea di gruppo/di ricerca**.
4) Fare clic sulla scheda **Aggiungi gruppo**.
5) Nel campo **Numero di telefono**, indicare il numero di telefono della nuova chiamata a gruppo.
6) Nel campo **Interno**, indicare il numero di interno della nuova chiamata di gruppo.

   : Se si desidera utilizzare il numero di interno 879, 890 o 891, occorre configurare l'impostazione tramite Manager E e non tramite WBM.

7) Nel campo **Nome**, indicare il nome della nuova chiamata a gruppo.
8) In **Tipo**, selezionare dall'elenco a discesa una delle seguenti possibilità:
   - Se si desidera configurare una chiamata di gruppo di tipo Libero, selezionare la voce **Libero**.
   - Se si desidera configurare una chiamata di gruppo di tipo Avviso di chiamata, selezionare la voce **Avviso di chiamata**.
9) Nell'elenco a discesa **Numero di telefono**, selezionare il numero di telefono dell'utente da assegnare alla chiamata di gruppo.
10) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Chiamata di gruppo alla pagina 680

15.1.5.5 Come visualizzare o modificare una chiamata di gruppo (Libero o Avviso di chiamata in attesa)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** fino alla chiamata di gruppo desiderata.
4) Fare clic sulla scheda **Modifica parametri gruppo**. Vengono visualizzate i valori attualmente impostati nei parametri del gruppo.
5) Se necessario, modificare i parametri desiderati della chiamata di gruppo.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Chiamata di gruppo alla pagina 680

15.1.5.6 Come cancellare una chiamata di gruppo (Libero o Avviso di chiamata in attesa)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** fino alla chiamata di gruppo desiderata.
4) Fare clic sulla scheda **Cancella gruppo**.
5) Fare clic su **Cancella** quindi su **OK**.

Concetti correlati

Chiamata di gruppo alla pagina 680

15.1.5.7 Come aggiungere o eliminare un membro di una chiamata di gruppo (Libero o Avviso di chiamata in attesa)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Selezionare una delle seguenti opzioni:
   - Se si desidera aggiungere un membro a una chiamata di gruppo, nella struttura dei menu selezionare **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** e infine la chiamata di gruppo desiderata. Fare clic sulla scheda **Aggiungi membro**. Nell'elenco a discesa **Numero di telefono** selezionare il numero di telefono dell'utente desiderato. Fare clic su **Applica**, quindi su **OK**.
   - Se si desidera eliminare un membro da una chiamata di gruppo, nella struttura dei menu selezionare **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** e infine il membro desiderato della chiamata di gruppo ((membro del gruppo) telefono nome). Fare clic sulla scheda **Cancella membro**. Fare clic su **Cancella** quindi su **OK**.

Concetti correlati

Chiamata di gruppo alla pagina 680

15.1.5.8 Come disattivare o attivare il rifiuto dell'avviso di chiamata per i membri del gruppo

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Navigare nella struttura dei menu in **Utente** > **Utente** > **…** fino all'utente desiderato (Indice - Numero di telefono - Nome).
4) Fare clic sulla scheda **Modifica i flag dell'utente**.
5) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione Rifiuto dell'avviso di chiamata, selezionare la casella di controllo **Rifiuto dell'avviso di chiamata in attesa**.
   - Per disattivare la funzione Rifiuto dell'avviso di chiamata, deselezionare la casella di controllo **Rifiuto dell'avviso di chiamata in attesa**.

   Nota: Se un gruppo viene configurato come gruppo Posto operatore, tutti i numeri che contiene vengono impostati automaticamente con l'opzione "Rifiuto dell'avviso di chiamata in attesa" su "false". Questo è valido anche per eventuali nuovi membri del gruppo Posto operatore. L'utente può impostare manualmente "Rifiuto dell'avviso di chiamata in attesa" su "true" per membri del gruppo Posto operatore allo scopo di attivare il tono di occupato per questi membri, ma non si tratta del comportamento predefinito.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Chiamata di gruppo alla pagina 680

15.2 Configurazione team / Gruppo team e Direttore/Segretaria / Gruppo Top

Una Configurazione team / Gruppo Team fornisce pratiche funzioni per i team. I numeri di telefono di tutti i membri del team vengono impostati tramite tasti MULAP (tasti di linea). In questo modo, ogni membro del team ha accesso a tutte le linee (ad esempio per la funzione risposta per assente) e può telefonare contemporaneamente su più linee. Un Direttore/Segretaria / Gruppo Top offre pratiche funzioni per le funzioni di direttore e segretaria (funzioni Top) per un massimo di tre direttori e tre segretari(e).

Nota: Durante la creazione di un MULAP dalle opzioni Team/ Top in WBM / Manager E non è consentito immettere numeri che iniziano con ** o ***.

15.2.1 Configurazione team / gruppo Team

In un telefono che dispone di funzioni per i team, il numero dell'utente e quelli degli altri membri del team vengono programmati su tasti MULAP (Multiple Line Appearance). Ciascun membro del team ha accesso a tutte le linee (ad es. risposta per assente/alle chiamate) e può telefonare contemporaneamente su più linee. A tale scopo vengono programmati tasti di chiamata diretta che consentono di eseguire direttamente le chiamate ai membri del team.

Tramite i tasti MULAP i membri del team possono accedere ai numeri di telefono di tutti i membri.Una chiamata in arrivo per un membro del team può ricevere risposta anche da tutti gli altri membri premendo il tasto MULAP lampeggiante.È inoltre possibile alternare fra più linee.Premendo un tasto MULAP un membro del team può indirizzare una chiamata uscente sulla linea corrispondente. Il destinatario può vedere il numero di tale linea sul display del proprio telefono.

Le chiamate in arrivo vengono segnalate contemporaneamente a tutti i membri del team visivamente, tramite i LED dei tasti MULAP. Per ciascun membro del team inoltre viene indicato se le chiamate in entrata devono essere segnalate anche acusticamente.

Tramite un tasto di chiamata di gruppo ciascun membro del team può scegliere se attivare la segnalazione delle chiamate in arrivo per singola linea.

Un amministratore con il profilo **Advanced** può configurare fino a tre utenti per configurazione team/gruppo Team tramite la procedura guidata **Configurazione team**. In **Modalità esperti**, un amministratore con il profilo **Expert** può configurare fino a dieci utenti per configurazione team/gruppo Team.

Un utente singolo può appartenere contemporaneamente a più gruppi. Quanto segue si applica ai gruppi di tipo Chiamata di gruppo, Gruppo di ricerca, Configurazione team/Gruppo team e Direttore/Segretaria / Gruppo Top: La somma di tutte le adesioni degli utenti a questi gruppi non deve superare 32.

A ciascuna configurazione team/gruppo Team è possibile assegnare un nome di massimo 16 caratteri.

Quando si definisce una configurazione team/gruppo Team, ai membri vengono assegnate le seguenti caratteristiche (le impostazioni possono essere modificate da un amministratore con il profilo **Expert** in **Modalità esperti**):

- **Master**

  Questo parametro trasforma un utente in un master della configurazione team/gruppo Team. Se il master attiva una linea questa vale per tutti i membri (telefoni) della configurazione team/gruppo Team.

  Impostazione predefinita: Master è il primo membro della configurazione team/gruppo Team.
- **Chiamata acustica**

  Se questo parametro è attivato, le chiamate in arrivo vengono segnalate acusticamente.

  Impostazione predefinita: parametro attivato.

- **Impegno automatico in uscita**

  Se questo parametro è attivato, sollevando il ricevitore la chiamata avviene automaticamente tramite la linea MULAP del membro. Se il parametro è disattivato, l'utente deve utilizzare il tasto MULAP prima della composizione.

  Impostazione predefinita: parametro attivato.
- **Nessuna risposta automatica in entrata**

  Se questo parametro è attivato non è possibile rispondere a una chiamata in arrivo semplicemente sollevando il ricevitore. È infatti necessario premere anche il tasto MULAP.

  Impostazione predefinita: parametro non attivato.
- **Rilascio automatico conferenza**

  Se il parametro è attivato, premendo il tasto MULAP la linea MULAP viene rilasciata per una conferenza. Questo stato viene segnalato a tutti gli altri membri dal lampeggiare del tasto MULAP. Premendo il tasto MULAP è possibile accedere alla conferenza.

  Impostazione predefinita: parametro non attivato.
- **Tasto MULAP configurato**

  Se il parametro è attivato, sul telefono viene configurato un tasto MULAP. Premendo il tasto l'impegno in uscita avviene sulla linea MULAP del master. L'utente chiamato visualizza il numero di telefono MULAP del master sul display.

  Impostazione predefinita: parametro non attivato.

Utilizzo dei tasti MULAP

Ciascun membro del team è assegnato alla propria linea (linea MULAP). La propria linea e quelle di tutti gli altri membri sono configurate come tasti MULAP (di linea). Quindi ciascun membro del team può utilizzare tutte le linee MULAP disponibili.

Il LED di un tasto MULAP è associato ai significati seguenti:

- spento: la linea corrispondente è libera e può essere utilizzata.
- acceso: la linea corrispondente è occupata.
- lampeggio veloce: chiamata sulla linea corrispondente.
- lampeggio lento: conversazione in attesa sulla linea corrispondente.

Utilizzo dei tasti di chiamata diretta

Ciascun membro del team dispone di un tasto di chiamata diretta per tutti gli altri membri del team. In questo modo i membri del team sono reciprocamente raggiungibili semplicemente premendo un tasto.

Il tasto Chiamata diretta può essere utilizzato anche per trasferire rapidamente una conversazione in corso al membro Team qui impostato.

Il LED di un tasto di chiamata diretta è associato ai significati seguenti:

- spento: il membro del team corrispondente non sta telefonando.
- acceso: il membro del team corrispondente sta telefonando o ha attivato la funzione Non disturbare.
- lampeggio veloce: il membro del team corrispondente chiama. È possibile rispondere alla chiamata premendo il tasto di chiamata diretta.

- lampeggio lento: il membro del team corrispondente viene chiamato e non sta rispondendo alla chiamata. È possibile rispondere alla chiamata premendo il tasto di chiamata diretta.

Tipo chiam.

Per ogni configurazione team/gruppo Team, l'amministratore con il profilo **Expert** può definire un segnale acustico all'arrivo delle chiamate esterne impostando il tipo di chiamata.Sono disponibili le seguenti opzioni:

- Tono di chiamata doppio (Impostazione predefinita)
- Tono di chiamata triplo
- Tono di chiamata breve/lungo/breve

Nei telefoni analogici è disponibile solamente l'impostazione predefinita. Le modifiche non hanno alcun effetto.

Casella fax per configurazione team/gruppo Team

Per ogni Configurazione team/gruppo Team è possibile configurare una casella fax, tramite la quale i membri del gruppo potranno ricevere messaggi fax direttamente tramite myPortal for Desktop o myPortal for Outlook.

Se per il master (il primo membro del gruppo) della configurazione team/gruppo Team è già stata configurata una casella fax, tale casella viene importata nelle impostazioni della configurazione team/gruppo Team. Eventuali caselle fax già configurate per gli altri membri verranno cancellate.

Allo scioglimento di una configurazione team/gruppo, solo il master originario (il primo membro) potrà utilizzare la casella fax.

Ordinazione di dispositivi per membri Mulap

I telefoni SIP possono essere integrati in un MULAP di base, a condizione che un dispositivo TDM/HFA sia stato definito come primo membro del MULAP di base. I telefoni IP possono essere integrati in un MULAP di base, a condizione che un TDM/HFA sia stato definito come primo membro del MULAP di base.

Possono essere integrati, ad esempio i telefoni cellulari dual mode configurati come utente Mobility Entry. I telefoni cellulari dual-mode supportano sia reti GSM/UMTS che WLAN. Tramite WLAN è possibile registrare un telefono cellulare dual mode come utente IP (client SIP) del sistema di comunicazione.

Gli utenti in mobilità, compresi gli utenti in mobilità GSM, Unify Phone e i client di Microsoft Teams, possono essere integrati in un MULAP di base, purché sia stato definito un dispositivo TDM/HFA come primo membro del MULAP di base.

Nota: La descrizione estesa di cui sopra si applica a entrambi i sistemi OpenScape Business X e OpenScape Business S, ma si limita a Team e Basic Mulap, e non a sottocapitoli con diciture simili come Executive/Secretary/Top Group.

Suggerimento: Nei telefoni SIP non è possibile programmare i tasti MULAP. Oltre a ciò non è possibile attivare o disattivare alcun servizio tramite codice. I messaggi a display specifici del MULAP di base non sono supportati.

Nota: I telefoni high end, come il CP 400/600/600E/700/700X/710, conservano le proprie voci del diario e hanno la capacità di presentare più informazioni. Ma per quanto riguarda le configurazioni di gruppo si basano sui dati di sistema poiché i gruppi sono configurati sul sistema e non sui telefoni. Di conseguenza, le informazioni sui gruppi potrebbero non essere visualizzate nelle voci del diario poiché seguono le limitazioni e la configurazione del sistema.

Dipendenze

Argomento	Dipendenza
Inoltro di chiamata	Un membro del team ha attivato l'inoltro delle chiamate per tutte le chiamate. In questo caso, tutte le chiamate dirette al proprio numero vengono deviate.
Non disturbare	Se il membro del team attiva la funzione Non disturbare, le chiamate in arrivo non vengono presentate/passate. **Nota:** Un intero team è occupato solo se tutti i membri del team hanno attivato la funzione Non disturbare.
Telefoni ISDN	Non è possibile integrare telefoni ISDN in una configurazione team/gruppo Team.
Linea di gruppo/di ricerca	Non è possibile integrare master Basic/Direttore MULAP in una configurazione team / gruppo Team.

Concetti correlati

Chiamata diretta alla pagina 632

Attività correlate

Come aggiungere la configurazione team / gruppo Team alla pagina 709
Come modificare la configurazione team / gruppo Team alla pagina 711
Come eliminare la configurazione team / gruppo Team alla pagina 711
Come aggiungere o cancellare un membro dalla configurazione team / gruppo Team alla pagina 715
Come modificare un membro della configurazione team / gruppo Team alla pagina 716
Come modificare le proprietà dei membri di un gruppo Team alla pagina 716
Come modificare l'assegnazione tasti sul telefono per configurazione team / gruppo Team alla pagina 717
Come aggiungere la casella fax alla configurazione team / gruppo Team alla pagina 717

15.2.2 Direttore/Segretaria / Gruppo Top

I gruppi Top si possono configurare quando sono necessarie funzioni Direttore e Segretaria (funzioni Top) di facile uso.

Le funzioni direttore/segretaria possono essere configurate in gruppi con massimo tre direttori e tre segretarie.

Suggerimento: Le formule "Direttore" e "Segretaria" sono valide anche per gruppi con più direttori e segretarie. Nel presente testo per "Direttore" si intende anche "Direttrice" e per "Segretaria" si intende anche "Segretario".

Ciascun membro top (direttore o segretaria) è associato a una propria linea, la cosiddetta linea MULAP (Multiple Line Appearance). Per ciascun membro Top, la propria linea e quelle di tutti gli altri membri sono configurate come tasti MULAP (di linea). Il numero MULAP viene visualizzato sul display dell'utente chiamato per le chiamate in uscita tramite la linea Direttore MULAP. La segretaria può effettuare chiamate utilizzando la propria linea MULAP o quella del direttore o delle altre segretarie. Se viene creata una connessione per un direttore, è possibile utilizzare la linea MULAP di quel direttore.

Vengono quindi programmati tasti di chiamata diretta tramite i quali il direttore può chiamare la segretaria e viceversa.

Le chiamate in arrivo vengono segnalate contemporaneamente a tutti i membri top visivamente, tramite i LED dei tasti MULAP. Per ciascun membro top inoltre viene indicato se le chiamate in entrata devono essere segnalate anche acusticamente. Viene emessa quindi la segnalazione acustica in base al tasto di commutazione chiamata.

Tramite un tasto di commutazione chiamata è possibile commutare la segnalazione delle chiamate in arrivo. Le chiamate in arrivo vengono segnalate al direttore o alla segretaria. Se il direttore preme il tasto di commutazione, le chiamate in arrivo vengono inoltre visualizzate in una finestra popup. È possibile rispondere alla chiamata solo tramite l'apposito tasto sul telefono, ma non utilizzando la finestra popup.

I telefoni della segretaria possono essere esclusi e reintegrati nella configurazione Direttore/Segretaria / gruppo Top grazie a un tasto chiamata di gruppo. La segnalazione delle chiamate ha la priorità.

Suggerimento: Se la segretaria si esclude dalla configurazione Direttore/Segretaria / gruppo Top tramite l'apposito tasto, senza attivare l'inoltro chiamate per il direttore, tutte le chiamate in arrivo non verranno segnalate né al direttore né alla segretaria.

Un direttore con il profilo **Advanced** può impostare fino a due direttori e fino a due segretarie per configurazione Direttore/Segretaria / gruppo Top utilizzando la procedura guidata **Direttore/Segretaria**. Un direttore con il profilo **Expert** può impostare fino a tre direttori e fino a tre segretarie per configurazione Direttore/Segretaria / gruppo Top entrando in **Modalità esperti**.

Per ogni Direttore si possono configurare fino a tre telefoni e per ogni Segretario fino a due.

Un utente singolo può appartenere contemporaneamente a più gruppi. Quanto segue si applica ai gruppi di tipo Chiamata di gruppo, Gruppo di ricerca, Configurazione team/Gruppo team e Direttore/Segretaria / Gruppo Top: La somma di tutte le adesioni degli utenti a questi gruppi non deve superare 32.

A ciascuna configurazione Direttore/Segretaria / gruppo Top è possibile assegnare un nome di massimo 16 caratteri.

Quando si definisce una configurazione Direttore/Segretaria / gruppo Top, ai membri vengono assegnate le seguenti caratteristiche (le impostazioni possono essere modificate da un amministratore con il profilo **Expert** in **Modalità esperti**):

- **Master**

  Questo parametro assegna a un membro le funzioni di Direttore. Sollevando il ricevitore le chiamate vengono indirizzate automaticamente tramite la linea MULAP di questo membro. Di norma le chiamate in arrivo sul numero Direttore MULAP corrispondente vengono segnalate solo visivamente.

  Impostazione predefinita: le funzioni Direttore vengono assegnate a tutte le configurazioni Direttore/Segretaria / gruppo Top.
- **Chiamata acustica**

  Se questo parametro è attivato, le chiamate in arrivo vengono segnalate acusticamente.

  Impostazione predefinita: il parametro è attivato per tutti i membri con funzione Segretaria.
- **Impegno automatico in uscita**

  Se questo parametro è attivato, sollevando il ricevitore la chiamata avviene automaticamente tramite la linea MULAP del membro. Se il parametro è disattivato, l'utente deve utilizzare il tasto MULAP prima della composizione.

  Impostazione predefinita: il parametro è attivo per tutti i membri.
- **Nessuna risposta automatica in entrata**

  Se questo parametro è attivato non è possibile rispondere a una chiamata in arrivo semplicemente sollevando il ricevitore. È infatti necessario premere anche il tasto MULAP.

  Impostazione predefinita: parametro non attivato.
- **Rilascio automatico conferenza**

  Se il parametro è attivato, premendo il tasto MULAP la linea MULAP viene rilasciata per una conferenza. Questo stato viene segnalato a tutti gli altri membri dal lampeggiare del tasto MULAP. Premendo il tasto MULAP è possibile accedere alla conferenza.

  Impostazione predefinita: parametro non attivato.
- **Tasto MULAP configurato**

  Se il parametro è attivato, sul telefono viene configurato un tasto MULAP. Premendo il tasto l'impegno in uscita avviene sulla linea Direttore MULAP. Il numero di telefono del Direttore MULAP viene visualizzato sul display dei chiamati.

  Impostazione predefinita: parametro attivato.

Utilizzo del tasto MULAP

Ciascun membro Top è assegnato alla propria linea (linea MULAP). Per ciascun membro Top, la propria linea e quelle di tutti gli altri membri sono configurate come tasti MULAP (di linea). Quindi ciascun membro Top può utilizzare tutte le linee MULAP disponibili.

Il LED di un tasto MULAP è associato ai significati seguenti:

- spento: la linea corrispondente è libera e può essere utilizzata.
- acceso: la linea corrispondente è occupata.
- lampeggio veloce: chiamata sulla linea corrispondente.
- lampeggio lento: conversazione in attesa sulla linea corrispondente o linea rilasciata per una conferenza.

Utilizzo dei tasti di chiamata diretta

Ciascun membro Top dispone di un tasto di chiamata diretta per tutti gli altri membri Top. In questo modo i membri Top sono reciprocamente raggiungibili semplicemente premendo un tasto.

Il tasto Chiamata diretta può essere utilizzato anche per trasferire rapidamente una conversazione in corso al membro Top qui impostato.

Il LED di un tasto di chiamata diretta è associato ai significati seguenti:

- Disattivato: il membro Top corrispondente non sta telefonando.
- acceso: il membro Top corrispondente sta telefonando o ha attivato la funzione Non disturbare.
- lampeggio veloce: il membro Top corrispondente chiama. È possibile rispondere alla chiamata premendo il tasto di chiamata diretta.
- lampeggio lento: il membro Top corrispondente viene chiamato e non sta rispondendo alla chiamata. È possibile rispondere alla chiamata premendo il tasto di chiamata diretta.

Tipo chiam.

Per ogni configurazione Direttore/Segretaria / gruppo Top, un amministratore con il profilo **Expert** può definire un segnale acustico all'arrivo delle chiamate esterne impostando il tipo di chiamata. Sono disponibili le seguenti opzioni:

- Tono di chiamata doppio (Impostazione predefinita)
- Tono di chiamata triplo
- Tono di chiamata breve/lungo/breve

Nei telefoni analogici è disponibile solamente l'impostazione predefinita. Le modifiche non hanno alcun effetto.

Caselle fax per la configurazione Direttore/Segretaria / gruppo Top

Per ogni configurazione Direttore/Segretaria / gruppo Top è possibile configurare una casella fax, mediante la quale i membri del gruppo potranno ricevere messaggi fax direttamente tramite myPortal for Desktop o myPortal for Outlook.

Se per il primo direttore della configurazione Direttore/Segretaria / gruppo Top è già stata configurata una casella fax, tale casella viene importata nelle impostazioni di tale configurazione/gruppo. Eventuali caselle fax già configurate per gli altri membri verranno cancellate.

Allo scioglimento della configurazione Direttore/Segretaria / gruppo Top, solo il primo direttore originario potrà utilizzare la sua casella fax.

Telefoni SIP

È possibile integrare telefoni SIP in una configurazione Direttore/Segretaria / gruppo Top. A tal fine, è necessario che il primo membro della configurazione (Direttore 1) Direttore/Segretaria / gruppo Top disponga di un telefono di sistema (ad esempio, telefono IP, HFA o SIP). UP0).

Possono essere integrati, ad esempio i telefoni cellulari dual mode configurati come utente Mobility Entry. I telefoni cellulari dual mode supportano sia reti GSM/UMTS che WLAN. Tramite WLAN è possibile registrare un telefono cellulare dual mode come utente IP (client SIP) del sistema di comunicazione.

Suggerimento: Nei telefoni SIP non è possibile programmare i tasti MULAP o per la chiamata diretta. Oltre a ciò non è possibile attivare o disattivare alcun servizio tramite codice. I messaggi a display specifici della configurazione Direttore/Segretaria / gruppo Top non sono supportati.

Nota: I telefoni high end, come il CP600, conservano le proprie voci del diario e hanno la capacità di presentare più informazioni. Ma per quanto riguarda le configurazioni di gruppo si basano sui dati di sistema poiché i gruppi sono configurati sul sistema e non sui telefoni. Di conseguenza, le informazioni sui gruppi potrebbero non essere visualizzate nelle voci del diario poiché seguono le limitazioni e la configurazione del sistema.

Dipendenze

Argomento	Dipendenza
Inoltro di chiamata	Un membro Top ha attivato l'inoltro delle chiamate per tutte le chiamate. In questo caso, tutte le chiamate dirette al proprio numero vengono deviate.
Non disturbare	Se il membro Top attiva la funzione Non disturbare, le chiamate in arrivo non vengono presentate/ passate.
Telefoni ISDN	Non è possibile integrare telefoni ISDN in una configurazione Direttore/Segretaria / gruppo Top.
Linea di gruppo/di ricerca	Non è possibile integrare master Basic/Direttore MULAP in una configurazione Direttore/Segretaria / gruppo Top.

Concetti correlati

Chiamata diretta alla pagina 632

Attività correlate

Come aggiungere un gruppo Direttore/Segretaria / Top alla pagina 712
Come modificare un gruppo Direttore/Segretaria / Top alla pagina 713
Come eliminare un gruppo Direttore/Segretaria / Top alla pagina 714

Come aggiungere o eliminare un membro dal gruppo Direttore/Segretaria / Top alla pagina 718
Come modificare un membro di un gruppo Direttore/Segretaria / Top alla pagina 718
Come modificare le proprietà dei membri di un gruppo Direttore/Segretaria / Top alla pagina 719
Come aggiungere la casella fax a un gruppo Direttore/Segretaria / Top alla pagina 719

15.2.3 Impostazione di funzioni Configurazione team / Gruppo Team e Direttore/Segretaria / Gruppi Top tramite procedure guidate

Diverse procedure guidate consentono di impostare in modo pratico la Configurazione team (Gruppi Team) e le funzioni Direttore/Segretaria (funzioni Top).

La procedura guidata **Configurazione team** consente di definire le configurazioni team (gruppi Team). Viene descritta la procedura nei seguenti casi configurabili tramite la procedura guidata:

- Come aggiungere la configurazione team / gruppo Team
- Come modificare la configurazione team / gruppo Team
- Come eliminare la configurazione team / gruppo Team

La procedura guidata **Direttore/Segretaria** consente di configurare con facilità le funzioni Direttore e Segretaria (funzione Top). Viene descritta la procedura nei seguenti casi configurabili tramite la procedura guidata:

- Come aggiungere un gruppo Direttore/Segretaria / Top
- Come modificare un gruppo Direttore/Segretaria / Top
- Come eliminare un gruppo Direttore/Segretaria / Top

Concetti correlati

Konfiguration von myPortal to go und Mobility Entry alla pagina 954

15.2.3.1 Come aggiungere la configurazione team / gruppo Team

La procedura guidata **Configurazione team** consente di definire configurazioni team (gruppi Team).

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Configurazione team**.
4) Fare clic su **Aggiungi** per configurare un nuovo team.

5) Dall'elenco a discesa **Primo telefono**, selezionare il numero di telefono del primo apparecchio della nuova configurazione team.
6) Fare clic su **OK & Avanti**.
7) Se non viene visualizzato alcun nome o se è necessario modificare il nome visualizzato, nel campo **Nome**, immettere il nome della nuova configurazione team.

   Nota: Il campo **Nome** sarà già precompilato con il nome del primo telefono della configurazione team, a condizione che sia stato assegnato un nome a quel telefono.
8) Nel campo **Numero interno**, inserire il numero interno della nuova configurazione team, nel caso in cui sia necessario modificare il numero interno visualizzato.

   Il campo del **Numero interno** viene già precompilato con il numero interno del primo telefono della configurazione team.

   : Se si desidera utilizzare il numero di interno 879, 890 o 891, occorre configurare l'impostazione tramite Manager E e non tramite WBM.

   ---
9) Nel campo **Interno**, immettere l'interno per la nuova configurazione team, nel caso in cui sia necessario modificare il numero interno visualizzato.

   Nota: Il campo **Interno** viene precompilato con il numero interno del primo telefono della configurazione team.
10) Nell'area **Fax**, nel campo **Numero interno**, inserire il numero interno della casella fax per la nuova configurazione team, nel caso in cui non sia visualizzato alcun numero o sia necessario modificare il numero visualizzato.

    Il campo **Numero interno** sarà già precompilato con il numero interno della casella fax del primo telefono della configurazione team, a condizione che per questo numero sia stata configurata una casella fax.
11) Nell'area **Fax**, nel campo **Numero interno**, inserire il numero interno della casella fax per la nuova configurazione team, nel caso in cui non sia visualizzato alcun numero interno o sia necessario modificare il numero interno visualizzato.

    Il campo **Interno** sarà già precompilato con il numero di selezione passante della casella fax del primo telefono della configurazione team, a condizione che per questo numero sia stata configurata una casella fax.
12) Attivare il flag **Team come membro del gruppo**.

    Il flag **Team come membro del gruppo** è configurabile solo quando il gruppo Team conta membri con lo stesso tipo di periferica, comportando la presenza di un singolo gruppo MULAP. Se il flag è attivato, il gruppo MULAP può essere aggiunto come membro in Gruppi.
13) Dall'elenco a discesa **Secondo telefono** selezionare il numero di telefono del secondo apparecchio della nuova configurazione team.
14) Dall'elenco a discesa **Terzo telefono**, selezionare il numero di telefono del terzo apparecchio della nuova configurazione team.
15) Fare clic su **OK & Avanti**.
16) Se si desidera configurare un'altra configurazione team, ripetere i passi da 4 a 15.
17) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Configurazione team / gruppo Team alla pagina 701

15.2.3.2 Come modificare la configurazione team / gruppo Team

La procedura guidata **Configurazione team** consente di modificare le configurazioni team (gruppi Team).

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Configurazione team**.
4) Fare clic su **Modifica** nella riga della configurazione team da modificare.
5) Modificare i parametri desiderati.
6) Solo con UC Smart: se necessario assegnare alla configurazione team una casella di posta:
   a) Dal menu a discesa selezionare **Tipo mailbox UC Smart** se la configurazione team deve ricevere una mailbox standard o una mailbox posto operatore (AutoAttendant).
   b) Solo con mailbox standard: se un chiamante può lasciare un messaggio nella casella vocale, selezionare la casella di controllo **Registrare**.
   c) Dall'elenco a discesa **Annuncio**, selezionare un annuncio di benvenuto.
   d) Se la password della casella vocale deve essere reimpostata, selezionare la casella di controllo **Reset password**.

   Nota: Se una casella vocale viene riconfigurata, la casella di controllo **Reset password** non deve essere selezionata. Consente di reimpostare la password per la casella vocale. In caso di riconfigurazione, l'utente deve cambiare comunque la password iniziale della casella vocale al primo accesso.
7) Fare clic su **OK & Avanti**.
8) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Configurazione team / gruppo Team alla pagina 701

15.2.3.3 Come eliminare la configurazione team / gruppo Team

La procedura guidata **Configurazione team** consente di eliminare le configurazioni team (gruppi Team).

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Configurazione team**.
4) Fare clic su **Modifica** nella riga della configurazione team da eliminare.
5) Fare clic su **Cancella dati**.
6) Fare clic su **OK** per confermare la cancellazione.
7) Fare clic su **OK & Avanti**, quindi su **Fine**.

Nota: Nelle applicazioni che utilizzano l'interfaccia CSTA (UC, OSCC, ecc.) quando si elimina un gruppo Team o un membro di tale gruppo, è necessario riavviare il sistema.

Concetti correlati

Configurazione team / gruppo Team alla pagina 701

15.2.3.4 Come aggiungere un gruppo Direttore/Segretaria / Top

La procedura guidata **Direttore / Segretaria** consente all'amministratore di configurare le funzioni Direttore e Segretaria (funzione Top).

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Direttore / Segretaria**.
4) Fare clic su **Aggiungi**, per aggiungere una nuova configurazione Direttore/ Segretaria (gruppo Top).
5) Nel campo **Nome**, indicare il nome della nuova configurazione Direttore/ Segretaria.
6) Nel relativo elenco a discesa, selezionare il numero di telefono desiderato della nuova configurazione Direttore/Segretaria.
7) Fare clic su **OK & Avanti**.
8) Nell'area **Fax**, nel campo **Numero di telefono**, inserire il numero di telefono della casella fax per la nuova configurazione Direttore/Segretaria,

nel caso in cui non sia visualizzato alcun numero o sia necessario modificare il numero visualizzato.

Il campo **Numero di telefono** sarà già precompilato con il numero di telefono della casella fax del primo Direttore della configurazione Direttore/Segretaria, a condizione che per questo telefono sia stata configurata una casella fax.

9) Nell'area **Fax**, nel campo **Selezione passante**, inserire il numero interno della casella fax per la nuova configurazione Direttore/Segretaria, nel caso in cui non sia visualizzato alcun numero interno o sia necessario modificare il numero interno visualizzato.

Il campo **Selezione passante** sarà già precompilato con il numero interno della casella fax del primo Direttore della configurazione Direttore/Segretaria, a condizione che per questo telefono sia stata configurata una casella fax.

: Se si desidera utilizzare il numero di interno 879, 890 o 891, occorre configurare l'impostazione tramite Manager E e non tramite WBM.

---

10) Selezionare una procedura per l'assegnazione dei tasti:

- Se nella prima o seconda console è necessario configurare i tasti per le funzioni Direttore/Segretaria, selezionare la casella di controllo **sulla prima/seconda console**.
- Se è necessario configurare i tasti per le funzioni Direttore/Segretaria nei primi tasti funzione liberi del telefono, selezionare la casella di controllo **sui primi tasti liberi**.

11) Fare clic su **OK & Avanti**.

12) Se si desidera definire un'altra configurazione Direttore/Segretaria, ripetere i passi da 4 a 11.

13) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Direttore/Segretaria / Gruppo Top alla pagina 705

15.2.3.5 Come modificare un gruppo Direttore/Segretaria / Top

La procedura guidata **Direttore / Segretaria** consente di modificare con facilità le funzioni Direttore e Segretaria (funzione Top).

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.

2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.

3) Fare clic su **Modifica**, per avviare la procedura guidata **Direttore / Segretaria**.

4) Nella riga della configurazione Direttore/Segretaria (gruppo Top) da modificare, fare clic su **Modifica**.

5) Modificare i parametri desiderati.
6) Solo con UC Smart: se necessario assegnare al gruppo Top una mailbox:
   a) Dal menu a discesa selezionare **Tipo casella postale UC Smart** se il gruppo Top deve ricevere una mailbox standard o una mailbox posto operatore (AutoAttendant).
   b) Solo con mailbox standard: se un chiamante può lasciare un messaggio nella casella vocale, selezionare la casella di controllo **Registrare**.
   c) Dall'elenco a discesa **Annuncio**, selezionare un annuncio di benvenuto.
   d) Se la password della casella vocale deve essere reimpostata, selezionare la casella di controllo **Reset password**.

   Nota: Se una casella vocale viene riconfigurata, la casella di controllo **Reset password** non deve essere selezionata. Consente di reimpostare la password per la casella vocale. In caso di riconfigurazione, l'utente deve cambiare comunque la password iniziale della casella vocale al primo accesso.
7) Fare clic su **OK & Avanti**.
8) Modificare le informazioni desiderate per la casella fax (**Fax**) e l'**Assegnazione tasti**.
9) Fare clic su **OK & Avanti**.
10) Fare clic su **OK & Avanti**, quindi su **Fine**.

Concetti correlati

Direttore/Segretaria / Gruppo Top alla pagina 705

15.2.3.6 Come eliminare un gruppo Direttore/Segretaria / Top

La procedura guidata **Direttore / Segretaria** consente di eliminare con facilità le funzioni Direttore e Segretaria (funzione Top).

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Direttore / Segretaria**.
4) Nella riga della configurazione Direttore/Segretaria (gruppo Top) da eliminare, fare clic su **Modifica**.
5) Fare clic su **Cancella dati**.
6) Fare clic su **OK** per confermare la cancellazione.
7) Fare clic su **OK & Avanti**, quindi su **Fine**.

Nota: Nelle applicazioni che utilizzano l'interfaccia CSTA (UC, OSCC, ecc.) quando si elimina un gruppo Direttore/

Segretaria o Top o un membro di tali gruppi, è necessario riavviare il sistema.

Concetti correlati

Direttore/Segretaria / Gruppo Top alla pagina 705

15.2.4 Impostazione di funzioni Configurazione team / Gruppo Team e Direttore/Segretaria / Gruppi Top tramite la Modalità esperti

Oltre alle possibilità di configurazione mediante procedura guidata, sono a disposizione di un amministratore con il profilo **Expert** ulteriori opzioni per l'impostazione di Configurazione team / Gruppo team e Direttore/Segretaria / Gruppo Top. A tal fine è necessario accedere alla **Modalità esperti**.

Viene descritta la procedura nei seguenti casi configurabili tramite la **Modalità esperti**:

- Come aggiungere o cancellare un membro dalla configurazione team / gruppo Team
- Come modificare un membro della configurazione team / gruppo Team
- Come modificare le proprietà dei membri di un gruppo Team
- Come modificare l'assegnazione tasti sul telefono per configurazione team / gruppo Team
- Come aggiungere la casella fax alla configurazione team / gruppo Team
- Come aggiungere o eliminare un membro dal gruppo Direttore/Segretaria / Top
- Come modificare un membro di un gruppo Direttore/Segretaria / Top
- Come modificare le proprietà dei membri di un gruppo Direttore/Segretaria / Top
- Come aggiungere la casella fax a un gruppo Direttore/Segretaria / Top

15.2.4.1 Come aggiungere o cancellare un membro dalla configurazione team / gruppo Team

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Suggerimento: La procedura guidata **Configurazione team** consente all'amministratore con il profilo **Advanced** di definire fino a tre membri (telefoni) per una configurazione team (gruppo Team). I membri aggiuntivi devono essere configurati da un amministratore con il profilo **Expert** tramite la **Modalità esperti** (vedere la descrizione seguente).

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.

3) Selezionare una delle seguenti opzioni:

- Se si desidera aggiungere un membro al gruppo Team (configurazione team), nella struttura dei menu selezionare **Chiamate in entrata** > **Team/Top** > **…** e infine il gruppo Team (configurazione team) desiderato. Fare clic sulla scheda **Aggiungi membro Team/Top**. Nell'elenco a discesa **Tipo** selezionare il Tipo di utente. Nell'elenco a discesa **N° tel.**, selezionare il numero di telefono dell'utente desiderato. Fare clic su **Applica**, quindi su **OK**.
- Se si desidera cancellare un membro dal gruppo Team (configurazione team), nella struttura dei menu selezionare **Chiamate in entrata** > **Team/Top** > **…** e infine il membro del gruppo Team (configurazione team) desiderato ((membro del gruppo) telefono nome). Fare clic sulla scheda **Cancella membro Team/Top**. Fare clic su **Cancella** quindi su **OK**.

Concetti correlati

Configurazione team / gruppo Team alla pagina 701

15.2.4.2 Come modificare un membro della configurazione team / gruppo Team

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Team/Top** > **…** fino al membro desiderato del gruppo Team (configurazione team) ((Membro gruppo) Numero telefonico Nome).
4) Fare clic sulla scheda **Modifica membro Team/Top**.
5) Modificare i parametri desiderati.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Configurazione team / gruppo Team alla pagina 701

15.2.4.3 Come modificare le proprietà dei membri di un gruppo Team

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Team/Top** > **…** fino al membro desiderato del gruppo Team (configurazione team) ((Membro gruppo) Numero telefonico Nome).
4) Fare clic sulla scheda **Modifica i parametri del gruppo Team/Top**.

5) Modificare le proprietà desiderate.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Configurazione team / gruppo Team alla pagina 701

15.2.4.4 Come modificare l'assegnazione tasti sul telefono per configurazione team / gruppo Team

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Team/Top** > **…** fino al gruppo Team (configurazione team) desiderato.
4) Fare clic sulla scheda **Modifica gruppo Team/Top**.
5) Selezionare una procedura per l'assegnazione dei tasti:
   - Se nella prima o seconda console è necessario configurare i tasti, selezionare la casella di controllo **sulla prima/seconda console**.
   - Se è necessario configurare i tasti nei primi tasti funzione liberi del telefono, selezionare la casella di controllo **sui primi tasti liberi**.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Configurazione team / gruppo Team alla pagina 701

15.2.4.5 Come aggiungere la casella fax alla configurazione team / gruppo Team

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Team/Top** > **…** fino al gruppo Team (configurazione team) desiderato.
4) Fare clic sulla scheda **Aggiungi casella fax**.
5) Nel campo **N° fax** del membro desiderato del gruppo Team (configurazione team), inserire il numero interno della casella fax.
6) Nel campo **DID fax** del membro desiderato del gruppo Team (configurazione team), inserire il numero di selezionare passante della casella fax.
7) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Configurazione team / gruppo Team alla pagina 701

15.2.4.6 Come aggiungere o eliminare un membro dal gruppo Direttore/Segretaria / Top

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Suggerimento: Con la procedura guidata **Direttore/Segretaria** l'amministratore con il profilo **Advanced** può definire fino a due direttori e fino a due segretarie per configurazione Direttore/Segretaria (gruppo Top). I membri aggiuntivi devono essere configurati da un amministratore con il profilo **Expert** tramite la **Modalità esperti** (vedere la descrizione seguente).

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Selezionare una delle seguenti opzioni:
   - Se si desidera aggiungere un membro al gruppo Top (configurazione Direttore/Segretaria), nella struttura dei menu selezionare **Chiamate in entrata** > **Team/Top** > **…** e infine il gruppo Top (configurazione Direttore/Segretaria) desiderato. Fare clic sulla scheda **Aggiungi membro Team/Top**. Nell'elenco a discesa **Tipo** selezionare il Tipo di utente. Nell'elenco a discesa **N° tel.**, selezionare il numero di telefono dell'utente desiderato. Fare clic su **Applica**, quindi su **OK**.
   - Se si desidera cancellare un membro dal gruppo Top (configurazione Direttore/Segretaria), nella struttura dei menu selezionare **Chiamate in entrata** > **Team/Top** > **…** e infine il membro del gruppo Top (configurazione Direttore/segretaria) desiderato ((membro del gruppo) telefono nome). Fare clic sulla scheda **Cancella membro Team/Top**. Fare clic su **Cancella** quindi su **OK**.

Concetti correlati

Direttore/Segretaria / Gruppo Top alla pagina 705

15.2.4.7 Come modificare un membro di un gruppo Direttore/Segretaria / Top

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Team/Top** > **…** fino al membro desiderato del gruppo Top (configurazione Direttore/segretaria) ((Membro gruppo) Numero telefonico Nome).

4) Fare clic sulla scheda **Modifica membro Team/Top**.
5) Modificare i parametri desiderati.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Direttore/Segretaria / Gruppo Top alla pagina 705

15.2.4.8 Come modificare le proprietà dei membri di un gruppo Direttore/Segretaria / Top

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Team/Top** > **…** fino al membro desiderato del gruppo Top (configurazione Direttore/segretaria) ((Membro gruppo) Numero telefonico Nome).
4) Fare clic sulla scheda **Modifica i parametri del gruppo Team/Top**.
5) Modificare le proprietà desiderate.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Direttore/Segretaria / Gruppo Top alla pagina 705

15.2.4.9 Come aggiungere la casella fax a un gruppo Direttore/Segretaria / Top

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Team/Top** > **…** fino al gruppo Top (Direttore/Segretaria) desiderato.
4) Fare clic sulla scheda **Aggiungi casella fax**.
5) Nel campo **N° fax** del membro desiderato del gruppo Top (configurazione Direttore/Segretaria), inserire il numero interno della casella fax.
6) Nel campo **DID fax** del membro desiderato del gruppo Top (configurazione Direttore/Segretaria), inserire il numero di selezione passante della casella fax.
7) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Direttore/Segretaria / Gruppo Top alla pagina 705

15.3 Basic MULAP e Direttore MULAP

Con Basic MULAP, un utente che utilizza più telefoni (ad esempio, telefono di rete fissa e cellulare) sarà raggiungibile con un numero unico. I direttori MULAP si possono configurare quando occorre utilizzare funzioni limitate Direttore e Segretaria.

15.3.1 MULAP di base

I MULAP di base possono essere configurati se un abbonato utilizza diversi telefoni (ad esempio, un telefono di rete fissa e un telefono cellulare) ma desidera essere raggiunto da un unico numero di telefono (numero di telefono MULAP di base).

Se un chiamante fa squillare il numero di telefono del MULAP di base, la chiamata viene segnalata visivamente a tutti i telefoni appartenenti al MULAP di base. L'abbonato può anche impostare se le chiamate in arrivo devono essere segnalate acusticamente per ogni singolo membro o no. Lo stato del MULAP di base cambia in occupato e gli altri chiamanti sentono il segnale di occupato quando rispondono a una chiamata.

Il numero di telefono del MULAP di base viene visualizzato sul display dell'utente chiamato per le chiamate in uscita tramite il trunk del MULAP di base.

Per ogni MULAP di base è possibile configurare fino a 20 membri.

A ciascun MULAP di base è possibile assegnare un nome contenente al massimo 16 caratteri.

Ciascuno dei telefoni degli abbonai è un membro del MULAP di base e a ogni membro possono essere assegnate le seguenti proprietà:

- **Master**

  Questo parametro trasforma un membro in un master del MULAP di base. Se un master attiva l'inoltro di chiamata, questa funzione si applica a tutti i membri (telefoni) del MULAP di base. Se il master attiva una richiamata automatica su un MULAP di base, la richiamata viene avviata non appena tutti i master sono liberi.

  Un abbonato non può essere incluso come master MULAP in gruppi di ricerca per più di 25 volte.

  Impostazione predefinita: Master è il primo membro del MULAP di base.
- **Chiamata acustica**

  Se questo parametro è attivato, le chiamate in arrivo vengono segnalate acusticamente.

  Impostazione predefinita: il parametro è attivo per tutti i master.
- **Impegno automatico in uscita**

  Se questo parametro è attivo, il trunk del MULAP di base viene chiamato automaticamente quando l'abbonato solleva il ricevitore. Se il parametro è disattivato, l'utente deve utilizzare il tasto MULAP prima della composizione.

  Impostazione predefinita: l'impegno automatico in uscita è assegnato a tutti i master.

- **Nessuna risposta automatica in entrata**

  Se questo parametro è attivato non è possibile rispondere a una chiamata in arrivo semplicemente sollevando il ricevitore. È infatti necessario premere anche il tasto MULAP.

  Impostazione predefinita: parametro non attivato.
- **Rilascio automatico conferenza**

  Se il parametro è attivato, premendo il tasto MULAP la linea MULAP viene rilasciata per una conferenza. Questo stato viene segnalato a tutti gli altri membri dal lampeggiare del tasto MULAP. Premendo il tasto MULAP è possibile accedere alla conferenza.

  Impostazione predefinita: parametro non attivato.
- **Tasto MULAP configurato**

  Se il parametro è attivato, sul telefono viene configurato un tasto MULAP. È possibile premere il tasto per configurare una chiamata in uscita attraverso il trunk del MULAP di base. Il numero del MULAP di base appare sul display dell'utente chiamato.

  Impostazione predefinita: parametro attivato.

Visualizzazione numero/nome

Quando si imposta una chiamata in uscita, viene assegnato un numero di stazione (numero di stazione locale o numero di gruppo MULAP).

Quando si risponde a una chiamata MULAP in entrata, viene assegnato il numero del gruppo MULAP.

Nel caso di chiamate a un MULAP:

- Prima di rispondere alla chiamata, sul display del chiamante viene visualizzo il nome MULAP e/o il numero MULAP chiamato.
- Dopo la risposta alla chiamata, sul display del chiamante viene visualizzo il nome della stazione e/o il numero MULAP dell'utente che risponde.
- In caso di chiamate da una stazione MULAP (tasto MULAP o preferenza), il display dell'utente chiamato e di quello che risponde mostrano sempre il nome della stazione e/o il numero MULAP.
- In generale, per gli impegni in uscita si applica quanto segue: Se una stazione effettua una chiamata utilizzando il numero della stazione locale, e la preferenza in uscita è diversa dal numero della stazione locale, il display dell'utente chiamato mostra sempre il numero della stazione della preferenza in uscita.

Utilizzo dei tasti MULAP

Il LED di un tasto MULAP può avere diversi stati con il seguente significato:

- spento: la linea corrispondente è libera e può essere utilizzata.
- acceso: la linea corrispondente è occupata.
- lampeggio veloce: chiamata sulla linea corrispondente.
- Lampeggio lento: una chiamata è in attesa sul relativo trunk o il relativo trunk è stato rilasciato per una conferenza.

Tipo chiam.

Per ogni MULAP di base, l'amministratore con il profilo **Esperto** può definire un segnale acustico all'arrivo delle chiamate esterne impostando il tipo di suoneria. Sono disponibili le seguenti opzioni:

- Tono di chiamata doppio (Impostazione predefinita)
- Tono di chiamata triplo
- Tono di chiamata breve/lungo/breve

Nei telefoni analogici è disponibile solamente l'impostazione predefinita. Le modifiche non hanno alcun effetto.

Ordinazione di dispositivi per membri Mulap

I telefoni SIP possono essere integrati in un MULAP di base, a condizione che un dispositivo TDM/HFA sia stato definito come primo membro del MULAP di base. I telefoni IP possono essere integrati in un MULAP di base, a condizione che un TDM/HFA sia stato definito come primo membro del MULAP di base.

Possono essere integrati, ad esempio i telefoni cellulari dual mode configurati come utente Mobility Entry. I telefoni cellulari dual-mode supportano sia reti GSM/UMTS che WLAN. Tramite WLAN è possibile registrare un telefono cellulare dual mode come utente IP (client SIP) del sistema di comunicazione.

Gli utenti in mobilità, compresi gli utenti in mobilità GSM, Unify Phone e i client di Microsoft Teams, possono essere integrati in un MULAP di base, purché sia stato definito un dispositivo TDM/HFA come primo membro del MULAP di base.

Nota: La descrizione estesa di cui sopra si applica a entrambi i sistemi OpenScape Business X e OpenScape Business S, ma si limita a Team e Basic Mulap, e non a sottocapitoli con diciture simili come Executive/Secretary/Top Group.

Suggerimento: Nei telefoni SIP non è possibile programmare i tasti MULAP. Oltre a ciò non è possibile attivare o disattivare alcun servizio tramite codice. I messaggi a display specifici del MULAP di base non sono supportati.

Dipendenze

Argomento	Dipendenza
Non disturbare	Se la funzione Non disturbare è attiva, le chiamate in arrivo non vengono più inoltrate.
Telefoni ISDN	Non è possibile integrare telefoni ISDN nei MULAP di base.

Attività correlate

Come aggiungere un Basic MULAP alla pagina 725
Come visualizzare o modificare il Basic MULAP alla pagina 726
Come cancellare il Basic MULAP alla pagina 727
Come aggiungere o eliminare un membro da un Basic MULAP alla pagina 727
Come modificare un membro in un gruppo Basic MULAP alla pagina 728

15.3.2 Direttore MULAP

I direttori MULAP si possono configurare quando occorre utilizzare funzioni limitate Direttore e Segretaria.

Tutti i membri di un Direttore MULAP sono raggiungibili al numero Direttore MULAP e ai propri numeri di telefono.

Suggerimento: Nel presente testo per "Direttore" si intende anche "Direttrice" e per "Segretaria" si intende anche "Segretario".

È possibile configurare fino a 20 membri per ciascun Direttore MULAP.

A ciascun Direttore MULAP è possibile assegnare un nome di massimo 16 caratteri.

Tramite il parametro descritto di seguito si definisce quali membri possono utilizzare una funzione Direttore e quali una funzione Segretaria in Direttore MULAP.

Se un chiamante seleziona il numero di telefono Direttore MULAP, la chiamata viene segnalata otticamente a tutti i telefoni Direttore MULAP corrispondenti. I membri con funzione Segretaria ricevono una segnalazione anche acustica delle chiamate in arrivo.

Il numero del Direttore MULAP viene visualizzato sul display dell'utente chiamato per le chiamate in uscita tramite la linea Direttore MULAP.

Ai membri di un Direttore MULAP possono essere assegnate le seguenti proprietà:

- **Master**

  Tramite questo parametro si possono assegnare funzioni Direttore a un membro. Sollevando il ricevitore le chiamate vengono indirizzate automaticamente tramite il numero Direttore MULAP. Le chiamate in arrivo sul numero Direttore MULAP vengono segnalate solo visivamente.

  Un utente può essere aggiunto come Master MULAP a gruppi di ricerca non più di 25 volte.

  Impostazione predefinita: le funzioni Direttore sono destinate al primo membro del Direttore MULAP.
- **Chiamata acustica**

  Se questo parametro è attivato, le chiamate in arrivo vengono segnalate acusticamente.

  Impostazione predefinita: il parametro è attivato per tutti i membri con funzione Segretaria.
- **Impegno automatico in uscita**

  Se questo parametro è attivato, sollevando il ricevitore la chiamata avviene automaticamente tramite il Direttore MULAP. Se il parametro è disattivato, l'utente deve utilizzare il tasto MULAP prima della composizione.

  Questo parametro non può essere utilizzato da membri con funzione Segretaria.

  Impostazione predefinita: il parametro è attivato per tutti i membri con funzione Direttore.

- **Nessuna risposta automatica in entrata**

  Se questo parametro è attivato non è possibile rispondere a una chiamata in arrivo semplicemente sollevando il ricevitore. È infatti necessario premere anche il tasto MULAP.

  Impostazione predefinita: parametro non attivato.
- **Rilascio automatico conferenza**

  Se il parametro è attivato, premendo il tasto MULAP la linea MULAP viene rilasciata per una conferenza. Questo stato viene segnalato a tutti gli altri membri dal lampeggiare del tasto MULAP. Premendo il tasto MULAP è possibile accedere alla conferenza.

  Impostazione predefinita: parametro non attivato.
- **Tasto MULAP configurato**

  Se il parametro è attivato, sul telefono viene configurato un tasto MULAP. Premendo il tasto l'impegno in uscita avviene sulla linea Direttore MULAP. Il numero di telefono del Direttore MULAP viene visualizzato sul display dei chiamati.

  Impostazione predefinita: parametro attivato.

Utilizzo del tasto MULAP

Il LED di un tasto MULAP è associato ai significati seguenti:

- spento: la linea corrispondente è libera e può essere utilizzata.
- acceso: la linea corrispondente è occupata.
- lampeggio veloce: chiamata sulla linea corrispondente.
- lampeggio lento: conversazione in attesa sulla linea corrispondente o linea rilasciata per una conferenza.

Tipo chiam.

Per ogni Executive MULAP, l'amministratore con il profilo **Expert** può definire un segnale acustico all'arrivo delle chiamate esterne impostando il tipo di chiamata. Sono disponibili le seguenti opzioni:

- Tono di chiamata doppio (Impostazione predefinita)
- Tono di chiamata triplo
- Tono di chiamata breve/lungo/breve

Nei telefoni analogici è disponibile solamente l'impostazione predefinita. Le modifiche non hanno alcun effetto.

Telefoni SIP

È possibile integrare telefoni SIP in un Direttore MULAP. A tal fine, è necessario che il primo membro del Direttore MULAP (Direttore 1) sia un telefono di sistema (ad esempio, un telefono HFA o UP0).

Possono essere integrati, ad esempio i telefoni cellulari dual mode configurati come utente Mobility Entry. I telefoni cellulari dual mode supportano sia reti GSM/UMTS che WLAN. Tramite WLAN è possibile registrare un telefono cellulare dual mode come utente IP (client SIP) del sistema di comunicazione.

Suggerimento: Nei telefoni SIP non è possibile programmare i tasti MULAP. Oltre a ciò non è possibile attivare o disattivare

alcun servizio tramite codice. I messaggi a display specifici del Direttore MULAP non sono supportati.

Dipendenze

Argomento	Dipendenza
Non disturbare	Dopo l'attivazione di Non disturbare, le chiamate in arrivo non vengono inoltrate.
Telefoni ISDN	Non è possibile integrare telefoni ISDN in un Direttore MULAP.

Attività correlate

Come aggiungere un Direttore MULAP alla pagina 728
Come visualizzare o modificare il Direttore MULAP alla pagina 729
Come cancellare il Direttore MULAP alla pagina 729
Come aggiungere o eliminare un membro da un Direttore MULAP alla pagina 729
Come modificare un membro di un Direttore MULAP alla pagina 730

15.3.3 Configurazione di Basic MULAP e Direttore MULAP

La configurazione di Basic MULAP e Direttore MULAP può essere eseguita esclusivamente da un amministratore con il profilo **Expert** tramite la **Modalità esperti**.

Viene descritta la procedura nei seguenti casi configurabili tramite la **Modalità esperti**:

- Come aggiungere un Basic MULAP
- Come visualizzare o modificare il Basic MULAP
- Come cancellare il Basic MULAP
- Come aggiungere o eliminare un membro da un Basic MULAP
- Come modificare un membro in un gruppo Basic MULAP
- Come aggiungere un Direttore MULAP
- Come visualizzare o modificare il Direttore MULAP
- Come cancellare il Direttore MULAP
- Come aggiungere o eliminare un membro da un Direttore MULAP
- Come modificare un membro di un Direttore MULAP

15.3.3.1 Come aggiungere un Basic MULAP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.

3) Nella struttura dei menu, fare clic su **Chiamate in entrata** > **Linea di gruppo/di ricerca**.
4) Fare clic sulla scheda **Aggiungi gruppo**.
5) Nel campo **Numero di telefono**, indicare il numero di telefono del nuovo Basic MULAP.
6) Nel campo **Interno** indicare il numero di interno del nuovo Basic MULAP.

: Se si desidera utilizzare il numero di interno 879, 890 o 891, occorre configurare l'impostazione tramite Manager E e non tramite WBM.

---

7) Nei campi **Nome** e **Cognome** indicare il nome del nuovo Basic MULAP.
8) Nell'elenco a discesa **Tipo**, selezionare **Basic MULAP**.
9) Nell'elenco a discesa **Numero di telefono**, selezionare il numero di telefono dell'utente da assegnare al gruppo Basic MULAP.
10) Fare clic su **Applica**, quindi su **OK**.

Nota: Nelle applicazioni che utilizzano l'interfaccia CSTA (UC, OSCC, ecc.), quando si crea un gruppo Basic MULAP o un membro di tale gruppo, è necessario riavviare il sistema.

Concetti correlati

MULAP di base alla pagina 720

15.3.3.2 Come visualizzare o modificare il Basic MULAP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** fino al Basic MULAP desiderato.
4) Fare clic sulla scheda **Modifica parametri gruppo**. Vengono visualizzate i valori attualmente impostati nei parametri del gruppo.
5) Se necessario, modificare i parametri desiderati del Basic MULAP.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

MULAP di base alla pagina 720

15.3.3.3 Come cancellare il Basic MULAP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** fino al Basic MULAP desiderato.
4) Fare clic sulla scheda **Cancella gruppo**.
5) Fare clic su **Cancella** quindi su **OK**.

Nota: Nelle applicazioni che utilizzano l'interfaccia CSTA (UC, OSCC, ecc.) quando si elimina un gruppo Basic MULAP o un membro di tale gruppo, è necessario riavviare il sistema.

Concetti correlati

MULAP di base alla pagina 720

15.3.3.4 Come aggiungere o eliminare un membro da un Basic MULAP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Selezionare una delle seguenti opzioni:
   - Se si desidera aggiungere un membro al Basic MULAP, nella struttura dei menu selezionare **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** e infine il Basic MULAP desiderato. Fare clic sulla scheda **Aggiungi membro**. Nell'elenco a discesa **Numero di telefono** selezionare il numero di telefono dell'utente desiderato. Fare clic su **Applica**, quindi su **OK**.
   - Se si desidera eliminare un membro dal Basic MULAP, nella struttura dei menu selezionare **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** e infine il membro del Basic MULAP desiderato ((membro del gruppo) telefono nome). Fare clic sulla scheda **Cancella membro**. Fare clic su **Cancella** quindi su **OK**.

Concetti correlati

MULAP di base alla pagina 720

15.3.3.5 Come modificare un membro in un gruppo Basic MULAP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** fino al membro desiderato del Basic MULAP ((Membro gruppo) Numero telefonico Nome).
4) Fare clic sulla scheda **Modifica membro**.
5) Modificare i parametri desiderati.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

MULAP di base alla pagina 720

15.3.3.6 Come aggiungere un Direttore MULAP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Nella struttura dei menu, fare clic su **Chiamate in entrata** > **Linea di gruppo/di ricerca**.
4) Fare clic sulla scheda **Aggiungi gruppo**.
5) Nel campo **Numero di telefono**, indicare il numero di telefono del nuovo Direttore MULAP.
6) Nel campo **Interno** indicare il numero di interno del nuovo Direttore MULAP.

: Se si desidera utilizzare il numero di interno 879, 890 o 891, occorre configurare l'impostazione tramite Manager E e non tramite WBM.

---

7) Nei campi **Nome** e **Cognome** indicare il nome del nuovo Direttore MULAP.
8) Nell'elenco a discesa **Tipo**, selezionare **Direttore MULAP**.
9) Nell'elenco a discesa **Numero di telefono**, selezionare il numero di telefono dell'utente da assegnare al gruppo Direttore MULAP.
10) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Direttore MULAP alla pagina 723

15.3.3.7 Come visualizzare o modificare il Direttore MULAP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** fino al Direttore MULAP desiderato.
4) Fare clic sulla scheda **Modifica parametri gruppo**. Vengono visualizzate i valori attualmente impostati nei parametri del gruppo.
5) Se necessario, modificare i parametri desiderati del Direttore MULAP.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Direttore MULAP alla pagina 723

15.3.3.8 Come cancellare il Direttore MULAP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** fino al Direttore MULAP desiderato.
4) Fare clic sulla scheda **Cancella gruppo**.
5) Fare clic su **Cancella** quindi su **OK**.

Nota: Nelle applicazioni che utilizzano l'interfaccia CSTA (UC, OSCC, ecc.) quando si elimina un gruppo Direttore MULAP o un membro di tale gruppo, è necessario riavviare il sistema.

Concetti correlati

Direttore MULAP alla pagina 723

15.3.3.9 Come aggiungere o eliminare un membro da un Direttore MULAP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Selezionare una delle seguenti opzioni:
   - Se si desidera aggiungere un membro come Direttore MULAP, nella struttura dei menu selezionare **Chiamate in entrata** > **Linea di gruppo/ di ricerca** > **…** e infine il Direttore MULAP desiderato. Fare clic sulla scheda **Aggiungi membro**. Nell'elenco a discesa **Numero di telefono** selezionare il numero di telefono dell'utente desiderato. Fare clic su **Applica**, quindi su **OK**.
   - Se si desidera eliminare un membro dal ruolo di Direttore MULAP, nella struttura dei menu selezionare **Chiamate in entrata** > **Linea di gruppo/ di ricerca** > **…** e infine il Direttore MULAP desiderato ((membro del gruppo) telefono nome). Fare clic sulla scheda **Cancella membro**. Fare clic su **Cancella** quindi su **OK**.

Concetti correlati

Direttore MULAP alla pagina 723

15.3.3.10 Come modificare un membro di un Direttore MULAP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** fino al membro desiderato del Basic MULAP ((Membro gruppo) Numero telefonico Nome).
4) Fare clic sulla scheda **Modifica membro**.
5) Modificare i parametri desiderati.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Direttore MULAP alla pagina 723

15.3.3.11 Come aggiungere un Basic MULAP in un gruppo

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Chiamate in entrata**.

3) Nella struttura dei menu, fare clic su Basic MULAP desiderato in **Chiamate in entrata > Linea di gruppo/di ricerca**.
4) Fare clic sulla scheda **Modifica parametri gruppo**. Vengono visualizzati i valori correntemente impostati nei parametri del gruppo.
5) Attivare il flag **MULAP come membro del gruppo**.
6) Fare clic sul gruppo desiderato nella struttura dei menu in **Chiamate in entrata > Linea di gruppo/di ricerca** per aggiungere un Basic MULAP come membro nel gruppo.
7) Fare clic sulla scheda **Aggiungi membro** e selezionare Basic MULAP dal menu a discesa nel campo **Numero di telefono**.
8) Fare clic su **Applica**, quindi su **OK**.

Limitazioni:

- Tutti i membri di Basic MULAP devono essere configurati con parametri M, R, A.
- Il numero massimo di membri del gruppo deve essere 20, compresi i membri di Basic MULAP.
- I membri di Basic MULAP non possono essere anche membri del gruppo.
- È consentito aggiungere un MULAP a:
  1) Linea con ricerca lineare
  2) Linea con ricerca ciclica
  3) Gruppo
- Non è consentito aggiungere un MULAP a:
  1) Avviso di chiamata in attesa
  2) RNA
- Un gruppo non può essere modificato in Chiamata in attesa o RNA se contiene un MULAP.

15.4 Gruppi casella vocale e gruppi fax

Attraverso un gruppo Casella vocale (segreteria telefonica) è possibile consentire l'accesso a messaggi vocali a un gruppo di utenti. Il numero di telefono del gruppo Casella vocale non consente di chiamare i membri di questo gruppo, ma di raggiungere direttamente la casella vocale (ovvero la segreteria telefonica) del gruppo. Attraverso un gruppo Casella fax (gruppo fax) è possibile consentire l'accesso a messaggi fax a un gruppo di utenti. Il numero di telefono del gruppo Casella fax consente di raggiungere direttamente la casella fax del gruppo.

15.4.1 Gruppo Casella vocale

Attraverso un gruppo Casella vocale (segreteria telefonica) è possibile consentire l'accesso a messaggi vocali a uno specifico gruppo di utenti. Il numero di telefono del gruppo Casella vocale non consente di chiamare i membri di questo gruppo, ma di raggiungere direttamente la casella vocale (ovvero la segreteria telefonica) del gruppo. Quando un messaggio vocale viene registrato nella casella vocale del gruppo, tale messaggio viene inoltrato alle caselle vocali di tutti i membri.

Tutti i membri ricevono il messaggio vocale contemporaneamente. Se un membro del gruppo cancella un messaggio vocale, tale messaggio viene cancellato anche dalle caselle vocali di tutti gli altri membri e da quella del gruppo. I messaggi vocali personali di tutti i membri non vengono influenzati.

Ciascun membro del gruppo Casella vocale è raggiungibile anche al proprio numero di telefono utente.

È possibile configurare fino a 20 membri per gruppo Casella vocale.

A ciascun gruppo Casella vocale è possibile assegnare un nome di massimo 16 caratteri.

Almeno un utente di un gruppo vocale deve disporre di una licenza Voicemail.

Dipendenze

Argomento	Dipendenza
Segnalazione delle chiamate	Non è possibile utilizzare il servizio *Segnalazione delle chiamate*.

Attività correlate

Come aggiungere un gruppo Casella vocale alla pagina 733
Come visualizzare o modificare il gruppo Casella vocale alla pagina 734
Come cancellare un gruppo Casella vocale alla pagina 734
Come aggiungere o cancellare un membro dal gruppo Casella vocale alla pagina 734
Come modificare un membro del gruppo Casella vocale alla pagina 735

15.4.2 Gruppo Casella fax

Attraverso un gruppo Casella fax (gruppo fax) è possibile consentire l'accesso a messaggi fax a uno specifico gruppo di utenti. Il numero di telefono del gruppo Casella fax consente di raggiungere direttamente la casella fax del gruppo. Quando un messaggio fax viene registrato nella casella fax del gruppo, tale messaggio viene inoltrato alle caselle fax di tutti i membri.

Tutti i membri ricevono il messaggio fax contemporaneamente. Se un membro del gruppo cancella un messaggio fax, tale messaggio viene cancellato anche dalle caselle fax di tutti gli altri membri e da quella del gruppo.

Ciascun membro del gruppo Casella fax è raggiungibile anche al proprio numero di telefono utente.

È possibile configurare fino a 20 gruppi Casella fax.

A ciascun gruppo Casella fax è possibile assegnare un nome di massimo 16 caratteri.

Almeno un utente di un gruppo fax deve disporre di una licenza fax.

Attività correlate

Come configurare un gruppo Casella fax alla pagina 735
Visualizzare o modificare il gruppo Casella fax alla pagina 736
Come aggiungere o cancellare un membro dal gruppo Casella fax alla pagina 737

15.4.3 Configurazione di gruppi casella vocale e gruppi casella fax

La configurazione di gruppi casella vocale e di gruppi casella fax può essere eseguita esclusivamente da un amministratore con il profilo **Expert** tramite la **Modalità esperti**.

Viene descritta la procedura nei seguenti casi configurabili tramite la **Modalità esperti**:

- Come aggiungere un gruppo Casella vocale
- Come visualizzare o modificare il gruppo Casella vocale
- Come cancellare un gruppo Casella vocale
- Come aggiungere o cancellare un membro dal gruppo Casella vocale
- Come modificare un membro del gruppo Casella vocale
- Come configurare un gruppo Casella fax
- Visualizzare o modificare il gruppo Casella fax
- Come cancellare un gruppo casella fax
- Come aggiungere o cancellare un membro dal gruppo Casella fax

15.4.3.1 Come aggiungere un gruppo Casella vocale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Nella struttura dei menu, fare clic su **Chiamate in entrata** > **Linea di gruppo/di ricerca**.
4) Fare clic sulla scheda **Aggiungi gruppo**.
5) Nel campo **Numero di telefono**, indicare il numero di telefono del nuovo gruppo Casella vocale.
6) Nel campo **Interno**, indicare il numero di selezione passante del nuovo gruppo Casella vocale.

   : Se si desidera utilizzare il numero di interno 879, 890 o 891, occorre configurare l'impostazione tramite Manager E e non tramite WBM.

7) Nel campo **Nome**, indicare il nome del nuovo gruppo Casella vocale.
8) Nell'elenco a discesa **Tipo**, selezionare la voce **Segreteria telefonica**.
9) Nell'elenco a discesa **Numero di telefono**, selezionare il numero di telefono dell'utente da assegnare al nuovo gruppo Casella vocale.
10) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Gruppo Casella vocale alla pagina 731

15.4.3.2 Come visualizzare o modificare il gruppo Casella vocale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** fino al gruppo Casella vocale desiderato.
4) Fare clic sulla scheda **Modifica parametri gruppo**. Vengono visualizzate i valori attualmente impostati nei parametri del gruppo.
5) Se necessario, modificare i parametri desiderati del gruppo Casella vocale.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Gruppo Casella vocale alla pagina 731

15.4.3.3 Come cancellare un gruppo Casella vocale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** fino al gruppo Casella vocale desiderato.
4) Fare clic sulla scheda **Cancella gruppo**.
5) Fare clic su **Cancella** quindi su **OK**.

Concetti correlati

Gruppo Casella vocale alla pagina 731

15.4.3.4 Come aggiungere o cancellare un membro dal gruppo Casella vocale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Selezionare una delle seguenti opzioni:
   - Se si desidera aggiungere un membro al gruppo casella vocale, nella struttura dei menu selezionare **Chiamate in entrata** > **Linea di gruppo/**

di ricerca > **…** e infine il gruppo casella vocale desiderato. Fare clic sulla scheda **Aggiungi membro**. Nell'elenco a discesa **Numero di telefono** selezionare il numero di telefono dell'utente desiderato. Fare clic su **Applica**, quindi su **OK**.

- Se si desidera eliminare un membro dal gruppo casella vocale, nella struttura dei menu selezionare **Chiamate in entrata** > **Linea di gruppo/ di ricerca** > **…** e infine il membro del gruppo casella vocale desiderato ((membro del gruppo) telefono nome). Fare clic sulla scheda **Cancella membro**. Fare clic su **Cancella** quindi su **OK**.

Concetti correlati

Gruppo Casella vocale alla pagina 731

15.4.3.5 Come modificare un membro del gruppo Casella vocale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **Linea di gruppo/di ricerca** > **…** fino al membro desiderato del gruppo Casella vocale ((Membro gruppo) Numero telefonico Nome).
4) Fare clic sulla scheda **Modifica membro**.
5) Modificare i parametri desiderati.
6) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Gruppo Casella vocale alla pagina 731

15.4.3.6 Come configurare un gruppo Casella fax

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Nella struttura dei menu fare clic su **Utente** > **Applicazioni UC** > **Gruppo fax**. Vengono visualizzati i gruppi casella fax già configurati.
4) Selezionare la riga libera successiva e immettere nel campo **Numero di telefono** il numero di telefono del nuovo gruppo casella fax.

5) Nel campo **Interno**, indicare il numero di interno del nuovo gruppo Casella fax.

: Se si desidera utilizzare il numero di interno 879, 890 o 891, occorre configurare l'impostazione tramite Manager E e non tramite WBM.

6) Nel campo **Nome**, indicare il nome del nuovo gruppo Casella fax.
7) Nell'elenco a discesa **Tipo**, selezionare la voce **Gruppo fax**.
8) Fare clic su **Applica**, quindi su **OK**.
9) Chiudere la finestra **Gruppo fax**.
10) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
11) Fare clic su **Gruppi**.
12) Click on the **Fax Group** tab.
13) Selezionare il nuovo gruppo Casella fax e fare clic su **Modifica**.
14) Selezionare una delle seguenti opzioni:
    - Se si desidera aggiungere un membro al gruppo Casella fax, selezionare il membro desiderato nell'elenco **Utenti**.
    - Se si desidera aggiungere più membri al gruppo Casella fax, premere <Ctrl> e selezionare i membri desiderati nell'elenco **Utenti**.
15) Fare clic su **Salva**.

Concetti correlati

Gruppo Casella fax alla pagina 732

15.4.3.7 Visualizzare o modificare il gruppo Casella fax

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Nella struttura dei menu fare clic su **Utente** > **Applicazioni UC** > **Gruppo fax**.
4) Nella struttura dei menu fare clic sul gruppo Casella fax desiderato.
5) Fare clic sulla scheda **Modifica parametri dell'utente**.
6) Se necessario, modificare i parametri desiderati del gruppo Casella fax.
7) Fare clic su **Applica**, quindi su **OK**.

Concetti correlati

Gruppo Casella fax alla pagina 732

15.4.3.8 Come cancellare un gruppo casella fax

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Click on **Groups**.
4) Click on the **Fax Group** tab.
5) Mark the desired fax box group and click **Remove**.

15.4.3.9 Come aggiungere o cancellare un membro dal gruppo Casella fax

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) In the navigation bar, click on **Expert Mode**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Click on **Groups**.
4) Click on the **Fax Group** tab.
5) Mark the desired fax box group and click **Edit**. The **Users** list is displayed with the existing members marked in it.
6) Selezionare una delle seguenti opzioni:
   - If you want to add a member to the fax box group, press the <Ctrl> key and select the new member in addition to the already existing members in the **Users** list.
   - If you want to remove a member from the fax box group, press the <Ctrl> key and deselect the desired member in the **Users** list.
7) Fare clic su **Salva**.

Concetti correlati

Gruppo Casella fax alla pagina 732

15.5 Chiamata diretta per gruppi

La funzione di chiamata diretta per gruppi consente il paging di membri interni di un gruppo.

15.5.1 Paging interno al gruppo

La funzione di paging interno al gruppo consente la chiamata diretta di utenti interni di un gruppo. Questa funzione viene denominata anche "Paging interno". I membri del gruppo occupati o che hanno attivato Non disturbare non ricevono il paging interno. Il membro del gruppo chiamato non può fornire una risposta tramite altoparlante. Per rispondere deve sollevare il ricevitore e condurre una normale conversazione a due.

La funzione di paging interno al gruppo può essere utilizzata tramite un tasto funzione appositamente programmato, la voce di menu **Chiamata diretta**, il codice o la selezione del numero di telefono del gruppo di destinazione. Un tasto funzione può essere programmato anche per un numero telefonico di un gruppo. Utilizzando questo tasto funzione viene stabilita immediatamente la connessione alla destinazione programmata.

Dipendenze

Argomento	Dipendenza
Non disturbare	Il paging interno non si applica ai membri del gruppo che hanno attivato la funzione Non disturbare.
Telefoni ISDN, SIP	Il servizio "Paging interno al gruppo" non può essere utilizzato con telefoni ISDN o SIP.

15.5.2 Trasferta al gruppo con paging interno

In una consultazione, la trasferta con altoparlante consente di trasferire la chiamata a un gruppo. In questo modo si avvia un paging interno al gruppo. non appena un utente del gruppo solleva il ricevitore o attiva l’altoparlante e l’altro riaggancia, la chiamata passa a una conversazione a due; Per gli altri membri del gruppo la conversazione viene interrotta.

La funzione di paging interno al gruppo può essere utilizzata tramite un tasto funzione appositamente programmato, la voce di menu **Chiamata diretta**, il codice o la selezione del numero di telefono del gruppo di destinazione. Un tasto funzione può essere programmato anche per un numero telefonico di un gruppo. Utilizzando questo tasto funzione viene stabilita immediatamente la connessione alla destinazione programmata.

Dipendenze

Argomento	Dipendenza
Non disturbare	Il paging interno non si applica ai membri del gruppo che hanno attivato la funzione Non disturbare.
Telefoni ISDN, SIP	Il servizio "Trasferta al gruppo con paging interno" non può essere utilizzato con telefoni ISDN o SIP.

15.6 UCD (Uniform Call Distribution)

Grazie al servizio Uniform Call Distribution (UCD) il sistema di comunicazione consente di distribuire in modo uniforme le chiamate in arrivo a un gruppo di utenti (Gruppo UCD).

I gruppi UCD vengono impostati per tutte le Hotline tecniche (ad es. assistenza clienti), nella gestione reclami, per le ricerche di mercato, nella ricezione e registrazione degli ordini (ad es. spedizionieri, Ticket Service) o per i servizi di emergenza.

Di norma la distribuzione delle chiamate avviene in modo che una chiamata entrante per un gruppo UCD viene inoltrata all'utente (agente) da più tempo inattivo. È comunque possibile definire altre regole di distribuzione.

Se non sono disponibili agenti per rispondere a una chiamata, questa viene inoltrata automaticamente a una coda. In base alla priorità e al tempo di attesa le chiamate vengono distribuite agli agenti che si liberano.

Per le chiamate in attesa è possibile riprodurre annunci o una musica.

Configurazione

La procedura guidata **Distribuzione delle chiamate** consente di configurare gruppi e utenti per una distribuzione delle chiamate (UCD) intelligente. Viene descritta la procedura nei seguenti casi configurabili tramite la procedura guidata:

- Come configurare la distribuzione delle chiamate / gruppi UCD
- Come aggiungere / cancellare agenti UCD
- Come modificare gli annunci/ la musica su attesa per UCD

Oltre alle possibilità di configurazione mediante procedura guidata, sono a disposizione di un amministratore con il profilo **Expert** ulteriori opzioni di configurazione in **Modalità esperti**.

15.6.1 Distribuzione delle chiamate / gruppo UCD

Un gruppo UCD comprende agenti (utenti) che fanno parte di un gruppo di lavoro e sono raggiungibili a un numero di telefono specifico. Una chiamata in arrivo, interna o esterna, viene assegnata automaticamente all'agente che risulta inattivo da più tempo.

Ciascun gruppo UCD può essere configurato utilizzando WBM (**Modalità esperti**) in modo che le chiamate per un agente vengano accettate automaticamente dal sistema di comunicazione (Automatic Incoming Call Connection AICC).

Se tutti gli agenti di un gruppo UCD sono occupati, le chiamate entranti possono essere inserite in una coda. Per ciascun gruppo UCD è possibile definire singolarmente il numero massimo di chiamate nella coda. Se tale valore viene superato, le chiamate successivo possono essere inoltrate ad una destinazione di overflow (destinazione esterna, altro gruppo UCD, utente o gruppo interno).

Se questa destinazione è un altro gruppo UCD e se anche tutti gli agenti di questo gruppo sono occupati, la chiamata resta nella coda del gruppo originario e inoltre viene inserita nella coda del secondo gruppo UCD (destinazione di overflow).

Per le chiamate in attesa si può riprodurre un annuncio o una musica.

A ciascun gruppo UCD è possibile assegnare un nome di massimo 16 caratteri.

Dipendenze

Argomento	Dipendenza
Deviazione di chiamata	La deviazione di chiamata verso un gruppo ACD/ UCD non viene seguita nei seguenti casi: • Se si chiama un gruppo di ricerca linea libera e un utente con una deviazione di chiamata a un gruppo UCD è nella serie, la deviazione di chiamata non avviene. In questo caso viene chiamato direttamente l'utente successivo del gruppo di ricerca. • Un utente è membro di una chiamata a gruppo con proprietà "Gruppo" e presenta una deviazione di chiamata a un gruppo UCD • Un utente è membro di un gruppo in caso di libero. Se viene chiamato il gruppo, la deviazione di chiamata al gruppo UCD non avviene. Eccezione: il primo utente immesso presenta la deviazione di chiamata a un gruppo UCD. Questa deviazione di chiamata viene eseguita.

15.6.1.1 Come configurare la distribuzione delle chiamate / gruppi UCD

La procedura guidata **Distribuzione delle chiamate** consente di configurare la distribuzione intelligente delle chiamate per un gruppo di utenti selezionati.

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **UCD**. Viene visualizzata una lista di tutti i gruppi UCD disponibili.
4) Per configurare un gruppo UCD, fare clic su **Modifica** nella riga del gruppo UCD desiderato.
5) Nel campo **Numero di telefono**, indicare il numero di telefono del nuovo gruppo UCD.
6) Nel campo **Interno**, indicare il numero di interno del gruppo UCD.

   : Se si desidera utilizzare il numero di interno 879, 890 o 891, occorre configurare l'impostazione tramite Manager E e non tramite WBM.

7) Nel campo **Nome**, indicare il nome del gruppo UCD.

8) Fare clic su **OK & Avanti**. Viene visualizzata la finestra **Assegnazione agenti UCD**.
9) Selezionare gli ID degli agenti UCD desiderati in **Scelta** e assegnarli al gruppo UCD facendo clic su **Aggiungi**.
10) Fare clic su **OK & Avanti**. Viene visualizzata la finestra **Modifica annuncio/overflow**.
11) Dall'elenco a discesa **Risponditori**, selezionare i risponditori del gruppo UCD. È possibile scegliere fra un annuncio (se configurato) o la musica su attesa interna (Music On Hold MoH). Una volta selezionato il risponditore, viene visualizzato il campo **Ritardo annuncio**.
12) Nel campo **Ritardo annuncio**, inserire il tempo espresso in secondi trascorso il quale un chiamante in coda di attesa ascolterà un annuncio.
13) Nell'elenco a discesa **Tempo di attesa tra agenti**, selezionare il tempo trascorso il quale una chiamata deve essere inoltrata all'agente UCD successivo del gruppo UCD.
14) Nell'elenco a discesa, selezionare la **Destinazione di overflow** per il gruppo UCD. È possibile selezionare una destinazione esterna, un altro gruppo UCD, un utente interno o un gruppo.

    Se come destinazione di overflow si seleziona **Destinazione esterna**, viene visualizzato il campo **Destinazione esterna** e l'elenco a discesa **Fascio**.

    a) Nel campo **Destinazione esterna**, inserire il numero di telefono della destinazione di overflow.
    b) Quando la destinazione di overflow esterna deve essere raggiunta tramite un fascio specifico, selezionare il fascio desiderato nell'elenco a discesa **Fascio**.
15) Fare clic su **OK** per applicare le impostazioni.
16) Se si desidera configurare altri gruppi UCD, ripetere i passi da 4 a 15.
17) Fare clic su **OK & Avanti**, quindi su **Fine**.

15.6.2 Agenti UCD

Gli utenti di un gruppo UCD (Agenti) formano un gruppo di lavoro che può essere impostato ad esempio nelle Hotline tecniche o nel reparto di acquisizione/registrazione degli ordini. Tutte le chiamate in arrivo vengono ripartite in modo uniforme fra gli utenti disponibili del gruppo UCD.

L'assegnazione degli agenti ai gruppi UCD avviene in base agli ID. Un ID può essere assegnato a un solo gruppo UCD. A un agente possono essere assegnati più ID. In tal modo è possibile per un agente partecipare a più gruppi UCD. Un agente può registrarsi ed essere attivo in un solo gruppo UCD.

Per poter utilizzare in modo efficace le funzioni UCD, gli agenti devono disporre di un telefono con display, tasti funzione e cuffia.

Registrazione / Disconnessione

Un agente può registrarsi tramite il proprio ID su qualsiasi telefono (esclusi i telefoni ISDN e SIP) del sistema di comunicazione. Una volta registrato, l'agente è disponibile e, finché non esce dal sistema, resta assegnato in modo permanente al telefono. Non è possibile registrarsi su un altro telefono. Dopo la disconnessione l'agente non è più disponibile per la distribuzione delle chiamate.

Gli agenti possono richiamare le funzioni UCD (Accesso/Registrazione, Disconnessione e Modifica dello stato utente) tramite il telefono, utilizzando i tasti funzione programmati, le voci di menu specifiche o i codici corrispondenti.

Stati utente

Dopo l'accesso, l'agente si trova nello stato **disponibile**. Se necessario, un agente può modificare il proprio stato utente oppure tale stato viene modificato automaticamente in base alle attività dell'agente. Lo stato corrente viene visualizzato sul display del telefono.

Viene visualizzato quanto segue:

Visualizzazione	Significato
disponibile	L'agente è disponibile e accetta chiamate UCD.
non disponibile	L'agente è disconnesso per un breve periodo dal proprio posto di lavoro (ad es. per una pausa).
post-elaborazione	L'agente si trova nel periodo di post-elaborazione. Durante questo periodo non riceve alcuna chiamata UCD. In base alla configurazione può trattarsi di un tempo di post-elaborazione individuale (l'agente stesso definisce la lunghezza del tempo di post-elaborazione modificando il proprio stato utente) o automatico (per tutti gli agenti è previsto un tempo di post-elaborazione a seguito di una chiamata UCD).
per <UCD-Nome gruppo>	L'agente riceve una chiamata UCD.

Al termine dell'orario di lavoro l'agente si disconnette e non risulta più disponibile per le chiamate UCD. Può essere comunque ancora raggiungibile al proprio numero di telefono personale.

Se tutti gli agenti di un gruppo UCD presentano lo stato **non disponibile**, le chiamate in arrivo vengono inoltrate a una destinazione di overflow (una destinazione esterna, un altro gruppo UCD, un utente interno o un gruppo).

Se un agente non risponde alla chiamata nonostante risulti registrato e disponibile, viene automaticamente impostato dal sistema di comunicazione nello stato **non disponibile**.

Dipendenze

Argomento	Dipendenza
Deviazione di chiamata	Se un agente attiva il servizio "Deviazione di chiamata", viene disconnesso automaticamente e non risulta più disponibile per le chiamate UCD.
Telefoni ISDN, SIP	Non è possibile utilizzare i telefoni ISDN o SIP.

15.6.2.1 Come aggiungere / cancellare agenti UCD

Con la procedura guidata **Distribuzione delle chiamate** è possibile aggiungere o eliminare agenti UCD a/da un gruppo UCD.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **UCD**. Viene visualizzata una lista di tutti i gruppi UCD disponibili.
4) Per aggiungere o eliminare agenti UCD da un gruppo UCD, nella riga del gruppo UCD desiderato fare clic su **Modifica**.
5) Fare clic su **OK & Avanti** per passare alla finestra **Assegnazione agenti UCD**.
6) Selezionare una delle seguenti opzioni:
   - Se si desidera aggiungere agenti UCD, selezionare gli ID degli agenti UCD desiderati in **Scelta** e assegnarli al gruppo UCD facendo clic su **Aggiungi**.
   - Se si desidera eliminare degli agenti UCD, selezionare i **membri** desiderati ed eliminarli dal gruppo UCD facendo clic su **Elimina**.
7) Fare clic su **OK & Avanti** per confermare le impostazioni.
8) Fare clic su **OK**.
9) Se si desidera modificare gli agenti UCD di un altro gruppo, ripetere i passi da 4 a 8.
10) Fare clic su **OK & Avanti**, quindi su **Fine**.

15.6.3 Post-elaborazione

Questo servizio consente all'agente un breve periodo per procedere all'elaborazione della chiamata appena conclusa prima di essere nuovamente disponibile per l'UCD. Durante questo periodo l'agente non riceve alcuna chiamata UCD.

Viene fatta distinzione tra:

- Tempo di post-elaborazione personalizzato

  L'agente definisce la durata del periodo modificando il proprio stato utente.
- Tempo di post-elaborazione automatico

  Il servizio UCD (Uniform Call Distribution UCD) viene configurato in modo che tutti gli agenti in tutti i gruppi UCD abbiano automaticamente a disposizione un tempo di post-elaborazione dopo la conclusione di una chiamata. La definizione del tempo di post-elaborazione automatico avviene in cicli chiamata, ovvero intervalli di 5 secondi.

  Un agente può aumentare manualmente il tempo di post-elaborazione automatico modificando il proprio stato utente.

Durante il tempo di post-elaborazione un agente può essere raggiunto al proprio numero di telefono personale.

15.6.3.1 Come modificare il tempo di post-elaborazione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Nella struttura dei menu fare clic su **Chiamate in entrata** > **UCD**.
4) Fare clic sulla scheda **Modifica parametri UCD**.
5) Nell'elenco a discesa **Tempo di elaborazione (cicli)**, selezionare il tempo a disposizione di tutti gli agenti UCD per l'elaborazione. La definizione si basa su cicli chiamata, ovvero intervalli di 5 secondi.
6) Fare clic su **Applica**, quindi su **OK**.

15.6.4 Assegnazione delle chiamate in base alla priorità

Le chiamate in entrata, interne ed esterne, per un gruppo UCD possono essere assegnate in base alla priorità. Le chiamate in coda vengono assegnate agli agenti del gruppo UCD in base alla priorità e al tempo di attesa.

Una chiamata in attesa con alta priorità riceve una risposta prima rispetto a una chiamata in attesa da un tempo superiore ma con priorità inferiore. Una chiamata in attesa con bassa priorità viene inoltrata prima a una destinazione di overflow rispetto a una chiamata con priorità superiore.

Per le chiamate esterne la priorità viene determinata in base alla linea (per Canale B), indipendentemente che si tratti di linee IP o TDM.

Esempi:

- Sistema di comunicazione con collegamento ISDN primario multiplex (interfaccia S_{2M}) e connessione ISDN punto - multipunto (interfaccia S_0)

  le chiamate in entrata sul collegamento ISDN primario multiplex sono normali chiamate dei clienti. Tutti i canali B dell'interfaccia S_{2M} mantengono quindi una priorità media. per le chiamate tramite connessione ISDN punto - multipunto si tratta di chiamate urgenti quali gli ordini di parti di ricambio. Tutti i canali B dell'interfaccia S_0 mantengono quindi una priorità elevata.
- Sistema di comunicazione con connessione ISDN punto - punto a un provider di servizi telefonia Internet ITSP e una connessione ISDN punto - multipunto (interfaccia S_0)

  Le chiamate in entrata sul numero del sistema (connessione punto - punto) per la telefonia IP sono normali chiamate dei clienti. Tutti i canali B dell'interfaccia LAN mantengono quindi una priorità media. per le chiamate tramite connessione ISDN punto - multipunto si tratta di chiamate urgenti quali gli ordini di parti di ricambio. Tutti i canali B dell'interfaccia S_0 mantengono quindi una priorità elevata.

Per le chiamate interne la priorità viene impostata per tutto il sistema e risulta quindi valida per tutte le chiamate interne.

10 livelli di priorità (1 = alta, 10 = bassa) disponibili.

L'impostazione predefinita è Chiamate interne Priorità = 10 e Chiamate esterne Priorità = 1.

15.6.4.1 Come modificare la priorità delle chiamate

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Nella struttura dei menu fare clic su **Chiamate in entrata** > **UCD**.
4) Fare clic sulla scheda **Modifica parametri UCD**.
5) Nell'elenco a discesa **Priorità interna** selezionare la priorità da assegnare a tutte le chiamate interne per tutti i gruppi UCD (1 = priorità più elevata, 10 = priorità più bassa).
6) Per ciascuna linea (Canale B) del relativo elenco a discesa **Priorità**, selezionare la priorità valida per le chiamate esterne da questa linea per tutti i gruppi UCD (1 = priorità più elevata, 10 = priorità più bassa). Per ciascun canale B si può impostare una priorità specifica.
7) Fare clic su **Applica**, quindi su **OK**.

15.6.5 Accettazione automatica chiamate UCD

Con questo servizio gli agenti possono accettare le chiamate in arrivo senza ulteriori operazioni (Automatic Incoming Call Connection, AICC).

Per poter utilizzare il servizio, il telefono di un agente deve essere dotato di cuffia e tasto fine chiamata. L'agente viene avvertito tramite un tono specifico dell'arrivo di una chiamata, che viene connessa automaticamente.

Una conversazione in corso può essere interrotta da un agente tramite il tasto fine chiamata.

Per impostazione predefinita, il servizio AICC non è attivato. L'attivazione avviene per singoli gruppi ed è valida per tutti gli agenti del gruppo UCD, indipendentemente dal fatto che siano dotati di telefono con cuffia.

15.6.5.1 Come modificare l'accettazione automatica di chiamate UCD

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **UCD** > **…** fino al gruppo UCD desiderato.
4) Fare clic sulla scheda **Modifica gruppo UCD**.

5) Selezionare una delle seguenti opzioni:
   - Se si desidera che gli agenti di questo gruppo UCD rispondano alle chiamate senza ulteriori azioni, nell'elenco a discesa **AICC** selezionare la voce **sì**.
   - Se si desidera che gli agenti di questo gruppo UCD non rispondano alle chiamate senza eseguire le normali azioni (ad esempio, sollevare il ricevitore), nell'elenco a discesa **AICC** selezionare la voce **no**.
6) Fare clic su **Applica**, quindi su **OK**.

15.6.6 Coda UCD

Se tutti gli agenti di un gruppo UCD sono occupati, le chiamate entranti possono essere inserite in una coda. Per le chiamate in attesa si può riprodurre un annuncio o una musica.

Se una chiamata in coda da un tempo specifico (ciclo principale) non riceve risposta dall'agente in stato **disponibile** da più tempo, tale agente viene impostato come **non disponibile** e la chiamata viene passata al prossimo agente. Se la chiamata non riceve risposta anche da questo agente entro un tempo specifico (ciclo secondario), anche questo secondo agente viene impostato come **non disponibile**. Se tutti gli agenti sono in stato **non disponibile**, la chiamata viene inoltrata alla destinazione di overflow.

Per ciascun gruppo UCD è possibile definire il numero massimo di chiamate in attesa nella coda. Se viene superato il numero massimo di chiamate in attesa, quelle successive possono essere inoltrate a una destinazione alternativa (overflow).

Come destinazione di overflow è possibile selezionare una destinazione esterna, un altro gruppo UCD, un utente interno o un gruppo. Se questa destinazione è un altro gruppo UCD e se anche tutti gli agenti di questo gruppo sono occupati, la chiamata resta nella coda del gruppo originario e inoltre viene inserita nella coda del secondo gruppo UCD (destinazione di overflow).

Un agente può richiamare il numero di chiamate presenti nella coda del proprio gruppo UCD tramite il tasto funzione programmato, una voce di menu o un codice specifico.

Chiamate in una coda d'attesa

Il numero massimo di chiamate in entrata nella coda è 30 per per i gruppi UCD da 1 a 59 e 72 per il gruppo UCD 60.

Il numero minimo di chiamate in coda è zero. Se viene configurato zero come numero minimo, non esiste alcuna coda. Le chiamate vengono inoltrate o assegnate direttamente alla destinazione di overflow quando non sono disponibili agenti.

15.6.6.1 Come modificare la coda UCD

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **UCD** > **…** fino al gruppo UCD desiderato.
4) Fare clic sulla scheda **Modifica gruppo UCD**.
5) Nell'elenco a discesa **Ciclo prim. chiam.**, selezionare il numero di cicli di chiamate primari. La definizione si basa su cicli chiamata, ovvero intervalli di 5 secondi. Viene impostato il tempo di permanenza della chiamata in coda se non viene accettata dall'agente che risulta disponibile da più tempo. Infine la chiamata viene inoltrata al successivo agente disponibile.
6) Nell'elenco a discesa **Ciclo sec. chiam.**, selezionare il numero di cicli di chiamate secondari. La definizione si basa su cicli chiamata, ovvero intervalli di 5 secondi. Viene impostato il tempo di permanenza della chiamata in coda se non viene accettata dal successivo agente disponibile.
7) Selezionare se deve essere effettuato un Cambio di annuncio:
   - Se il chiamante che si trova in coda d'attesa deve ascoltare l'annuncio solo una volta, nell'elenco a discesa **Cambio di annuncio**, selezionare la voce **Una sola volta**.
   - Se il chiamante che si trova in coda d'attesa deve ascoltare l'annuncio ciclicamente, nell'elenco a discesa **Cambio di annuncio**, selezionare la voce **Ciclico**.
8) Nel campo **Ritardo annuncio** inserire il tempo trascorso il quale un chiamante in coda di attesa ascolterà un annuncio. Tale tempo è espresso in secondi.
9) Fare clic su **Applica**, quindi su **OK**.

15.6.7 Overflow UCD

Le chiamate UCD possono essere inoltrate a una destinazione di overflow se non ricevono risposta da alcun agente di un gruppo UCD, se non è configurata una coda, se il numero massimo di chiamate per la coda è stato raggiunto.

Nota: Il concetto di Overflow UCD definisce solo una destinazione di overflow, la seconda voce CDL. Pertanto, gli annunci vengono riprodotti solo quando la chiamata raggiunge la destinazione di overflow UCD e non per l'intero ciclo di squilli. Quando una chiamata abbandona la destinazione di overflow UCD, si attiva la musica su attesa predefinita.

Per ciascun gruppo UCD è possibile definire singolarmente il numero massimo di chiamate nella coda. Se questo numero viene superato, le chiamate successive vengono inoltrate alla destinazione di overflow.

Se non si desidera configurare una coda, è possibile impostare zero come numero massimo di chiamate in coda. In questo modo le chiamate senza risposta vengono immediatamente inoltrate alla destinazione di overflow.

Dipendenze

Argomento	Dipendenza
AutoAttendant	Non è consentito l'uso di un AutoAttendant come destinazione di overflow.

15.6.7.1 Come modificare overflow UCD

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.
3) Navigare nella struttura dei menu in **Chiamate in entrata** > **UCD** > **…** fino al gruppo UCD desiderato.
4) Fare clic sulla scheda **Modifica gruppo UCD**.
5) Nel campo **Chiam. in coda**, immettere il numero massimo di chiamate in attesa. Le chiamate aggiuntive vengono inoltrate automaticamente alla destinazione di overflow.
6) Nel campo **Tempo superam.**, immettere il tempo desiderato. Tale tempo è espresso in secondi.

   Nota: questa impostazione è rilevante solo se è collegata un'applicazione UCD esterna. Se non si risponde alla chiamata mediante l'applicazione UCD entro il periodo impostato, la chiamata viene rielaborata in base alle indicazioni di Call Management nel sistema di comunicazione.
7) Fare clic su **Applica**, quindi su **OK**.

15.6.8 Servizio notte UCD

È possibile configurare un servizio notturno individuale per ogni gruppo UCD. da parte di qualsiasi agente del gruppo UCD. Dopo l'attivazione, tutte le chiamate dirette a questo gruppo UCD vengono indirizzate alla destinazione del servizio notturno.

Come destinazione notte è possibile definire un utente interno, un altro gruppo, un annuncio/una musica su attesa, la casella vocale del sistema di comunicazione o una destinazione esterna.

Attivazione / Disattivazione

L'attivazione/la disattivazione del servizio notte UCD può avvenire tramite un tasto funzione, la voce di menu corrispondente o il codice specifico. L'attivazione consente di inserire il numero di telefono della destinazione del servizio notte desiderata.

Per informazioni sul servizio notturno del sistema di comunicazione, vedere Servizio notturno.

Dipendenze

Argomento	Dipendenza
Stato utente	L'attivazione del servizio notte UCD non modifica lo stato corrente dei singoli operatori/agenti. La disconnessione forzata degli agenti ancora connessi non viene eseguita.
Servizio notte del sistema di comunicazione	Il servizio notte UCD e quello del sistema di comunicazione possono essere attivati/disattivati in modo indipendente. Esempio: un gruppo UCD è stato definito come destinazione notte per il sistema di comunicazione. Le chiamate che raggiungono questo gruppo UCD tramite il servizio notte del sistema di comunicazione restano in questo gruppo, indipendentemente dalle impostazioni del gruppo stesso per il servizio notte.
Conversazioni in corso	Le conversazioni in corso non vengono influenzate dall'attivazione del servizio notte UCD.

15.6.9 Annunci/ Musica su attesa per UCD

Per le chiamate è possibile riprodurre musica (Musica su attesa, MoH) o annunci, se non ricevono una risposta immediata da agenti del gruppo UCD. Gli annunci possono essere assegnati in riferimento ai singoli gruppi UCD.

Le opzioni disponibili sono:

- Musica su attesa MOH

  Per le chiamate è possibile riprodurre musica da un'origine integrata nel sistema di comunicazione. È possibile caricare file con musica su attesa dal PC al sistema di comunicazione.

  Per ulteriori informazioni, vedere Musica su attesa
- Annunci

  Per le chiamate in attesa si può riprodurre un annuncio integrato. È possibile caricare ulteriori annunci dal PC al sistema di comunicazione.

  Per ulteriori informazioni, vedere Annunci

Il tempo che precede la riproduzione dell'annuncio è configurabile (**Ritardo annuncio**). Per non far riprodurre l'annuncio, impostare il valore più elevato (600 secondi). Si presuppone che la chiamata riceverà una risposta entro questo intervallo di tempo.

15.6.9.1 Come modificare gli annunci/ la musica su attesa per UCD

Con la procedura guidata **Distribuzione delle chiamate** è possibile configurare annunci e/o musica su attesa per i gruppi UCD.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **UCD**. Viene visualizzata una lista di tutti i gruppi UCD disponibili.
4) Per modificare gli annunci / la musica su attesa di un gruppo UCD, nella riga del gruppo desiderato fare clic su **Modifica**.
5) Fare clic su **OK & Avanti** finché non viene visualizzata la finestra **Modifica annunci**.
6) Dall'elenco a discesa **Risponditori** selezionare i risponditori del gruppo UCD. È possibile scegliere fra un annuncio (se configurato) o la musica su attesa interna (Music On Hold MoH). Una volta selezionato il risponditore, viene visualizzato il campo **Ritardo annuncio**.
7) Nel campo **Ritardo annuncio** inserire il tempo espressa in secondi trascorso il quale un chiamante in coda di attesa ascolterà un annuncio.
8) Fare clic su **OK** per applicare le impostazioni.
9) Se si desidera modificare gli annunci/la musica su attesa di un altro gruppo UCD, ripetere i passi da 4 a 8.
10) Fare clic su **OK & Avanti**, quindi su **Fine**.

15.6.10 Trasferimento a gruppi UCD

Le chiamate interne ed esterne possono essere trasferite a gruppi UCD. Se una chiamata non ottiene risposta entro un determinato lasso di tempo ha luogo una richiamata.

Il tempo di richiamata viene definito tramite il parametro di temporizzazione **Monitoraggio trasferta prima della risposta a un gruppo UCD**. L'impostazione predefinita prevede 300 secondi. Questa impostazione può essere modificata da un amministratore con il profilo **Expert** in **Modalità esperti**.

Dipendenze

Argomento	Dipendenza
Annunci	Nelle conversazioni esterne trasferite possono essere trasmessi degli annunci. Questo non è possibile per le conversazioni interne.
Tempo di attesa/ripresa	Per il trasferimento a gruppi UCD il tempo di attesa/ripresa è diverso rispetto a quello per il trasferimento a un utente.

15.6.10.1 Come modificare il tempo di richiamata per chiamate trasferite a gruppi UCD

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Sistema** > **Temporizzazioni**.
4) Per il parametro temporale **Controllo della trasferta senza consenso a un gruppo UCD**, inserire il tempo di richiamata (impostazione predefinita = 300 secondi). Se non si risponde alla chiamata entro questo periodo, viene effettuata una richiamata.
   a) Nell'elenco a discesa **Base**, selezionare la base temporale desiderata.
   b) Nel campo **Fattore**, inserire il valore per il quale deve essere moltiplicata la base temporale.
5) Fare clic su **Applica**, quindi su **OK**.

15.6.11 Rilascio di chiamate UCD tramite linee analogiche

Se non si risponde a chiamate UCD su linee analogiche entro il tempo prestabilito, le chiamate vengono rilasciate. In questo modo si impedisce il blocco delle linee analogiche.

Il tempo di rilascio viene definito mediante il parametro temporale **Controllo di una chiamata UCD su una linea analogica**. L'impostazione predefinita prevede 300 secondi. Questa impostazione può essere modificata in **Modalità esperti** da un amministratore con il profilo **Expert** (da 0 a 255 minuti).

15.6.11.1 Come modificare il tempo di rilascio per chiamate UCD su linee analogiche

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Sistema** > **Temporizzazioni**.
4) Per il parametro temporale **Controllo di una chiamata UCD su una linea analogica**, selezionare il tempo di rilascio desiderato (impostabile da 0 a 255 minuti, impostazione predefinita = 300 secondi). Se non si risponde alla chiamata entro questo tempo, la chiamata viene rilasciata.
   a) Nell'elenco a discesa **Base**, selezionare la base temporale desiderata.
   b) Nel campo **Fattore**, inserire il valore per il quale deve essere moltiplicata la base temporale.
5) Fare clic su **Applica**, quindi su **OK**.

16 Routing delle chiamate

Il sistema di comunicazione offre diversi modi per assegnare le chiamate a una destinazione desiderata, ad esempio le abilitazioni (Controllo della composizione), servizio giorno e notte, Least Cost Routing e servizi di controllo chiamate. Le chiamate di emergenza possono essere eseguite da qualsiasi configurazione.

16.1 Autorizzazioni (controllo della composizione)

Le autorizzazioni (controllo della composizione) regolano l'accesso dell'utente a connessioni esterne che possono generare costi.

Concetti correlati

Configurazione degli utenti alla pagina 443

16.1.1 Gruppi di abilitazione e classi di servizio

Ogni utente è assegnato a un gruppo di abilitazione in cui sono definite le abilitazioni dell'utente per le chiamate in entrata e in uscita.

Per ogni fascio, nel gruppo di abilitazione è definita una delle seguenti classi di servizio:

- **Interno**

  L'utente può fare solo telefonate interne.
- **Semiabilitato**

  L'utente può solamente rispondere a chiamate esterne.
- **Lista nr. permessi** 1-6

  L'utente può comporre solo i numeri di telefono esterni definiti nella lista nr. permessi. In caso non sia stato inserito nessun numero, si applica la semiabilitazione alla linea urbana.
- **Lista nr. vietati** da 1 6

  L'utente non può comporre i numeri di telefono esterni definiti nella lista nr. vietati. In caso non sia stato inserito nessun numero, si applica l'abilitazione alla linea urbana.
- **Abilitato**

  L’utente può ricevere ed effettuare chiamate senza restrizioni.

Alcuni dei 15 possibili gruppi di abilitazione sono assegnati a tutti i fasci con la stessa classe di servizio e sono chiamati con nomi significativi (ad esempio, gruppo di abilitazione **Internazionale** con classe di servizio **Ufficio completo** o gruppo di abilitazione **In entrata** con la classe di **Ufficio parziale**. I nomi dei gruppi di abilitazione possono essere modificati dall'amministratore.

Nota: Per impostazione predefinita, ogni utente appartiene al gruppo d'abilitazione 7. Tale impostazione può essere modificata. Inoltre ogni linea appartiene al gruppo d'abilitazione 7, ma questo aspetto non è configurabile. Pertanto il gruppo

d'abilitazione 7 non deve essere utilizzato e occorre assegnarvi un accesso senza restrizioni a ogni fascio.

Dipendenze

Argomento	Dipendenza
Destinazioni di selezione breve	Le destinazioni di selezione breve possono essere selezionate in qualsiasi momento, indipendentemente dal gruppo di abilitazione assegnato.
LCR	I gruppi di abilitazione (controllo della composizione) e l'abilitazione LCR sono diversi.
Deviazione di chiamata	In una deviazione di chiamata si applica il livello di abilitazione del chiamante.

16.1.1.1 Come modificare il nome di un gruppo di abilitazione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura ad albero fare clic su **Giorno:Gruppo di abilitazione**.

   Nota: Nella struttura ad albero è anche possibile fare clic su **Notte:Gruppo di abilitazione**, il risultato sarà lo stesso.

4) Nella struttura dei menu fare clic sul gruppo di abilitazione desiderato.
5) Fare clic sulla scheda **Modifica gruppo d'abilitazione**.
6) Nel campo **Gruppo di abilitazione** modificare il nome del gruppo di abilitazione.
7) Fare clic su **Applica**, quindi su **OK**.

16.1.1.2 Come modificare le classi di abilitazione di un gruppo di abilitazione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura ad albero fare clic su **Giorno:Gruppo di abilitazione**.
4) Nella struttura dei menu fare clic sul gruppo di abilitazione desiderato.
5) Fare clic sulla scheda **Modifica gruppo d'abilitazione**.
6) Per il servizio giorno, per ogni fascio utilizzato, dall'elenco a discesa selezionare la classe di abilitazione.

7) Se necessario, selezionare la classe di abilitazione per la **Rete** per il servizio giorno.
8) Nella struttura dei menu fare clic su **Notte:Gruppo di abilitazione**.
9) Nella struttura dei menu fare clic sul gruppo di abilitazione precedentemente modificato.
10) Fare clic sulla scheda **Modifica gruppo d'abilitazione**.
11) Per il servizio notte, per ogni fascio utilizzato, dall'elenco a discesa selezionare ora la classe di abilitazione.
12) Se necessario, selezionare anche qui l'abilitazione per la **Rete** per il servizio notte.
13) Fare clic su **Applica**, quindi su **OK**.

16.1.1.3 Come visualizzare tutti gli utenti di un gruppo di abilitazione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura ad albero fare clic su **Giorno:Gruppo di abilitazione**.

Nota: Nella struttura ad albero è anche possibile fare clic su **Notte:Gruppo di abilitazione**, il risultato sarà lo stesso.

---

4) Nella struttura dei menu fare clic sul gruppo di abilitazione desiderato.
5) Fare clic sulla scheda **Mostra membri del gruppo**. Verranno visualizzati tutti gli utenti a cui è assegnato il gruppo di abilitazione selezionato con il proprio nome e numero di telefono.

16.1.2 Liste nr. permessi e vietati

Con le liste nr. permessi e nr. vietati è possibile definire quali numeri di telefono l'utente potrà comporre e quali no.

Le liste nr. permessi contengono le sequenze di cifre ammesse all'inizio di un numero di telefono. L'utente può comporre solo i numeri di telefono esterni definiti nella lista nr. permessi. Assicurarsi che la lista comprenda anche tutti i numeri di emergenza necessari!

Le liste nr. vietati contengono le sequenze di cifre non ammesse all'inizio di un numero di telefono. L'utente non può comporre i numeri di telefono esterni definiti nella lista nr. vietati. Assicurarsi che la lista non comprenda alcun numero di emergenza!

L'**Elenco dei numeri di emergenza** è un caso speciale della lista nr. permessi. L'utente può comporre solo i numeri di telefono di emergenza contenuti in tale lista. Assicurarsi che la lista comprenda tutti i numeri di emergenza necessari!

Nelle liste non devono essere inseriti i numeri completi. Ad esempio, per permettere agli utenti di comporre numeri 0800xxx (numeri verdi), occorre

inserire qui solo `0800`. Poiché gli elenchi si riferiscono solo alle chiamate in uscita, non è necessario indicare il codice di linea urbana con il numero di telefono inserito. L'immissione del carattere `#` al primo posto della lista di un numeri non consentiti impedisce il bypass del controllo composizione per i telefoni di sistema, se una linea esterna analogica viene impegnata con il tipo di selezione DTMF e si commuta su DTMF durante la composizione.

Mediante speciali **filtri di analisi**, l'amministratore può determinare per qualsiasi lista dei numeri vietati, quali cifre non devono essere confrontate con la relativa lista dei numeri vietati. Il sistema di comunicazione nasconde l'area delle cifre prima dell'analisi del numero composto. Proibendo i caratteri `*` e `#`, gli utenti possono inserire tali caratteri per bypassare il controllo della selezione.

Limiti di configurazione

Caratteristica	Numero
Lista nr. permessi 1: estesa, 100 voci	1
Liste nr. permessi 2-6: breve, 10 voci	5
Lista nr. vietati 1: estesa, 50 voci	1
Liste nr. vietati 2-6: breve, 10 voci	5
Numero di caratteri delle voci delle liste (cifre 0 - 9 e caratteri * e #)	26

16.1.2.1 Come creare un elenco dei numeri di emergenza

Con la procedura guidata **Abilitazione** è possibile creare un elenco di numeri di emergenza per il gruppo di autorizzazione "Numeri di emergenza".

Prerequisiti

Si è connessi al WBM.

Il sistema di comunicazione è collegato a una linea urbana.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Abilitazione**.
4) Nel campo di input immettere un numero di emergenza, quindi fare clic su **Aggiungi**. Il numero di telefono viene importante nell'elenco dei numeri di telefono di emergenza.
5) Se si desidera inserire altri numeri nell'elenco dei numeri di emergenza, ripetere il passaggio precedente.
6) Fare clic più volte su **OK&Avanti** fino quando non si chiude la configurazione con **Esci**.

16.1.2.2 Come creare una lista nr. permessi e una lista nr. vietati

Con la procedura guidata **Abilitazione** è possibile creare una lista dei numeri permessi e una dei numeri vietati.

Prerequisiti

Si è connessi al WBM.

Il sistema di comunicazione è collegato a una linea urbana.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** > **Classi di autorizzazione**.
4) Fare clic su **OK & Avanti**.
5) Nel campo di input immettere un numero di telefono permesso senza il codice di accesso linea urbana, quindi fare clic su **Aggiungi**. Il numero di telefono viene inserito nella lista nr. permessi.
6) Se si desidera inserire altri numeri nella lista nr. permessi, ripetere il passaggio precedente.
7) Fare clic su **OK & Avanti**.
8) Nel campo di input immettere un numero di telefono vietato senza il codice di accesso linea urbana, quindi fare clic su **Aggiungi**. Il numero di telefono viene inserito nella lista nr. vietati.
9) Se si desidera inserire altri numeri nella lista nr. vietati, ripetere il passaggio precedente.
10) Fare clic più volte su **OK&Avanti** fino quando non si chiude la configurazione con **Esci**.

16.1.2.3 Come creare altri liste nr. permessi

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura dei menu fare clic su **Autorizzazioni** > **Liste nr.permessi**.
4) Nella struttura dei menu fare clic sulla lista dei numeri permessi desiderata.
5) Fare clic sulla scheda **Aggiungi numero di telefono**.
6) Immettere il **Numero di telefono** esterno senza codice del fascio.
7) Fare clic su **Applica**, quindi su **OK**.
8) Se si desidera aggiungere altri numeri di telefono, ripetere i passi da 6 e 7.
9) Se si desidera creare altre liste dei numeri permessi, ripetere i passaggi da 4 a 7.
10) Nella scheda **Mostra lista** è possibile visualizzare tutti i numeri telefonici della lista nr. permessi.

16.1.2.4 Come creare altre liste nr. vietati

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura dei menu fare clic su **Autorizzazioni** > **Liste nr.vietati**.
4) Nella struttura dei menu fare clic sulla lista dei numeri vietati desiderata.
5) Fare clic sulla scheda **Aggiungi numero di telefono**.
6) Immettere il **Numero di telefono** esterno senza codice del fascio.
7) Fare clic su **Applica**, quindi su **OK**.
8) Se si desidera aggiungere altri numeri di telefono, ripetere i passi da 6 e 7.
9) Se si desidera creare altre liste dei numeri vietati, ripetere i passaggi da 4 a 7.
10) Nella scheda **Mostra lista** è possibile visualizzare tutti i numeri telefonici della lista nr. vietati selezionata.

16.1.2.5 Come visualizzare tutti i numeri di telefono di una lista nr. vietati

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura dei menu fare clic su **Autorizzazioni** > **Liste nr.vietati**.
4) Nella struttura dei menu fare clic sulla Lista nr. vietati che contiene il numero desiderato.

16.1.2.6 Come visualizzare tutti i numeri di telefono di una lista nr. permessi

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura dei menu fare clic su **Autorizzazioni** > **Liste nr.permessi**.
4) Nella struttura dei menu fare clic sulla Lista nr. permessi che contiene il numero desiderato.

16.1.2.7 Come modificare i filtri di analisi per la lista dei numeri vietati

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura dei menu fare clic su **Autorizzazioni** > **Liste nr.vietati**.
4) Nella struttura dei menu fare clic sulla Lista nr. vietati che contiene il numero desiderato.
5) Fare clic sulla scheda **Modifica filtri di analisi**.
6) Nei menu a discesa **Dalla cifra** e **Alla cifra** digitare un intervallo.

   Ciò consente di configurare un intervallo all'interno del numero di telefono. La posizione iniziale dell'area viene selezionata dall'elenco a discesa **Dalla cifra**, mentre la posizione iniziale dall'elenco **Alla cifra**. .

   Il valore predefinito di ***** e **#** è inteso quale blocco di questi caratteri, in quanto * e # potrebbero essere utilizzati come caratteri "dummy" non valutati centralmente ed eviterebbero quindi il controllo della selezione. Inserendo * e # nella lista nr. vietati questi caratteri non hanno effetto e vengono valutati solo i caratteri composti.
7) Nel campo **Carattere** immettere il carattere o i caratteri che si desidera nascondere.
8) Fare clic su **Applica**, quindi su **OK**.

16.1.3 Lista nera

All'interno del sistema OpenScape Business è disponibile una lista nera che consente il blocco di chiamate in entrata da specifici numeri di chiamanti (CLI) e di chiamate senza numero del chiamante o presentazione limitata del numero del chiamante.

La lista nera supporta fino a 100 numeri con un massimo di 25 cifre in formato canonico (ad es. +4989) o in formato internazionale (ad esempio, 004989). I caratteri supportati sono le cifre da 0 9 e il carattere "+". Il carattere "+" si riferisce al prefisso internazionale che è configurato nel sistema. Deve essere sempre inserito nella prima posizione. Sono consentiti i frammenti di numeri a partire dall'inizio del numero del chiamante (CLI). Durante l'immissione di un numero nella lista nera viene eseguito un controllo logico. Il numero viene rifiutato se è già stato inserito o se è coperto da un frammento di numero.

La verifica dei numeri dei chiamanti trasmessi avviene sempre utilizzando il formato internazionale. I numeri dei chiamanti vengono convertiti nel formato internazionale in base ai dati del percorso, se vengono trasmessi in altri formati.

La lista nera viene applicata a tutte le linee gestite tramite centrale telefonica configurate nel sistema. Essa supporta più provider di telefonia/centrali telefoniche con codici di paese/area diversi.

Per ogni chiamata bloccata dalla lista nera viene creata una voce del registro eventi.

All'interno di una rete OpenScape Business, la lista nera deve essere configurata in ogni nodo connesso a provider di telefonia/centrali telefoniche, rispettivamente, nei gateway. Le chiamate interne alla rete non sono limitate dalla lista nera.

La lista nera può essere abilitata/disabilitata dall'amministratore di sistema. Inoltre, è possibile impostare un flag separato per il blocco delle chiamate anonime.

I registri di servizio contengono informazioni sui numeri chiamati bloccati. Le voci di registro che corrispondono ai numeri chiamati bloccati contengono l'EventText **!Chiamata in lista nera:**. Per trovare il numero chiamato che è stato bloccato, è necessario controllare le ultime due cifre della voce del registro. Queste cifre (in forma esadecimale) corrispondono alla posizione nella lista nera che contiene il numero bloccato. Se queste cifre sono ff, la chiamata bloccata è anonima.

Dipendenze

Le chiamate con soppressione CLI non vengono bloccate come chiamate anonime dal sistema nel caso in cui all'interno del sistema sia impostato il flag **Ignora la soppressione del numero di telefono**. In questo caso, il numero del chiamante deve essere inserito esplicitamente nella lista nera. Nelle impostazioni predefinite di fabbrica, il flag **Ignora la soppressione del numero di chiamata** è disabilitato. Esso può essere abilitato solo tramite Manager E.

La funzionalità di mobilità del sistema può essere influenzata dalla lista nera se i numeri di cellulari di utenti Mobility sono inseriti nella lista nera. In questo caso, la chiamata alla porta DISA in modalità Call Through viene bloccata dalla lista nera.

16.1.3.1 Come creare una lista nera per le chiamate in arrivo in Modalità esperti

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia > Classi di autorizzazione.**
3) Dal struttura dei menu fare clic su **Classi di autorizzazione > Lista nera**.
4) Fare clic sulla scheda **Aggiungi numero di telefono**.
5) Immettere il **Numero di telefono**.
6) Fare clic su **Applica**, quindi su **OK**.
7) Se si desidera aggiungere altri numeri di telefono, ripetere i passi da 5 e 6.

8) I numeri di chiamata aggiunti della lista nera vengono visualizzati nella scheda **Mostra lista** in **Lista nera** o in **Lista nera** nella struttura dei menu.

L'amministratore di sistema dovrebbe essere in grado di bloccare i chiamanti indesiderati in modo permanente.

- Abilitare la casella di controllo **Blocca chiamate anonime** nell'area Chiamate anonime per bloccare una chiamata in entrata anonima.

  Nota: Le chiamate anonime sono definite come le chiamate per le quali il numero del chiamante non verrà visualizzato all'utente.

- Attivare la casella di controllo **Funzione lista nera attiva** nell'area Lista nera per bloccare numeri di telefono specifici.

  Nota: La funzione di lista nera si basa solo sul numero chiamante fornito dal provider.

16.1.3.2 Come modificare/eliminare numeri di telefono nella lista nera

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Server telefonia > Classi di servizio.**

3) Dal struttura dei menu fare clic su **Classi di autorizzazione > Lista nera**.

4) Nella struttura dei menu fare clic sulla Lista nera che contiene il numero desiderato.

5) L'amministratore può modificare o eliminare la voce selezionata.

Per modificare la voce selezionata:

- Fare clic sulla scheda **Modifica numero di telefono**.
- Immettere il numero di telefono desiderato nel campo **Numero di telefono**.
- Fare clic su **Applica**, quindi su OK.

Per eliminare la voce selezionata:

- Fare clic sulla scheda **Cancella numero di telefono**.
- Immettere il numero di telefono desiderato nel campo **Numero di telefono**.
- Fare clic su **Applica**, quindi su OK.

6) L'amministratore di sistema dovrebbe essere in grado di bloccare i chiamanti indesiderati in modo permanente.

   - Abilitare la casella di controllo **Blocca chiamate anonime** nell'area **Chiamate anonime** per bloccare una chiamata in entrata anonima

     Nota: Le chiamate anonime sono definite come le chiamate per le quali il numero del chiamante non verrà visualizzato all'utente.

   - Attivare la casella di controllo **Funzione lista nera attiva** nell'area **Lista nera** per bloccare numeri di telefono specifici.

     Nota: La funzione di lista nera si basa solo sul numero chiamante fornito dal provider.

16.1.3.3 Come visualizzare i numeri di telefono nella lista nera

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Server telefonia > Classi di servizio.**
3) Dal struttura dei menu fare clic su **Classi di autorizzazione > Lista nera**.
4) I numeri di telefono sono visualizzati in **Lista nera** nella struttura dei menu o nella scheda **Mostra lista** nell'area **Lista nera**.

16.1.3.4 Come creare una lista nera per le chiamate in arrivo in Configurazione

È possibile creare una lista nera con la procedura guidata **Lista nera per chiamate in entrata**.

Prerequisiti

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Lista nera per chiamate in entrata**.
4) Nel campo di input immettere un numero di telefono permesso, quindi fare clic su **Aggiungi**. Il numero di telefono viene aggiunto alla lista nera.
5) Fare clic su OK & Avanti.
6) Se si desidera inserire altri numeri nella lista nera, ripetere i passaggi 4 e 5.

7) Se si desidera eliminare un numero di telefono, fare clic su **Elimina**.
8) Fare clic più volte su **OK&Avanti** fino quando non si chiude la configurazione con **Esci**.

16.1.4 Servizio notturno

Durante la notte, le chiamate in entrata e in uscita possono essere gestite in modo diverso rispetto al giorno. Le chiamate in entrata possono essere reindirizzate a una destinazione di servizio notte e gli utenti interni possono disporre di abilitazioni per il telefono diverse rispetto al giorno. La commutazione a livello di sistema tra il giorno e la notte viene eseguita automaticamente in un momento definito dall'amministratore.

Servizio notte pianificato

Servizio notturno variabile

Tutti i telefoni possono essere utilizzati come destinazione del servizio notturno a condizione che il relativo gruppo di abilitazione consenta le chiamate in entrata. Un telefono provvisto esclusivamente di autorizzazione interna non può essere utilizzato come destinazione del servizio notturno. Nel caso in cui per la destinazione del servizio notturno sia attivata la deviazione di chiamata, le eventuali chiamate seguiranno questa destinazione.

A un gruppo di abilitazione durante il servizio notte possono essere assegnate altre classi di abilitazione rispetto al giorno, ad esempio per evitare un abuso dell'utilizzo delle linee urbane.

Per il servizio notte è anche possibile definire un posto di rinvio diverso da quello del servizio giorno. Il posto di rinvio può essere un singolo terminale o un gruppo.

Il sistema di comunicazione attiva e disattiva il servizio notturno in base ad una pianificazione determinata dall'amministratore.

Suggerimento: Con il servizio notte pianificato valgono le regole definite per TUTTI gli utenti del sistema di comunicazione. È prevista anche una commutazione dell'abilitazione a tempo in cui tutti gli utenti sono suddivisi in gruppi (profili).

Il servizio notturno variabile viene attivato e disattivato manualmente da un utente autorizzato. Le chiamate seguono le liste di destinazione delle chiamate configurate dall'amministratore.

Per impostazione predefinita, il primo utente (il numero di telefono "100") di un sistema di comunicazione può attivare o disattivare il servizio notte. L'amministratore può autorizzare fino a cinque utenti all'attivazione e disattivazione del servizio notturno.

Servizio notte UCD

Per ogni gruppo UCD si può impostare un servizio notte personalizzato. Questo può essere attivato e disattivato indipendentemente dal servizio notturno di sistema, da parte di qualsiasi agente del gruppo UCD di distribuzione delle chiamate. Lo stato attuale dei singoli agenti e le chiamate esistenti non sono

interessate da tale servizio. Dopo l'attivazione, tutte le chiamate dirette a questo gruppo UCD di distribuzione delle chiamate vengono indirizzate alla destinazione del servizio notturno.

La destinazione del servizio notturno può essere un altro gruppo UCD di distribuzione delle chiamate, un utente interno o una destinazione esterna.

16.1.4.1 Come assegnare le abilitazioni per servizio notte manuale

La procedura guidata **Abilitazioni** consente di assegnare l'abilitazione dei singoli utenti a commutare tramite il proprio telefono il sistema di comunicazione dal servizio giorno a quello notte (e viceversa). La commutazione tra servizio giorno e notte avviene tramite telefono inserendo un codice.

Prerequisiti

Si è connessi al WBM. Il sistema di comunicazione è collegato a una linea urbana.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Abilitazione**.
4) Fare clic più volte su **OK & Avanti** fino a raggiungere la finestra **Utente abilitato per il servizio notte**.
5) Selezionare l'utente desiderato dall'elenco in **Utenti**, quindi premere **Aggiungi**. Successivamente, l'utente viene visualizzato nell'elenco **Utenti abilitati**.
6) Fare clic su **OK & Avanti**.
7) Nella finestra **Panoramica** viene visualizzato un elenco di tutti le abilitazioni assegnate.
8) Fare clic su **Fine**.

16.1.4.2 Come eliminare le abilitazioni per servizio notte manuale

La procedura guidata **Abilitazioni** consente di cancellare l'abilitazione degli utenti a commutare dal servizio giorno a quello notte.

Prerequisiti

Si è connessi al WBM. Il sistema di comunicazione è collegato a una linea urbana.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Abilitazione**.
4) Fare clic più volte su **OK & Avanti** fino a raggiungere la finestra **Utente abilitato per il servizio notte**.

5) Selezionare l'utente desiderato (di cui si desidera cancellare l'abilitazione) dall'elenco in **Utenti abilitati**, quindi premere **Elimina**.
6) Fare clic su **OK & Avanti**.
7) Nella finestra **Panoramica** viene visualizzato un elenco di tutti le abilitazioni assegnate.
8) Fare clic su **Fine**.

16.1.4.3 Come configurare il servizio notte pianificato

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura dei menu, fare clic su **Servizio notte automatico** > **Lunedì** ("Lunedì" è indicato solo a titolo di esempio, sono disponibili tutti i giorni della settimana).
4) In **Modifica zona**, selezionare una delle quattro zone possibili alla quale occorre applicare un'abilitazione specifica.
5) In **Inizio** e **Fine**, definire il tempo (in ore e minuti) per questa abilitazione.
6) In **Nr. tel. notte**, selezionare l'utente autorizzato.

   Nel campo **Servizio notte auto**, viene visualizzata l'impostazione per ogni zona.
7) Fare clic su **Applica**, quindi su **OK**.
   Quando il servizio notturno è attivo, nella pagina di destinazione del portale di amministrazione viene visualizzato il messaggio **Il sistema è correntemente in funzione in modalità notte**.

16.1.4.4 Come configurare un giorno speciale per il servizio notte pianificato

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Dal struttura dei menu fare clic su **Autorizzazioni** > **Giorni speciali**.
4) Con **>>** o **<<** selezionare l'anno per il quale si vuole impostare i giorni lavorativi.
5) Con **>>** o **<<** selezionare il mese per il quale si vuole impostare i giorni lavorativi.
6) Nel calendario fare clic sul giorno che si desidera impostare come giorno lavorativo.
7) Nel campo **Nome** indicare la denominazione del giorno lavorativo.
8) Fare clic su **Applica**, quindi su **OK**.

16.1.4.5 Come eliminare un giorno speciale per il servizio notte pianificato

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura dei menu, fare clic su **Autorizzazioni** > **Servizio notte auto** > **Giorni speciali**.
4) Fare clic su **Giorno** a sinistra del giorno lavorativo da cancellare, sul Cestino.
5) Fare clic su **Applica**, quindi su **OK**.

16.1.5 Commutazione automatica COS a tempo

Con la commutazione automatica a tempo dell'abilitazione, gli utenti vengono raggruppati in cosiddetti profili utente in cui è definito quale gruppo di abilitazione viene utilizzato in uno specifico intervallo temporale della settimana. Per ogni profilo utente può essere configurata una pianificazione.

Dipendenze

Differenze tra "commutazione automatica COS a tempo" e "servizio notte pianificato":

- La commutazione automatica dell'abilitazione a tempo si applica solo per il servizio giorno, non per quello notte.
- Raggiungimento della destinazione di chiamata tramite Gestione chiamata:

  L'istradamento viene eseguito tramite Gestione chiamate ed è indipendente dalla commutazione abilitazione automatica a tempo. Ci sono diverse liste delle chiamate per il servizio giorno e notte.
- Con il servizio notte pianificato è possibile distinguere solo fra notte e giorno e vale per TUTTI gli utenti.
- Destinazioni di rinvio

  La destinazione di rinvio è determinata solo dal servizio notte temporizzato.
- Gruppo d'abilitazione:

  Durante la notte il gruppo di abilitazione è in relazione costante (configurabile) con l'utente; la commutazione automatica COS a tempo non ha quindi alcuna influenza.

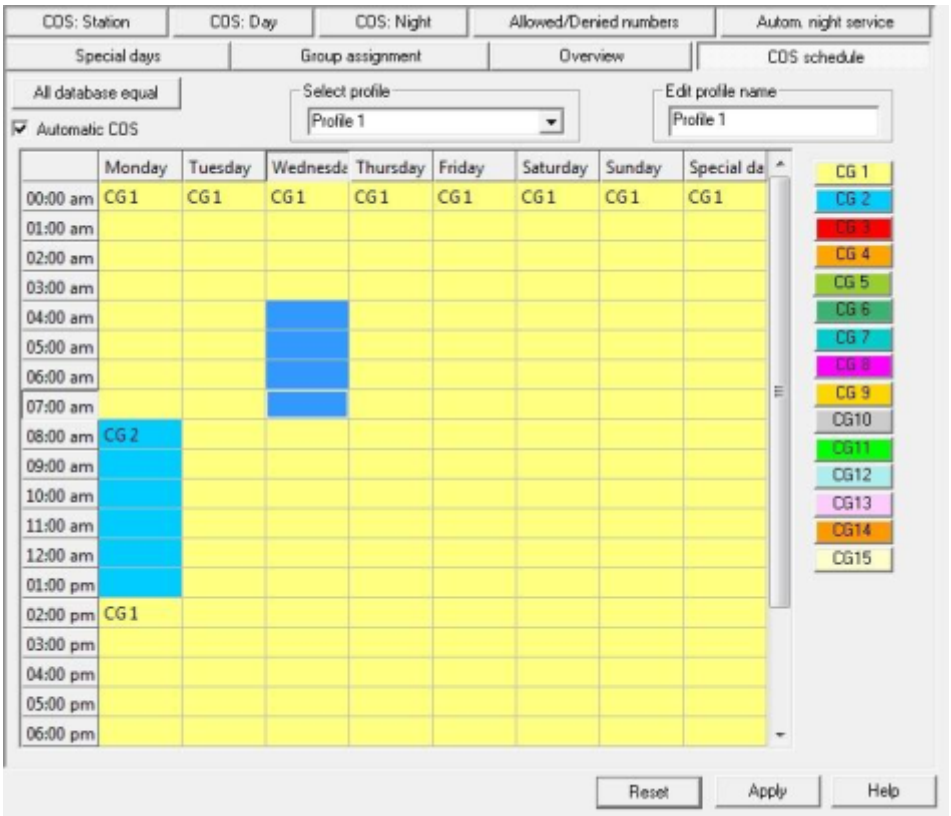
  Durante il giorno il gruppo di abilitazione può venire modificato in ore specifiche del giorno o trovarsi in una relazione fissa (configurabile) con l'utente.

Argomento	Dipendenze
Servizio notturno	Il servizio "Notte" è prioritario rispetto alla funzione "Commutazione automatica COS a tempo". Se è attivato il servizio notte, il gruppo di abilitazione viene gestito come al solito e utilizzato per il servizio notte. La pianificazione è rilevante solo durante il giorno.
Rete	La commutazione automatica dell'abilitazione (COS) e il servizio notte non sono disponibili su tutti i nodi.

16.1.5.1 Pianificazione

La pianificazione viene utilizzata per controllare le classi di abilitazioni per la commutazione automatica dell'abilitazione a tempo. È possibile configurare fino a otto commutazioni dell'abilitazione al giorno, per ogni giorno della settimana.

Ogni giorno inizia alle ore 00:00. Inserendo l'ora finale nelle singole colonne si definiscono i fusi orari. Nel seguente esempio di una pianificazione sono descritte le singole commutazioni basate sulle abilitazioni con CG2, CG4 e CG5.



Un utente può fare parte di diversi gruppi di abilitazione per giorno e notte.

Se è impostata la funzione Commutazione Automatica COS a livello di sistema per il servizio giorno, il profilo e la pianificazione determinano il gruppo di abilitazione a cui viene assegnato un utente. Durante il servizio notte, l'utente appartiene allo stesso gruppo di abilitazione a cui era stato assegnato in precedenza (mediante il servizio notte).

Per impostazione predefinita, la commutazione automatica dell'abilitazione (COS) a tempo è disattivata

Il sistema di comunicazione supporta un solo fuso orario (ora universale). I gruppi di utenti remoti che operano in diversi fusi orari sono configurati con il fuso orario del sistema di comunicazione.

La pianificazione può essere configurata solo con Manager E.

16.1.6 VBZ (restrizioni di traffico)

Con il servizio VBZ (restrizioni di traffico) si definiscono gli utenti del sistema di comunicazione che possono stabilire connessioni con altri utenti. Questa funzione viene utilizzata ad esempio per i sottosistemi.

Attraverso le restrizioni di traffico è possibile configurare a quali linee hanno accesso i singoli utenti per le chiamate in arrivo e in uscita..

La funzione VBZ non consente accesso alle applicazioni, ma esclusivamente alla telefonia. L'indicazione dello stato presenza non risulta impedita dalle limitazioni di accesso VBZ.

La funzione VBZ si compone di due passaggi:

- Creazione di gruppi con restrizioni di traffico
- Configurazione di matrici di restrizione del traffico

Suggerimento: La funzione VBZ non deve essere utilizzata assieme alla funzione UC, in quanto comporterebbe limitazioni.

16.1.6.1 Gruppi con restrizioni di traffico

I gruppi con restrizioni di traffico permettono di gestire le chiamate consentite e vietate tra utenti e linee del sistema di comunicazione.

Con i gruppi con restrizioni di traffico, gli utenti e le linee vengono raggruppati assieme.

Tramite Assegnazione gruppi, è possibile assegnare i singoli utenti e le singole linee del sistema di comunicazione a un gruppo con restrizioni di traffico. Codificando la matrice di collegamento, è possibile quindi ricorrere a questi gruppi per definire gli utenti che possono stabilire connessioni tra loro e le linee a cui questi hanno accesso.

Per impostazione predefinita, tutti gli utenti e le linee urbane sono assegnati al gruppo con restrizioni di traffico 1. In questo modo tutti gli utenti hanno accesso illimitato agli altri utenti e alle altre linee, sia in entrata che in uscita. La matrice Col definisce quali dei gruppi con restrizioni di traffico abbiano la possibilità di eseguire chiamate con gli altri gruppi con restrizioni di traffico.

È possibile configurare un massimo di 64 gruppi con restrizioni di traffico.

16.1.6.2 Assegnazione dei numeri brevi del sistema a gruppi con restrizione di traffico

A ogni gruppo con restrizioni di traffico viene assegnato un intervallo di destinazioni di selezione breve del sistema centrali. Se un utente compone una selezione breve del sistema, il sistema verifica che egli disponga della necessaria autorizzazione sulla base del gruppo con restrizioni di traffico a cui appartiene. Se la selezione breve del sistema rientra nell'intervallo di selezioni brevi del sistema assegnato a tale gruppo con restrizioni di traffico, la chiamata viene effettuata, in caso contrario viene visualizzato un messaggio di errore.

Se un utente sceglie una destinazione di selezione breve, viene determinato il gruppo con restrizioni di traffico corrispondente. Ciò determina se l'utente è autorizzato o meno a utilizzare le destinazioni di selezione breve. Se non è abilitato viene emesso un messaggio di errore che segnala questo stato

Gli intervalli di destinazioni di selezione breve possono sovrapporsi nei gruppi con restrizioni di traffico.

Per impostazione predefinita, tutti i numeri di selezione breve sono assegnati al gruppo con restrizioni di traffico 1.

Nei gruppi con restrizioni di traffico, gli intervalli dei numeri brevi di sistema possono sovrapporsi. Sono ammessi ad es.:

Gruppo con restrizioni di traffico	Intervallo di selezioni brevi
1	0000-7999
2	0050-0150
3	0200-0500

Tuttavia, non è consentito inserire in un gruppo con restrizioni di traffico singole selezioni brevi del sistema o più intervalli di selezioni brevi del sistema invece di un unico intervallo. Non sono ammessi ad es.:

Gruppo con restrizioni di traffico	Intervallo di selezioni brevi
1	0000, 0005, 0010
2	0050-0100, 0300-0500

16.1.6.3 Come assegnare un utente ad un gruppo con restrizioni di traffico

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura dei menu fare clic su **Autorizzazioni** > **Assegnazione gruppi** > **Assegnazione gruppi**.
4) Per un utente visualizzato nella colonna **Utente**, nel menu a tendina **Gruppo** selezionare la voce con il gruppo con restrizioni di traffico desiderato.
5) Fare clic su **Applica**, quindi su **OK**.

16.1.6.4 Come assegnare una linea ad un gruppo con restrizioni di traffico

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura dei menu fare clic su **Abilitazioni** > **Assegnazione gruppi** > **Assegnazione della linea ad un gruppo con restrizioni di traffico**.
4) Per la linea visualizzata nella colonna **Linee**, nel menu a tendina **Gruppo** selezionare la voce con il gruppo con restrizioni di traffico desiderato.
5) Fare clic su **Applica**, quindi su **OK**.

16.1.6.5 Come modificare la matrice VBZ

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Autorizzazioni**.
3) Nella struttura dei menu fare clic su **Autorizzazioni** > **Matrice Col**.
4) Per modificare le opzioni di connessione, procedere come segue:
   - Per bloccare tutte le possibilità di connessione, premere il fare clic su **Blocca tutto**.
   - Per attivare tutte le possibilità di connessione, fare clic su **Rilascia tutto**.
   - Per rilasciare solo le possibilità di connessione interne al gruppo, fare clic su **Solo inter. al gruppo**.
   - Per modificare in modo specifico una possibilità di connessione tra due gruppi con restrizioni di traffico, fare clic sul campo nel punto di incrocio di questi gruppi con restrizioni di traffico nella matrice Col. Fare ripetutamente clic su tale campo per attivare o bloccare le possibilità di connessione per un fascio, per l'altro fascio o per entrambi i fasci.
5) Fare clic su **Applica**, quindi su **OK**.

16.1.7 Chiave elettronica centrale/commutazione dell’abilitazione

La chiave elettronica centrale consente ad un utente autorizzato (ad esempio l'amministratore) di impostare un blocco completo delle funzioni del telefono per altri utenti. Solo i seguenti servizi risultano ancora disponibili: Chiamate interne, Selezione breve del sistema e Conferenza con utenti interni. Questa chiave elettronica può essere disattivata dall'utente bloccato inserendo la propria chiave elettronica telefonica o nuovamente dall'utente abilitato.

Il codice di blocco del telefono (chiave elettronica), con il quale l'utente può attivare o disattivare il blocco del telefono, non è necessario per attivare il blocco.

Per impostazione predefinita, l'utente autorizzato è il numero di telefono "100" (riconfigurato).

16.1.8 Chiave elettronica individuale (blocco del telefono)

Con la chiave elettronica personale non è possibile effettuare conversazioni esterne o modificare le impostazioni utente.

Dai telefoni bloccati è comunque possibile comporre i numeri di emergenza.

Le chiamate interne sono ancora possibili.

Una connessione di chiamate entranti a utenti interni è comunque possibile.

Sui telefoni esclusi sono disponibili solo i servizi che non richiedono alcuna composizione esterna. L'unica eccezione è il servizio Selezione breve del sistema.

Come promemoria dello stato di esclusione del telefono, l'utente riceve un tono lungo (tono di composizione speciale). Nei telefoni con display viene inoltre visualizzato il messaggio "Telefono escluso".

L'utente può, tramite un tasto o un codice, dopo avere immesso la chiave elettronica personale, escludere l'apparecchio o riabilitarlo.

Prima del primo utilizzo del blocco telefono è necessario configurare il codice di blocco del telefono. Per impostazione predefinita, tale codice è 00000 per tutti i telefoni e può essere modificato per ogni singolo telefono. A tal fine, il telefono in questione deve essere sbloccato. Il codice deve sempre essere di 5 cifre. che può essere composto da sole cifre (0 - 9). Se l'utente ha dimenticato il codice di blocco telefono, può farlo riportare al valore predefinito (00000) rivolgendosi a un utente autorizzato (primo utente del sistema con il numero di telefono "100" o l'amministratore).

16.1.8.1 Come reimpostare le singole chiavi elettroniche

Con la procedura guidata **Nome utente e rilascio** è possibile resettare la chiave elettronica di un telefono.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Nome utente e sblocco**. Viene visualizzata la finestra **Configurazione del nome e sblocco per utenti e gruppi**.
4) Selezionare la casella di controllo **Reimposta PIN**.
5) Fare clic su **OK & Avanti**, quindi su **Fine**.

16.1.9 Rifiuto chiam.con add.al chiamante per linea esterna (solo per Brasile)

Rifiuto chiam.con add.al chiamante per linea esterna consente il rilascio automatico delle chiamate con addebito in entrata. Questa funzione è disponibile soltanto impostando come paese il Brasile. In tutti gli altri paesi, l'impostazione viene ignorata.

È possibile configurare singolarmente le linee analogiche. La funzione Rifiuto chiam.con add.al chiamante può essere configurata singolarmente per ogni linea esterna analogica. Se la funzione è abilitata per una linea esterna, un tronco abilitato, 1 s (valore predefinito) dopo la risposta a una chiamata in arrivo viene aperto il loop per 2 s (valore predefinito). In questo modo, vengono abilitate sulla rete le chiamate con addebito, mentre le altre chiamate rimangono invariati.

16.1.10 Rifiuto chiam.con add.al chiamante per utente (solo per Brasile)

La funzione Rifiuto chiam.con add.al chiamante può essere impostata singolarmente per ogni utente, semplificando il rifiuto automatico delle chiamate in entrata con addebito. Ciò vale anche nel caso di deviazione di chiamata, risposta per assente, rinvio, ecc.

Vi è inoltre la possibilità di configurare la funzione Rifiuto chiam.con add.al chiamante a livello di sistema. Ciò si applica quando non viene composto il numero di un utente singolo ma quello di un gruppo di ricerca (o nel caso venga composto un numero sbagliato).

16.2 LCR (Least Cost Routing, Instradamento a minor costo)

La funzione LCR (Least Cost Routing) consente di selezionare automaticamente su quale rotta instradare una connessione in uscita. Questa può essere instradata tramite la rete pubblica, gestori di rete diversi (ITSP) o rete privata. In base al piano di composizione, alla tabella delle rotte e alle regole di composizione viene selezionata la rotta di connessione più appropriata per la chiamata.

Le connessioni possono essere chiamate, connessioni dati analogiche tramite fax e modem, nonché connessioni dati ISDN.

16.2.1 Funzionalità LCR

Con la funzione LCR (Least Cost Routing) è possibile definire con quale operatore effettuare ad esempio, una chiamata locale, una chiamata a un cellulare o internazionale. Tramite il sistema di comunicazione si definisce un operatore conveniente, quindi si effettuano tutte le conversazioni corrispondenti con questo operatore.

Se nel piano di composizione viene individuato un modello che corrisponde al numero telefonico selezionato, viene ricercato un fascio adeguato nella tabella delle rotte (Ciascuna linea è assegnata a un fascio. Vedere Accesso alla linea urbana tramite linee analogiche e digitali). Viene inoltre verificato se l'abilitazione LCR è adeguata per questa voce della tabella delle rotte. Le

abilitazioni LCR e la differenza tra LCR e il controllo di selezione è descritta al capitolo Abilitazioni LCR.

Tramite la funzionalità LCR, è possibile definire quali utenti del sistema di comunicazione possono accedere a determinati fasci e linee (ad es. per assicurarsi che l'invio dei fax avvenga sempre tramite TDM e non ITSP). Viene verificato se il chiamante dispone dell'abilitazione necessaria prevista nel controllo selezione per occupare un fascio in fase di valutazione da parte dell'LCR. Questo test può essere disattivato per le linee trasversali (linee PABX) mediante la configurazione.

Le cifre selezionate vengono memorizzate temporaneamente finché le tabelle delle rotte con le classi di servizio LCR non sono state valutate. Al termine di questa fase viene stabilita la connessione in base alle regole di composizione. È possibile emettere un tono di chiamata per segnalare all'utente la disponibilità per la composizione.

Quando si configurano regole di composizione è possibile immettere informazioni per l'utente chiamante, ad esempio che la connessione viene instradata tramite un provider specifico che offre servizi di telefonia (nome del provider) o che la connessione utilizza una linea più costosa. Queste informazioni possono essere visualizzate sullo schermo, emesse come segnali acustici o in entrambe le modalità.

In generale:

- Se è attivato il servizio LCR, viene eseguita la verifica ad ogni selezione esterna (eccezione: Eccezione: composizione di un codice di linea o tasto di linea.
- Se LCR determina che non è possibile utilizzare la rotta preferita, il sistema di comunicazione ricerca un'alternativa (di solito più costosa) nella tabella delle rotte.
- Le cifre possono essere trasmesse singolarmente o a pacchetti, in base al metodo accesso e alla tabella delle rotte.
- Se la tabella dei numeri di selezione passante è vuota, viene usata la tabella dei numeri interni. Si applicano le regole corrispondenti di questa tabella.

Suggerimento: Anche nei sistemi di comunicazione con linee analogiche (HKZ) è necessario configurare un numero sede (prefisso internazionale/prefisso interurbano/eventuale numero del sistema).

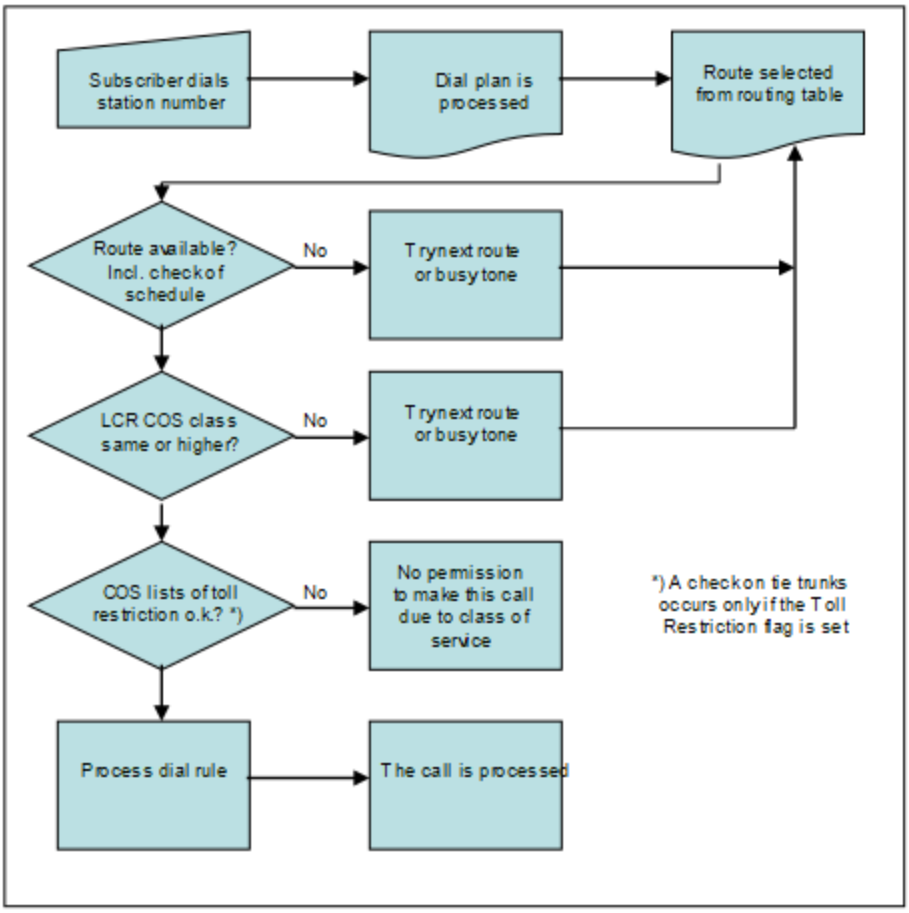
Oltre a ciò, è necessario configurare un numero di selezione passante; se la tabella dei numeri di selezione passanti è vuota, configurare un numero di selezione passante della propria connessione linea esterna analogica (HKZ). In questo modo ci si assicura che vengano raggiunte tutte le destinazioni esterne.

Informazioni specifiche del sistema

Il sistema di comunicazione valuta un totale di 24 caratteri.

Il sistema di comunicazione può gestire fino a 1000 piani di composizione e 254 tabelle delle rotte con 16 ingressi ciascuna.

Diagramma di flusso LCR



Trasmissione selezione

Esistono due tipi di trasmissione della composizione: cifra per cifra e in blocco. Nella trasmissione sincrona, ogni cifra viene inviata ed elaborata direttamente al momento della composizione (requisiti: l'analisi LCR è completa, ovvero la voce relativa al piano di composizione è chiaramente identificata e le abilitazioni sono verificate). Con la selezione in blocco, vengono creati e inviati blocchi di cifre (ovvero impegno della linea e composizione avvengono dopo un certo tempo o al riconoscimento di un codice di fine composizione esplicito).

Per i fasci degli ITSP, la trasmissione della selezione deve sempre avvenire in preselezione. L'impostazione del fascio è effettiva sull'intera tabella delle rotte.

Solo per gli USA: Carrier Select Override

La funzione Carrier Select Override può essere implementata mediante impegno selettivo della linea (codice, tasto). In questo caso, il meccanismo LCR viene completamente bypassato.

Dipendenze

Argomento	Dipendenza
Pianificazione	Se in un sistema nel quale è stata eseguita la migrazione da HiPath 3000, è presente una configurazione LCR con pianificazione, queste voci sono ancora effettive e possono essere gestite con Manager E.
Selezione breve del sistema	Per il funzionamento corretto delle destinazioni di selezione breve centrali, in Destinazioni di selezione breve deve essere utilizzato il codice di accesso LCR, seguito dal numero di destinazione.
Tasti con il nome	I tasti nominativi delle destinazioni esterne devono essere programmati con il codice di accesso LCR.
Autorizzazione (controllo della composizione)	Anche le classi di autorizzazione del controllo composizione vengono utilizzate da LCR. Per le linee PBX, può essere disattivato il controllo selezione; la configurazione viene eseguita tramite un flag.
Prime Line	Se la funzione "Impegno automatico della linea" (Prime Line) è attivata presso il centralino, non è possibile usare il servizio LCR. Le due funzioni si escludono a vicenda.

16.2.1.1 Come attivare LCR

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Suggerimento:

Alcune voci specifiche, ad es. Prefisso interurbano o Numero utente sono già state definite nella procedura guidata **Installazione di base**. Le modifiche manuali a questi campi sono esclusivamente riservate a tecnici esperti. Se si commette un errore nella configurazione di LCR, è possibile che le connessioni in uscita non funzionino o funzionino in modo inadeguato.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **LCR**.
3) Fare clic sulla scheda **Flag LCR**..
4) Selezionare la casella di controllo **Activate LCR**.
5) Fare clic su **Applica**, quindi su **OK**.

16.2.2 Piano di composizione LCR

Nel Piano di composizione viene ricercato un modello che corrisponda alle cifre selezionate (sequenza cifre). Il risultato viene utilizzato come criterio per selezionare la tabella delle rotte. Viene inoltre verificato se l'abilitazione LCR dell'utente è adeguata per questa voce del piano di composizione.

Il modello di sequenza di composizione è associato nel piano di composizione a una tabella delle rotte che, a sua volta determina altri parametri necessari per stabilire la connessione.

Il piano di composizione viene riunito in un solo campo per scopi di identificazione e configurazione. La tabella rappresenta i numeri 4922000 e 1603656260 all'immissione nel piano di selezione.

Campo 1		Campo 2		Campo 3		Campo 4		Campo 5
0	C	492	–	2000				
0	C	160	–	365	–	62	–	60

Per i numeri di telefono sono valide le voci seguenti:

0 . . . 9	cifre consentite
–	trattino di separazione di campo
C	tono di selezione simulato (può essere specificato fino a 3 volte). Questa voce può anche essere interpretata come trattino di separazione dei campi.
Caratteri globali	
X	Cifra desiderata fra 0 . . 9
N	Cifra desiderata fra 2 . . 9
Z	seguono una o più cifre fino alla fine della selezione

Una sequenza di cifre può essere suddivisa in massimo 10 campi.

I trattini di separazione di campo vengono utilizzati per la suddivisione della stringa di cifre in singoli campi valutabili separatamente. Esempio: dopo la prima cifra viene immesso un carattere di separazione, in modo che uno "0" venga riconosciuto come campo separato e possa simulare un'abilitazione di linea.

Grazie a questa separazione, i campi possono essere ripetuti/ordinati in modo diverso nel piano di composizione. I campi del piano di composizione rappresentati con i caratteri di separazione "–" e "C", possono essere controllati singolarmente per ripetere, mascherare, scambiare o aggiungere cifre.

Un carattere "#" o "*" nella sequenza di cifre selezionata dall'utente indica il termine della composizione/la commutazione della procedura di composizione. Per questo motivo questi caratteri non sono consentiti in un piano di selezione.

Le voci con caratteri globali devono essere sempre introdotte da una cifra di selezione univoca, allo scopo di evitare conflitti tra le diversi voci con caratteri globali.

Le voci dei codici di addebito (PKZ) possono essere forzate per piano di composizione. In questo caso si applica il processo di verifica di tali voci.

Se vi sono più piani di composizione che corrispondono a una stringa di composizione, viene utilizzato quello che presenta una corrispondenza maggiore. Esempio: viene composto 00894711, sono disponibili le voce del piano di composizione 0CZ e 0C089Z -> viene eseguito 0C089Z. La posizione delle voci all'interno del piano di composizione è irrilevante, non è necessario alcun ordinamento delle voci.

OpenScape Business può analizzare numeri composti con una lunghezza di 24 caratteri.

Voci LCR durante la configurazione iniziale del sistema di comunicazione

Alla prima messa in servizio del sistema di comunicazione vengono inseriti diversi valori predefiniti nel piano di composizione LCR. Fino al piano di composizione 34 compreso, le voci lato sistema per chiamate di emergenza, informazioni, numeri speciali, impegno predefinito delle linee per PSTN e ITSP, UC Suite, collegamenti per annunci, rete e forrmati internazionali di composizione sono preimpostati nelle linee ISDN. Quest'area può essere influenzata da modifiche alla configurazione apportate in altri punti (ad esempio modifiche al flag **Numero sede**). Pertanto, quando cambia il numero del sito, occorre assicurarsi che l'impegno della linea predefinita funzioni come previsto (ciò è importante per la composizione di numeri pubblici).

Suggerimento: Dal piano di composizione LCR 36, vi sono voci liberamente disponibili.

16.2.2.1 Come modificare il piano di composizione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Fare clic su **Piano di composizione**.
4) In **Modifica piano di composizione** vengono elencati i singoli piani di composizione e si possono modificare i seguenti campi:
   - **Nome**
   - **Cifre selezionate**
   - **Tabella delle rotte**
   - **Codice add.**
   - **Controllo della composizione**

     Il flag di controllo della composizione si riferisce esclusivamente al tipo di fascio PABX. Per il fascio linea urbana non ha importanza, ovvero non è

possibile disattivare il controllo selezione per le linee esterne da questo punto.

- **Servizio d'emergenza**

Nota: Facendo clic sulla freccia blu accanto al campo **Tabella delle rotte** si apre direttamente la relativa tabella delle rotte.

---

5) Fare clic su **Applica**, quindi su **OK**.

16.2.3 Tabella delle rotte LCR

Nella tabella delle rotte LCR viene ricercato un fascio adeguato (ciascuna linea deve essere assegnata a un fascio). Quindi viene verificato se l'abilitazione (controllo della composizione) è adeguata per il fascio. Anche la regola di composizione dipende dal fascio assegnato.

La tabella delle rotte descrive

- il fascio assegnato alla rotta,
- la regola di selezione,
- l'abilitazione LCR (Class Of Service, COS) necessaria,
- la possibilità di avviso tariffe elevate (segnale).
- il gateway dedicato e
- l'ID nodo GW.

La ricerca nella tabella avviene dall'alto verso il basso, in sequenza gerarchica. Viene verificato se il fascio è libero o se l'utente dispone dell'abilitazione LCR richiesta. In questo caso, il numero viene composto secondo la regola di composizione impostata nella tabella delle rotte, se ciò è consentito dal livello di abilitazione (controllo della selezione) e dall'assegnazione a gruppi con restrizioni di traffico tra l'utente e la linea.

Se il percorso primario della tabella è occupato, LCR seleziona quello successivo (possibilmente in base alla convenienza). Ciò può essere segnalato all'utente tramite un segnale acustico e/o ottico.

Possono essere create fino a 254 tabelle ciascuna con 16 rotte.

Gateway dedicato

Un gateway dedicato è un nodo partner fisso in un sistema di reti IP (Gateway dedicato > Forzato). Se per il fascio di rete IP viene configurato un gateway dedicato con il corrispondente ID nodo GW, il routing avviene obbligatoriamente tramite questo gateway.

Per una configurazione a gateway multiplo, viene specificato un gateway dedicato sulla base della configurazione dell'utente.

16.2.3.1 Come modificare tabelle delle rotte

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Fare clic su **Tabella delle rotte**.
4) Vengono visualizzate tutte le tabelle delle rotte:
   - **1-Table**
   - **2-Table**
   - **nn-Table**

   Suggerimento: Le tabelle delle rotte da 1 a 15 sono intese per le voci predefinite o sono configurabili tramite procedura guidata. Durante la migrazione, vengono automaticamente inserite le voci presenti in questa tabella delle rotte.

   Tuttavia, questo meccanismo non impedisce la duplicazione delle voci inserite. È consigliata una post-elaborazione manuale delle tabelle delle rotte.
5) Fare clic su quella desiderata. Viene visualizzata la tabella selezionata con la scheda **Modifica tabella di routing**.
6) In **Modifica tabella di routing** vengono elencate le singole tabelle di routing e si possono modificare i seguenti campi:
   - **Fascio**
   - **Regola di composizione**

     Nota: Facendo clic sulla freccia blu accanto alla regola desiderata, è possibile visualizzare e modificare le proprietà delle regole di composizione.
   - **Abil. min. (Abilitazione LCR)**
   - **Avvertenza**
   - **Gateway dedicato**
   - **ID nodo GW**
7) Fare clic su **Applica**, quindi su **OK**.

16.2.4 Abilitazione LCR

Ciascun utente viene assegnato a un'abilitazione LCR (Class Of Service, COS). Un utente può impegnare una rotta se la sua abilitazione LCR è di livello superiore o uguale a quella della tabella delle rotte; un utente con abilitazione 7 non può cioè impegnare una rotta che richiede l’abilitazione 8. Per impostazione predefinita, tutti gli utenti sono configurati con il massimo livello di abilitazione LCR (15).

Dipendenze

Argomento	Dipendenza
Abilitazione alla linea urbana	L'abilitazione (controllo della composizione) ha precedenza rispetto alle abilitazioni LCR. L'abilitazione (controllo della composizione) può essere attivata e disattivata per le linee trasversali.
Assegnazione dei gruppi VBZ	Il numero viene composto solo quando la matrice Col lo consente.

16.2.4.1 Come assegnare e modificare l'abilitazione LCR

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Fare doppio clic su **Classi di servizio**.
4) Assegnare in **Modifica classe di servizio LCR**, Nel campo **Abilitazione** un'abilitazione LCR o modificare un'abilitazione esistente.

   Se tratta dell'abilitazione di un utente per LCR. Il campo non ha alcun effetto sull'abilitazione alla linea urbana.
5) Fare clic su **Applica**, quindi su **OK**.

16.2.5 Regole di composizione LCR

Grazie alle regole di composizione LCR i numeri di telefono immessi possono essere trasformati in nuove sequenze di cifre, come desiderato. La conversione delle cifre consente di accedere a vari gestori di rete. La regola di composizione utilizzata viene definita tramite il percorso/il fascio nella tabella delle rotte.

Informazioni specifiche del sistema

Il sistema di comunicazione consente di utilizzare fino a 254 regole di composizione nella tabella delle regole di composizione LCR. Il nome di una regola di composizione può contenere massimo 16 caratteri.

Le regole richiamano i singoli campi del piano di composizione per le seguenti procedure:

- Ripetizione delle cifre
- Mascheramento delle cifre
- Scambio di cifre
- Aggiunta di cifre
- Commutazione del tipo di selezione
- Riconoscimento del tono di selezione.

- Aggiunta di pause di selezione

Regola di composizione

È possibile definire fino a 254 regole di composizione con una lunghezza di massimo 40 caratteri.

La tabella delle regole di composizione LCR viene definita anche tabella di routing.

Definizione delle regole di composizione (formato della regola di selezione)

- A:

  Ripetere i campi restanti (trasmettere). "A" trasmette tutti i campi di cifre successivi. Il punto di riferimento è l'ultimo delimitatore nel campo delle cifre composte nel piano di composizione.

  Se "A" è inserito senza riferimento esplicito, indica tutte le cifre dopo il codice di accesso, ovvero, "A" corrisponde a "E2A"#
- B:

  Viene utilizzato in un collegamento in rete multi-gateway quando un numero esterno chiamato di tipo (TON, type of number) "sconosciuto", deve essere istradato verso il nodo multi-gateway. Per assicurare che questo numero di telefono sia univoco, viene esteso in numero nazionale o internazionale secondo il TON nell'LCR. Questo è necessario se i numeri DID non sono univoci e devono essere configurati nel formato nazionale o internazionale.
- D (n):

  selezionare la stringa di cifre (da 1 a 25). Nella stringa di cifre, "D" può ricorrere più volte e può trovarsi in posizioni qualsiasi.
- E (n):

  Invio del contenuto del campo (da 1 a 10). "E" può ricorrere più volte e trovarsi in posizioni qualsiasi. La successione di "E" in relazione a (n) è a piacere. Un determinato campo può essere attivato più volte, anche in sequenza. "E", ad eccezione di "E1" (codice di accesso), può essere compreso fra altri parametri a piacere.

  Con la selezione a passi (contrapposta a quella a blocchi), l'ultimo elemento della regola di selezione non può essere E(n), bensì E(n)A.
- M (n):

  codice di autorizzazione (da 1 a 16). Questa lettera non deve trovarsi sull'ultima posizione.
- P (n):

  P (n) può verificarsi più di una volta nella stringa e può trovarsi in qualsiasi posizione. P (n) può essere circondato da altri parametri. (Da 1 a 60 volte l'unità di pausa a livello di sistema).
- S:

  switch, commutazione del tipo di selezione da DC a DTMF (in CONNECT, PROGRESS o CALL PROC con PI). Nella stringa di cifre, "S" può ricorrere una sola volta e non deve essere sull'ultima posizione. Dopo "S" non può più essere utilizzato il parametro "C".

- C:

  Nella stringa di cifre, il carrier "C" può essere inserito una sola volta. Le cifre successive vengono trasmesse senza pausa di selezione e utilizzate in "Single Stage", "Two Stage", "DICS" e "PRI" per l'accesso al carrier.
- U:

  applicazione del tipo di selezione SUB-indirizzo. Nella stringa di cifre, "U" può ricorrere una sola volta e non deve essere sull'ultima posizione. Dopo "U", i parametri "S", "P" e "C" non possono essere più utilizzati.
- N (n) (Solo per USA!):

  gruppo SFG della rete (da 1 a 5) o numero di banda (1)
- L (solo per USA!)

  "L" può trovarsi solo alla fine della stringa. "L" significa che la chiamata viene trattata come una chiamata di emergenza.

Esempio:

Il sistema deve inserire automaticamente un prefisso provider.

La regola di composizione D010xxA significa: il sistema compone prima il prefisso del provider (010xx), quindi tutte le cifre dopo il codice di accesso selezionate dall'utente (A).

16.2.5.1 Come modificare le regole di composizione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Fare clic su on **Regola di composizione**. Vengono visualizzate tutte le regole di composizione.
4) Nella struttura dei menu, fare clic sulla regola desiderata.
5) È possibile modificare i seguenti campi:
   - **Nome regola**
   - **Formato della regola di selezione**
   - **Metodo del gestore di rete** (**Sconosciuto**, **Gestore di rete principale**, **MCL Single Stage**, **MCL Two Stage**, **Corporate Network**, **Dial In Control Server**, **Primary Rate Interface**)
   - **Tipo** (**Sconosciuto**, **Prefisso internazionale**, **Prefisso località**, **Numero del sistema**)
6) Fare clic su **Applica**, quindi su **OK**.

16.2.6 Gestore di rete

È possibile associare un gestore di rete a ciascun fascio. La scelta del rispettivo gestore di rete viene definita tramite la regola di selezione per LCR.

Sconosciuto

Nessuna informazione esplicita sul gestore di rete.

Gestore di rete principale

In caso di impegno di una linea del gestore di rete principale, la composizione dei numeri viene semplificata utilizzando la selezione in blocco o cifra per cifra nella rete pubblica.

MCL Single Stage

Con MCL Single Stage, si utilizza un prefisso per selezionare il gestore di rete desiderato, quindi si compone il numero di telefono. La composizione viene eseguita sul canale D nel caso di una linea ISDN e come composizione normale per linee urbane analogiche.

MCL Two Stage

Con MCL Two Stage, si utilizza un prefisso per selezionare il gestore di rete desiderato. Dopo una fase di sincronizzazione, viene inviato prima un codice di autorizzazione configurabile e successivamente il numero di telefono di destinazione sotto forma di caratteri DTMF

Per la sincronizzazione a tempo deve essere programmato un intervallo compreso tra 2 e 12 secondi.

Corporate Network

La rete aziendale è collegata direttamente al sistema di comunicazione. La funzione LCR determina, sulla base del numero composto dall'utente, la linea e instrada la chiamata tramite il fascio di linee della rete pubblica o tramite quello della rete aziendale.

Dial-In Control Server

Con questo tipo di LCR, è possibile selezionare il gestore di rete desiderato con un prefisso tramite Dial-In Control Server (DICS) e successivamente trasmettere il numero di telefono e un codice di autorizzazione configurabile nell'indirizzo SUB. La composizione avviene quindi nel canale D.

Primary Rate Interface (interfaccia multiplex primaria) (solo per USA)

Nel caso di Primary Rate Interface, la scelta del gestore di rete o del Calling Service viene codificata nel messaggio SETUP tramite i seguenti elementi informativi: Network Specific Facility, Operator System Access e Transit Network Selection.

Dipendenze

Argomento	Dipendenza
Ricezione/inoltro di informazioni sulla chiamata	La disattivazione temporanea o permanente della visualizzazione del numero di telefono non deve essere attiva.
ISDN/SUB indirizzamento	Il servizio ISDN "SUB" deve essere richiesto ovvero abilitato nella rete pubblica.

16.2.7 Impegno mirato delle linee urbane

Le linee urbane possono essere impegnate dagli utenti in modo mirato.

Normalmente, viene assegnata priorità di accesso alla linea esterna sulla base del Least Cost Routing. Solitamente, al primo posto viene indicato il provider con le condizioni più vantaggiose, al secondo il provider con le condizioni meno vantaggiose rispetto al primo, e così via.

Se un utente desidera eseguire una chiamata tramite un provider non configurato al primo posto (ad esempio perché questo è competitivo per le chiamate interurbane), è possibile selezionare tale provider in modo mirato digitando un codice di linea o premendo un tasto di linea.

Digitando un codice, l'utente ha inoltre la possibilità di comporre un numero di telefono valido solo per ISDN (se come provider è configurato ad esempio Vodafone).

Per impostazione predefinita, viene configurato un codice (88) per un impegno mirato della linea tramite ISDN. Tutti i codici possono essere configurati e successivamente modificati dall'amministratore.

16.2.7.1 Come configurare il codice per l'occupazione mirata delle linee urbane ISDN

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Fare clic su **Piano di composizione**. Viene visualizzato un elenco con i singoli piani di composizione.
4) Nel campo **Nome** inserire il nome desiderato per il piano di composizione.
5) In **Cifre selezionate** inserire il codice e l'abbreviazione esatta (ad esempio, **88CZ**).

   Nota: 88 è il codice predefinito configurato nel sistema per l'impegno mirato di una linea ISDN.

   Per informazioni sulle abbreviazioni C e Z, vedere Piano di composizione LCR.
6) In **Tabella delle rotte** digitare **1**.
7) Fare clic su **Applica**, quindi su **OK**.

16.2.7.2 Come visualizzare i codici di accesso diretto per l'impegno selettivo della linea esterna

La procedura guidata **Linea esterna ISDN / analogica / ITSP** consente di visualizzare i codici per l'impegno selettivo delle linee esterne ISDN.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Il sistema di comunicazione è collegato a una linea urbana analogica.

Passo a passo

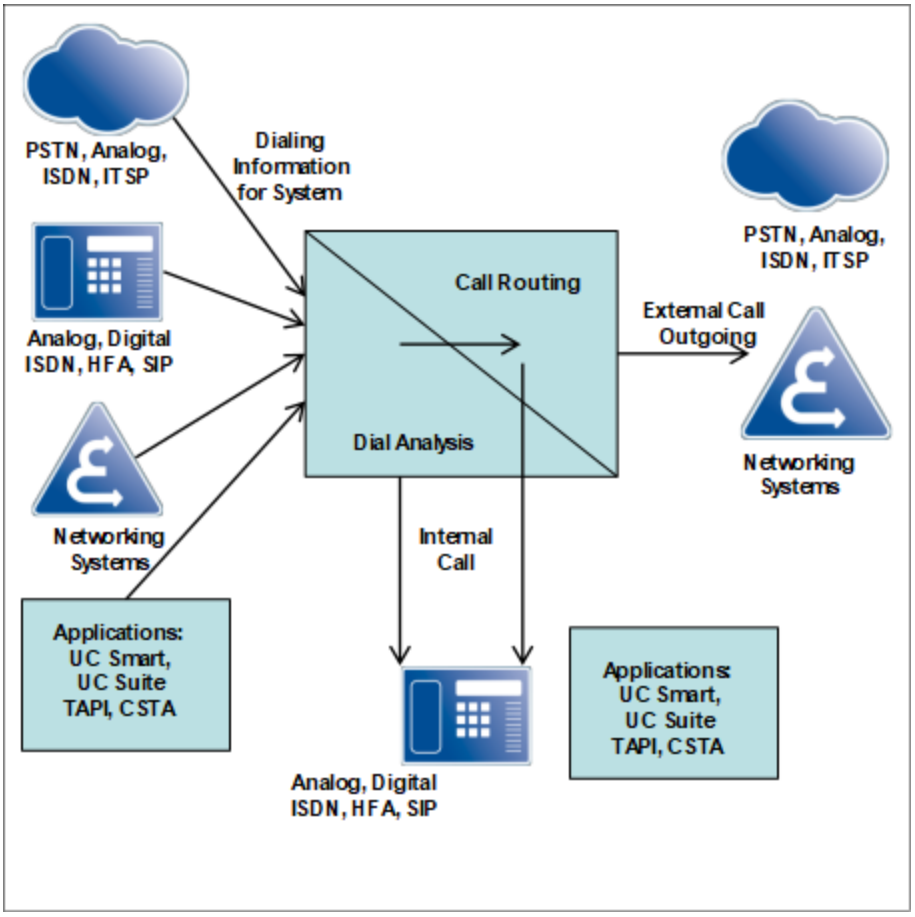
1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Linea esterna ISDN / analogica / ITSP**.
4) Fare clic più volte su **OK & Avanti** fino a raggiungere la finestra **Codici di accesso diretto alla linea esterna**.
5) Per impostazione predefinita, viene visualizzato il codice di accesso diretto alla linea ISDN. Con gli ITSP configurati, vengono visualizzati i codici corrispondenti.
6) Fare clic su **OK & Avanti**, quindi su **Fine**.

16.3 Analisi del numero composto e routing delle chiamate

In questo capitolo, viene illustrata la relazione tra l'analisi delle cifre composte e il routing delle chiamate. Spiega come il sistema di comunicazione valuta i numeri di telefono che vengono composti da utenti, linee e applicazioni di vario tipo per raggiungere una destinazione specifica e come avviene il routing al termine dell'analisi delle cifre. Le funzioni di sistema rilevanti a tal fine sono state per la maggior parte descritte nei precedenti capitoli. In questo capitolo viene descritta la selezione con un numero di telefono pubblico all'interno di un nodo/una connessione di rete.

L'analisi digitale

- del sistema di comunicazione registra e valuta tutti i numeri di telefono composti sulla base dei dati di configurazione
- Verifica le abilitazioni (ad esempio sulla base di classi di servizio per utenti, flag utenti, giorno/notte, numeri consentiti e vietati, abilitazioni LCR, pianificazioni, matrici di connessione ecc.).
- Determina se un numero può essere composto internamente o se deve venire impegnata una linea. Ciò vale per la composizione di numeri interni al sistema, interni alla rete e pubblici.
- normalizza i numeri di telefono, ovvero rende i numeri di telefono componibili da parte del sistema di comunicazione. (ad es. trasforma il formato canonico da "+49nnn" a "00049nnn", dove il primo "0" è il codice di accesso principale del PBX)
- I numeri eventualmente troncati (le prime cifre del numero di destinazione potrebbero dover essere troncate per le chiamate in entrata con impegno della linea, al fine di identificare le destinazioni DID con il formato breve)



16.3.1 Panoramica Routing delle chiamate/LCR

Una chiamata in arrivo viene sottoposta a vari test nel sistema di comunicazione e quindi inoltrata in modo appropriato.

Verifica 1 (destinazione chiamata Internet?)

- Le destinazioni con numero di telefono in formato canonico vengono prima convertiti in numeri componibili (a livello di interfaccia utente) o provvisti di TON=Internazionale (interfaccia ITSP).
- Per i numeri di destinazione di linee, la porzione del numero relativa al numero di sistema (PABX) del fascio corrispondente viene rimossa, se necessario.
- Le chiamate interne vengono analizzate tramite il piano di composizione interno, le chiamate dall'esterno tramite il piano di composizione dei numeri di selezione passante.

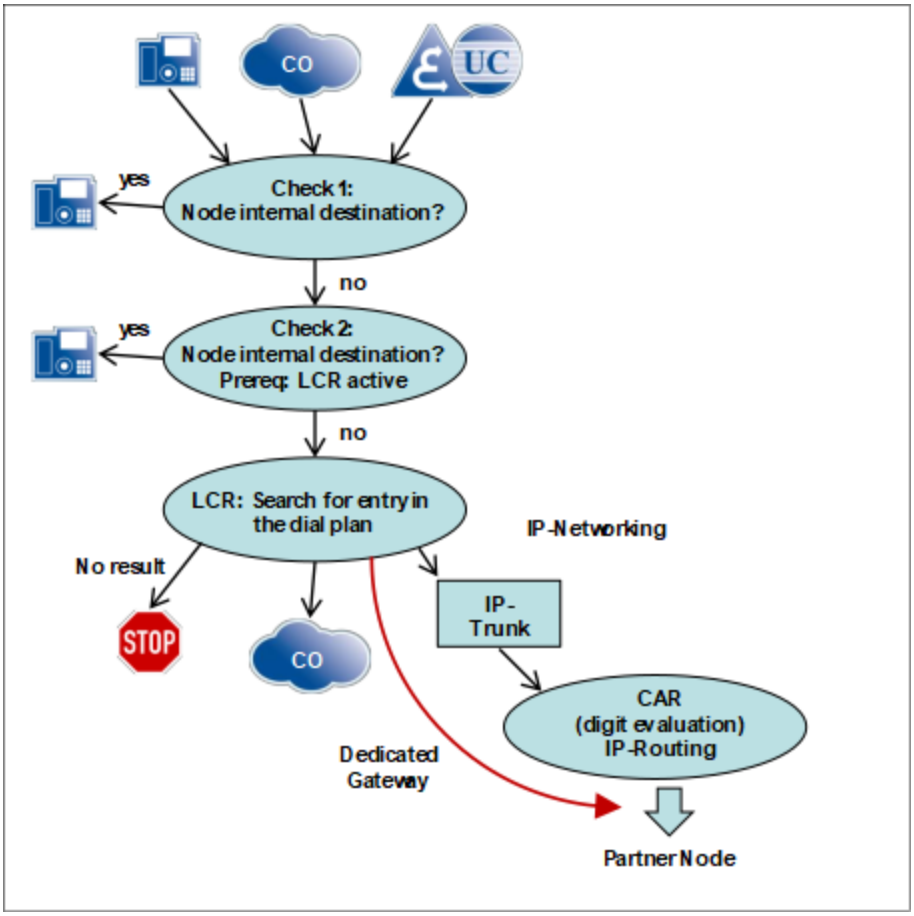
Verifica 2 (destinazione chiamata Internet?)

- Utenti, applicazioni, client o altri sistemi di comunicazione selezionano i numeri di destinazione nel formato pubblico (ad esempio, 0 0049nnn)
- Condizione: il codice di linea urbana predefinito (ad esempio "0") è stato configurato
- Dal numero di destinazione viene rimossa la porzione del numero sede (sede gateway) e valutato sulla base del piano di composizione del numero

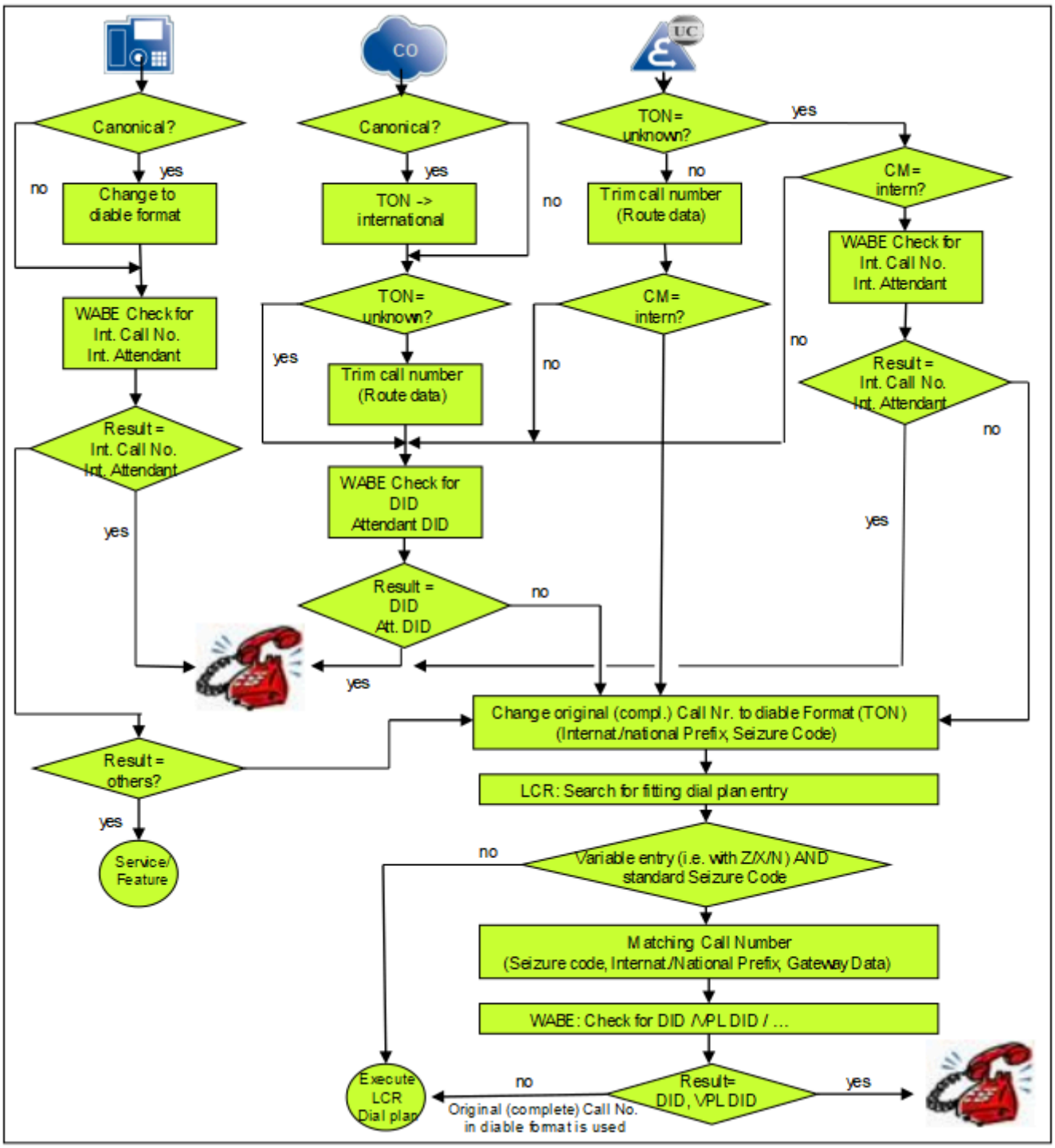
di selezione passante, indipendentemente dal fatto che si tratti di una chiamata interna o esterna.

- Se non è stata trovata alcuna destinazione di chiamata interna, il numero di telefono selezionabile, non abbreviato (!) viene elaborato nell'LCR e la chiamata viene instradata di conseguenza tramite una linea.

All'interno di una connessione di rete IP, il parametro Tabella delle rotte-LCR "Gateway dedicato" consente l'indirizzamento diretto di un nodo per un numero selezionato, bypassando l'analisi della composizione CAR.



16.3.2 Diagramma di flusso analisi della composizione



Spiegazione del diagramma di flusso:

Tedesco	Inglese	Spiegazione
WABE		Analisi del numero composto

Tedesco	Inglese	Spiegazione
CM	CM	Classmark, identifica il chiamate come chiamante esterno o chiamante interno (sulla rete)
TONO	TONO	Type Of Number, tipo di numero: Unknown (Sconosciuto), Subscriber (Utente), National (Prefisso nazionale) o International (Prefisso internazionale) e viene utilizzato sia per il numero di telefono di destinazione che per il numero di telefono di origine.
DID	DID	Numero DID
TNR RNR	N. tel. int.	Numero interno
Int. Attendant	VPL INT	Numero console posto operatore per chiamate interne
DID VPL	DID VPL	Numero console posto operatore per chiamate esterne
SERVIZIO	SERVIZIO	Codice servizio
LCR	LCR	Least Cost Routing

Per l'analisi delle cifre, i client UC si comportano come utenti controllati tramite CSTA.

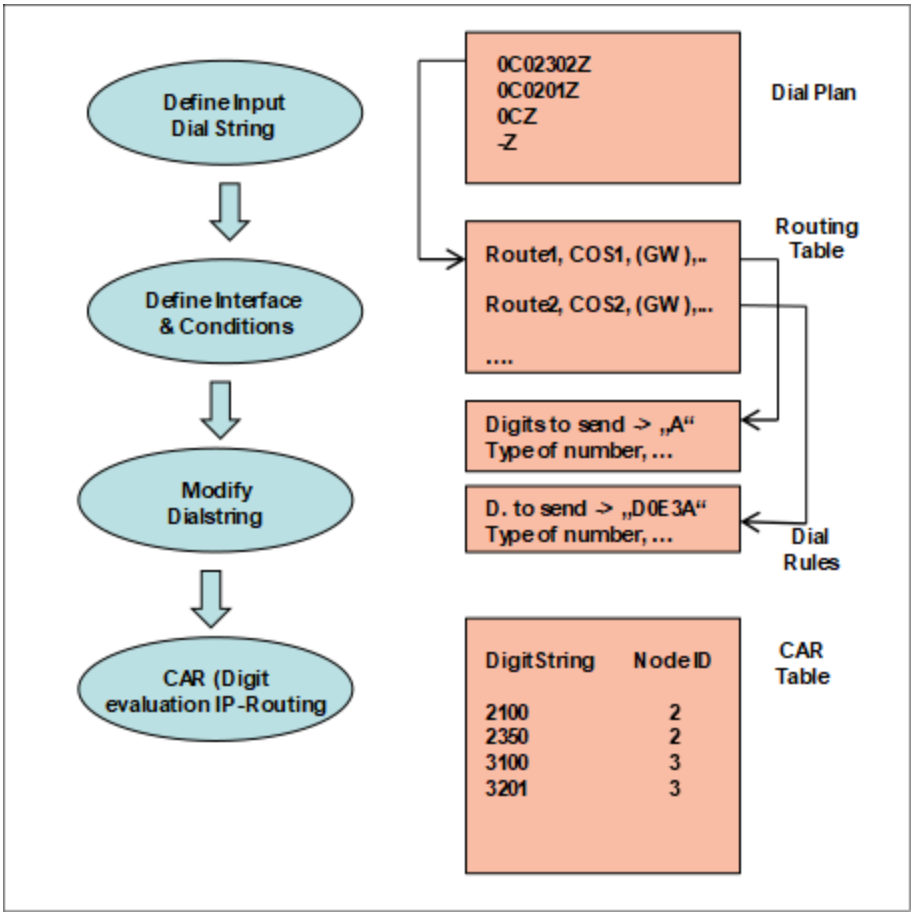
Per quanto riguarda l'analisi del numero composto, l'UC Suite si comporta per come una linea SIP-Q.

16.3.3 Call Routing e LCR nella rete

Per la connessione in rete, le funzioni Call Routing ed LCR svolgono un ruolo importante. Le chiamate vengono istradate sulla base del piano di composizione e delle regole di composizione. Il gateway dedicato svolge un ruolo particolare.

LCR base

Voci LCR durante la configurazione iniziale



Se l'impegno della linea non ha esito positivo, le voci della tabella delle rotte (routing table) vengono elaborate in sequenza in un loop.

Nota: la regola -z deve essere rimossa dalla configurazione dei sistemi indipendenti.

Alla prima messa in servizio del sistema di comunicazione vengono inseriti diversi valori predefiniti nel piano di composizione LCR. Fino al piano di composizione 35 compreso, le voci lato sistema per chiamate di emergenza, informazioni, numeri speciali, impegno predefinito delle linee per PSTN e ITSP, UC Suite, rete e formati internazionali di composizione sono preimpostati nelle linee ISDN.

Quest'area può essere influenzata da modifiche alla configurazione (ad esempio modifiche al flag **Numero sede**). Pertanto, quando cambia il numero sede, occorre assicurarsi che l'impegno della linea predefinita funzioni come previsto (importante per la composizione di numeri di rete pubblica).

Suggerimento: Dal piano di composizione LCR 36, vi sono voci liberamente disponibili.

16.3.3.1 Gateway dedicato

Il gateway dedicato è rilevante solo con una rete IP.

Perché è necessario un gateway dedicato?

Come si possono impostare destinazioni in modo permanente tramite configurazione?

Esempi di applicazioni per un gateway dedicato

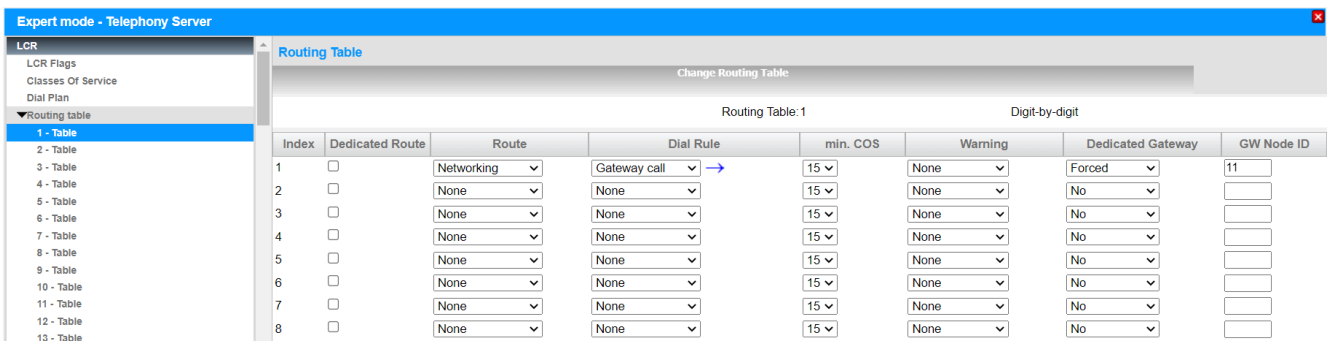
Il gateway dedicato a WBM

È possibile configurare i seguenti valori:

- La tabella CAR di ogni sistema di comunicazione include i numeri di telefono a livello di rete degli altri nodi e viene ciclicamente aggiornata (sovrascritta) in modo automatico in concomitanza con gli aggiornamenti. Pertanto, le tabelle CAR non sono adatte per utilizzare in modo permanente le voci aggiunte manualmente.
- Vengono inseriti solo numeri validi a livello di rete, ovvero non è possibile alcun routing specifico di un nodo (ad esempio, "0" per il rispettivo nodo gateway)
- Mediante l'uso di un indirizzamento diretto nell'LCR
- Il gateway dedicato indirizza direttamente il nodo di destinazione utilizzando l'ID del nodo (indirizzo IP)
- Quando si utilizzano gateway dedicati, le tabelle CAR vengono bypassate (vedere la figura precedente).

Indirizzamento diretto

- di gateway TDM per l'impegno delle linee esterne ("0CZ")
- di gateway TDM per implementare breakout tramite codici separati
- di nodi di rete interni che devono essere raggiungibili tramite numeri di rete pubblica
- di gateway TDM i cui utenti sono assegnati a una connessione di rete con gateway multiplo (collegati a un OpenScape Business S) (ad esempio, l'utente 1 appartiene per definizione al gateway 1 e l'utente 2 al gateway 2).
- di gateway e chiamate la cui origine NON PUÒ essere associata a un gateway specifico in una configurazione con gateway multiplo (ad esempio il gruppo di fax di un Contact Center UC)



No	L'analisi dei numeri di telefono viene eseguita tramite le tabelle CAR (nessun **ID nodo GW** richiesto)

Forzato	Viene eseguito l'istradamento al gateway corrispondente (ID nodo GW = n)
Più sedi (Multi Location)	Solo per configurazioni con gateway multiplo: con la configurazione gateway multiplo di OpenScape Business S, l'utente riconosce l'assegnazione al rispettivo gateway e può pertanto istradare le chiamate in uscita in modo selettivo sul gateway appropriato. Nella configurazione **Più sedi**, l'ID nodo GW viene utilizzato solo se tramite l'assegnazione degli utenti non può essere identificato alcun gateway (impostazione predefinita).

16.3.4 Scenari: analisi della composizione e routing delle chiamate

I relativi parametri e le dipendenze richieste per l'esecuzione delle procedure nel sistema di comunicazione vengono descritti per mezzo di scenari.
Gli scenari rappresentati possono integrarsi uno con l'altro, a seconda dell'applicazione.

Sistema singolo

Sistema collegato in rete come sottosistema (senza linea esterna)

Sistema di reti con gateway multiplo

1) L'utente A chiama l'utente B tramite numero di telefono interno
2) L'utente A chiama l'utente B tramite un numero della rete pubblica
3) L'utente A chiama un utente interno tramite linea urbana
4) La linea esterna ISDN chiama l'utente A
5) Configurazioni speciali e relativi effetti:

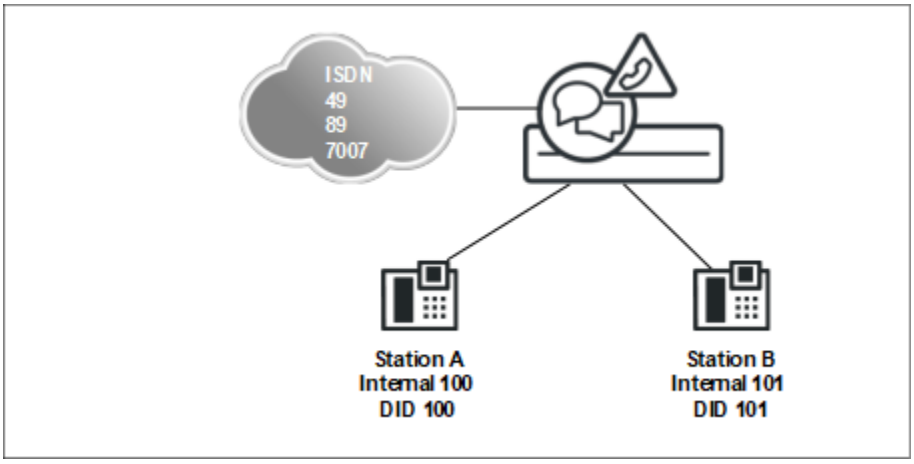
2 fasci linea esterna

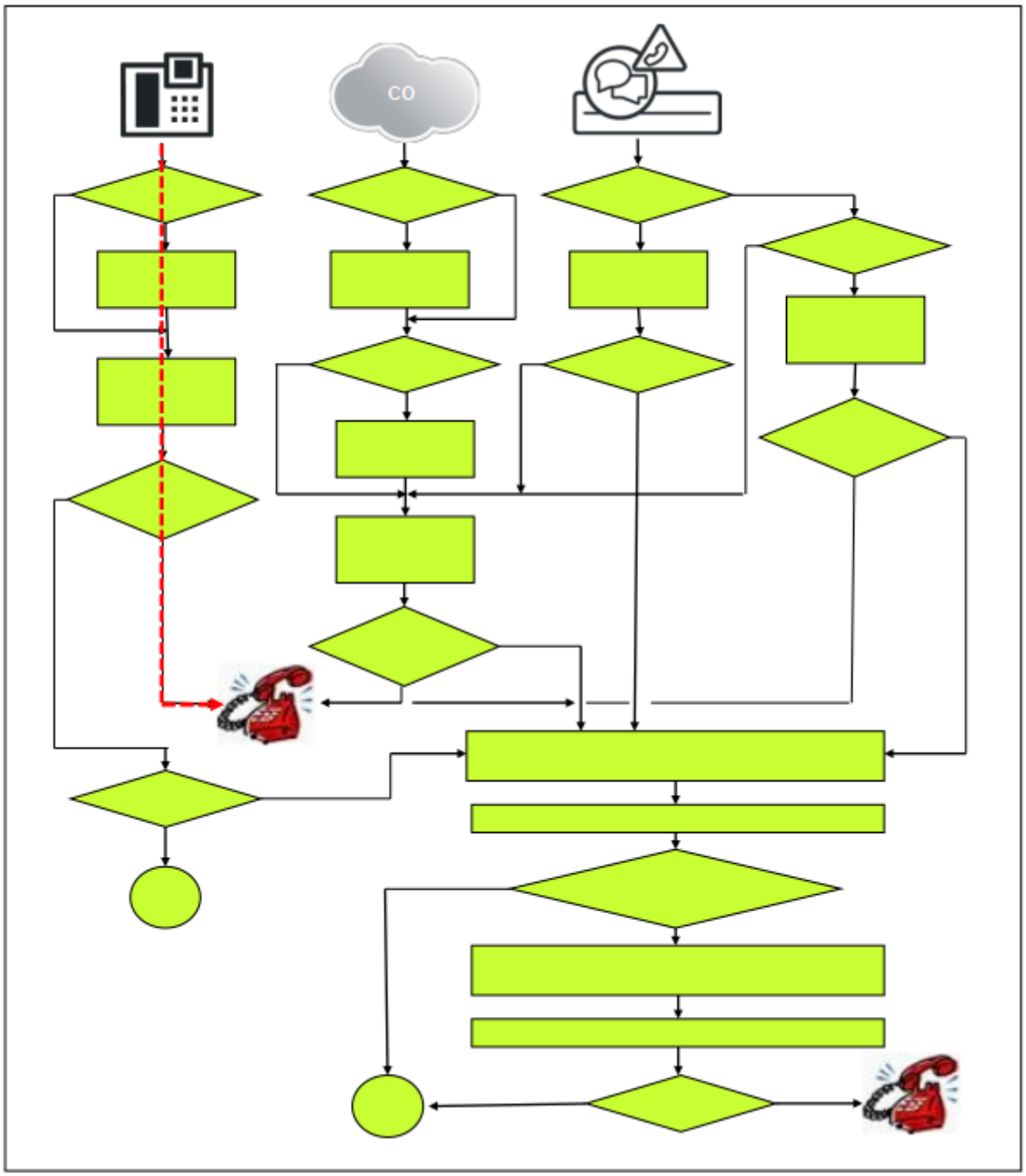
1) L'utente A chiama l'utente C tramite numero di telefono interno
2) L'utente A chiama l'utente C tramite il numero di telefono pubblico nel sistema di reti
3) La linea esterna ISDN chiama l'utente C

1) Il gateway 1 della linea esterna ISDN chiama l'utente D
2) L'utente D chiama un utente esterno tramite linea urbana

16.3.4.1 L'utente A chiama l'utente B tramite numero di telefono interno

Configurazione di entrambi i numeri interni



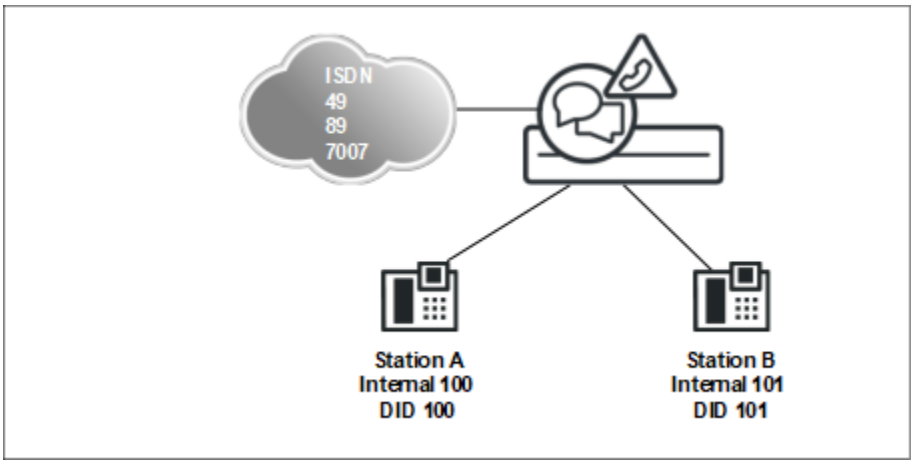


	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

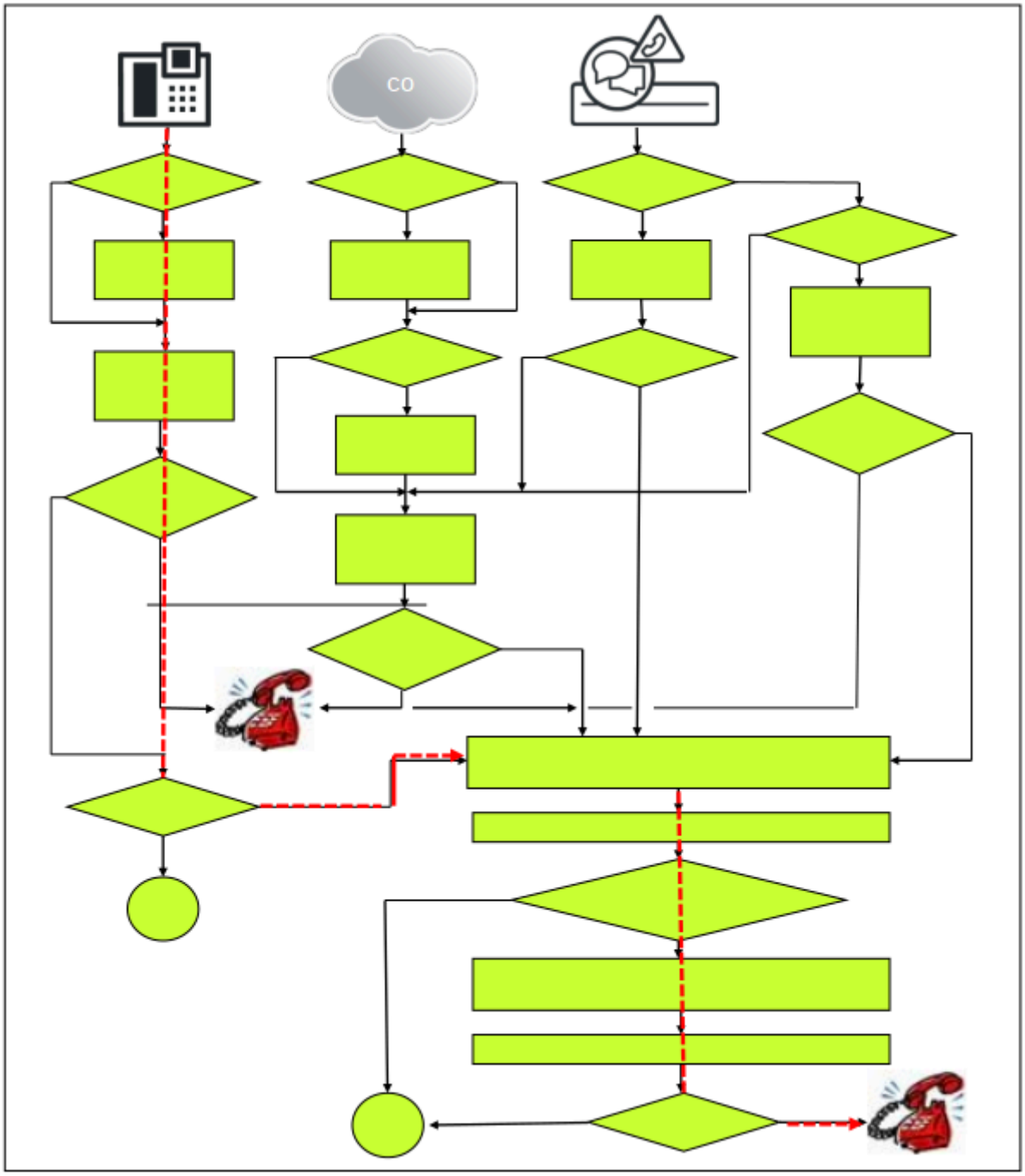
16.3.4.2 L'utente A chiama l'utente B tramite un numero della rete pubblica

Configurazione

Dipendenze del "Numero sede" (posizione gateway)

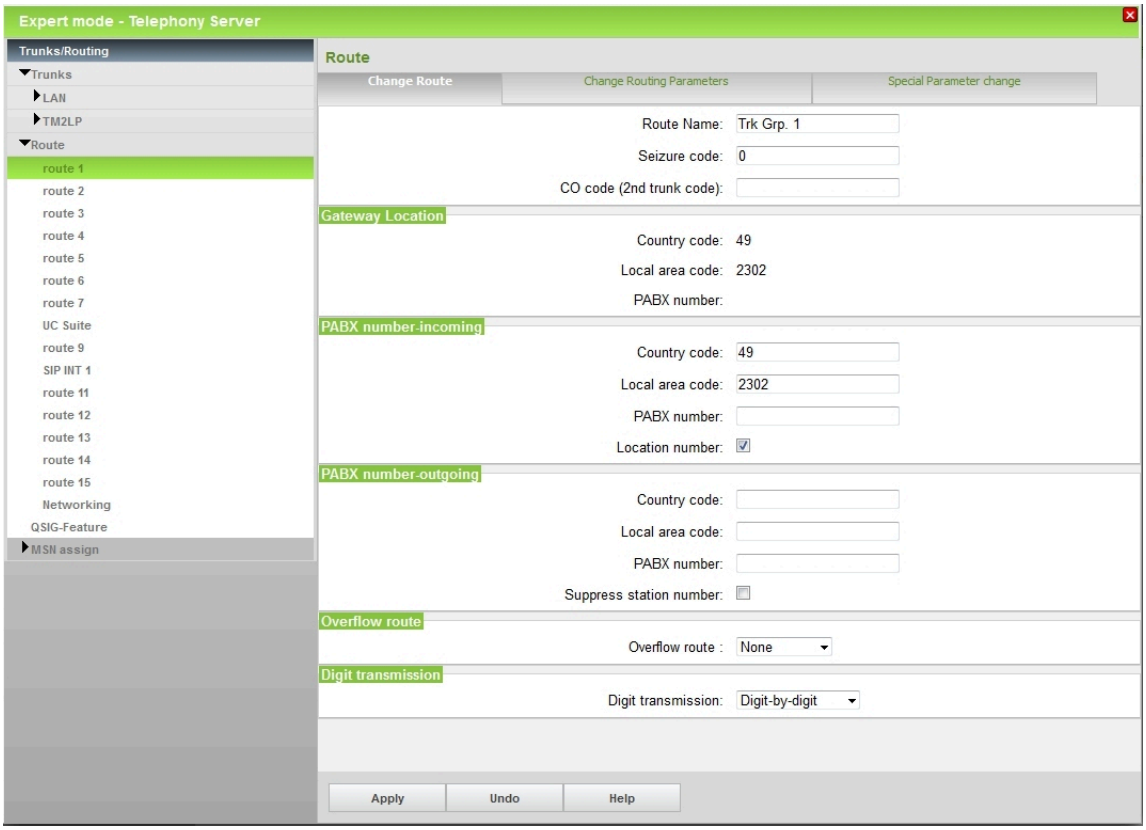


La chiamata viene istradata nel sistema interno, poiché il numero di destinazione è un utente DID del proprio sistema.



	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

Dopo il numero di telefono di destinazione utilizzando la posizione del gateway è stato spogliato, viene utilizzato per trovare il numero spogliato nella (DID) piano numero DID per una destinazione.

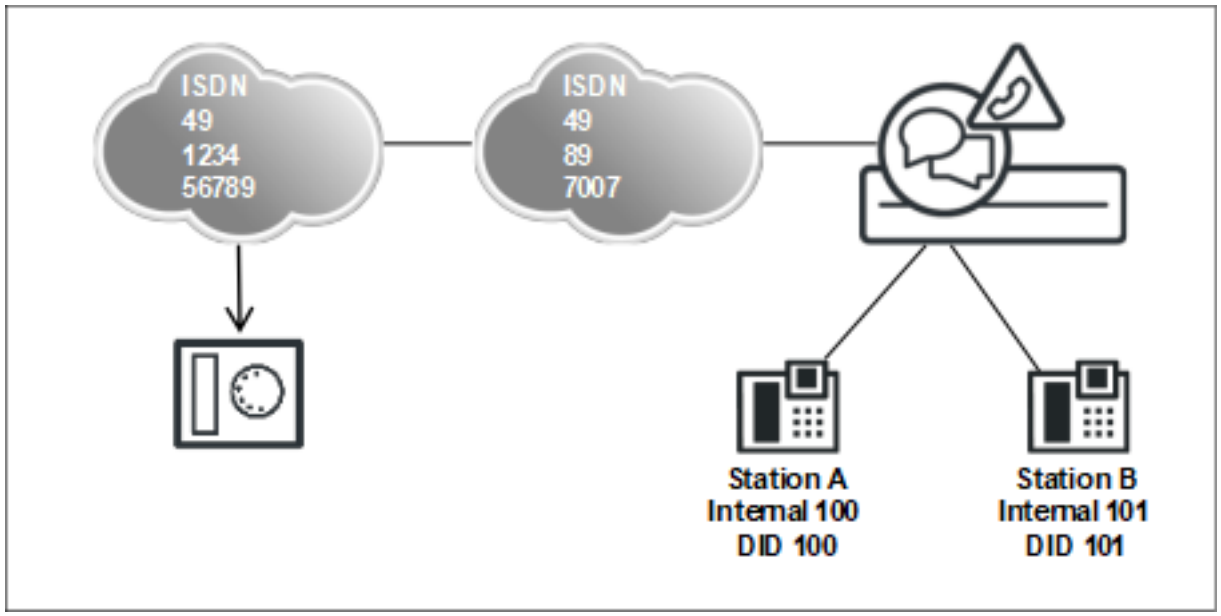


Il numero sede (sito gateway) viene analizzato durante la composizione sulla base del numero di telefono pubblico. Se le porzioni rilevanti del numero di telefono coincidono con questo numero, la tabella DID viene analizzata e in caso di corrispondenza, al destinazione interna in questione viene chiamata (nessun impegno della linea!). Impostando il flag Numero sito, i dati del sito vengono trasferiti automaticamente dai dati del fascio appropriati (numero PABX in entrata) e non richiedono alcuna modifica negli scenari standard.

Nella tabella DID possono essere inseriti solo numeri di telefono validi assegnati a questo sistema, poiché in caso contrario possono verificarsi effetti di mascheramento con i numeri di telefono nella rete pubblica. Può verificarsi in alcuni casi che venga chiamata una destinazione interna identificata tramite un numero DID non valido, anche se la chiamata era intesa per una destinazione esterna.

Le modifiche del flag "Numero sede" possono influenzare in alcune condizioni le voci LCR predefinite e preimpostate. Pertanto, quando cambia il numero della sede, occorre assicurarsi che l'impegno della linea predefinita funzioni come previsto. Ciò è importante per la composizione di numeri pubblici.

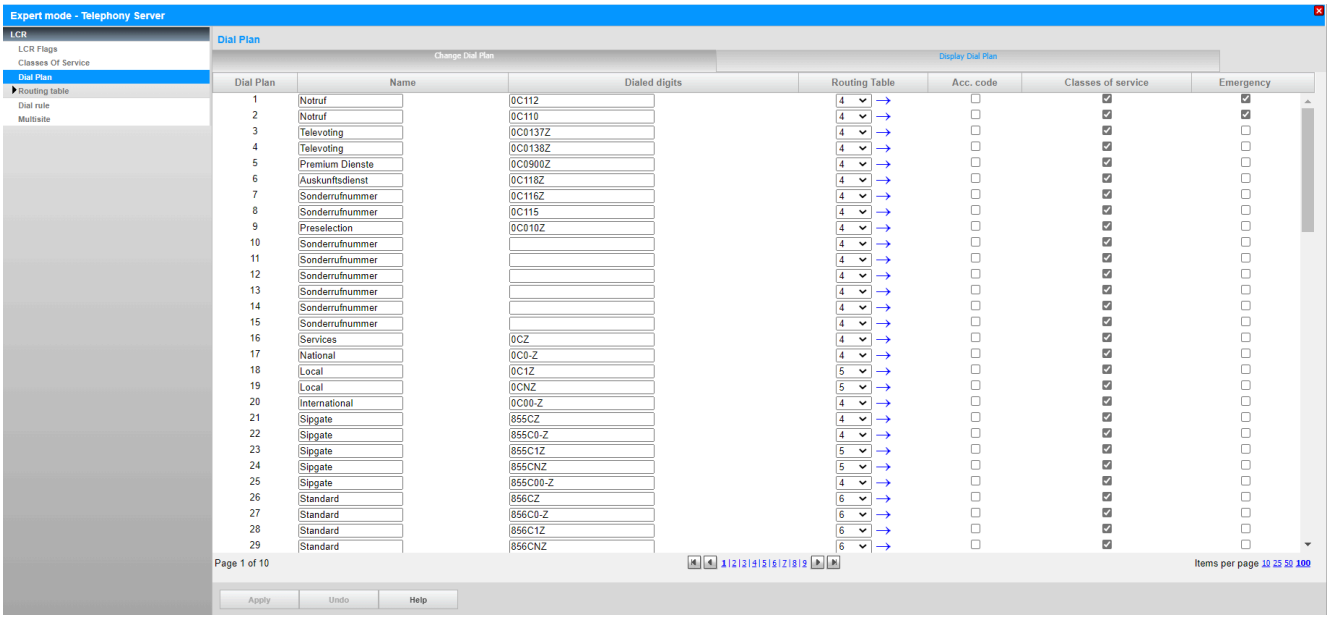
16.3.4.3 L'utente A chiama un utente interno tramite linea urbana



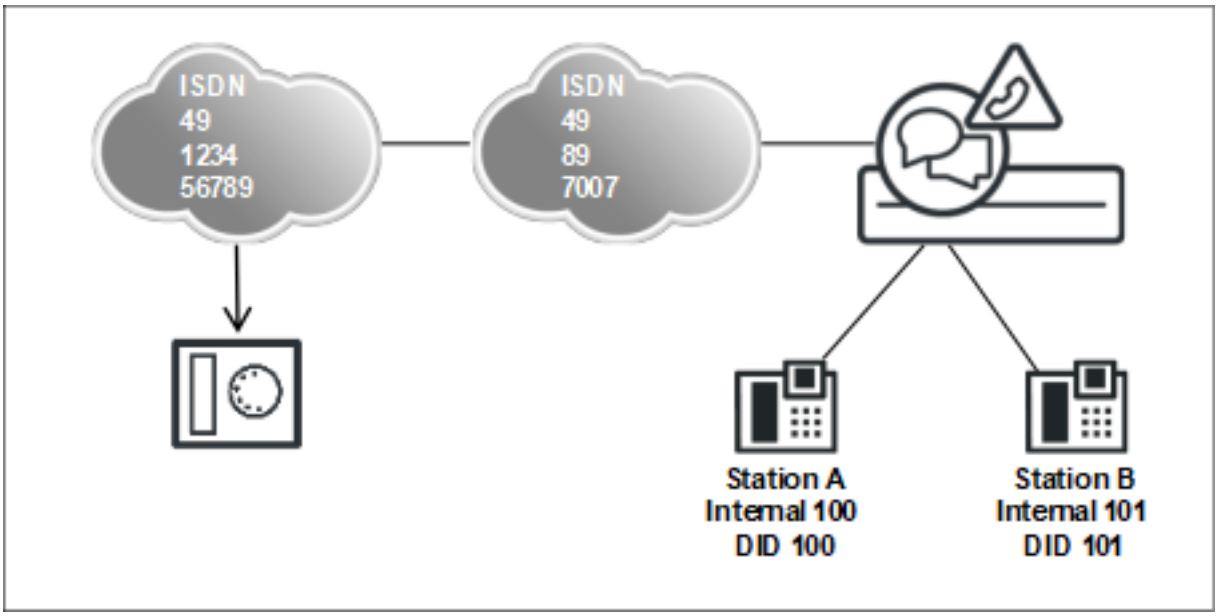
La chiamata viene instradata mediante LCR, in quanto la destinazione non si trova nel proprio sistema di comunicazione.

Oltre ai dati del precedente scenario "L'utente A chiama l'utente B tramite un numero di rete pubblica" nell'LCR deve essere presente una voce adatta del piano di composizione per l'impegno della linea esterna (ad esempio, "0CZ").

La tabella delle rotte LCR e il piano di composizione devono essere configurati di conseguenza.

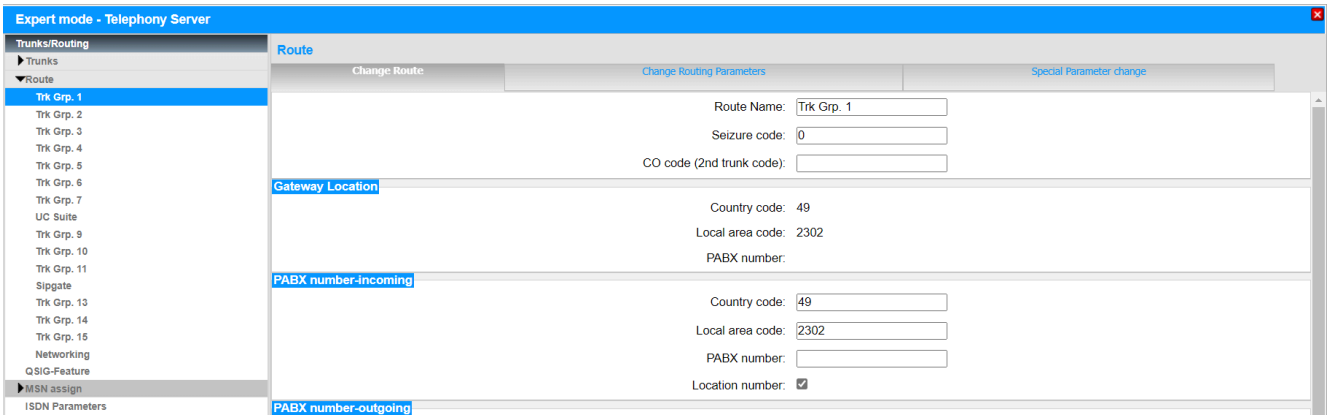


16.3.4.4 La linea esterna ISDN chiama l'utente A



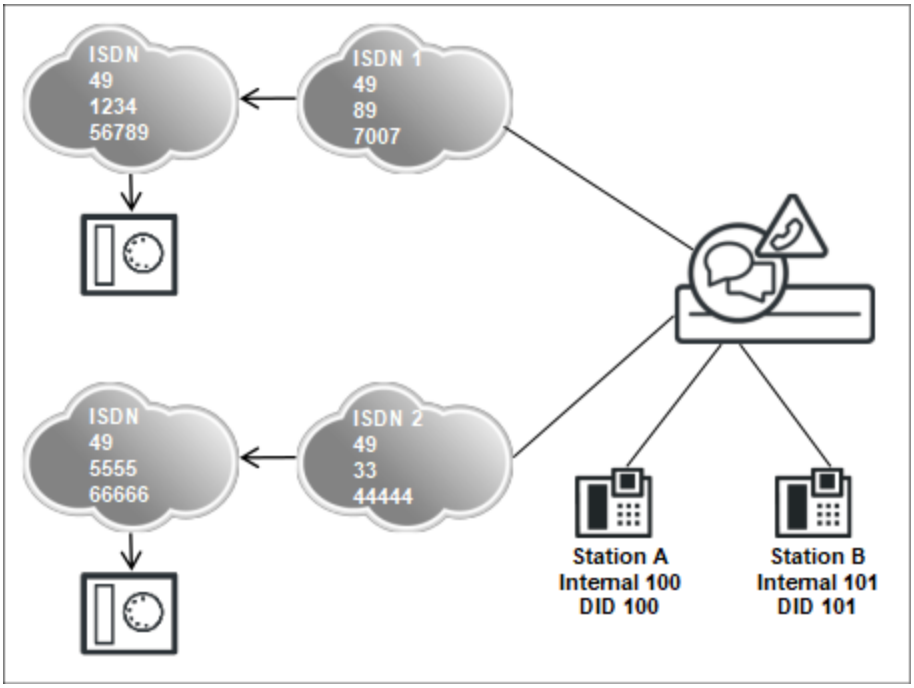
All'arrivo di una chiamata in arrivo su una linea ISDN, il numero di destinazione viene privato del fascio mediante i dati di configurazione disponibili nel centralino (numero centralino per chiamate in arrivo). Utilizzando la parte restante del numero di destinazione (DID), viene eseguita una ricerca della destinazione nel piano di composizione DID.

I parametri del sito gateway o il flag **Numero sede** non svolgono alcun ruolo per questo scenario.

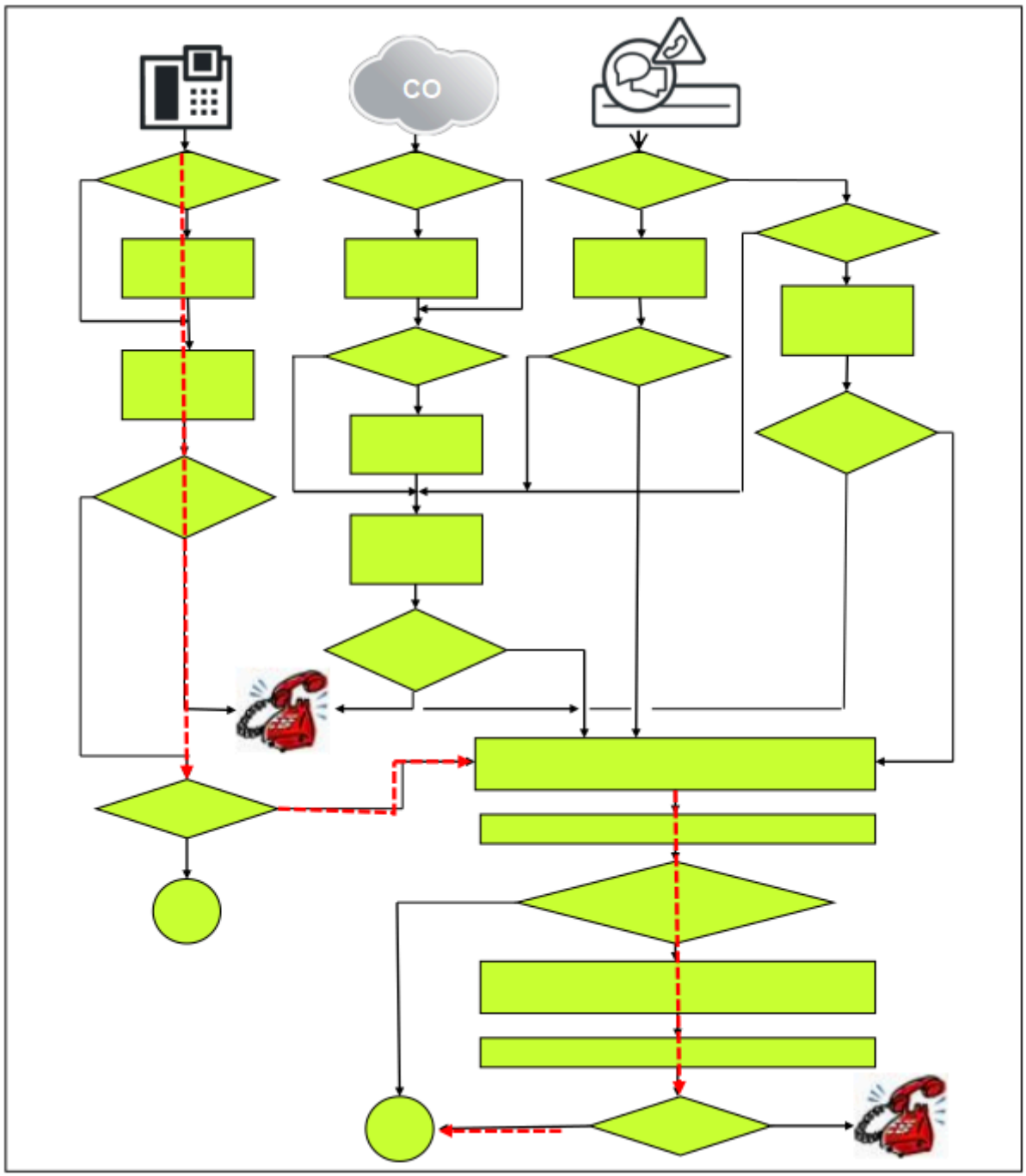


16.3.4.5 Configurazioni speciali

Configurazioni speciali e relativi effetti: 2 fasci linea esterna



L'utente A chiama un utente esterno tramite linea urbana 1 o 2



Esempio:

- Un cliente desidera utilizzare una connessione ISDN 1 standard. Questo viene configurato come numero della sede.
- In aggiunta viene utilizzata una seconda connessione ISDN 2 per applicazioni speciali.

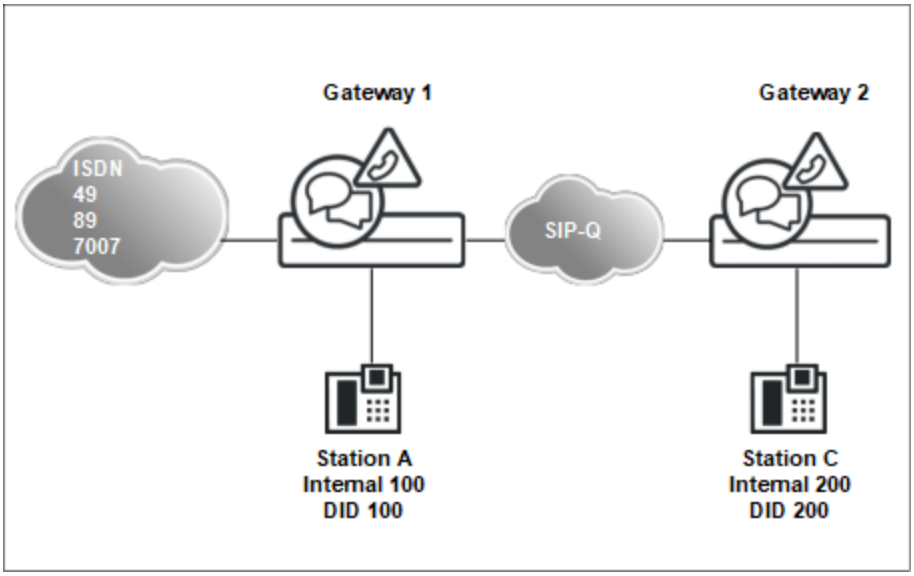
Note e limitazioni:

- Solo UNA linea esterna (ISDN 1 = posizione del sistema) è supportata pienamente, ovvero non può esservi alcuna configurazione multi-tenant (servizi multi-tenant) con connessioni alle linee urbane aventi gli stessi livelli di abilitazione.

- La linea esterna ISDN 2 aggiuntiva può essere utilizzato per le chiamate di base (in entrata/uscita).
- In scenari di switching complessi, in alcune circostanze non è possibile garantire una corretta rappresentazione dei numeri di telefono.
- Per il collegamento di applicazioni è supportato solo il numero di telefono locale, come per la composizione di destinazioni interne con numero di telefono pubblico.
- La configurazione, in relazione a fasci e LCR, può essere basata sugli esempi precedenti.

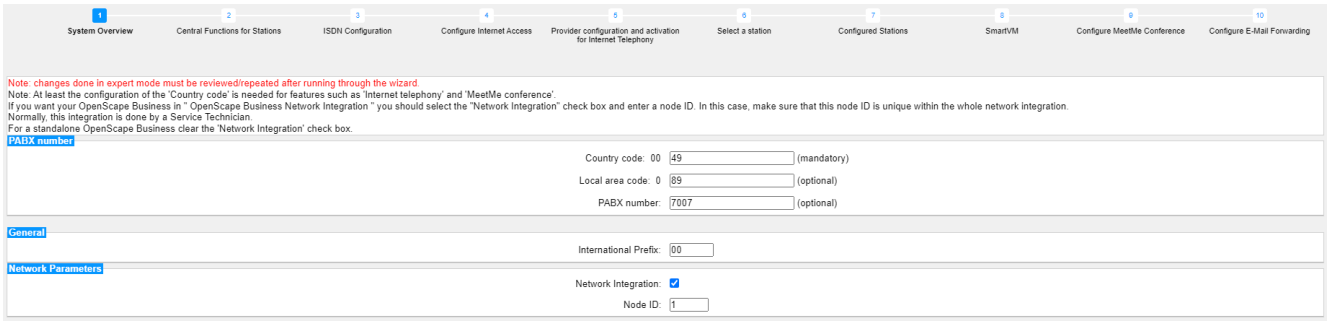
16.3.4.6 L'utente A chiama l'utente C tramite numero di telefono interno

Sistema di comunicazioni collegato in rete come sottosistema (senza linea esterna)



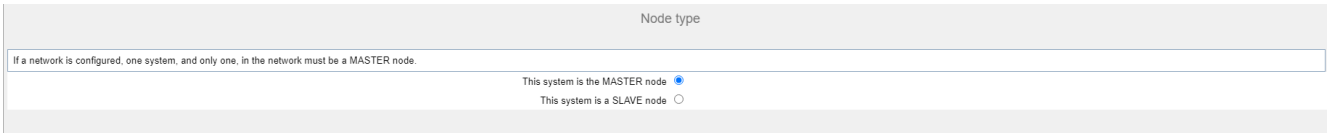
Requisiti richiesti per i sistemi indipendenti prima del collegamento in rete:

- Entrambi i sistemi di comunicazione dispongono di indirizzi IP univoci e sono inclusi nella rete IP del cliente.
- Entrambi i sistemi di comunicazione sono amministrati usando il WBM nella rete del cliente.
- Nell'installazione base, per il collegamento in rete a ogni sistema di comunicazione viene assegnato un ID nodo univoco (ad esempio, Sistema 1 = ID nodo 1 e Sistema 2 = ID nodo 2).
- Definizione della numerazione nell'installazione di base dei sistemi 1 e 2: nella definizione della numerazione dei sistemi indipendenti occorre prendere in considerazione la necessità di una numerazione chiusa nel futuro sistema di reti.
- Questo esempio presuppone che sia usata la numerazione di tipo chiuso (obbligatoria per l'uso della UC Suite!) e che la configurazione sia eseguita tramite la procedura guidata Rete. Con una numerazione di tipo aperto (possibile con UC Smart) non viene usata la procedura guidata Rete. Non viene usata neanche per una connessione con OpenScape Voice e OpenScape 4000.



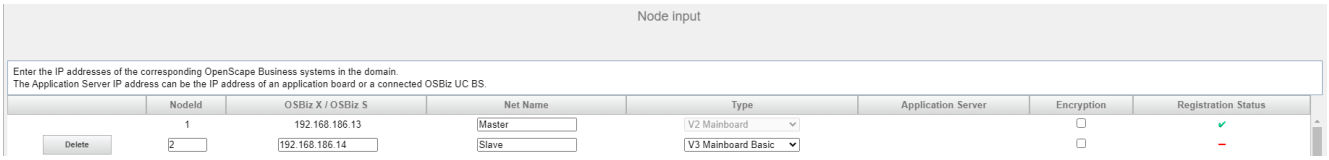
Avvio della procedura guidata Rete nel sistema 1. Questo sistema (nodo) viene impostato come master. Il master dispone di diverse funzioni centralizzate nel sistema di reti (ad esempio l'amministrazione, la gestione delle licenze nel server centrale, CSP a livello di rete).

Se nel sistema di reti è presente un OpenScape Business S, questo dovrebbe preferibilmente essere configurato come master (larghezza di banda, prestazioni).



Per ogni nodo vengono inseriti gli indirizzi IP, in questo modo i sistemi possono trovarsi a vicenda in modo indipendente al termine dell'amministrazione. In **Tipo** sono inseriti i sistemi OpenScape Business.

Questa finestra di dialogo deve essere compilata anche per il nodo 2 (slave).



Al termine della configurazione, i due sistemi (nodi) sincronizzano i propri numeri di telefono e inseriscono i numeri di telefono degli altri nodi nella tabella CAR.

Con la creazione delle tabelle CAR, è possibile la telefonia interna a livello di rete con numeri di telefono interni. La UC Suite è attivata anche a livello di rete. Gli altri passaggi per una messa in servizio completa della rete sono descritti negli altri scenari.

Il controllo delle voci CAR è possibile selezionando il percorso **Modalità esperti** > **Gateway voce** > **Rete** > **Routing**.

Per una panoramica della sincronizzazione automatica nel sistema di reti, vedere nel WBM (stato di sincronizzazione).

È ora possibile gestire altri nodi con accesso diretto utilizzando la voce di menu **Rete** disponibile nella barra di navigazione.

16.3.4.7 L'utente A chiama l'utente C tramite il numero di telefono pubblico nel sistema di reti

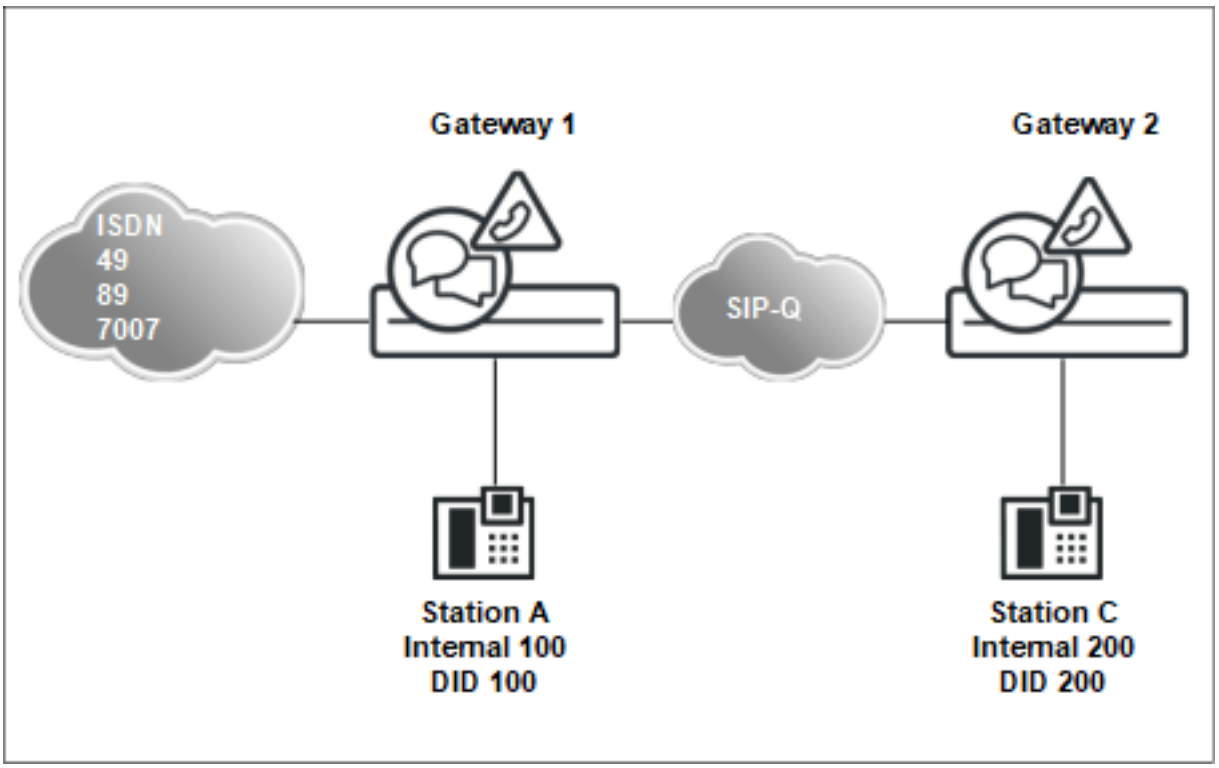
Sistema di comunicazioni collegato in rete come sottosistema

Configurazione del nodo 1, configurazione nell'LCR tramite gateway dedicato

Configurazione del nodo 2, configurazione del fascio "Rete"

Configurazione del nodo 2, configurazione del numero della sede nel fascio linea esterna "dummy"

Configurazione del nodo 2, configurazione nell'LCR tramite gateway dedicato



Particolarità di questo scenario:

- Il sistema 1 riconosce che il numero di destinazione non appartiene al proprio sistema. Nell'LCR viene eseguita un'ulteriore ricerca. Il gateway dedicato deve essere utilizzato nell'LCR del sistema 1 per l'indirizzamento diretto dell'ID nodo del sistema 2. Il numero di destinazione non è il numero interno della rete (si troverebbe nella tabella CAR), ma un numero di telefono di rete pubblica che può essere composto dagli utenti in tre diverse lunghezze:

  lungo = 00049897007nnn

  medio = 00897007nnn

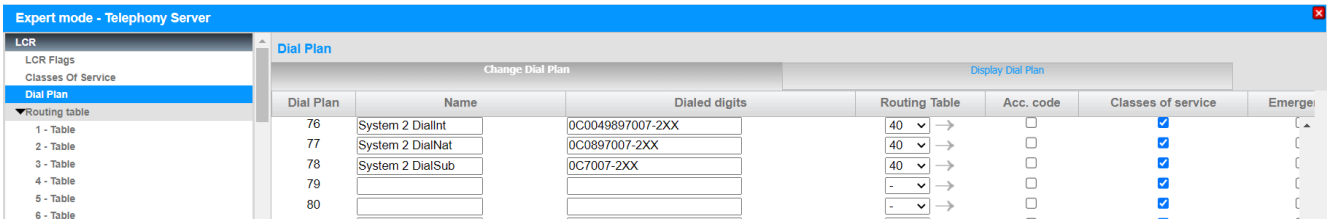
  corto = 07007nnn

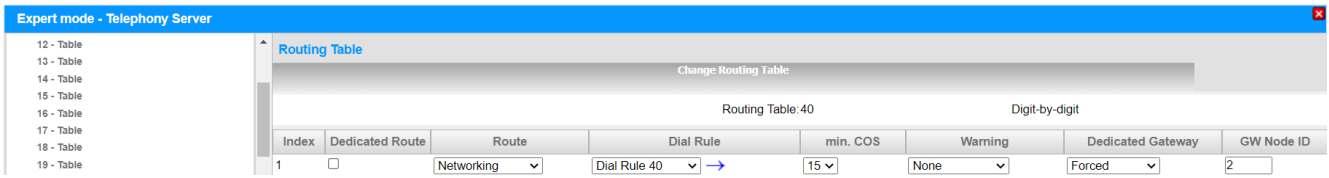
  L'esempio presuppone che tutti i numeri di selezione passante 2xx sono utenti del sistema 2.

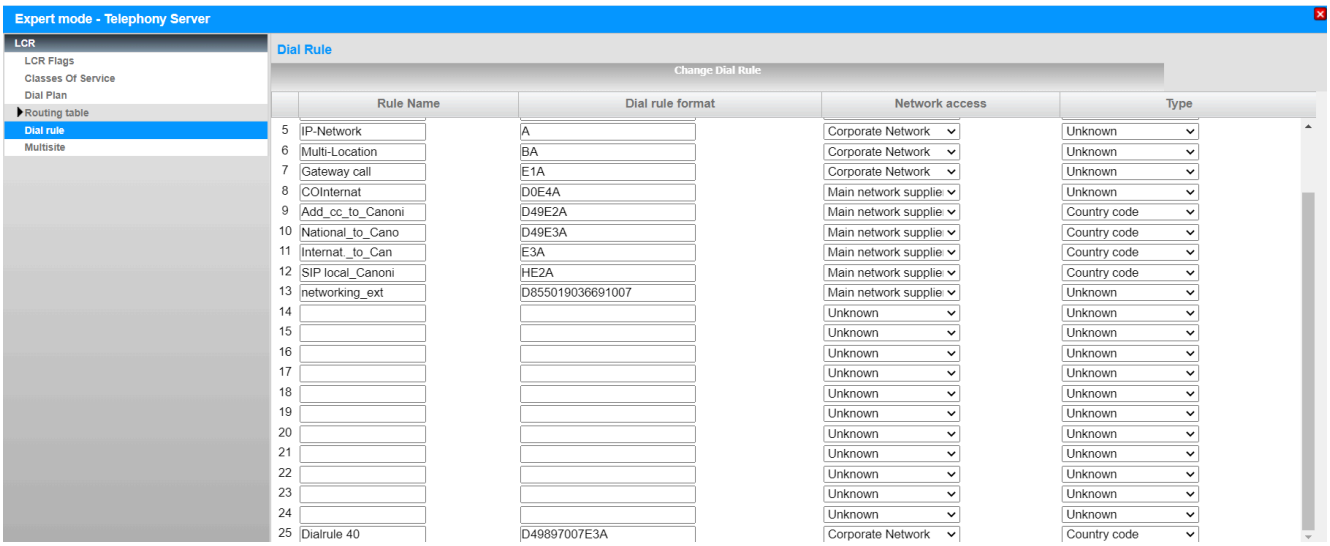
  Nota: Le voci del piano di composizione devono essere configurate in modo che TUTTI i numeri di telefono coinvolti appartengano realmente al sotto-nodo (sistema di reti). In caso di particolarità del piano di composizione, ciò può

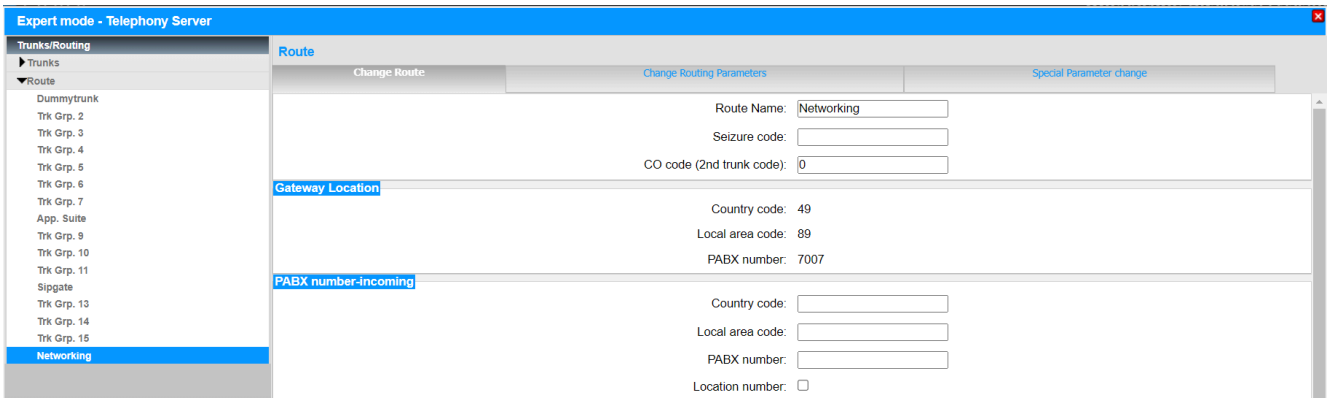
comprendere un grande numero di voci, ad esempio in caso di connessione di linea condivisa o di una configurazione MSN.

- Nel nodo 2, viene inserito un numero della sede con i dati predefiniti del nodo 1 (gateway) tramite un "fascio esterno fittizio". In questo modo, è possibile eseguire lo stripping del numero di telefono di destinazione dalla composizione del numero di rete pubblica prima della ricerca di una destinazione interna nel nodo 2.

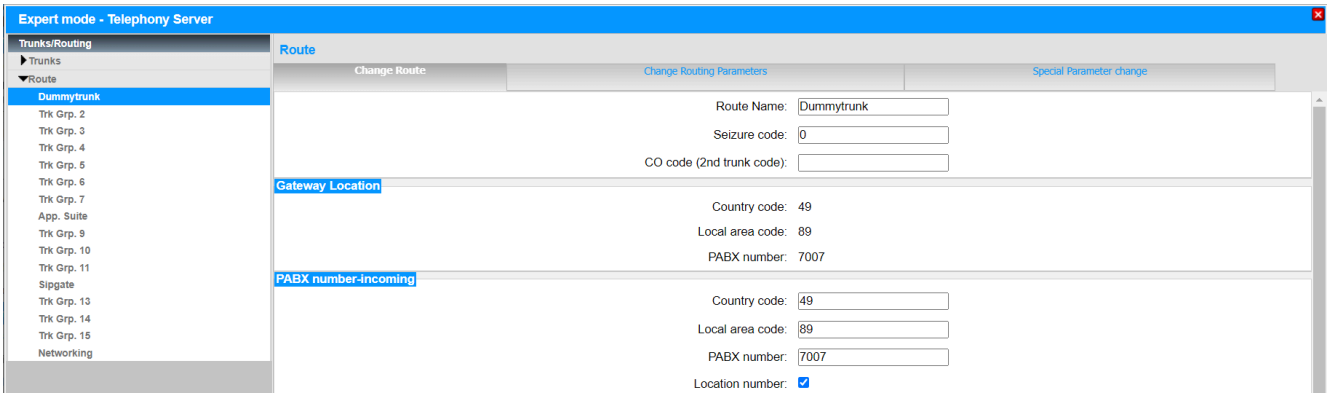








Nella scheda **Modifica parametri di routing** occorre inserire il tipo di fascio **PABX**.



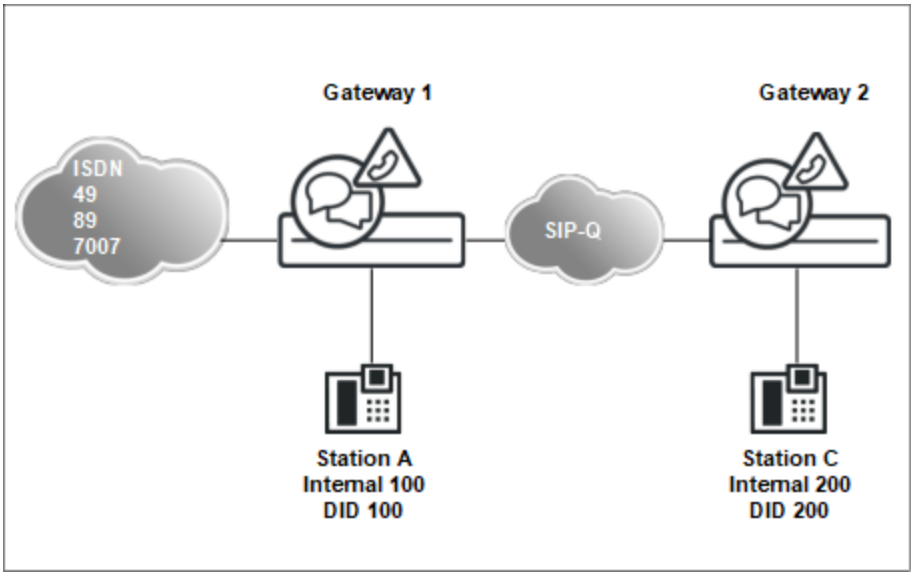
Nella scheda **Modifica parametri di routing** occorre inserire il tipo di fascio **CO**.

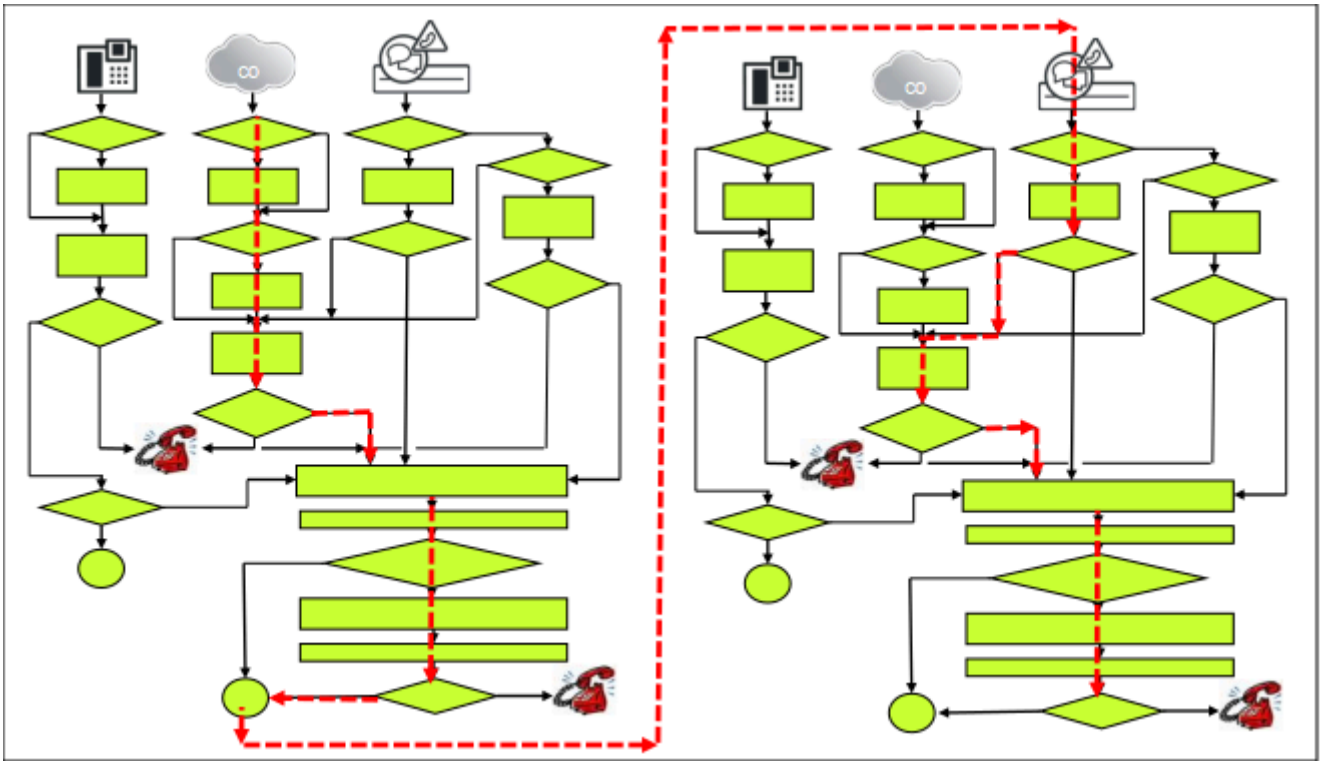
Nel nodo 2, tutti i numeri di telefono pubblici che non appartengono al proprio nodo vengono indirizzati al nodo 1 (scelta predefinita ad esempio 0CZ)

16.3.4.8 La linea esterna ISDN chiama l'utente C

Sistema collegato in rete come sottosistema

Particolarità di questa configurazione





Esempio: chiamata in arrivo con il numero di destinazione con TON = Utente

- Il nodo 1 deve essere configurato come descritto nello scenario precedente.

  In entrambi i casi, l'indirizzamento del nodo 2 avviene mediante il numero pubblico, indipendentemente dal fatto che l'origine della connessione si trovi nel nodo 1 (utente del sistema 1) o nella rete pubblica.

  Suggerimento: Le voci del piano di composizione devono essere configurate in modo che TUTTI i numeri di telefono coinvolti appartengano realmente al sotto-nodo (sistema di reti). In caso di particolarità del piano di composizione, ciò può comprendere un grande numero di voci, ad esempio in caso di connessione di linea condivisa o di una configurazione MSN.

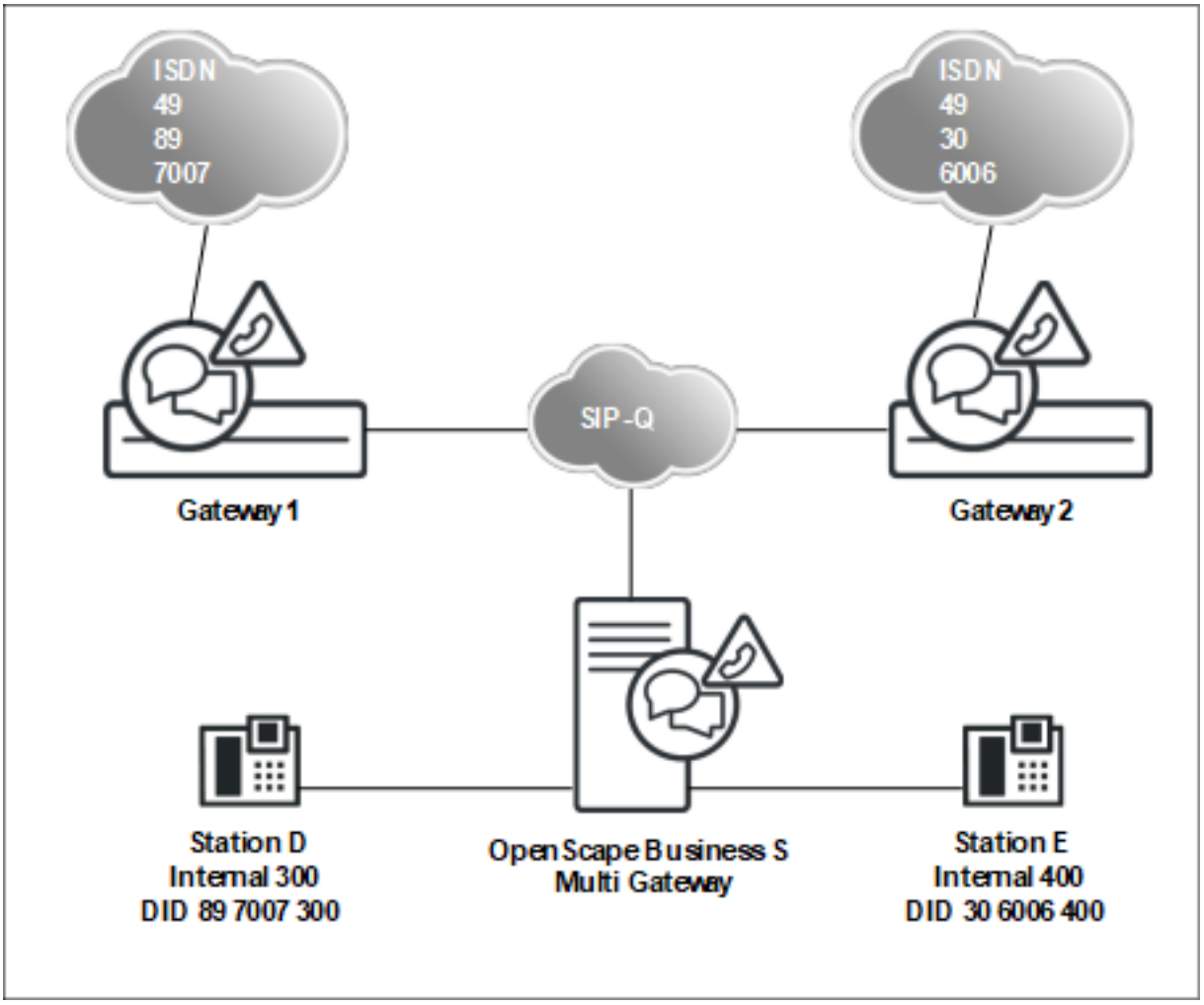
- Anche il nodo 2 deve essere configurato come descritto nello scenario precedente.

16.3.4.9 Il gateway 1 della linea esterna ISDN chiama l'utente D

Sistema collegato in rete in configurazione con gateway multiplo

Configurazione

Configurazione del Gateway multiplo, OpenScape Business S

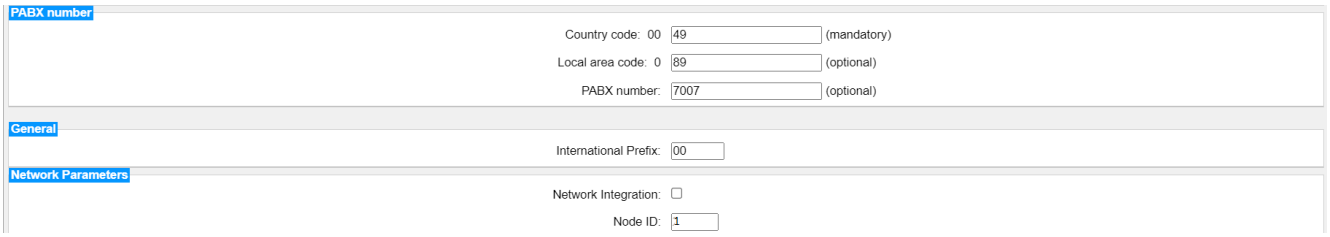


Esempio: chiamata in arrivo con il numero di destinazione con TON = Utente

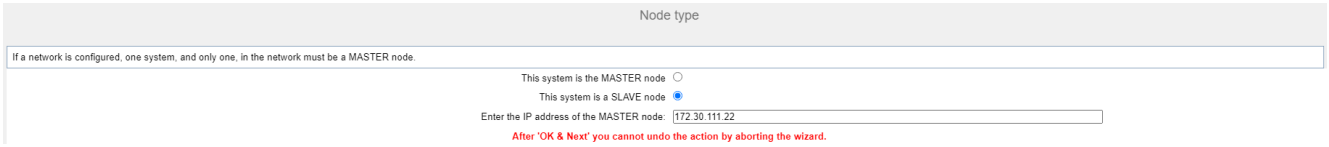
Particolarità in questo scenario:

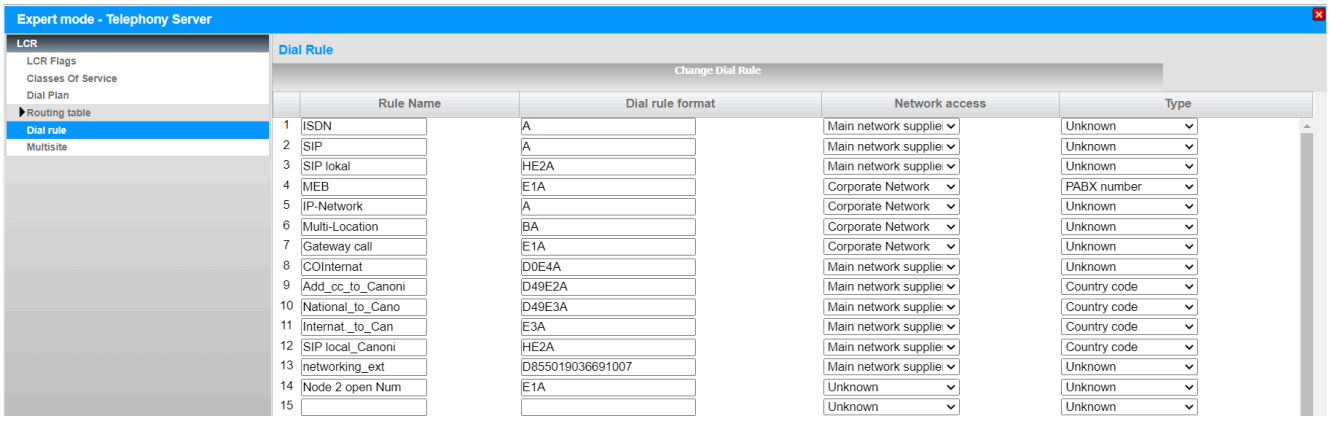
- Il gateway 1 viene in generale configurato come nello scenario precedente (gateway 1), tramite l'installazione di base prima e successivamente eseguendo la procedura guidata Rete. Differenza essenziale: i gateway vengono configurati come slave, OpenScape Business S viene configurato come master (prestazioni, larghezza di banda, concessione licenze).
- In questo esempio, vengono richiamate solo le principali differenze con il precedente scenario.

Installazione di base del Gateway 1



Procedura guidata Rete per Gateway 1





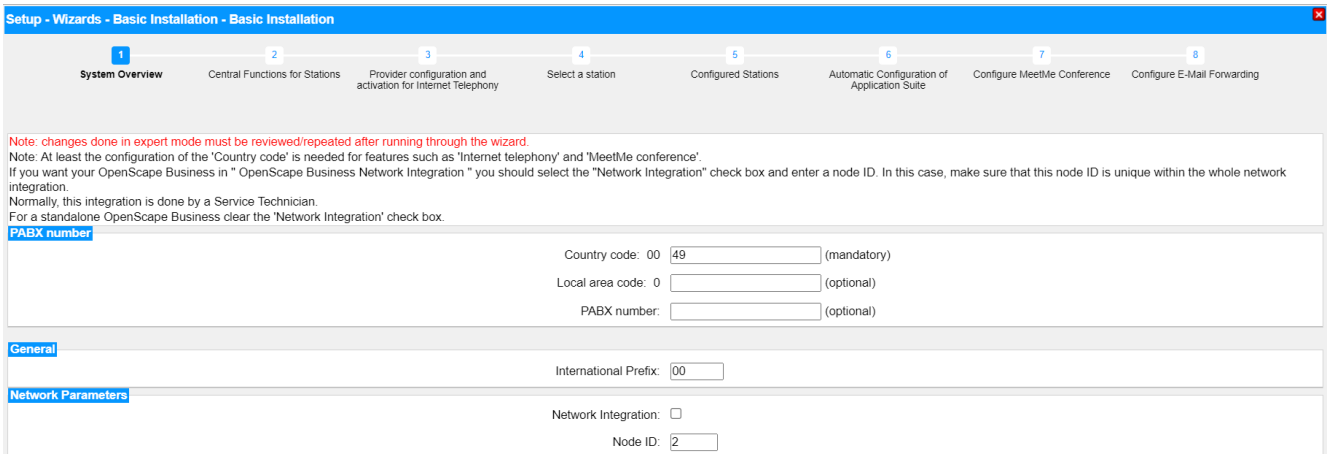
In OpenScape Business S, il numero di destinazione è inserito già nel formato nazionale, come DID.

"BA" (Broaden All) è importante solo per il gateway.

"BA" è necessario solo se si è ricevuto un numero di destinazione originale TON sconosciuto, ovvero contenente solo la porzione di estensione "short DID".

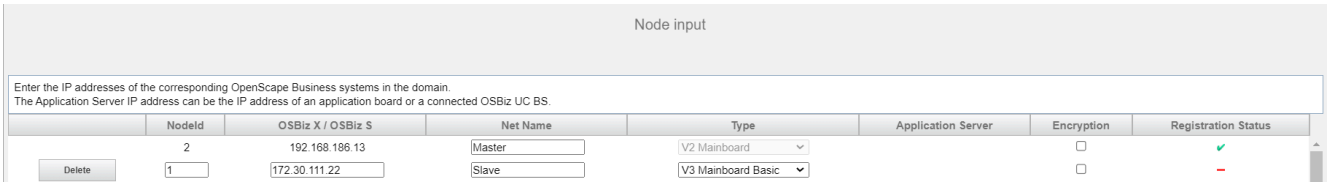
- Una volta completata l'installazione di base, viene eseguita la procedura guidata Rete.
- Per ogni utente di OpenScape Business S viene configurato quanto segue:
  - Numero interno in formato breve (ad esempio 300)
  - Numero DISA nel formato nazionale (ad esempio 02 7007 300)
  - ID nodo gateway associato

Installazione di base di OpenScape Business S, Gateway multiplo



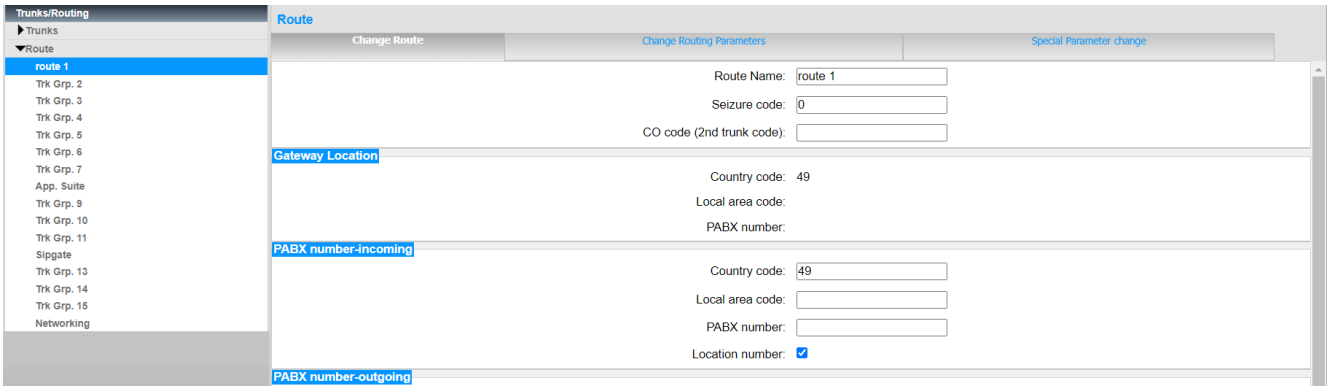
Suggerimento: Per i dati di sistema inserire solo il codice paese, il resto del numero di telefono completo è inserito nella voce DID dell'utente.

Procedura guidata Rete per OpenScape Business S, MultiGateway



Selezionare MultiGateway nella configurazione di rete.

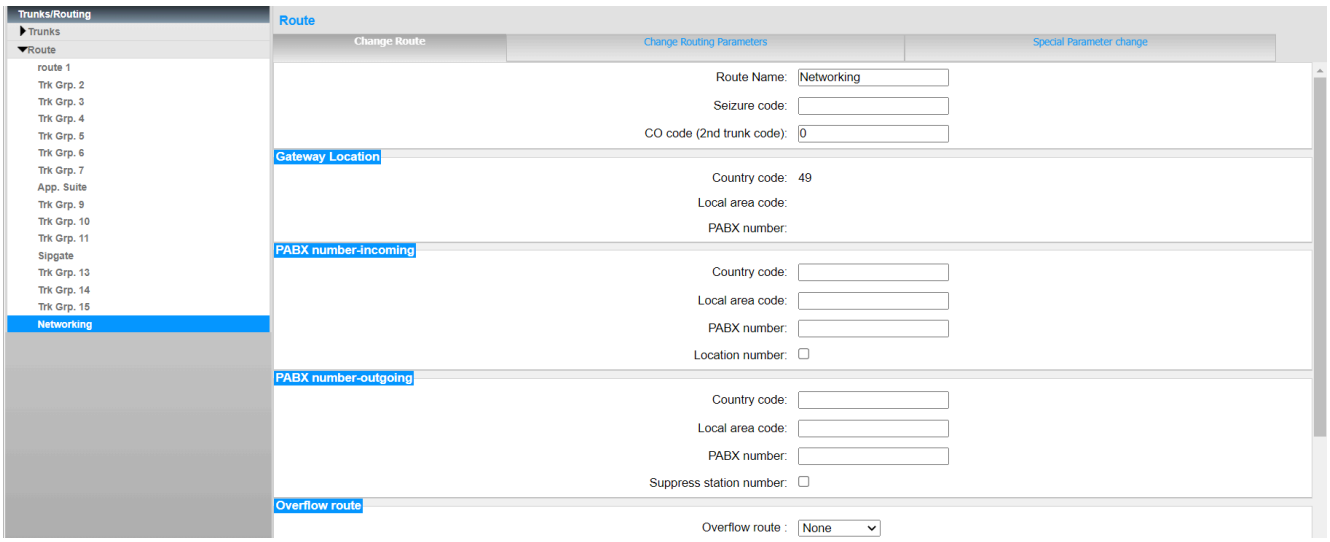
Fasci di OpenScape Business S, Gateway multiplo



Il codice del paese è già precompilato nella procedura guidata.

Parametri di routing: tipo di fascio linea urbana

Questo fascio diventa il tipo di fascio "linea urbana".



Parametri di routing: tipo di numero in uscita = nazionale, tipo fascio PABX

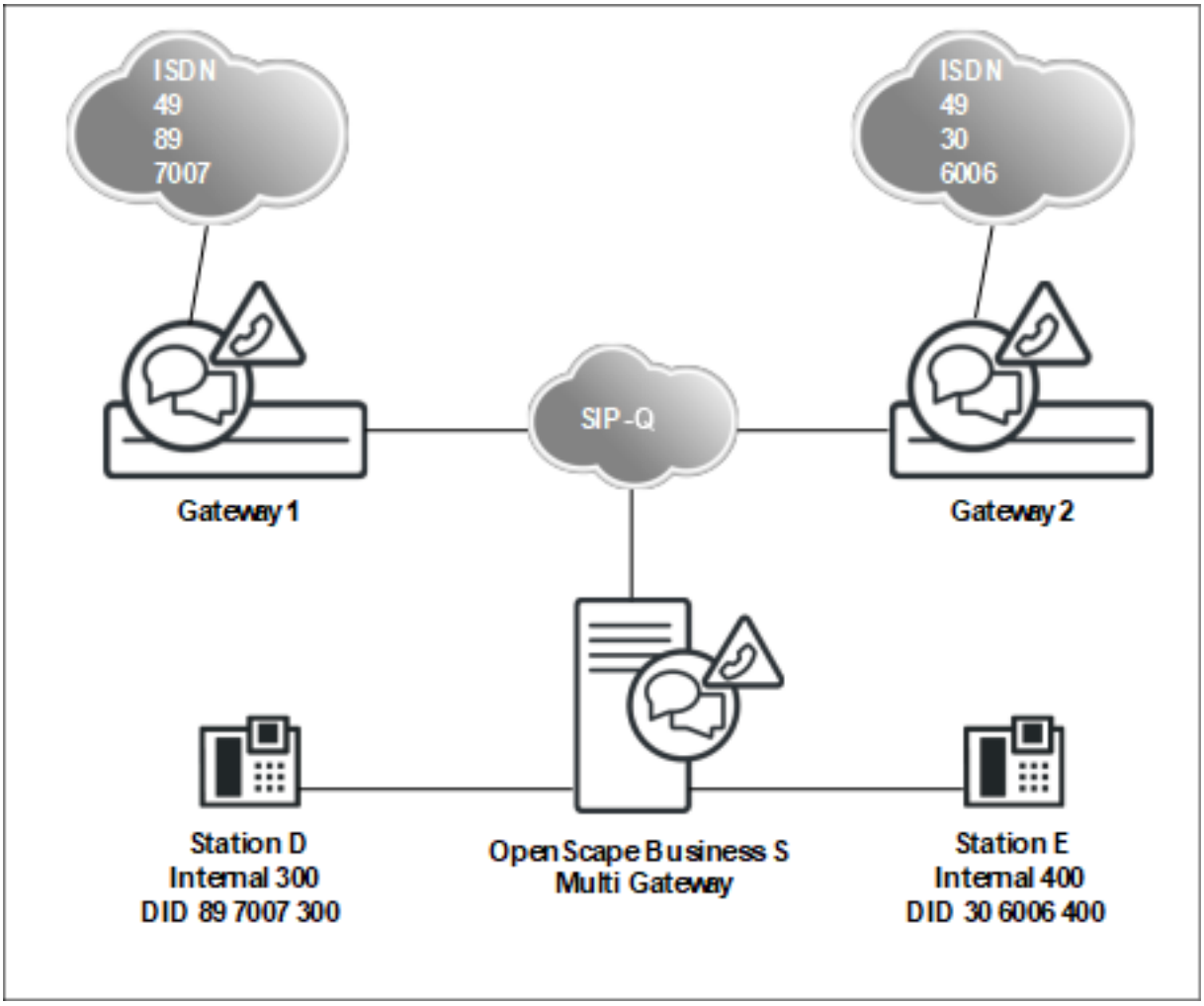
Questo fascio diventa il tipo di fascio "PABX" o occorre digitare nel parametro Tipo n., in uscita l'opzione **Prefisso interurbano**.

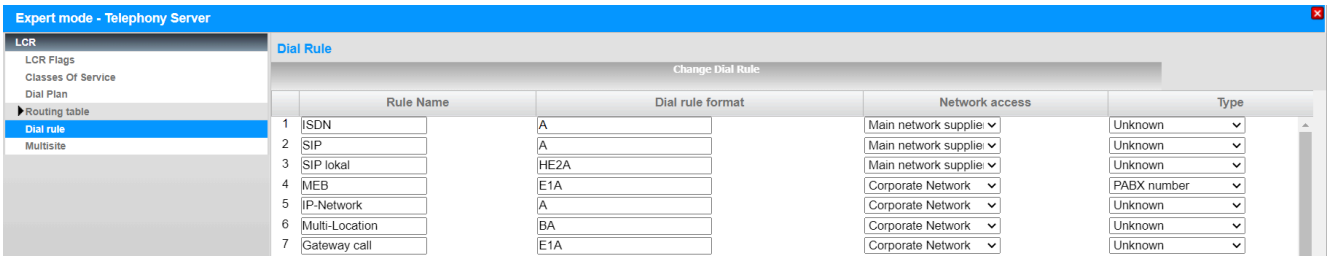
16.3.4.10 L'utente D chiama un utente esterno tramite linea urbana

Sistema collegato in rete in configurazione con gateway multiplo

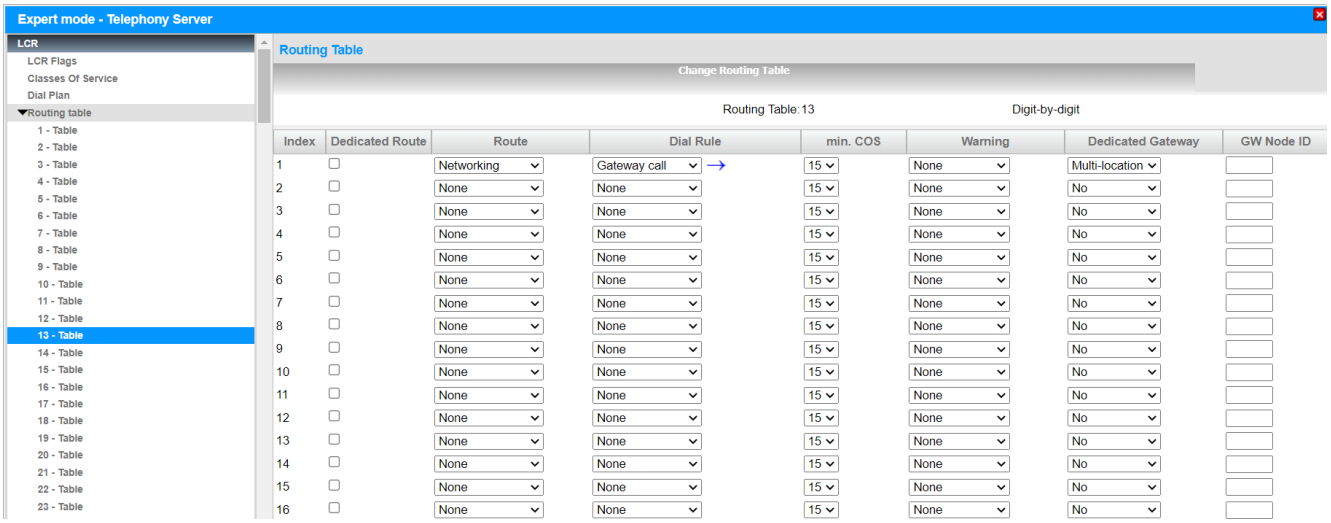
Configurazione di OpenScape Business S, Gateway multiplo

Routing di OpenScape Business S, gateway multiplo, ai gateway





	Rule Name	Dial rule format	Network access	Type
1	ISDN	A	Main network supplie	Unknown
2	SIP	A	Main network supplie	Unknown
3	SIP lokal	HE2A	Main network supplie	Unknown
4	MEB	E1A	Corporate Network	PABX number
5	IP-Network	A	Corporate Network	Unknown
6	Multi-Location	BA	Corporate Network	Unknown
7	Gateway call	E1A	Corporate Network	Unknown



L'installazione del gateway 1 è uguale a quella dell'esempio precedente. Questo vale anche per il gateway 2.

16.4 Chiamate di emergenza

Il sistema di comunicazione e i telefoni collegati offrono varie opzioni per interrompere una chiamata di emergenza. L'amministratore può configurare una Hotline normale o a tempo o un servizio di emergenza.

Se il periodo di attivazione non è ancora iniziato o se il sistema di comunicazione si trova nel periodo di failover, le chiamate di emergenza possono sempre essere eseguite dai primi due telefoni attivi.

Requisiti

Il call center di emergenza è raggiungibile digitando la cifra per la linea urbana (ad esempio, 0) e il numero di emergenza, (ad esempio, 112). Dalle applicazioni, la composizione del numero di telefono di destinazione per le chiamate di emergenza deve essere eseguita premettendo il codice di linea urbana.

Sequenza di base

Caso 1: Selezione di chiamata di emergenza tramite linea PSTN

Caso 2: Selezione di chiamata di emergenza tramite ITSP

Caso 3: Accordo speciale con ITSP o provider PSTN

Caso 4: Chiamate di emergenza con Mobile Logon (IP Mobility)

Le chiamate di emergenza vengono eseguite da un utente del sistema di comunicazione mediante la selezione di un codice per la linea urbana e del numero di emergenza. Il numero chiamata emergenza viene trasmesso dal sistema di comunicazione al rispettivo provider (PSTN o ITSP).

La chiamata di emergenza viene effettuata nella rete locale a cui il terminale del sistema di comunicazione è assegnato. Occorre osservare quanto segue: tutti

gli utenti che non si trovano nella stessa località del sistema di comunicazione (ad esempio utenti Mobility, CallMe (operatori remoti) o utenti con telefoni collegati alla WAN) devono digitare il numero di emergenza tramite un cellulare o altro telefono di rete fissa per inviare la chiamata di emergenza sulla rete locale della propria località.

Non tutti gli ITSP supportano le chiamate di emergenza. In questo caso, deve essere utilizzata la configurazione LCR per assicurare che le chiamate di emergenza vengano istradate tramite PSTN.

Nei casi in cui non tutti gli utenti del sistema di comunicazione siano ubicati nella stessa località, ma tuttavia siano assegnati permanentemente a una singola località senza un PSTN proprio, è possibile concordare con il provider una procedura personalizzata per le segnalazioni di emergenza Ad es.: In funzione dell'ID del chiamante, la chiamata di emergenza potrebbe essere istradata dal provider verso la rete locale appropriata, come concordato. Questo tipo di accordi viene concluso su base individuale e non è soggetto a linee guida.

Mobile Logon (Mobility IP) consente agli utenti di cambiare l'apparecchio telefonico, continuando a utilizzare il proprio numero di telefono.

In questo caso, le telefonate sono possibili finché i telefoni sono collegati presso la stessa località del gateway. Tutti gli utenti che non si trovano presso lo stesso sito del gateway (ad esempio, utenti Mobility, operatori remoti CallMe, terminali collegati via WAN) dovranno comporre il numero di emergenza tramite un cellulare o altro apparecchio fisso per realizzare la chiamata di emergenza nella rete locale della propria località.

Suggerimento: Per ogni scenario MultiGateway in cui è configurato il servizio Mobile Logon, si applicano requisiti speciali. La configurazione corrispondente viene descritta nella sezione "Chiamate di emergenza in combinazione con Mobile Logon".

16.4.1 Hotline a tempo / Hotline

Per ogni utente si può attivare una funzione Hotline. Questo determina se eseguire la connessione a una destinazione Hotline immediatamente quando viene sollevato il ricevitore (Hotline) o dopo un tempo prestabilito (Allarme dopo timeout).

Hotline a tempo

Se l'utente entro il tempo predefinito digita una qualsiasi cifra, non viene stabilita **alcuna** connessione alla destinazione Hotline.

Il ritardo viene configurato dall'amministratore centralmente e può essere attivato e disattivato per i singoli utenti.

Hotline

Quando la Hotline è attivata, l'utente non ha **alcuna** possibilità di digitare un numero di telefono dopo aver sollevato il ricevitore. È possibile comporre un numero di telefono prima di sollevare il ricevitore. Sollevando il ricevitore, l'utente raggiunge automaticamente la destinazione Hotline interna o esterna predefinita.

L'utente viene sempre inoltrato come previsto dalle impostazioni della destinazione Hotline.

Informazioni specifiche del sistema

L'amministratore può configurare 6 destinazioni Hotline e la durata del ritardo (0-99 secondi). Se l'amministratore imposta un tempo di ritardo pari a 0, la destinazione Hotline viene chiamata immediatamente.

Dipendenze

Argomento	Dipendenza
Non disturbare	Se presso l'utente di destinazione è attivata la funzione Non disturbare, il chiamante sente il segnale di occupato.

16.4.1.1 Come configurare e modificare le destinazioni Hotline

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu selezionare **Sistema** > **Rinvio/PO/Hotline**.
4) In **Hotline** è possibile definire 6 diverse destinazioni Hotline (**Nr. di telefono di destinazione**).
5) Fare clic su **Applica**, quindi su **OK**.

16.4.1.2 Come modificare il tempo di ritardo Hotline

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema**.
4) Fare clic su **Rinvio/PO/Hotline**.
5) In Hotline è possibile modificare il **tempo di hotline** (ritardo in secondi).
6) Fare clic su **Applica**, quindi su **OK**.

16.4.1.3 Come configurare A tempo o Hotline per un utente

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Nella struttura dei menu fare clic su **Utente**.
4) Fare clic ad es. su **Client IP**.
5) Fare clic ad es. su **Client di sistema**.
6) Selezionare l'utente desiderato, quindi **A tempo** o **Hotline** nel campo della modalità **Hotline**.
7) Una volta definita la modalità è necessario impostare il **numero delle destinazioni Hotline** nel campo Hotline.
8) Fare clic su **Applica**, quindi su **OK**.

16.4.2 Rilascio della linea per una chiamata di emergenza

Se si effettua una chiamata di emergenza e non sono disponibili linee libere, viene eseguita un'interruzione forzata. L'utente che effettua la chiamata di emergenza viene assegnato automaticamente alla linea libera.

L'interruzione della connessione funziona sulle linee ISDN e ITSP.

L'utente può, se le linee sono occupate, eseguire un'interruzione manuale o automatica della connessione.

- Automatica: il servizio Instradamento a minor costo (LCR) è attivato ed in esso è memorizzato un numero di emergenza.
- Manuale: il servizio "Rilascio linea" è sempre attivo per la console posto operatore e può essere eseguito tramite un tasto o un codice.

Informazioni specifiche del sistema

L'amministratore può configurare una quantità a piacere di numeri di emergenza.

Perché sia possibile l'interruzione automatica della connessione quando tutte le linee sono occupate, il numero di emergenza deve essere inserito nel piano di composizione del sistema LCR e deve essere attivato il flag Chiamata di emergenza in *Modalità esperti*.

16.4.2.1 Come attivare/disattivare l'interruzione della connessione per chiamata di emergenza

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **Routing**.
3) Nella struttura dei menu selezionare **LCR** > **Piano di composizione**.
4) Nella finestra **Modifica piano di composizione**, selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **N. chiamata emergenza** per il numero di telefono corrispondente.
   - Per disattivare la funzione, deselezionare la casella di controllo **N. chiamata emergenza** per il numero di telefono corrispondente.
5) Fare clic su **Applica**, quindi su **OK**.

16.4.3 Solo per USA e Canada: servizio d'emergenza E911

Il servizio di emergenza avanzato E911 trasmette, oltre al numero di telefono, informazioni sulla posizione geografica (ad es. indirizzo) del chiamante.

La stazione di pronto intervento che riceve la chiamata non deve quindi attendere la comunicazione vocale della sede della chiamata.

Negli USA si accede a questo servizio solo componendo il numero di emergenza 911.

Per il servizio di emergenza E911 a ciascun terminale utente associato a un interno deve essere assegnato un LIN (Location Identification Number) valido dall'amministratore. A due connessioni utente vicine va assegnato lo stesso LIN. Un database nella centrale del servizio d'emergenza, dove sono memorizzati tutti i LIN, identifica il nome e l'indirizzo del chiamante sulla base del LIN trasmesso.

Dipendenze

Argomento	Dipendenza
CLIP	Per gli USA il LIN è attivato. Se si attiva CLIP (Calling Line Identification Presentation) per gli USA, LIN viene disattivato automaticamente.

16.4.3.1 Come modificare CLIP / Lin

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Nella struttura dei menu fare clic su **Utente**.
4) Fare clic ad es. su **Client IP**.
5) Fare clic sulla scheda **Modifica utente**.
6) Nel campo **CLIP/Lin** immettere il LIN a 16 cifre per l'utente corrispondente.

7) Fare clic su **Applica**, quindi su **OK**.

16.4.4 Chiamate di emergenza in combinazione con Mobile Logon

Se si utilizza il servizio Mobile Logon in un sistema di reti MultiGateway, passando a un altro telefono può cambiare anche la posizione fisica. Sono quindi necessarie misure particolari per il routing di chiamate di emergenza.

Descrizione dell'algoritmo per la composizione di una chiamata di emergenza

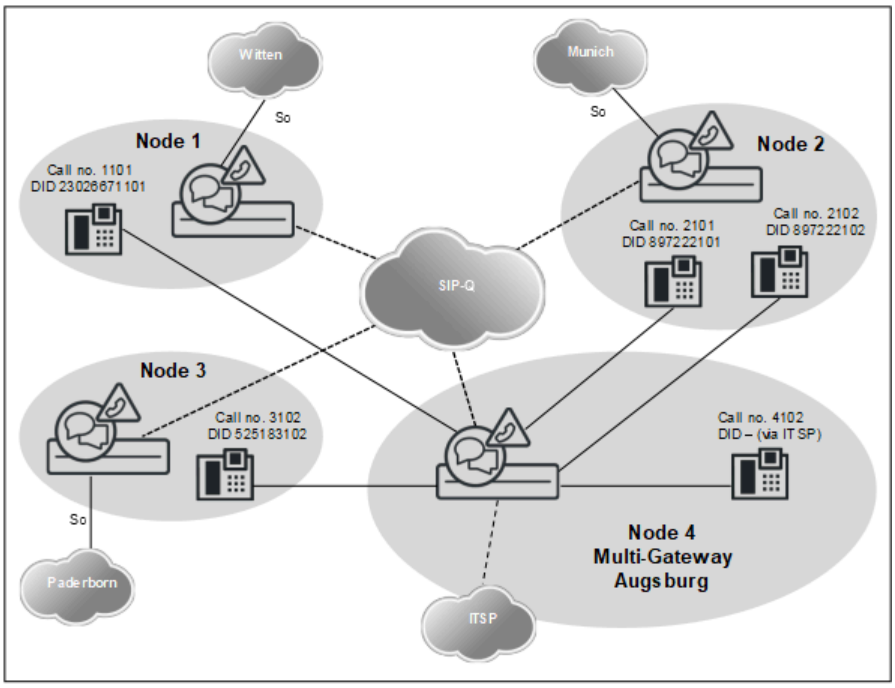
Se un utente seleziona il numero di telefono d'emergenza (codice nell'LCR), l'algoritmo controlla se per il telefono è stato configurato un numero di telefono d'emergenza. Questo viene quindi impiegato per la creazione di un numero di telefono derivato da utilizzare sul sistema di reti per l'istradamento della chiamata tramite il gateway corretto.

Ciascun numero contrassegnato nel piano di composizione come numero di emergenza presenta inoltre un rimando a una voce della tabella delle rotte. Ciascuna voce nella tabella delle rotte che appartiene a un numero di emergenza deve essere associata a una classe di autorizzazione (COS) "bassa". Una classe di autorizzazione bassa significa che ogni utente è autorizzato a effettuare chiamate di emergenza.

16.4.4.1 Configurazione dello scenario di emergenza

La configurazione dello scenario di emergenza mostra, per un singolo sistema di reti MultiGateway, i passaggi di configurazione da eseguire.

Trattamento dei numeri di emergenza



Mobile Logon è supportato solo all'interno di un nodo, ciò significa che i cambiamenti di località, e quindi i requisiti speciali per le chiamate di emergenza, sono rilevanti solo per i telefoni che possono essere utilizzati sul nodo MultiGateway (4). In generale, tutti i telefoni in questione connessi al nodo 4 si trovano fisicamente in località diverse.

- In tutti i telefoni in questione è necessaria una voce per le chiamate di emergenza (porzione del collegamento del numero di telefono in formato canonico del nodo locale + codice impegno del fascio per le chiamate di emergenza)
- La voce LCR (nodo_4 locale) nella seguente tabella è necessaria solo se al nodo 4 (MultiGateway) sono disponibili fisicamente i telefoni. Viene inoltre premesso il numero località, che però non è completo (solo prefisso internazionale). A tal fine, è necessario che sia disponibile un accesso ITSP al nodo 4, che supporti le chiamate di emergenza nella rete locale.
- Per la composizione con un telefono viene utilizzata una regola LCR contrassegnata come chiamate di emergenza (ad esempio, 0C11x).
- I numeri di telefono di emergenza memorizzati nel telefono (e trasferiti al sistema quando si accede ad esso), vengono confrontati con i dati relativi alla posizione del sistema (prefisso internazionale, prefisso interurbano, numero del sistema).

  Se è diverso, viene creato un numero di emergenza "lungo":

  – Eliminazione del codice di accesso: 0112 -> 112
  – Aggiunta di <Codice impegno LDAP><Prefisso internazionale><Numero di emergenza programmato>: ad esempio, 112 -> 0 00 49897220 112
- Il numero di emergenza "esteso" viene istradato tramite LCR, utilizzando regole LCR specifiche o direttamente sulla linea urbana locale o tramite linee incrociate con il nodo partner e da qui alla linea urbana.

Suggerimento: Poiché il numero di telefono completo del nodo locale non è stato inserito con precisione nel telefono, è necessario inserire una regola LCR adatta per le chiamate di emergenza locali presso il sito del MultiGateway.

Configurazione dei dati località per il nodo 4

Parametri del fascio

Nodo 4, telefoni

Panoramica delle voci rilevanti per una chiamata di emergenza nell'LCR del nodo 4

Nodo 4	Nodo gateway
Località Paese G.	49
Località rete locale G.	
Località sistema G.	
Prefisso internazionale	00
Prefisso nazionale	0
Codice impegno LDAP	0

Fascio	Tipo n., in uscita	Tipo RNR
Servizi di rete	Nazionale	Int./DID

Fascio rete	
Prefisso per linea esterna (2° codice di linea urbana)	0

Luogo Witten	
Call Number (Numero di telefono)	1101
Emergency Number (numero chiamata emergenza)	4923026670

Luogo Monaco	
Call Number (Numero di telefono)	2101
Emergency Number (numero chiamata emergenza)	49897220

Luogo Paderborn	
Call Number (Numero di telefono)	3102
Emergency Number (numero chiamata emergenza)	49525180

Luogo Augusta	
Call Number (Numero di telefono)	4102
Emergency Number (numero chiamata emergenza)	490

Piano di composizione			Tabella delle rotte			Regola di composizione		
Nome	Cifre selezionate	Uso in emergenza	Fascio	Gateway dedicato	ID gateway	Regola di composizione	Metodo	Tipo
Chiamata di emergenza 5	0C112	X	Servizi di rete	Gateway multiplo	1	E1A	Corp. Rete	Sconosciuto
Chiamata di emergenza 5	0C0110	X						
Linea urbana	0CZ							
Chiamata di emergenza_a_1	0C00492302667-0-11X	X	Servizi di rete	Forzato	1	E3A	Corp. Rete	Sconosciuto
Chiamata di emergenza_a_2	0C004989722-0-11X	X			2			
Chiamate_di_emergenza_a_3	0C004952518-0-11X	X			3			
Chiamate_di_emergenza_4locale 6	0C0049-0-11X	X	ITSP	No		E4A	Fornitore rete principale	Sconosciuto

16.4.5 E112 Servizio di chiamata di emergenza europeo

Il servizio di emergenza avanzato E112 trasmette, oltre al numero di telefono, informazioni sulla posizione geografica (ad es. indirizzo) del chiamante.

Le informazioni geografiche vengono trasmesse in un documento XML standardizzato. I contenuti del documento dipendono dal Paese e dall'ITSP. Pertanto è necessario immettere solo i gruppi di dati necessari forniti dal proprio ITSP (ad es. in Svizzera si utilizza solo il campo NAM).

Il servizio viene attivato mediante la configurazione di numeri di emergenza in LCR e definendo le informazioni di posizione appropriate.

16.4.5.1 Come aggiungere un ID Loc ITSP a un utente

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Gateway voce**.
3) Nella struttura dei menu, fare clic su **Impostazioni ID Loc ITSP**.
4) Inserire un valore per il parametro **Nome ID Loc** (obbligatorio) e i parametri definiti per le informazioni sulla posizione ricevute dal proprio ITSP (ad es. in Svizzera si utilizza solo il campo NAM).
5) Fare clic su **Applica**, quindi su **OK**.

   Un ID indice viene assegnato automaticamente all'**ID Loc ITSP**.
6) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
7) Nella struttura dei menu fare clic su **Utente**.
8) Fare clic ad es. su **Client IP**.
9) Fare clic sulla scheda **Modifica utente**.
10) Immettere l'indice pertinente del campo ID Loc ITSP.
11) Fare clic su **Applica**, quindi su **OK**.

16.5 CAC (Call Admission Control)

Con la funzione Call Admission Control (CAC), la larghezza di banda utilizzata può essere limitata riducendo il numero di chiamate.

Il sistema di comunicazione offre tre possibilità di variare la larghezza di banda necessaria:

---

[5] Con le regole sopra indicate, in questo esempio è possibile riconoscere la situazione di emergenza, ma senza alcun istradamento. Per l'istradamento delle chiamate di emergenza, viene utilizzato il numero di emergenza derivato "lungo".

[6] Poiché gli utenti presso il sito del MultiGateway sono collegati fisicamente, è necessario inserire una regola LCR separata per l'accesso locale alle chiamate di emergenza (tramite il fascio ITSP).

- Limitazione del numero di chiamate simultanee tramite ITSP
- Limitazione della necessità di banda per le chiamate tramite gateway
- Limitazione del numero di chiamate negli scenari di collegamento in rete

16.5.1 Limitazione del numero di chiamate simultanee tramite ITSP

Il numero massimo di chiamate effettuate tramite un ITSP può essere limitato configurando la larghezza di banda disponibile in upload. Riducendo il numero di queste chiamate (chiamate Internet), è possibile ridurre ulteriormente i requisiti di banda.

Le relative impostazioni possono essere effettuate mediante le procedure guidate **Rete/Internet** e **Telefonia centrale**.

Il numero di chiamate possibili tramite un ITSP può essere visualizzato in **Modalità esperti** selezionando **Telefonia** >**Gateway voce** > **Parametri SIP**.

Le chiamate Internet sono:

- Chiamate ITSP
- Chiamate Unify Phone
- Chiamate myPortal for Teams
- Chiamate myPortal@work
- Chiamate Device@Homes

Solo le chiamate LAN myPortal@work e pure WebRTC non riservano larghezza di banda perché il payload è diretto.

16.5.2 Limitazione della necessità di banda per le chiamate tramite gateway

La configurazione dei codec consentiti per le chiamate gateway può influenzare la larghezza di banda.

Se vengono impostati solo codec compressi, la larghezza di banda richiesta è inferiore. Se si utilizzano codec misti, il livello di priorità dei codec non compressi può essere ridotto, in questo modo verranno utilizzati con una frequenza minore.

Le corrispondenti impostazioni vengono eseguite in **Modalità esperti** selezionando **Telefonia** > **Gateway voce** > **Modifica parametri codec**.

16.5.3 Limitazione del numero di chiamate negli scenari di collegamento in rete

Il sistema di comunicazione prevede due modi per controllare la larghezza di banda nei possibili scenari di connessione alla rete.

Limitazione per il numero di linee su altri nodi della rete

Limitazione della larghezza di banda tramite la selezione di codec specifici

Assegnando un certo numero di linee agli altri nodi della rete, è possibile impostare un limite superiore per tutte le chiamate simultanee possibili da e per questo nodo.

La larghezza di banda disponibile può essere definita mediante configurazione dei codec utilizzati da e per il partner (indirizzo IP di destinazione).

Le corrispondenti impostazioni vengono eseguite in **Modalità esperti** selezionando **Telefonia** > **Gateway voce** > **Aggiungi parametri codec di destinazione**.

16.6 Sistema ad uso comune

La capacità totale del sistema di comunicazione può essere suddivisa dal punto di vista organizzativo in un massimo di sei sottosistemi. In questo modo più aziende possono condividere un sistema di comunicazione.

La funzione Sistema ad uso comune (multi-tenant) viene realizzata utilizzando le funzioni esistenti. Ciò significa che non è necessaria alcuna configurazione esplicita di sottosistemi.

Il controllo delle connessioni consentite e vietate tra i singoli nodi e linee viene eseguito tramite gruppi con restrizioni di traffico.

Servizi nel sistema a uso comune:

- Rinvio
- Numero del sistema
- Lista chiamate
- Inclusione
- DISA
- Chiamata diretta
- Registrazione dettagli chiamata
- Destinazioni hotline
- Testi informativi, Testi assenza
- Chiamate interne
- Rubrica interna
- Stampa CDB
- Servizio notturno
- Posizione di parcheggio
- Gruppi con restrizioni di traffico
- Casella vocale
- Controllo della composizione

Il sistema di comunicazione può essere utilizzato come sistema "multi-tenant" e quindi essere utilizzato contemporaneamente da più clienti. Tutte le funzioni hanno le stesse funzionalità per tutti gli utenti.

Fanno eccezione alcune risorse che devono essere suddivise tra i diversi tenant (aziende). Queste possono essere assegnate a uno, alcuni o tutti i tenant. Le risorse da suddividere sono:

- Utenti

- Fasci
- Posto operatore
- Stazione di rinvio
- Risponditori, casella vocale
- Gruppi con restrizioni di traffico
- Apriporta
- Linee DISA

Con i gruppi con restrizioni di traffico, si definisce la capacità di ciascuno dei tenant di accedere agli altri.

Per ogni tenant, è possibile configurare destinazioni hotline separate.

Dipendenze

Argomento	Dipendenze
GEZ	È presente solo un punto di gestione degli addebiti per tutti i tenant.
Chiamate interne	Sono possibili chiamate interne tra utenti di sezioni diverse, a condizione che sia consentito dai gruppi con restrizioni di traffico.
LCR	L'impegno automatico della linea è configurabile solo a livello di sistema.
Stampa CDB	Il database può essere stampato solo per l'intero sistema.
Rubrica interna	Vengono visualizzati i nomi di tutti gli utenti e i numeri di selezione breve.
Commutazione	Non è possibile trasferire linee sulle quali non è stata effettuata alcuna selezione.
Rinvio	Il rinvio è programmabile solo a livello di sistema.

16.6.1 Selezione breve del sistema negli impianti comuni

La funzione di selezione breve in sistemi multi-tenant consente di selezionare destinazioni di selezione breve in funzione dei gruppi con restrizioni di traffico. A tal fine, tramite WBM è possibile assegnare una serie di destinazioni di selezione breve ai gruppi con restrizioni del traffico corrispondenti.

Dipendenze

Argomento	Dipendenze
Numeri di telefono est.	Le destinazioni di selezione breve possono contenere solo numeri di telefono esterni.
	Il numero di telefono esterno deve essere inserito unitamente al codice del fascio e al codice di impegno della linea.

Argomento	Dipendenze
Nomi selezione breve	Ad ogni destinazione di selezione breve può essere assegnato un nome
Apparecchio porta	L'apparecchio porta non può chiamare alcuna destinazione di selezione breve.
Gruppi con restrizioni di traffico	Non è possibile assegnare più intervalli di numeri di selezione breve a un gruppo con restrizioni di traffico.

17 Attendant

OpenScape Business offre funzioni di console posto operatore per ogni esigenza, quali AutoAttendant e Attendant basati su telefono e PC.

Panoramica delle procedure guidate disponibili

	Adatta per	Hardware	Licenze
AutoAttendant			
Company AutoAttendant (UC Smart)	UC Smart	OpenScape Business X OpenScape Business S	richiesto
Company AutoAttendant (UC Suite)	UC Suite	OpenScape Business X3/X5/ X8 con UC Booster Card o UC Booster Server OpenScape Business S	richiesto
Attendant basati su telefono			
OpenStage Attendant			
Attendant basati su PC			
OpenScape Business Attendant	UC Smart	PC e telefono, UP_{0E}	richiesto
- OpenScape Business BLF	UC Smart	Base IP	
myAttendant	UC Suite	OpenScape Business X3/X5/ X8 con UC Booster Card o UC Booster Server OpenScape Business S	richiesto

17.1 AutoAttendant

Assieme, AutoAttendant e la casella vocale offrono un servizio posto operatore automatico integrato e funzionalità di storage per i messaggi, ad esempio per la sede della società. AutoAttendant riproduce per i chiamanti un annuncio di benvenuto. Durante o dopo questo annuncio, il chiamante può essere istradato automaticamente a un interno o a una casella vocale inserendo delle cifre.

A tal fine, sono disponibili diverse funzioni che consentono la commutazione con annunci, ad esempio "Premere 1 per il reparto tecnico, 2 per il reparto commerciale". Dopo la digitazione delle cifre desiderate, il chiamante viene connesso ai colleghi dei reparti vendita o assistenza.

Company AutoAttendant non è assegnato ad alcun numero di telefono interno ma a un'istanza centrale. Un interno può essere assegnato a diversi Company AutoAttendant e mailbox. Ciò consente all'utente di essere deviato singolarmente al corrispondente Company AutoAttendant. Dopo la deviazione, per il chiamante viene riprodotto l'annuncio della mailbox personale o l'annuncio centralizzato dell'azienda. Con Company AutoAttendant è tuttavia possibile riprodurre gli annunci singolarmente in base all'interno, indipendentemente dalla mailbox personale.

Panoramica delle funzioni

- Rinvio dopo l'annuncio di una destinazione configurata
- Annuncio basato sullo stato: è possibile riprodurre per l'interno (libero od occupato) diversi annunci a seconda dello stato.
- Annunci diversi per giorno/notte (la commutazione viene eseguita manualmente o automaticamente)
- Controllo centralizzato tramite servizio notturno automatico
- Post-selezione di un numero a scelta fino alla lunghezza configurata (disattivabile)
- Selezione breve (= selezione diretta dall'esterno) verso destinazioni preconfigurate (numero o mailbox a scelta)

  Complessivamente sono consentiti 4 elenchi con un totale di 10 destinazioni e una destinazione di rinvio. L'elenco attivo viene determinato dall'annuncio di saluto selezionato.
- Post-selezione di un numero a scelta fino alla lunghezza configurata. La funzione Postselez. (suffisso) può anche essere disattivata per evitare di incorrere in addebiti indesiderati.
- AutoAttendant a passaggi multipli

  Le caselle di posta AutoAttendant possono essere configurate come destinazioni di selezione breve(manuale 1-4, Giorno/Notte). Ciò consente il concatenamento delle caselle di posta.

  In questo caso Company AutoAttendant funziona come in una deviazione di chiamata: la chiamata viene inoltrata da una casella postale concatenata alla successiva e ogni volta viene riprodotto l'annuncio. Nel complesso sono disponibili fino a 100 caselle di posta AutoAttendant.
- Selezione rapida

  Gli annunci possono essere disattivati per garantire un trasferimento più rapido.
- Annuncio prima della risposta con segnalazione in parallelo (senza selezione breve)

  Se per il chiamante è stato riprodotto l'annuncio di benvenuto, la chiamata viene segnalata all'utente con tono acustico e indicazione visiva. Se l'utente solleva il ricevitore, l'annuncio viene interrotto e l'utente viene connesso con il chiamante. Se l'utente non solleva il ricevitore, l'annuncio viene riprodotto completamente fino a quando il chiamante non ripone il ricevitore o non viene inoltrato tramite Gestione chiamate.
- Riconoscimento del tono di occupato
- Inoltro di chiamate fax (riconoscimento automatico tono fax) a una destinazione fax preconfigurata.
- Richiamata

  In caso di richiamata (ad eccezione di una chiamata fax), il chiamante viene trasferito alla casella associata, se presente e se è attivata la registrazione dei messaggi.

Nota: Per garantire il rinvio automatico al posto di rinvio tramite il sistema Voicemail, è richiesto l'inserimento di un codice di posto (predefinito 9, Stati Uniti 0).

Nota: L'amministrazione (TUI) di una casella postale AutoAttendant può essere eseguita solo da un telefono. Per questo motivo, la password della casella postale di AutoAttendant deve assolutamente essere diversa da quella della casella postale personale del telefono!

Esempi di applicazioni

- Esempio 1: **Annunci indipendenti da standby o emergenze**

  Fuori dagli orari di lavoro il cliente viene deviato su AutoAttendant per (ad esempio utilizzando il servizio notturno). Su richiesta, AutoAttendant si collega al tecnico dell'assistenza in servizio o propone di lasciare un messaggio nella casella postale centrale. In questo caso, un annuncio determina l'inoltro ai diversi numeri di telefono cellulare del tecnico.
- Esempio 2: **Servizi domenicali diversi per studi medici**

  Il servizio domenicale corrente non prevede più la deviazione alla segreteria telefonica o a una cassetta AB. Il cliente ha configurato diversi AutoAttendant in base al numero di rappresentanti. Gli AutoAttendant vengono configurati e nel fine settimana vengono attivati con una deviazione (servizio notturno) verso il relativo AutoAttendant. In questo caso è l'inverso: più annunci portano alla stessa mailbox.

17.1.1 Company AutoAttendant (UC Smart)

Company AutoAttendant (UC Smart) è una soluzione tipo AutoAttendant per la soluzione di comunicazione unificata UC Smart. Può essere utilizzato come AutoAttendent personale e come AutoAttendant centrale. La configurazione iniziale viene eseguita tramite il WBM, successivamente può essere controllato e configurato tramite telefono.

Company AutoAttendant (UC Smart) può essere utilizzato in due modalità:

- **AutoAttendant personale**

  L'AutoAttendant personale è assegnato a un utente o a un gruppo e risponde al numero di chiamata dell'utente o del gruppo originariamente chiamato (ad esempio, `12345678-100`).

  L'AutoAttendant personale è raggiungibile attraverso la casella vocale del gruppo di ricerca (numero predefinito 351). Viene utilizzato tramite le porte SmartVM (porte EVM) di tipo "PhoneMail" che devono essere assegnate tutte a questo gruppo di ricerca.

  Non è consentito il funzionamento in parallelo con la UC Suite.

- **AutoAttendant centrale**

  L'AutoAttendant centrale serve come console posto operatore e risponde a un proprio numero telefonico (ad esempio `12345678-0`). Indipendentemente dal fatto che si tratti di una chiamata diretta a AutoAttendant o di una chiamata deviata, il comportamento è sempre lo stesso.

  L'AutoAttendant centrale è raggiungibile attraverso uno o più dei propri gruppi di ricerca (numero predefinito: 352). Viene utilizzato tramite le porte

SmartVM (porte EVM) di tipo "Standard" che devono essere assegnate a uno o più gruppi di ricerca (max. 100).

Per impostazione predefinita è configurato un Company AutoAttendant (indice gruppo 3) con 2 porte SmartVM. I nomi e i tipi di porte possono essere utilizzati con la procedura guidata **Telefonia centrale** > **SmartVM** (vedere anche Come configurare la casella vocale (SmartVM)).

L'elenco di selezione breve e l'upload di annunci possono essere modificati in Modalità esperti **Telefonia** > **Interfacciamenti** > **SmartVM** (vedere Come caricare, salvare ed eliminare i singoli annunci di benvenuto). Inoltre, è possibile configurare e attivare altri Company AutoAttendant (UC Smart) (max. 99).

È consentito il funzionamento in parallelo con la UC Suite.

Company AutoAttendant (UC Smart) è soggetto a licenze (licenza Company AutoAttendant). Se non è disponibile alcuna licenza, le "regole" di Company AutoAttendant vengono ignorate, le chiamate vengono inoltrate al posto di rinvio centrale.

17.1.1.1 Come configurare un AutoAttendant aziendale impostato

Ad esempio, durante il giorno deve essere impostato un annuncio prima della risposta con la possibilità di registrazione (ad esempio casella postale 100). Di notte, viene eseguito un rinvio alla casella notte dopo l'annuncio corrispondente; la casella dispone inoltre di funzionalità di registrazione (anche Mailbox 100).

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

UC Smart è attivo.

Per impostazione predefinita, durante il servizio sia giorno che notte, dopo l'annuncio viene eseguito un rinvio al posto di rinvio.

Per impostazione predefinita, le funzioni di selezione breve e postselezione non sono attivate.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Connessione**.
3) Nella struttura dei menu fare clic su **Interfacciamento** > **SmartVM**.
4) Nella struttura dei menu fare clic su **AutoAttendant**.
5) Nella riga dell'AutoAttendant desiderato (ad esempio `352`) deselezionare la casella di controllo **Intercetta dopo annuncio** per inserire i caratteri di selezione rapida durante la riproduzione dell'annuncio di benvenuto.
6) Selezionare la casella di controllo **nessuna selezione suffisso**. In questo modo è possibile immettere solo caratteri di selezione rapida (e non numeri di telefoni interni).
7) Fare clic su **Applica**, quindi su **OK**.
8) Nella struttura dei menu, fare clic su **AutoAttendant** e successivamente sulla voce dell'AutoAttendant desiderato (ad esempio `352`).
9) Fare clic sulla scheda **Modifica destinazioni selez. breve/rinvio giorno**.

10) Nella riga **Selezione breve 0** dall'elenco a discesa **Seleziona** selezionare l'utente per il posto di rinvio (ad esempio, l'utente 100) e nell'elenco a discesa **Tipo** selezionare la voce **Mailbox**.
11) Nella riga **Rinvio** dall'elenco a discesa **Seleziona** selezionare l'utente per il posto di rinvio (ad esempio l'utente 100).
12) Fare clic su **Applica**, quindi su **OK**.
13) Fare clic sulla scheda **Modifica destinazioni selez. breve/rinvio notte**.
14) Nella riga **Rinvio** dall'elenco a discesa **Seleziona** selezionare l'utente per il posto di rinvio (ad esempio, l'utente 100) e nell'elenco a discesa **Tipo** selezionare la voce **Mailbox**.
15) Fare clic su **Applica**, quindi su **OK**.
16) Nella struttura dei menu fare clic su **SmartVM**.
17) Per evitare un duplice annuncio di benvenuto nella mailbox di rinvio, nella riga del posto di rinvio (ad esempio, utente 100) dal menu a discesa **Annuncio** selezionare la voce **Nessuno**. A questo punto, il tono di segnalazione della registrazione viene riprodotto immediatamente dopo l'annuncio di benvenuto del Company AutoAttendant.
18) L'annuncio di benvenuto del Company AutoAttendant può essere modificato tramite un telefono o selezionando **Modalità esperti** > **Manutenzione** > **SmartVM** (vedere Configurazione della casella vocale (SmartVM)).

17.1.1.2 Come configurare un nuovo Company AutoAttendant

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

UC Smart è attivo.

Licenze attivate

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Configurare innanzitutto il gruppo di ricerca:

a) Nella struttura di navigazione, fare clic su **Telefonia** > **Chiamate in entrata**.

b) Nella struttura dei menu, fare clic su **Chiamate in entrata** > **Linea di gruppo/di ricerca**.

c) Fare clic sulla scheda **Aggiungi gruppo**.

d) Nel campo **Numero di telefono** inserire il numero di telefono del nuovo AutoAttendant (ad esempio `353`).

e) Nel campo **Interno** inserire il numero di interno del nuovo AutoAttendant (ad esempio `353`).

: Se si desidera utilizzare il numero di interno 879, 890 o 891, occorre configurare l'impostazione tramite Manager E e non tramite WBM.

---

f) Nel campo **Nome** inserire il nome del nuovo AutoAttendant (ad esempio `AutoAttendant 353`).

g) Nell'elenco a discesa **Tipo**, selezionare la voce **Linea con ricerca ciclica**.

h) Nell'area **Membro gruppo**, dall'elenco a discesa Numero di telefono, selezionare l'AutoAttendant desiderato, (ad esempio **745 SmartVM 7**).

i) Fare clic su **Applica**, quindi su **OK**.

j) Per aggiungere un'altra porta AutoAttendant al gruppo di ricerca, nella struttura dei menu in **Linea di gruppo/di ricerca** fare clic sull'AutoAttendant desiderato e successivamente sulla scheda **Aggiungi membro**. In **Numero di telefono**, selezionare un'altra porta AutoAttendant (ad esempio **746 SmartVM 8**).

k) Fare clic su **Applica**, quindi su **OK**.

3) Configurare la mailbox dell'AutoAttendant:

a) Nella struttura di navigazione, fare clic su **Telefonia** > **Interfacciamento**.

b) Nella struttura dei menu, fare clic su **Interfacciamenti** > **SmartVM**.

c) Nella struttura dei menu, fare clic su **AutoAttendant**.

d) Nella riga dell'AutoAttendant desiderato (ad esempio `353`), selezionare all'occorrenza le due caselle di controllo:

Intercetta dopo annuncio: se attivato, il chiamante può inserire un numero di selezione breve durante la riproduzione dell'annuncio per l'opzione di commutazione.

nessuna selezione suffisso: se attivato, può essere immesso solo il numero di selezione breve e non un numero interno.

e) Fare clic su **Applica**, quindi su **OK**.

f) Nella struttura dei menu, fare clic su **SmartVM**.

g) Fare clic su

h) Nella scheda **Modifica caselle postali SmartVM**, nella riga dell'AutoAttendant desiderato, in **Annuncio**, selezionare l'annuncio di benvenuto desiderato.

i) Nella riga dell'AutoAttendant desiderato, selezionare la casella di controllo **AutoAttendant**.

j) Fare clic su **Applica**, quindi su **OK**.

4) Configurare l'opzione di commutazione (ad esempio "0" per connessione e "1" per annuncio):
   a) Nella struttura dei menu fare clic su **SmartVM** e quindi su **AutoAttendant**.
   b) Nella struttura dei menu, in **AutoAttendant**, fare clic sulla voce dell'AutoAttendant desiderato (ad esempio `352`).
   c) Fare clic sulla scheda **Modifica destinazioni selez. breve/rinvio giorno**.
   d) Nella riga **Selezione breve 0**, in **Numero di telefono**, inserire il numero a cui deve essere collegato, quindi nell'elenco a discesa **Tipo**, selezionare la voce **Numero di telefono**.
   e) Nella riga **Selezione breve 1** dall'elenco a discesa **Seleziona**, selezionare l'utente per il posto di rinvio (ad esempio, l'utente 100) e nell'elenco a discesa **Tipo**, selezionare la voce **Mailbox**.
   f) Nella riga **Rinvio** dall'elenco a discesa **Seleziona**, selezionare il Company AutoAttendant (ad esempio `353`).
   g) Fare clic su **Applica**, quindi su **OK**.
   h) Se il flag **nessuna selezione suffisso** è disattivato, durante la riproduzione dell'annuncio possono essere composti anche numeri interni. Per evitare un abuso, l'utilizzo delle tariffe **Limite numero chiamata** deve essere verificato o limitato, in modo che non sia possibile comporre numeri di telefono esterni (vedere **Modalità esperti** > **Telefonia** > **SmartVM** > **Modifica parametri SmartVM**).

17.1.2 Company AutoAttendant (UC Suite)

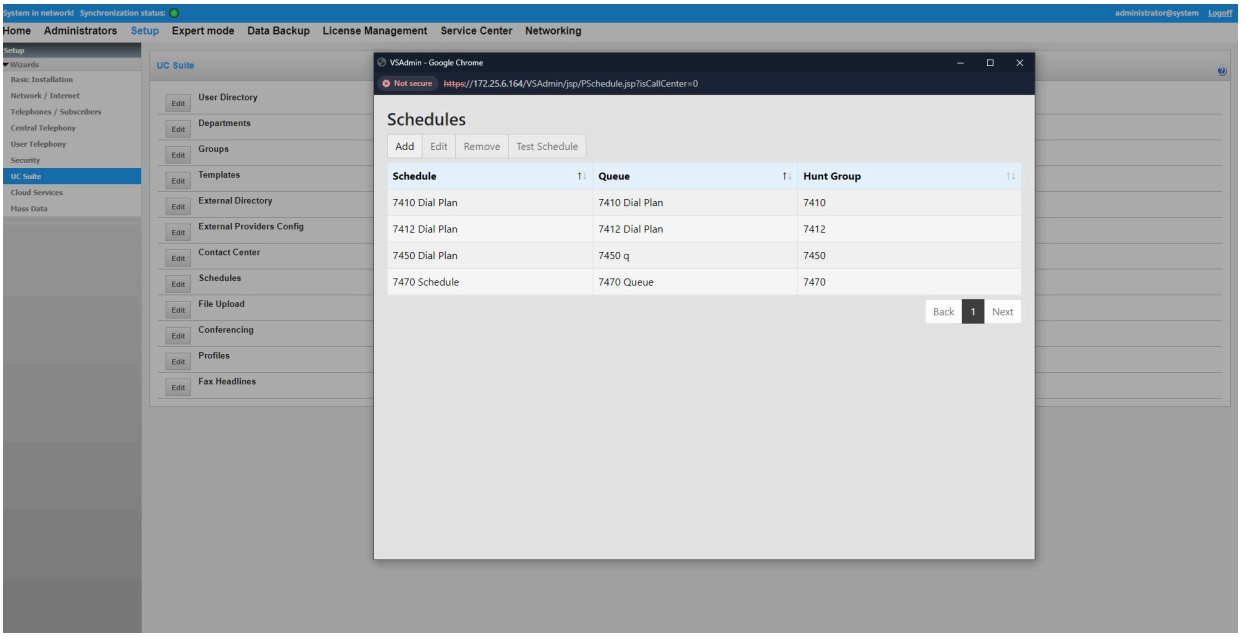
Company AutoAttendant centrale (UC Suite) è una console posto operatore che può essere configurata solo dall'amministratore. Per facilitare l'installazione e la configurazione, sono disponibili cinque modelli personalizzabili da parte dall'amministratore.

L'amministratore può configurare Company AutoAttendant (UC Suite) utilizzando pianificazioni e regole. Le pianificazioni consentono di scegliere diverse possibilità di composizione del numero, ad esempio in base al nome.

17.1.2.1 Pianificazioni

Le pianificazioni e le regole ivi contenute (Call Control Vector, CCV) consentono di definire per ogni coda d'attesa come le chiamate in arrivo verranno gestite in giorni o orari specifici.

Ad esempio, è possibile definire una regola per i giorni lavorativi per il primo turno (dalle 6:00 alle 14:00), una per il secondo turno (dalle 14:00 alle 22:00) e una per il turno notturno (dalle 22:00 alle 06:00). Per i weekend, è possibile definire una regola specifica. Per ciascuna di queste regole, è possibile indicare se è necessario riprodurre un annuncio e/o dove devono essere inoltrate le chiamate.



A una pianificazione deve essere assegnata almeno una regola (Call Control Vector CCV). Le regole determinano, per il periodo di validità di una pianificazione, come vengono gestite le chiamate in entrata. Le regole si applicano solo alle chiamate e non ai fax e alle e-mail.

Le regole vengono create con l'Editor regole grafico (Editor CCV) collegando oggetti CCV predefiniti; dopo la definizione possono essere memorizzate con un nome a libera scelta.

Le regole memorizzate possono essere assegnate a una o più pianificazioni come regola predefinita (CCV predefinito) o regola eccezione (CCV eccezione). L'apertura, la modifica e il risalvataggio sono possibili in qualsiasi momento tramite l'Editor regole.

Se a una pianificazione è stata assegnata una regola predefinita (CCV predefinito), tale pianificazione può essere memorizzata con un nome a libera scelta. Una pianificazione con una regola predefinita diventa valida dopo l'assegnazione a una coda di attesa di 24 ore al giorno e 365 giorni all'anno. Se in occasioni e orari specifici (pausa, fine settimana, giorno festivo, vacanza ecc.) sono valide altre regole, è possibile assegnarvi una pianificazione corrispondente sotto forma di regole eccezione (CCV eccezione). In questo modo, è possibile definire come devono essere gestite ad esempio le chiamate in arrivo durante il periodo di vacanza. In questo caso le pianificazioni vacanze hanno la priorità rispetto alle altre pianificazioni e regole.

Editor regole (Editor CCV)

Con l'Editor regole è possibile creare delle regole sulla base di oggetti CCV predefiniti. L'ordinamento degli oggetti CCV e delle relative proprietà definisce come le chiamate in arrivo verranno gestite.

Nota: Una regola ha un limite superiore di 500 oggetti CCV.

Sono disponibili i seguenti oggetti CCV predefiniti:

Suggerimento: Per tutti gli oggetti CCV indicati valgono inoltre le due seguenti proprietà generali:

Descrizione: possibilità opzionale di descrivere l'oggetto CCV, ad esempio Annuncio di benvenuto.

Elabora dopo digitazione: indicazione del numero di cifre richieste senza spazi, virgole o altri caratteri. Questa indicazione si riferisce all'oggetto CCV precedente. Se in tale oggetto è stato inserito 9 in Cifre accettate, è necessario inserire un 9 anche qui.

- **Riproduci messaggio**

  Determina la riproduzione dell'annuncio desiderato. È possibile selezionare un qualsiasi file audio nella UC Suite. Inoltre, è possibile importare un nuovo file audio nella UC Suite o registrare un nuovo messaggio e successivamente importarlo come file audio nella UC Suite.

  La riproduzione dell'annuncio occupa sempre un Media Stream Channel.

  Proprietà:

  – **Nome file**: scelta di un annuncio (file audio nel formato WAV)
  – **Interrompi digitazione**: Indicazione di un tasto o combinazione di tasti su tastiera con la quale un chiamante può interrompere la riproduzione dell'annuncio.
  – **Gestione file**: tramite questo pulsante è possibile caricare un file audio in formato wav o creare un nuovo file vocale con il registratore.
- **Disconnetti chiamante**

  Determina l'interruzione della connessione

  Dopo questo oggetto CCV non può essere inserito alcun altro oggetto CCV.
- **Vai a CCV**

  Crea un loop a un altro oggetto CCV

  Proprietà:

  – **CCV di destinazione**: scelta dell'oggetto CCV

- **Elabora dopo digitazione**

  Determina l'esecuzione di uno o più oggetti CCV successivi, in base alle cifre qui indicate (Elabora dopo digitazione).

  Proprietà:

  – **Nome file**: scelta di uno o più annunci (file audio in formato WAV)
  – **Lista di riproduzione**: elenco di tutti gli annunci selezionati (file audio in formato WAV) in una sequenza di riproduzione
  – **Timeout digitazione**: tempo espresso in secondi per il quale il sistema di comunicazione rimane in attesa dell'immissione della cifra.

    Se entro tale tempo non viene immessa alcuna cifra, il messaggio viene riprodotto di nuovo.
  – **Collegamento a**: elenco di cifre con destinazione.

    Le cifre e le destinazioni possono essere aggiunte, modificate ed eliminate.
  – **Gestione file**: tramite questo pulsante è possibile caricare un file audio in formato wav o creare un nuovo file vocale con il registratore.

  Il contenuto della lista di riproduzione viene visualizzato nell'Editor regole mediante una descrizione che compare quando si posiziona il puntatore del mouse sull'oggetto CCV.
- **Trasferimento a passaggio singolo**

  Questa funzione dipende dall'impostazione **SST AutoAttendant normale** (WBM, **Modalità esperti**: **Applicazioni** > **OpenScape Business UC Suite** > **Server** > **Impostazioni generali**):

  – **SST AutoAttendant normale** attivato (impostazione predefinita, non per USA): determina il trasferimento della chiamata indipendentemente che la destinazione sia libera, occupata o non disponibile.

    Suggerimento: Se l'utente ha attivato il rifiuto dell'avviso di chiamata in attesa, la chiamata viene inoltrata quando l'utente di destinazione è libero. L'avviso di chiamata in attesa su occupato non viene inviato.

  – **SST AutoAttendant normale** disattivato (impostazione predefinita, solo per USA): determina il trasferimento della chiamata se la destinazione è libera.

    Se la destinazione è occupata, e il rifiuto dell’avviso di chiamata è disattivato o se la destinazione non è disponibile, viene riprodotto un messaggio per il chiamante. Il chiamante può scegliere se lasciare un

messaggio nella casella vocale dell'utente o se comporre il numero di telefono di un'altra destinazione.

Se la destinazione è occupata e il rifiuto dell’avviso di chiamata è stato attivato, la chiamata non viene trasmessa.

Dopo questo oggetto CCV non può essere inserito alcun altro oggetto CCV.

Proprietà:

– **Interno di destinazione**: indicazione del numero interno o di selezione passante esterno con il numero della linea impegnata. Non sono consentiti spazi, virgole o altri caratteri.

Il numero di telefono dell'interno di destinazione viene visualizzato nell'oggetto CCV.

Nota: Dopo il trasferimento a passaggio singolo, il sistema scollega la chiamata dopo aver squillato per 5 minuti.

- **Registra nella casella postale**

  Devia la chiamata alla casella vocale desiderata di un utente o di un gruppo casella vocale

  Dopo questo oggetto CCV non può essere inserito alcun altro oggetto CCV.

  Proprietà:

  – **Casella postale utente**: indicazione del numero di telefono della casella vocale di un utente o di un gruppo casella vocale

  Il numero di telefono e il nome della casella vocale o del gruppo casella vocale vengono visualizzati nell'Editor regole mediante una descrizione che compare quando si posiziona il puntatore del mouse sull'oggetto CCV.

- **Trasferimento consultazione**

  Determina il trasferimento della chiamata a una destinazione interna. Durante il trasferimento, viene riprodotta musica su attesa per il chiamante (Music On Hold, MOH, della UC Suite).

  A differenza del trasferimento a passaggio singolo dell'oggetto CCV, in questo caso è necessario aggiungere altri due oggetti CCV. In altre parole, è necessario definire come deve comportarsi il sistema di comunicazione quando la destinazione di chiamata è occupata o la chiamata non viene risposta. Di norma in questi casi viene riprodotto un annuncio per il chiamante.

  Proprietà:

  – **Interno di destinazione**: indicazione del numero interno.

    Nel proprio nodo sono supportati solo numeri interni. L'inoltro a destinazioni esterne, utenti virtuali, altri AutoAttendant, UCD (tra cui

Contact Center) e destinazioni esterne CallMe non è consentito! Per questi scenari, deve essere utilizzato l'SST (Single Step Transfer).

– **Timeout squillo (sec.)**: tempo espresso in secondi entro il quale è necessario rispondere alla chiamata.

  Se la chiamata non viene risposta entro tale tempo, passerà di nuovo al sistema di comunicazione, che utilizzerà l'oggetto CCV successivo.

  Suggerimento: Il tempo qui indicato deve essere più breve di quello configurato per l'inoltro di chiamata (tempo predefinito per l'inoltro di chiamata = 15 secondi). Vedere Come configurare un inoltro di chiamata.

– **Ritira chiamata se inoltrata / deviata dall'apparecchio di destinazione**: opzione (vale solo per un numero interno).

  Se questa opzione viene attivata, viene eseguito un test della destinazione di chiamata. Se per la destinazione di chiamata è stato attivato un inoltro chiamate o una deviazione di chiamata, la chiamata ritorna al sistema di comunicazione che utilizzerà l'oggetto CCV successivo.

– **Quando si trasferisce una chiamata, verificare lo stato di presenza**: opzione

  Se questa opzione è attivata, viene eseguito un test dello stato di presenza della destinazione di chiamata. Se viene rilevato uno stato diverso da Ufficio, la chiamata viene restituita al sistema di comunicazione e si utilizza l'oggetto CCV successivo.

  Nota: Se una chiamata in entrata proviene da un numero soppresso/sconosciuto e la risposta alla chiamata viene eseguita dalla UC Suite AutoAttendant e trasferita tramite Trasferta monitorata, il numero del chiamante visualizzato sarà il numero della UC Suite.

• **Componi per nome**

  Determina la richiesta al chiamante di inserire le prime tre lettere del cognome dell'utente desiderato tramite la tastiera.

  Se esiste un utente corrispondente alle lettere iniziali specificate, viene stabilita la connessione.

  Se vi sono più utenti con le lettere iniziali specificate, al chiamante vengono annunciati i nomi di questi utenti (massimo 10 utenti). Se un utente non ha registrato un annuncio col nome, viene annunciato invece il numero di telefono. Una volta scelto l'utente desiderato, viene stabilita la connessione.

  Se nessun utente corrisponde alle lettere iniziali indicate, il chiamante riceve il messaggio corrispondente.

  Suggerimento: I tasti della tastiera reagiscono alla prima pressione del tasto. Ad ogni pressione del tasto viene verificato se esistono cognomi di utenti con le lettere assegnate al tasto.

  Esempio: nella rubrica interna sono presenti i seguenti cinque cognomi con le lettere iniziali T, U e V: Taylor, Taler,

Ullrich, Vasquez e Volterra. Per creare un abbinamento con l'utente Taylor, si devono premere i tasti seguenti: 8 2 9

Dopo questo oggetto CCV non può essere inserito alcun altro oggetto CCV.

Proprietà:

– **Metodo**: scelta tra **Trasferisci a interno** o **Registra nella casella postale**.

  In base al metodo selezionato viene realizzata una connessione all'utente desiderato o alla relativa casella vocale. Sono supportati solo gli utenti interni che sono registrati con nome e cognome nella rubrica interna.

- **Componi interno**

  Determina la richiesta al chiamante di inserire il numero di telefono dell'utente desiderato tramite la tastiera.

  Se il chiamante compone il numero di telefono di un utente virtuale, gli viene richiesto di inserire il numero di un altro utente. Successivamente viene stabilita una connessione. Se l'utente desiderato non risponde, la chiamata viene accettata dalla sua casella vocale.

  Dopo questo oggetto CCV non può essere inserito alcun altro oggetto CCV.

  Proprietà:

  – **Metodo**: scelta tra **Trasferisci a interno** o **Registra nella casella postale**.

    In base al metodo selezionato viene realizzata una connessione all'utente desiderato o alla relativa casella vocale. Sono supportati solo gli utenti interni della rete per i quali è registrato il numero di telefono nella rubrica interna.

- **Imposta lingua**

  Determina la selezione della lingua per i singoli messaggi predefiniti, in base al numero di telefono del chiamante. Occorre notare che vengono considerati solo gli annunci predefiniti (annunci di sistema) e nessun annuncio personale.

  È ad esempio possibile impostare il sistema in modo che per un numero di telefono con il prefisso internazionale +49 venga riprodotto un annuncio in tedesco, mentre per un numero con il prefisso internazionale +39 un messaggio in italiano.

  Proprietà:

  – **Lingua predefinita**: elenco a discesa per la scelta di una lingua.

    La scelta qui selezionata viene applicata a tutti i numeri di telefono per i quali non è stata definita una propria lingua.
  – **Motivo**: indicazione del numero di telefono che deve essere assegnato a una lingua specifica.

    È possibile utilizzare i seguenti segnaposto: * = qualsiasi cifra, ? = qualsiasi cifra.
  – **Lingua**: elenco a discesa per la scelta della lingua che deve essere assegnata ai numeri di telefono (**Motivo**).

  È possibile assegnare a una lingua tanti numeri di telefono quanti lo si desidera (**Motivo**).

- **Istradamento CLI**

  Determina l'inoltro di una chiamata a uno o più oggetti CCV consecutivi mediante il numero di telefono del chiamante.

  È ad esempio possibile impostare il sistema in modo che per un numero di telefono con il prefisso internazionale +49 venga riprodotto un annuncio in tedesco (oggetto CCV **Riproduci messaggio**) e successivamente venga inoltrata la chiamata a un interno (oggetto CCV **Trasferimento a passaggio singolo**). È inoltre possibile utilizzare il prefisso interurbano (es. 089 per Monaco di Baviera).

  Nel contesto di UC Suite e CLI Routing, gli utenti devono considerare scenari specifici, come le chiamate in entrata da MS Teams Native SIP Trunk. Se si intende inviare verso OpenScape Business i numeri dei chiamanti in formato canonico, compreso il prefisso internazionale, è necessario stabilire regole CLI Routing aggiuntive.

  Ad esempio, se i chiamanti da MS Teams hanno numeri nel formato +49777555XXXX, e 777555 è la parte comune di questi numeri, gli utenti devono creare regole di routing CLI pertinenti che incorporino questa parte comune (777555).

  Proprietà:

  – **Predefinito**: elenco a discesa per la scelta dell'oggetto CCV.

    L'oggetto CCV qui selezionato viene utilizzato per tutti i numeri di telefono per cui non è definita alcuna destinazione.
  – **Motivo**: indicazione del numero di telefono a cui occorre assegnare uno specifico oggetto CCV.

    È possibile utilizzare i seguenti segnaposto: * = qualsiasi cifra, ? = qualsiasi cifra.
  – **Descrizione**

    Fornitura di una spiegazione.

    Per il **Motivo** +49 (=prefisso internazionale tedesco) è ad esempio possibile inserire Germania.

    Il testo qui inserito viene visualizzato nell'Editor regole.
  – **Destinazione**: elenco a discesa per la selezione dell'oggetto CCV che dovrà essere assegnato al numero di telefono (**Motivo**) come destinazione.

  A un oggetto CCV è possibile assegnare come destinazione tanti numeri di telefono quanti lo si desidera (**Motivo**).
- **Diramare se variabile**

  Determina l'inoltro di una chiamata a uno o più oggetti CCV consecutivi mediante una condizione.

  È ad esempio possibile definire se per i chiamanti deve essere riprodotto un annuncio ("si prega di richiamare più tardi..."), non appena in una coda d'attesa sono presenti più di 20 chiamate.

  Proprietà:

  – **Variabile**: selezione di **Chiamate** o **Agenti disponibili**.

    A seconda delle variabili selezionate, il numero di chiamate in attesa in una coda o il numero di agenti disponibili (compresi gli agenti impegnati in post-elaborazioni) viene usato come condizione predefinita. Nel

relativo elenco a discesa, selezionare la condizione (**minore di** , **maggiore di** , **minore o uguale a**, **maggiore o uguale a**, **uguale a**) e nel relativo campo di input, inserire il valore comparativo.

– **Condizione soddisfatta**: elenco a discesa per la selezione dell'oggetto CCV che deve essere utilizzato come destinazione se la condizione viene soddisfatta.
– **Condizione non soddisfatta**: elenco a discesa per la selezione dell'oggetto CCV che deve essere utilizzato come destinazione se la condizione non viene soddisfatta.

Il numero di agenti disponibili in una coda d'attesa dipende dai seguenti cambiamenti di stato degli agenti:

– Accesso di un agente alla coda di attesa tramite "Connetti/Login": --> +1
– Disconnessione di un agente dalla coda di attesa tramite "Disconnetti/ Logout": --> -1
– Agente con stato "Pausa":-->-1
– Agente con stato "Disponibile dopo la pausa":--> +1

Il numero di agenti disponibili in una coda d'attesa **non** dipende dai seguenti cambiamenti di stato degli agenti:

– Agente allo stato "Squilla"
– Agente allo stato "Conversazione"
– Agente allo stato "Post-elaborazione"
– Agente allo stato "Chiamata persa"
– Agente allo stato "Scaduta"

17.1.2.1.1 Come aggiungere un'Eccezione in CCV

Se in occasioni e orari specifici (pause, fine settimana, festività, vacanze, ecc.) devono essere applicate altre regole, è possibile assegnarle alla pianificazione sotto forma di regole eccezione come Eccezione CCV. In questo modo, è possibile definire come devono essere gestite ad esempio le chiamate in arrivo durante il periodo di vacanza. In questo caso le pianificazioni vacanze hanno la priorità rispetto alle altre pianificazioni e regole.

Passo a passo

1) Andare su **Modalità esperti > Applicazioni > OpenScape Business UC Suite**.
2) Fare clic su **Pianificazioni**, selezionare una delle pianificazioni disponibili e fare clic su **Modifica**.

È possibile fare clic su **Aggiungi** per creare una nuova pianificazione.

3) Fare clic su **Aggiungi** nell'area **Eccezioni**.
4) Compilare il campo **Descrizione**, se si desidera.
5) Selezionare il tipo di eccezione da una delle opzioni disponibili:

- **Entro l'intervallo di ore**: selezionare un'ora, un giorno e una ricorrenza specifici per l'eccezione
- **Entro l'intervallo di date/ore**: selezionare una data, un'ora, un giorno e una ricorrenza specifici per l'eccezione
- **Pianificazioni vacanze**: selezionare una data di una vacanza specifica per l'eccezione
- **Ripetizione annuale**: selezionare se l'eccezione si ripeterà ogni anno o meno

6) Fare clic su **Salva**.

17.1.2.2 Modelli

Di seguito sono riportati modelli standardizzati precompilati per Company AutoAttendant (UC Suite), modificabili e adattabili in base alle proprie esigenze specifiche.

Modello 1 - 7410 CCV: Chiamata con commutazione (senza casella vocale)

Per il chiamante viene riprodotto un annuncio. Successivamente viene richiesta la pressione di un tasto (cifra) e verrà messo in comunicazione con un utente. Se il chiamante non preme alcun tasto, verrà messo in comunicazione con il posto di rinvio (per impostazione predefinita 100).



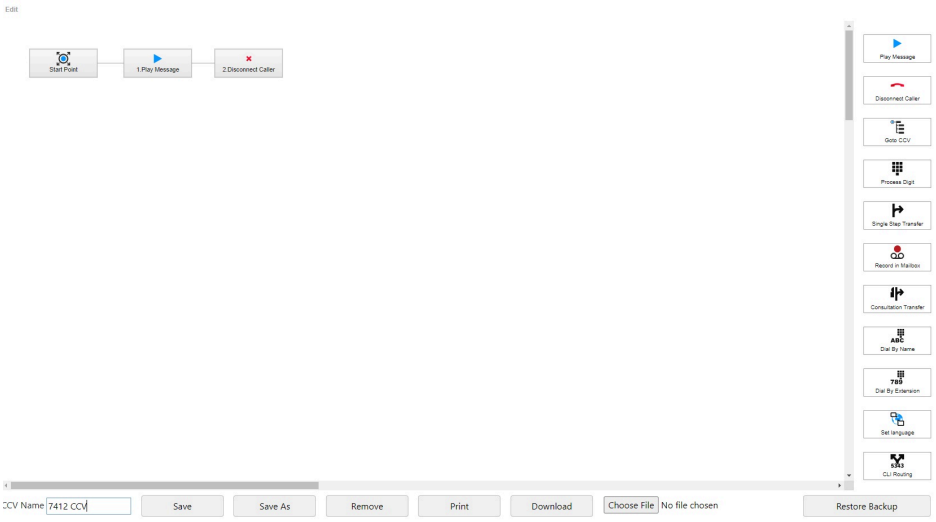
Modello 2 - 7411 CCV: Annuncio prima della risposta

Per il chiamante viene riprodotto un annuncio. Successivamente viene inoltrato al posto di rinvio 100.



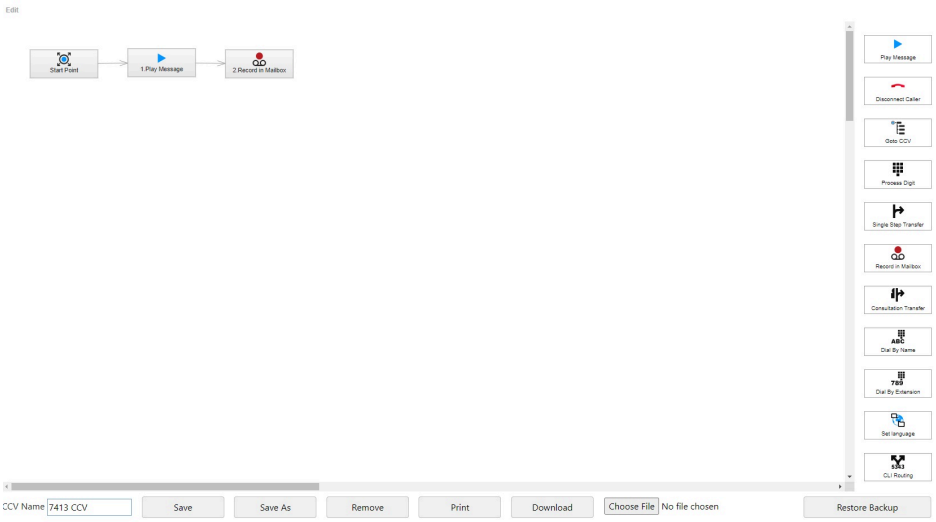
Modello 3 - 7412 CCV: Chiamata al di fuori dell'orario di ufficio

In caso di chiamata in entrata al di fuori dell'orario di ufficio, per il chiamante viene riprodotto un annuncio. Successivamente la connessione viene terminata.



Modello 4 - 7413 CCV: Chiamata al di fuori dall'orario di ufficio con deviazione della chiamate a una casella postale

In caso di chiamata in entrata al di fuori dell'orario di ufficio, per il chiamante viene riprodotto un annuncio. Successivamente gli viene chiesto di parlare a una casella postale e può lasciare un messaggio.



17.2 OpenStage Attendant

Le funzioni posto operatore possono essere eseguite con un telefono OpenStage appositamente configurato. OpenStage Attendant funge anche da posto di rinvio.

Layout dei tasti

OpenStage Attendant è la destinazione di tutte le chiamate per le quali non vi è alcuna possibilità di composizione o che sulla base dei criteri di assegnazione delle chiamate non potrebbero raggiungere alcun utente (rinvio). La console posto operatore inoltra quindi le chiamate in arrivo agli utenti desiderati.

I seguenti telefoni OpenStage possono fungere da Attendant:

- OpenStage 30
- OpenStage 40
- OpenStage 60
- OpenStage 80

In caso di telefono OpenStage configurato come console posto operatore i tasti funzione sono liberamente programmabili come segue:

- Servizio notturno
- Rubrica
- Chiam. in coda
- Inclusione
- In attesa
- Esterno 1
- Esterno 2 (non per OpenStage 40)
- Tasto vuoto non assegnato (non per OpenStage 40)

17.3 OpenScape Business Attendant

OpenScape Business Attendant offre funzioni posto operatore e l'integrazione di una rubrica per OpenScape Business. OpenScape Business Attendant può essere ampliato per poter visualizzare stati presenza e BLF (indicatori "occupato") a livello di rete.



Principali funzioni posto operatore:

- Gestione delle chiamate in attesa o accettate
- Informazioni sulla conversazione attiva
- Parcheggiata, chiamata in attesa
- Elenco chiamate
- Diario per chiamate risposte, perse e in uscita
- Casella vocale personale

Applicazione Rubrica:

- Contatti Outlook
- LDAP (connessione tramite servizio OpenDirectory)
- Rubrica personale

Stato BLF

- Libero, occupato, chiamato, deviazione

Visibilità presenza:

- ufficio, riunione, malattia, pausa, fuori sede, vacanza, pranzo, a casa

  Nota: A seconda delle impostazioni di sistema da parte dell'amministratore, lo stato di presenza "malato" potrebbe non essere disponibile.

- Modifica dello stato presenza per gli utenti del proprio nodo (attualmente non per utenti di altri nodi)

In OpenScape Business Attendant è possibile scegliere tra due stili di interfaccia.

È possibile collegare un massimo di 8 OpenScape Business Attendant per sistema di comunicazione (max. 8 licenze per OpenScape Business X1/X3/X5/X8 e OpenScape Business S).

La concessione della licenza per OpenScape Business Attendant viene eseguita tramite il WBM.

Requisiti tecnici

- PC Windows standard
- Uso di Terminal Server con i telefoni HFA (per i requisiti richiesti, vedere Requisiti richiesti per client PC della UC Suite)
- Interfaccia USB e interfaccia LAN, a seconda del terminale utilizzato
- Schermo con una risoluzione di almeno 1024 x 768 pixel, secondo schermo opzionale per visualizzare il secondo BLF
- Scheda grafica con profondità di colore 16 bit (minimo 256 colori)
- Accesso a Internet per supporto e aggiornamenti

Sistema operativo

- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bit o 64 bit)
- Microsoft Windows Vista (32 bit)
- Microsoft Windows Server 2015 (32 bit / 64 bit) come Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) come Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) come Microsoft Terminal Server

Il supporto di OpenScape Business Attendant per Microsoft Windows XP e Microsoft Windows Server 2003 termina in concomitanza con il termine del supporto da parte di Microsoft. Il prodotto sarà ancora supportato, ma non testato nei dettagli.

Telefoni supportati

- OpenStage 40/60/80 HFA
- openStage 30T/40T/60T/80T
- OpenScape DeskPhone CP 100/200/205/400/600/600E/700/700X
- OpenScape DeskPhone CP 110/210/410/710

Nota: In OpenScape DeskPhone CP 200/205/210, il nome dell'utente non viene visualizzato per una chiamata esterna.

I dispositivi precedenti (ad esempio, optiPoint 410/420/500) sono in parte ancora supportati. Per i dispositivi testati e approvati, consultare le rispettive release note.

Facile installazione plug-and-play

Per la prima configurazione di OpenScape Business Attendant viene utilizzata la procedura guidata che presenta la finestre di dialogo necessarie per le diverse impostazioni.

ad esempio:

- Interrogazione del tipo di terminale
- Interrogazione e verifica dell'accesso al sistema
- Interrogazione e verifica di un eventuale sistema di reti disponibile
- Integrazione automatica del BLF.

17.3.1 OpenScape Business BLF

Il campo indicatore occupato, BLF, di OpenScape Business è un'applicazione indipendente che consente di visualizzare gli stati Occupato. Le funzioni opzionali sono la visualizzazione e l'impostazione dello stato presenza, nonché la possibilità di stabilire connessioni per il telefono assegnato.

Requisiti tecnici

Funzioni principali:

- OpenScape Business BLF è scalabile e configurabile singolarmente
  - 10 - 350 campi BLF (pulsanti utente), a seconda della risoluzione dello schermo
- Funzioni telefoniche
  - Componi
  - Risposta alla chiamata
  - Disconnetti
- Impostazione dello stato presenza (per i propri utenti)
- Rubrica (rubrica del sistema)
- Registro chiamate

Per l'uso di OpenScape Business BLF, è necessaria una licenza OpenScape Business BLF, più una licenza Utente UC.

- PC Windows standard
- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bit o 64 bit)
- Microsoft Windows Vista (32 bit)
- Microsoft Windows Server 2015 (32 bit / 64 bit) come Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) come Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) come Microsoft Terminal Server
- Schermo con una risoluzione di almeno 1024 x 768 pixel
- Scheda grafica con profondità di colore 16 bit (minimo 256 colori)
- Interfaccia LAN
- Mouse e tastiera standard

- Accesso a Internet per supporto e aggiornamenti

17.3.2 Esempi di configurazione per OpenScape Business Attendant e OpenScape Business BLF

Nei seguenti capitoli sono riportati esempi per la configurazione generale di OpenScape Business Attendant, OpenScape Business BLF.

17.3.2.1 Scenario 1: OpenScape Business Attendant collegato a un singolo sistema OpenScape Business

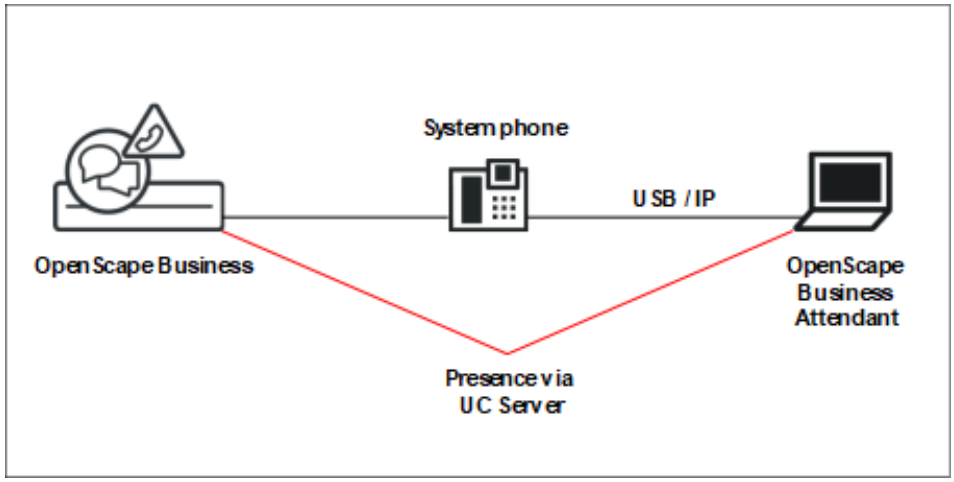
Prerequisiti

La licenza per OpenScape Business Attendant è disponibile

Terminale con licenza valida

Licenza per UC Smart o UC Suite per le informazioni sulla presenza (opzionale)

L'indirizzo IP per l'interfaccia Web Service di UC Smart e della UC Suite è diverso. Con UC Smart, il WSI è sempre in esecuzione nel sistema di comunicazione; con la UC Suite, invece, viene eseguito sulla scheda applicazioni o sul server applicazioni (vedere UC Smart e UC Suite). Se Booster Server è in uso, l'indirizzo IP di Booster Server deve essere utilizzato mentre è in uso OCAB, l'indirizzo IP di OCAB deve essere utilizzato. È necessario utilizzare l'IP del sistema di comunicazione solo se entrambi i componenti non sono collegati.



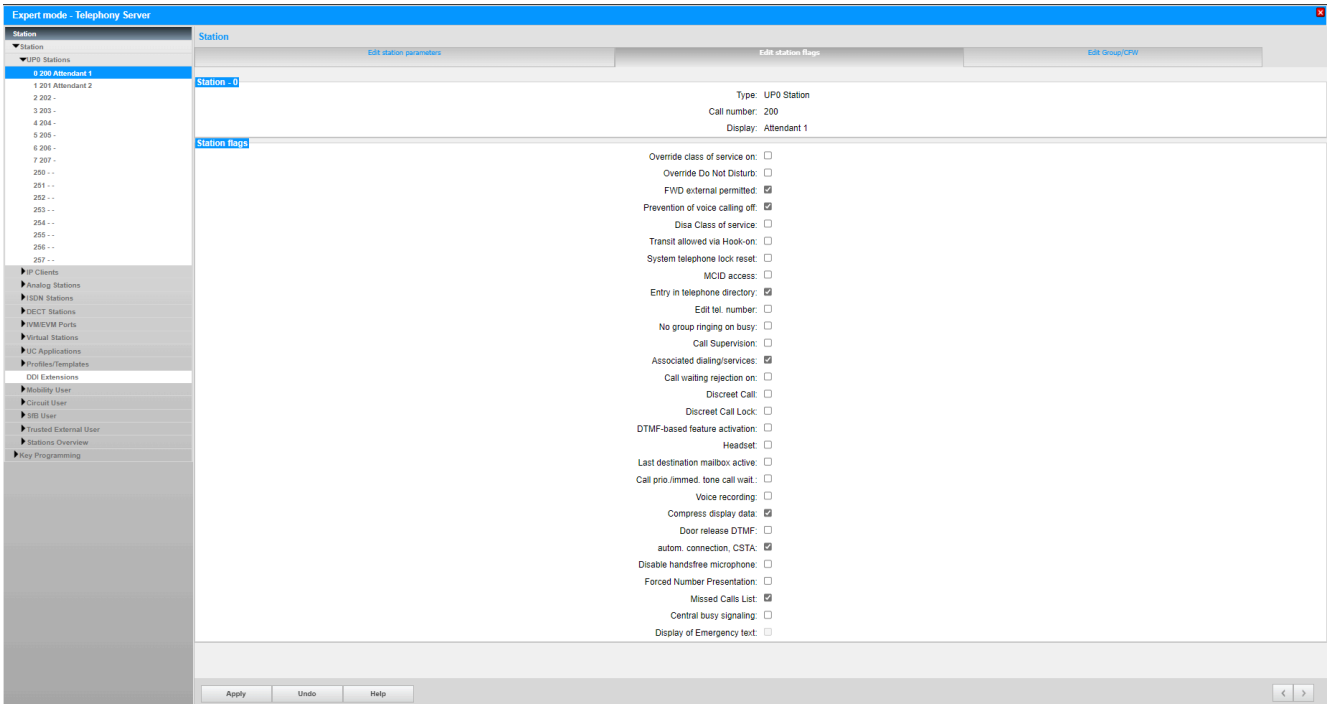
Passo a passo

1) Impostazione di un utente come Attendant tramite WBM o Manager E (optiPoint 500, OpenStage 30T, 40T, 60T, 80T o OpenStage 40HFA, 60HFA, 80 HFA).

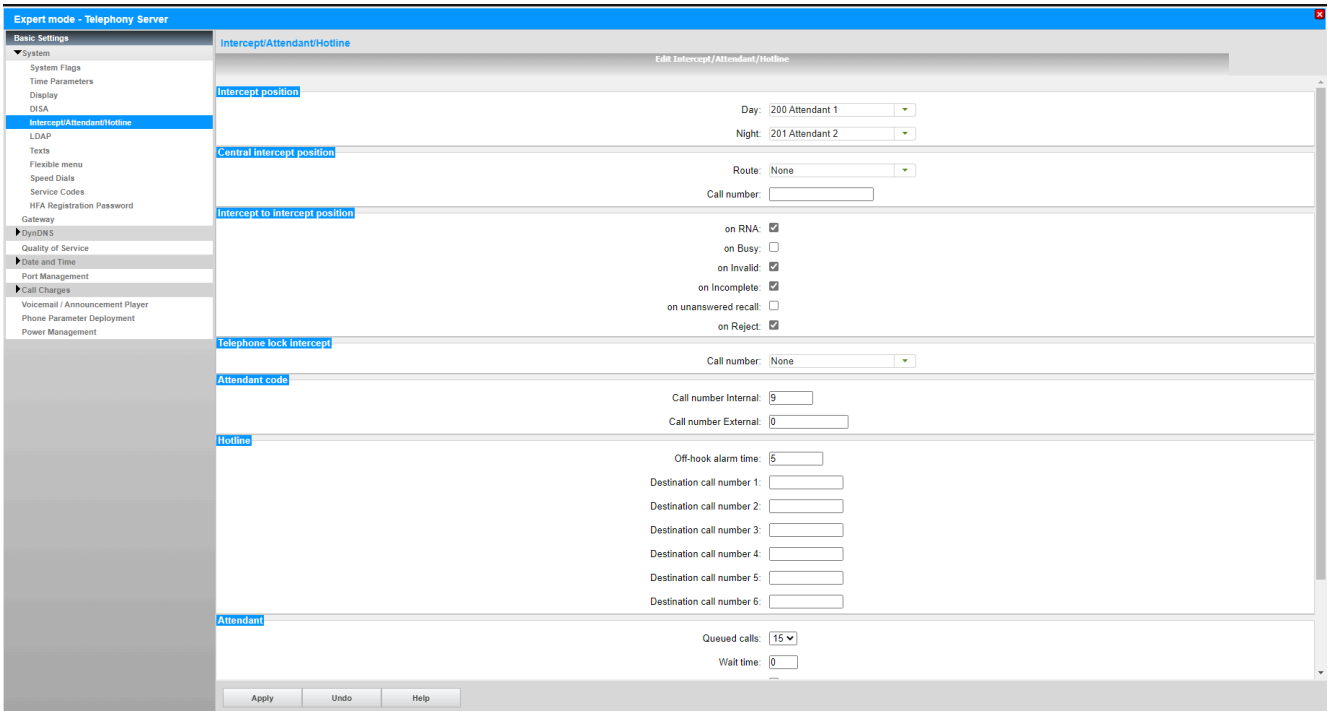
Suggerimento: I telefoni SIP o CMI non sono rilasciati.

2) Attivare l'opzione **Servizi associati**. Ciò è necessario per poter attivare e disattivare in OpenScape Business Attendant le funzionalità per gli altri utenti.

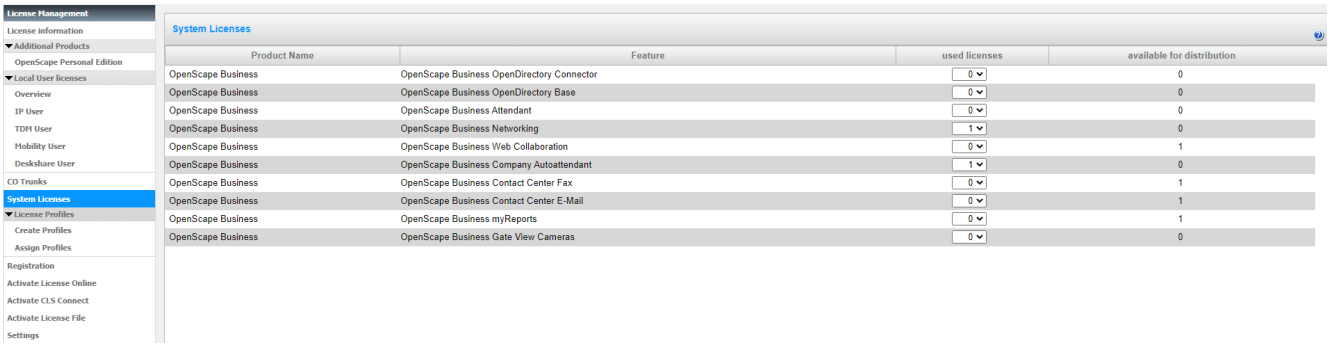
3) Attivare **Ignora "Non disturbare"** e disattivare **Rifiuto dell'avviso di chiamata in attesa**.



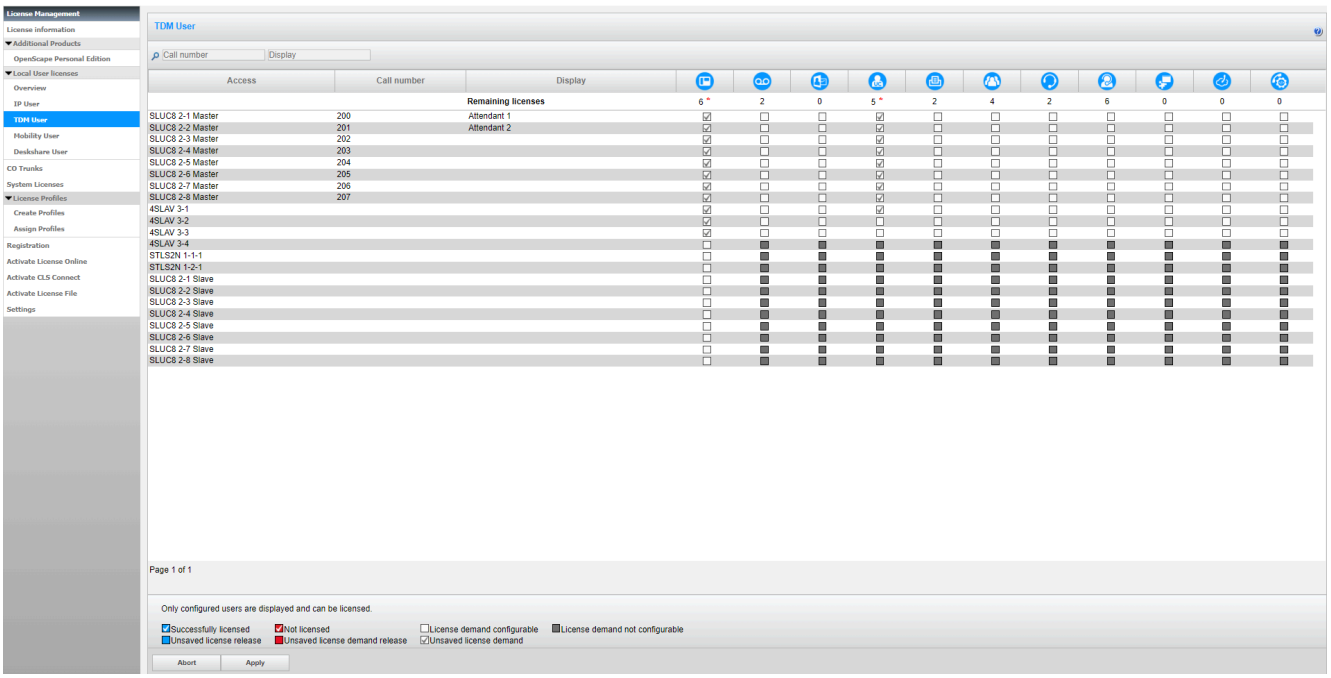
4) Configurare i criteri di rinvio e i codici Attendant (definire le opzioni di rinvio e i numeri di telefono della console posto operatore).



5) Concessione della licenza per OpenScape Business Attendant



6) Concessione della licenza per lo stato di presenza



7) Opzionale: durante la configurazione di un Attendant come utente IP, configurare nel telefono una password per l'accesso da parte dell'utente.

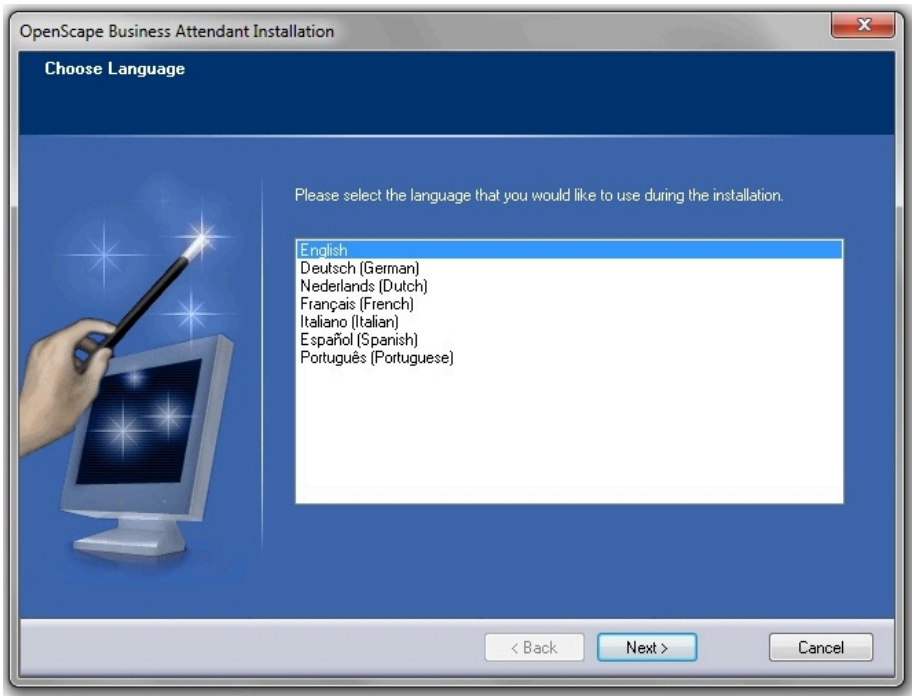


8) Installazione del driver USB

USB - driver COM (CallBridge) per optiPoint 500, OpenStage 30T e OpenStage 40T

USB - driver RNDIS per OpenStage 60T e OpenStage 80T

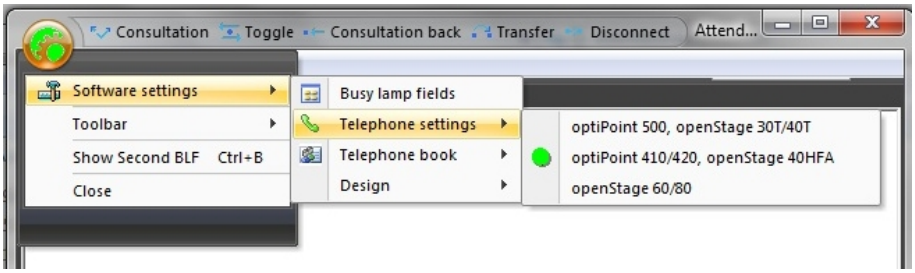
9) Installare OpenScape Business Attendant utilizzando la routine di installazione (accettazione del contratto di licenza, indicazione del percorso di memorizzazione e della lingua di OpenScape Business Attendant).

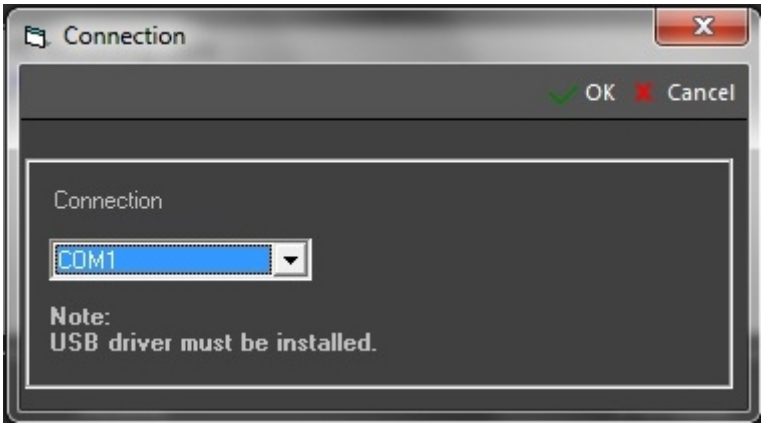


Dopo l'installazione e al primo avvio del programma, la procedura guidata di configurazione si avvia automaticamente e richiede le seguenti impostazioni:

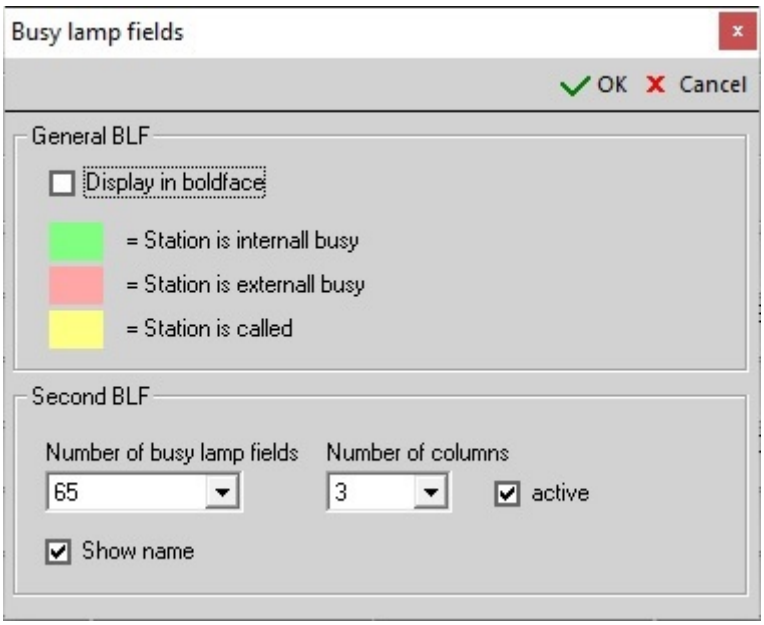
- Tipo di telefono
- Se viene usata la funzione Presence

Configurazione per l'accesso ad Attendant:

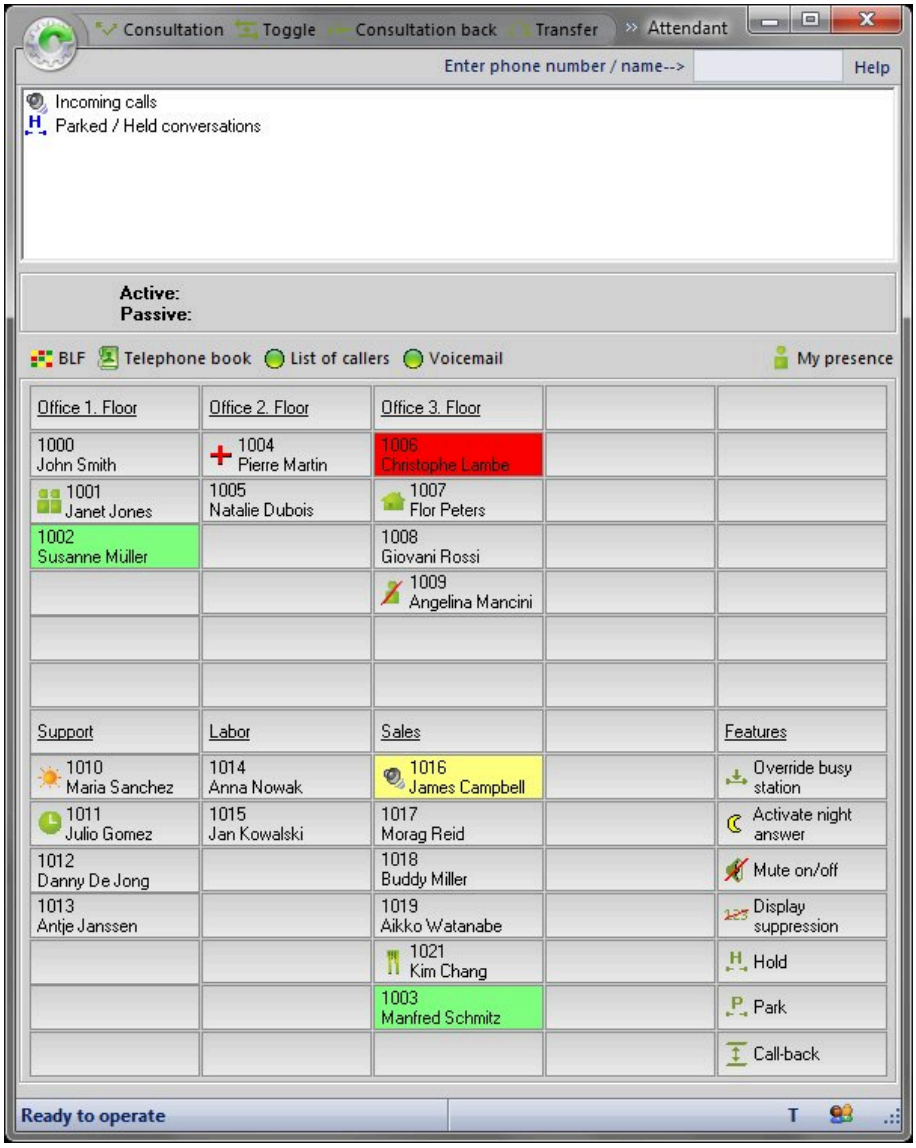




Una volta eseguito l'accesso al sistema di comunicazione, è possibile compilare automaticamente la funzione BLF.



Suggerimento: Assegnare e verificare le impostazioni di sicurezza (http o https) con il WBM.



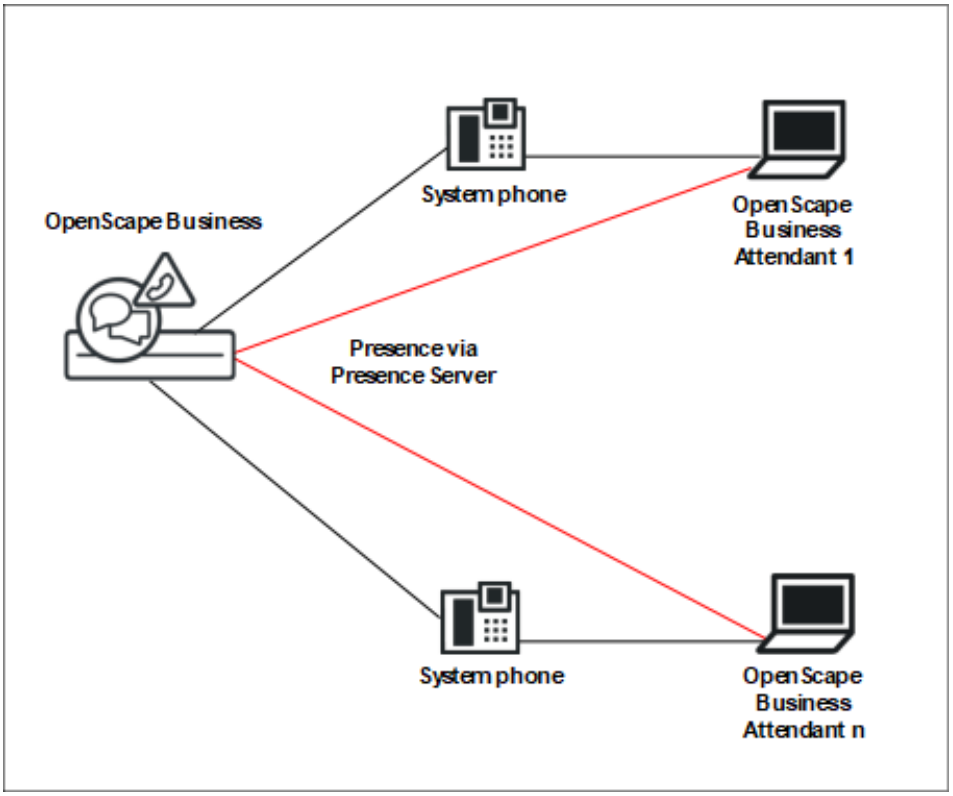
17.3.2.2 Scenario 2: Due o più OpenScape Business Attendant collegati a un singolo sistema OpenScape Business

Prerequisiti

Oltre allo scenario 1 si applicano i seguenti requisiti:

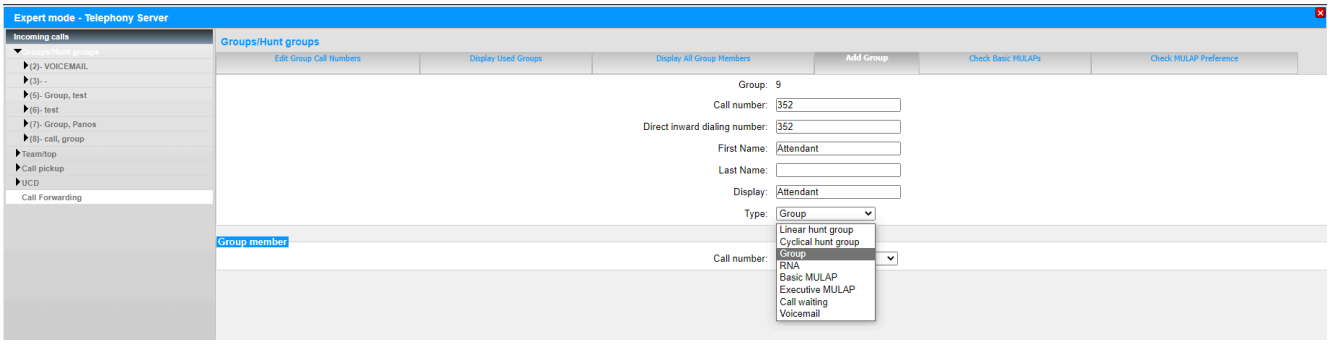
Licenze sufficienti per UC Smart o UC Suite per le informazioni sulla presenza (opzionale)

Configurazione gruppi

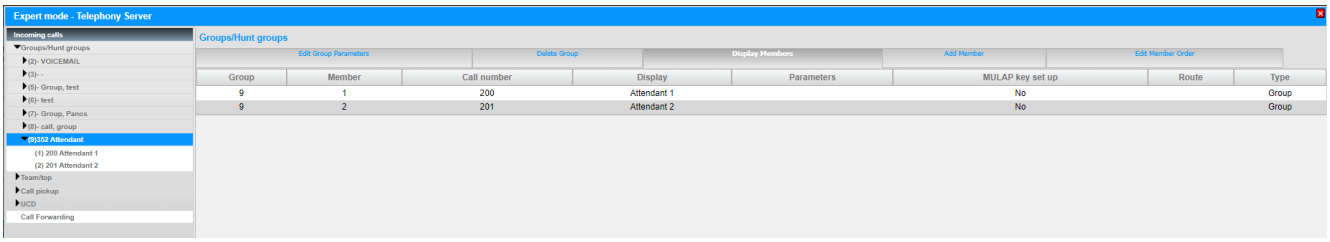


Passo a passo

1) Configurazione di un utente come Attendant tramite WBM (vedere esempio di configurazione 1).
2) Definire un gruppo: sono supportati i gruppi di ricerca (lineare e ciclica) e i gruppi di chiamata.



3) Assegnazione degli Attendant (l'utente corrispondente) al gruppo.



Suggerimento: Configurare i criteri di rinvio e i codici Attendant (definire le opzioni di rinvio e i numeri di telefono della console posto operatore). In questi casi, il posto di rinvio è il numero di telefono del gruppo.

17.3.2.3 Scenario 3: collegamento in rete di OpenScape Business con i propri OpenScape Business Attendant (BLF e stato presenza a livello di rete tramite WSI)

Prerequisiti

Licenza per UC Smart per le informazioni sulla presenza (opzionale)

È possibile utilizzare più di un solo OpenScape Business Attendant esclusivamente nelle reti UC Smart. WSI (server presenze di OpenScape Business) fornisce gli stati riagganciato e informazioni sulla presenza nell'intera rete. Per funzionalità a livello dell'intera rete, le reti UC Suite richiedono myAttendant.

17.3.2.4 Scenario 4: collegamento in rete di OpenScape Business con OpenScape Business Attendant centrale (BLF e stato presenza a livello di rete tramite WSI)

Prerequisiti

Licenza per UC Smart per le informazioni sulla presenza (opzionale)

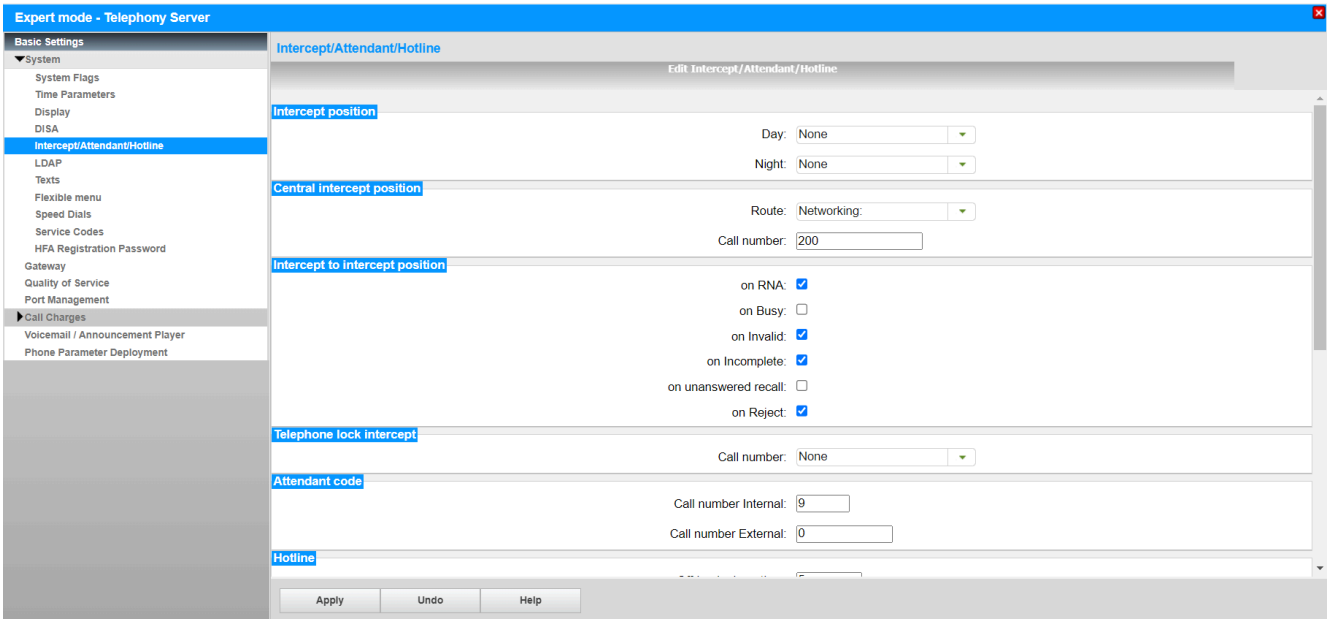
È possibile utilizzare più OpenScape Business Attendant solo nelle reti UC-Smart. WSI (Presence server di OpenScape Business) fornisce informazioni sugli stati Riagganciato e Presenza in tutta la rete. Le reti UC-Suite necessitano di myAttendant per la funzionalità a livello di rete.

Posto di rinvio centrale (nel nodo in cui non è configurato alcun OpenScape Business Attendant)

Passo a passo

1) Configurazione di OpenScape Business Attendant secondo l'esempio 1.

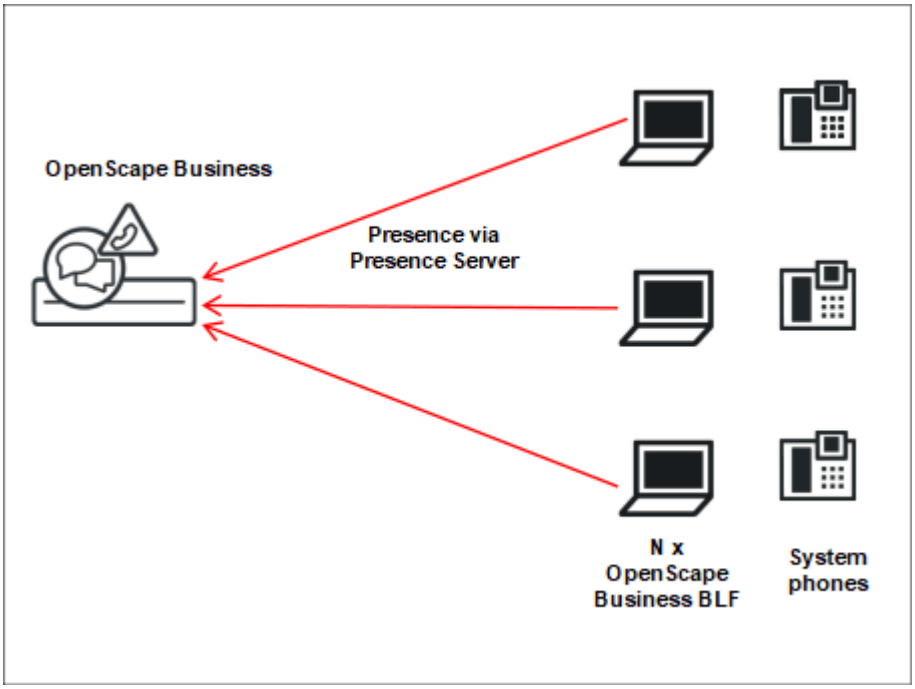
2) Nel nodo (in cui non è configurato alcun OpenScape Business Attendant) inserire il posto di rinvio centrale.



17.3.2.5 Scenario 5: OpenScape Business BLF collegato a un singolo sistema OpenScape Business

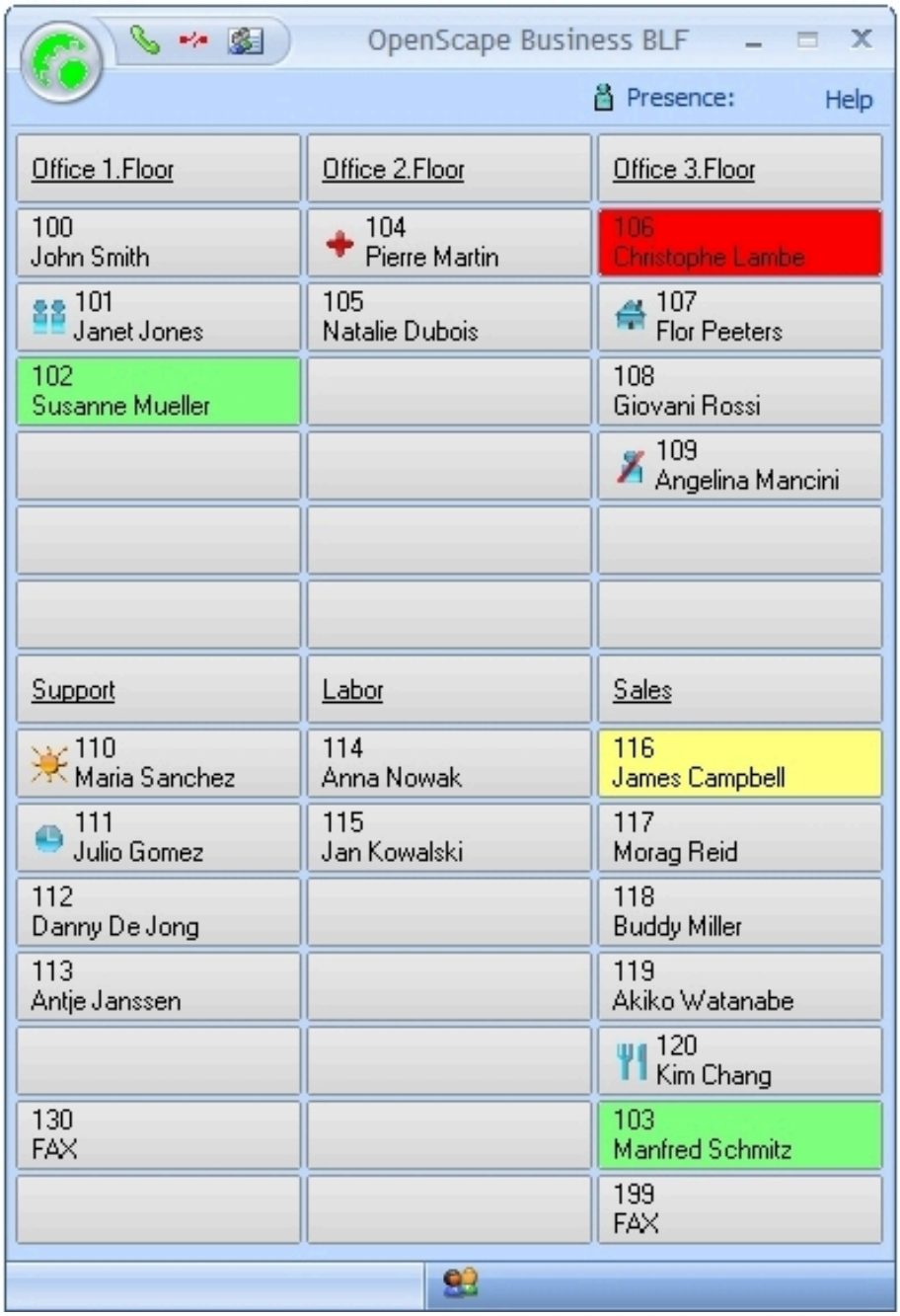
Prerequisiti

- È disponibile una licenza OpenScape Business BLF per utente
- I telefoni sono già assegnati
- È disponibile una licenza Utente UC per ogni utente



Passo a passo

1) Configurazione del telefoni tramite WBM
2) Configurazione del Presence Server tramite WBM
3) Installazione e avvio di OpenScape Business BLF
4) Dopo il primo avvio, viene eseguita l'assegnazione automatica (opzionale) del BLF di OpenScape Business.



17.3.2.6 Scenario 6: OpenScape Business BLF collegato a un sistema di reti OpenScape Business (stato BLF e Presenza tramite WSI)

Prerequisiti

- È disponibile una licenza OpenScape Business BLF per utente
- I telefoni sono già assegnati
- È disponibile una licenza Utente UC per ogni utente
- OpenScape Business BLF può essere utilizzato nelle reti UC Smart, non nelle reti UC Suite. WSI (Presence server di OpenScape Business) fornisce informazioni sugli stati Riagganciato e Presenza in tutta la rete.

Passo a passo

1) Configurazione del telefoni tramite WBM

2) Installazione e avvio di OpenScape Business BLF

3) Dopo il primo avvio, viene eseguita la connessione al WSI e l'assegnazione manuale del BLF. In questo caso, il BLF può essere assegnato a utenti sulla rete.

17.4 myAttendant

myAttendant mette a disposizione dell'utente numerose funzioni posto operatore. È possibile gestire gli utenti in modo agevole, mediante appositi pulsanti utente. Per la distribuzione di messaggi (vocali, fax, istantanei, SMS, e-mail) è possibile utilizzare il Centro messaggi.

Principali funzioni posto operatore

È possibile collegare un massimo di 20 myAttendant per sistema di comunicazione (per nodo di rete). La configurazione massima del sistema di reti è la somma delle capacità dei sistemi di comunicazione collegati in rete. Lo stato presenza e lo stato del telefono vengono visualizzati per tutti gli utenti della rete. Nel Centro messaggi di myAttendant vengono visualizzati gli utenti del proprio sistema di comunicazione.

- Gestione delle chiamate in attesa o accettate
- Vengono visualizzate le informazioni sulla conversazione attiva
- Parcheggiata, viene visualizzata la chiamata in attesa
- Lista chiamanti
- Diario per chiamate aperte, pianificate, interne, esterne, risposte, perse e in uscita
- Applicazione Rubrica
  - LDAP (ad esempio, ODS)
  - Rubrica personale/Contatti di Outlook
  - Rubrica interna, per tutti gli utenti collegati in rete

- Stato BLF di tutti gli utenti interni del proprio sistema e di tutti gli utenti della rete
  - Stato telefono: libero, occupato, chiamato, deviazione, non disturbare
  - Stato presenza: ufficio, CallMe, riunione, malattia, pausa, fuori sede, vacanza, pranzo, a casa (a livello di rete)

  Nota: A seconda delle impostazioni di sistema da parte dell'amministratore, lo stato di presenza "malato" potrebbe non essere disponibile.
- Sono disponibili tre stili dell'interfaccia
- È possibile collegare un massimo di 20 myAttendant per sistema di comunicazione (max. 20 licenze per OpenScape Business X3/X5/X8 e OpenScape Business S). La concessione delle licenze di myAttendant avviene tramite il WBM.

Requisiti tecnici (per i dettagli, vedere le informazioni di vendita)

- PC Windows standard
- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bit o 64 bit)
- Microsoft Windows Vista (32 bit)
- Possibile utilizzo di Terminal Server

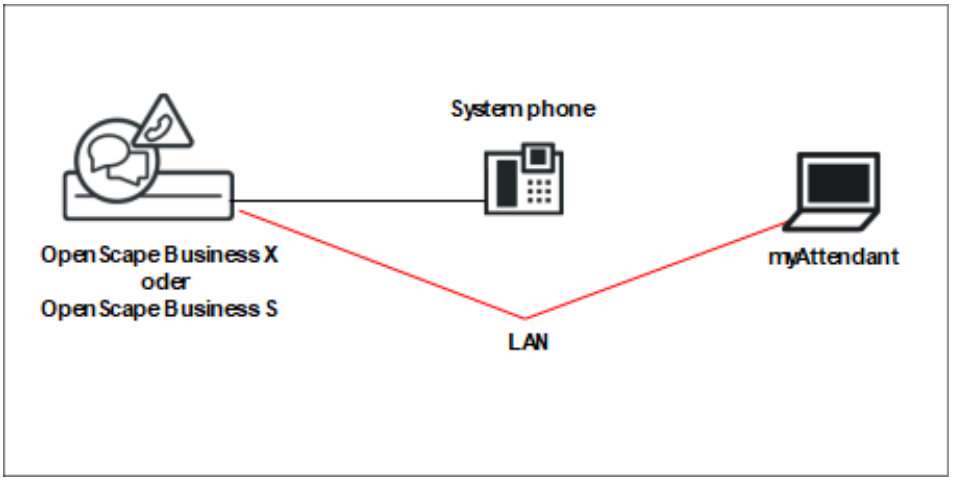
Software aggiuntivo

- Occorre installare Oracle Java 8 o superiore o, in alternativa, OpenJDK 8 (vedere **Centro assistenza** > **Software**)

Telefoni supportati

- OpenStage 40/60/80 HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/410/710 HFA
- Telefoni SIP con supporto RFC 3725, ad es. OpenScape Desk Phone IP 35G/55G SIP, OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X SIP, OpenScape Desk Phone CP 110/210/410/710 SIP
- OpenStage 30T/40T/60T/80T

Facile installazione plug-and-play, i primi passaggi richiesti per l'installazione vengono inviati all'utente dal sistema (se è stato configurato il proprio indirizzo e-mail).



17.4.1 Gestione utenti

In myAttendant, gli utenti possono essere gestiti tramite i pulsanti utente, la rubrica interna, la rubrica esterna e la rubrica personale.

Pulsanti utente

I pulsanti utente si trovano nella scheda **Predefinito** e sono un componente della finestra principale di myAttendant.

There are 100 user buttons available on a user buttons tab by default. You can change the default number of user buttons per tab any time you want.

Per impostazione predefinita, i pulsanti utente sono ordinati alfabeticamente in base al cognome.

You can configure multiple tabs for user buttons and select the names for these user buttons freely.

Internal, external and personal contacts (users) can be assigned to user buttons.

17.4.2 Centro messaggi

Nel **Centro messaggi** di myAttendant è possibile registrare e gestire messaggi vocali, fax, istantanei, nonché e-mail ed SMS.

È inoltre possibile gestire i messaggi per altri utenti. Per questo è necessario avere ricevuto i necessari permessi.

Nell'elenco utenti vengono visualizzati tutti gli utenti del sistema di comunicazione, con i relativi stati presenza o assenza. Nella posizione più in alto è mostrato lo stato dell'utente, con la Panoramica messaggi sotto forma di elenco a discesa. Gli altri utenti seguono in ordine alfabetico.

In base alle opzioni selezionate in Panoramica messaggi, vengono visualizzati diversi dettagli del messaggio, ad esempio informazioni sui messaggi in formato tabellare, che possono essere selezionate per ulteriori elaborazioni.

I vari tipi di messaggio supportano le seguenti azioni:

- I **messaggi vocali** possono essere ascoltati, eliminati, inoltrati.
- I **messaggi** LAN possono essere letti, modificati ed eliminati.
- I **messaggi fax** possono essere inoltrati.

Messaggi LAN

I messaggi LAN possono essere creati solo da un utente di myAttendant. Vengono utilizzati come una sorta di "bacheca" per gli utenti, che consente di divulgare le informazioni (ai singoli utenti). Questi messaggi possono essere visualizzati, modificati o cancellati; non è possibile inviarli ad altri utenti.

17.4.3 Scenario 1: come configurare myAttendant collegato a un singolo sistema OpenScape Business

Prerequisiti

La licenza per myAttendant è disponibile

Telefono con licenza valida

Server applicazioni o scheda applicazioni disponibile

La UC Suite viene attivata tramite la procedura guidata installazione di base

Passo a passo

1) Configurazione del telefono per la console posto operatore tramite il WBM

2) Disattivare **Rifiuto dell'avviso di chiamata in attesa** in **Modalità esperti**, in **Utenti** > **Client IP** > **Client di sistema** > **Utenti** > **Modifica i flag dell'utente**.

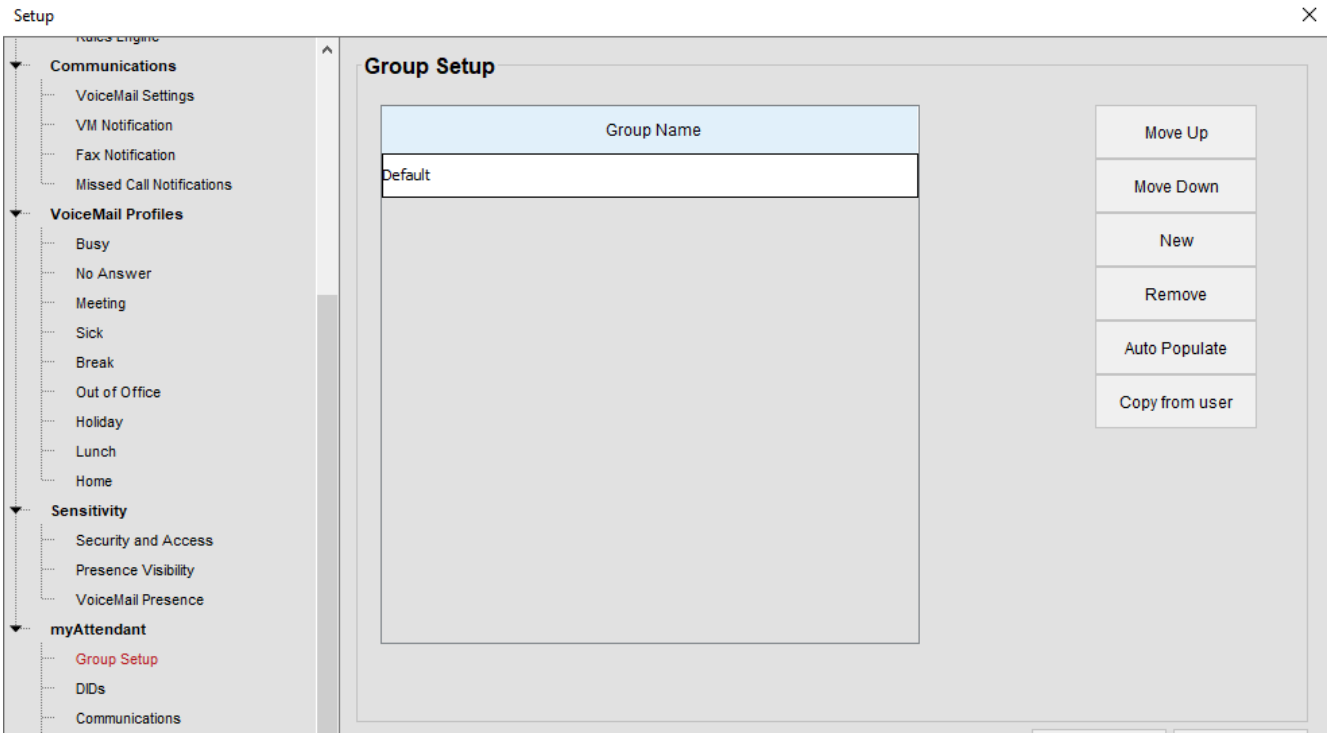
3) Attivare il servizio **Attesa immediata per chiamate posto operatore** in **Modalità esperti** in **Server telefonia** > **Impostazione di base** > **Sistema > Rinvio** > **PO** > **Hotline**.

4) Controllo e modifica dei criteri di rinvio e i codici Attendant (definire le opzioni di rinvio e i numeri di telefono della console posto operatore).

5) Concessione della licenza di myAttendant

6) Una volta eseguito l'accesso al sistema di comunicazione, è possibile compilare automaticamente la funzione BLF. Ciò può essere configurato

in myAttendant in **Configurazione > myAttendant > Configurazione gruppo.**



17.4.4 Scenario 2: come configurare due o più myAttendant collegati a un singolo sistema OpenScape Business

Lo scenario 2 è basato sullo scenario 1 e viene addizionalmente configurato.

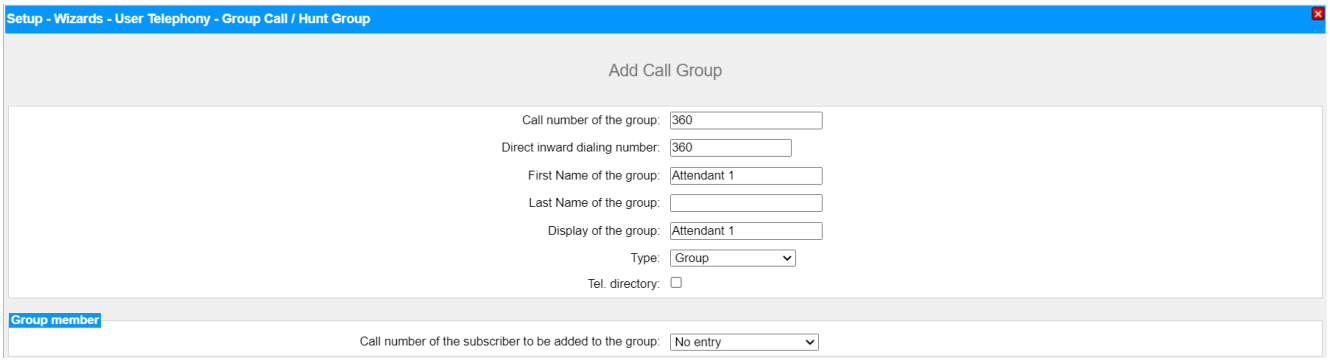
Prerequisiti

Licenze sufficienti per myAttendant

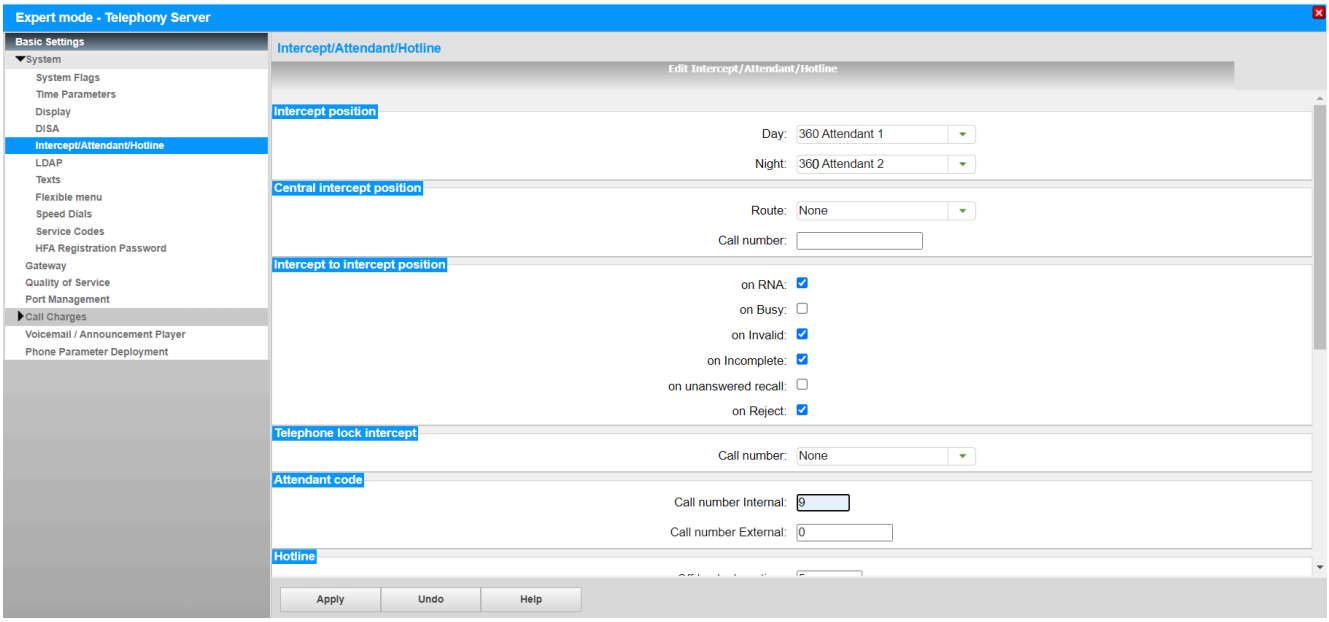
Telefono con licenza valida

Passo a passo

1) Configurare un gruppo (costituito solo da console posto operatore) in WBM **Configurazione** > **Telefonia utente** > **Chiamata di gruppo / Gruppo di ricerca** > **Aggiungi**.



2) Durante la configurazione della console posto operatore OpenStage selezionare questo gruppo.



17.4.5 Scenario 3: come configurare un collegamento in rete di OpenScape Business con myAttendant centrale

Lo scenario 3 riprende lo scenario 1 e 2 e presenta ulteriori configurazioni. Il nodo 1 viene collegato in rete con il nodo 2. La console posto operatore centrale è nel nodo 2.

Prerequisiti

Disponibilità di licenze sufficienti per myAttendant

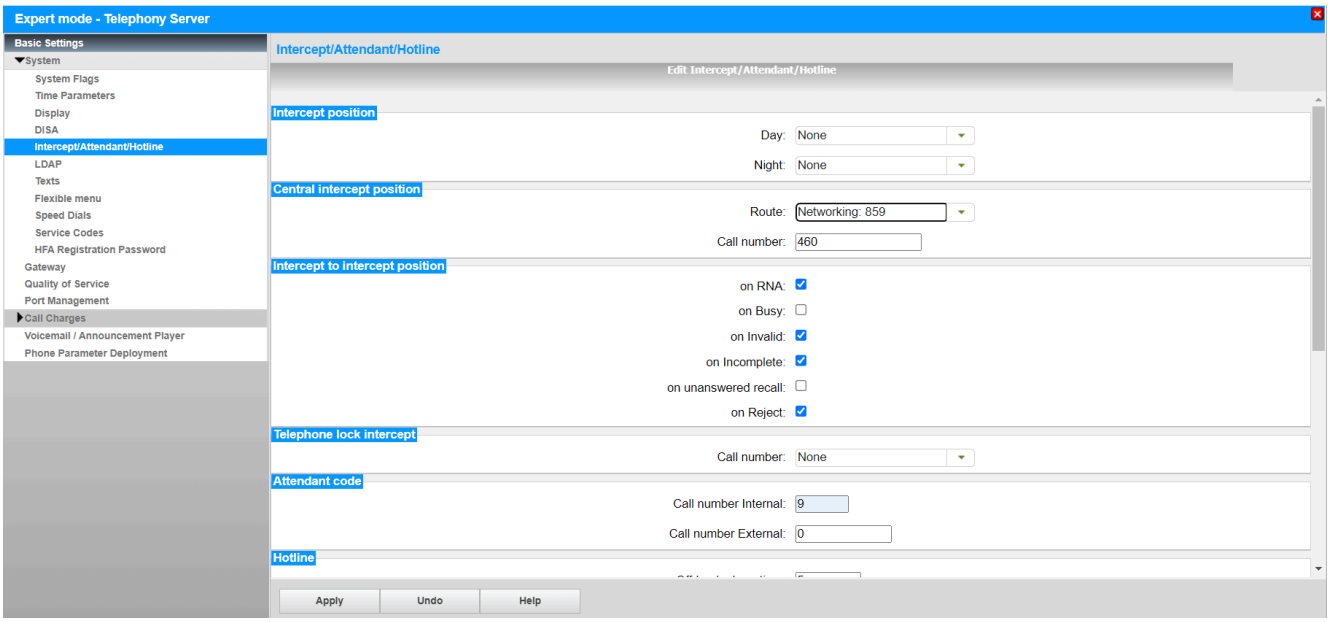
Le licenze per la rete sono disponibili

Telefono con licenza valida

LCR è configurato

Passo a passo

1) Configurare un posto di rinvio centrale nel nodo 1. Il posto di rinvio centrale deve essere creato in un nodo in cui NON è configurato alcuna console posto operatore.



2) Configurare la console posto operatore per il sistema 2 (come nel precedente scenario 2).
3) Installare myAttendant con i dati utente del nodo 2.

17.5 Posto di rinvio

Il sistema di comunicazione consente di deviare ad un determinato posto di rinvio tutte le chiamate esterne che non sono assegnate a nessun utente o che non hanno ottenuto risposta, in modo che nessuna chiamata vada persa. I criteri di rinvio possono essere configurati dall'amministratore.

Il posto di rinvio può essere un singolo terminale, un gruppo o un risponditore:

- Posto di rinvio (posto operatore)
- Utenti
- Gruppo di ricerca
- Gruppo MULAP
- Chiamata di gruppo
- Risponditore esterno

Non è possibile selezionare un gruppo UCD come posto di rinvio.

Se nel sistema è configurato un posto di rinvio, in caso di rinvio vi vengono inoltrate le chiamate. Se non è configurato alcun posto di rinvio, le chiamate rinviate vengono segnalate al primo utente IP.

Se un utente interno è configurato come posto di rinvio, verrà automaticamente assegnata ad esso la configurazione dei tasti predefinita. Inoltre il posto di rinvio può essere abilitato per la funzione "Inclusione".

L'amministratore può assegnare al posto di rinvio un codice di posto (2 cifre) a cui questo sia direttamente raggiungibile sia per l'interno che per l'esterno.

Un rinvio è valido per tutto il sistema e viene quindi applicato allo stesso modo a tutti gli utenti dei sistemi ad uso comune. Vedere anche "Posto di rinvio centrale nel sistema di reti" nel capitolo relativo alla rete.

Criteri di rinvio

L'amministratore imposta le situazioni in cui attivare il rinvio. Gli stati possibili sono i seguenti:

- Su libero

  La chiamata segue le voci presenti in Call Management (ad esempio un inoltro di chiamata configurato). Se nessun utente risponde alla chiamata, viene instradata al posto di rinvio.
- Su occupato, se non è più possibile eseguire l'inoltro.

  Innanzitutto il sistema verifica la possibilità di segnalare la chiamata in attesa. In caso negativo, la chiamata segue le voci presenti in Call Management (ad esempio un inoltro di chiamata configurato). Se nessun utente risponde alla chiamata, viene instradata al posto di rinvio. Il rinvio su occupato si riferisce esclusivamente alla prima chiamata, non a quelle commutate o in uscita. Se giunge una richiamata di un utente esterno e l'apparecchio di destinazione è occupato, invece di essere rinviata immediatamente, viene segnalato un avviso di chiamata.
- Con selezione errata

  Se il numero selezionato non è stato configurato o non è attivo.
- Con selezione incompleta

  Se il numero selezionato risulta troppo breve. Qualora sia disponibile un posto di rinvio centrale, la selezione incompleta non verrà valutata.
- In caso di richiamata senza risposta

  Qualora una chiamata esterna non ottenga alcuna risposta sia in seguito ad una trasferta rapida, che ad una richiamata alla destinazione originaria, il rinvio avrà luogo trascorso il tempo preimpostato.
- Al rifiuto

  Se la chiamata viene rifiutata da un utente interno, seguirà le voci presenti in Call Management (ad esempio un inoltro di chiamata configurato). Se nessun utente risponde alla chiamata, viene instradata al posto di rinvio.
- Con numero di telefono non disponibile

  Come con selezione errata.
- Con inoltro di chiamata concatenato

  Se una chiamata inoltrata incontra un'altra deviazione di chiamata e se con questo evento il numero di concatenazioni consentite viene superato, ha luogo un rinvio. Il numero di concatenazioni consentite dipende dai valori definiti per l'inoltro di chiamata. È consentito un massimo di tre concatenazioni.
- Con chiave elettronica

  Se un utente seleziona un codice del fascio ad un telefono con chiave elettronica attivata, ha luogo il rinvio. Per questo caso l'amministratore configura un posto di rinvio specifico.
- Con annuncio (solo con UC Suite)

  Se un utente seleziona il codice di posto (a 2 cifre) mentre ascolta un annuncio della casella vocale o di AutoAttendant, avviene il rinvio. Per questo caso l'amministratore configura un posto di rinvio specifico.

Dipendenze

Argomento	Dipendenza
Chiamate dati	Le chiamate dati vengono interrotte e non rinviate.
Gruppo di ricerca	Da un gruppo di ricerca non vengono effettuati rinvii; la chiamata viene di nuovo inoltrata al primo apparecchio della linea con ricerca, dove vi resta.
Programmazione tasti standard	La programmazione tasti standard comprende anche il tasto **Mostrare il numero delle chiamate**. Può essere assegnato solo a 6 terminali. Una volta raggiunto il limite non è più possibile assegnare alcuna programmazione tasti standard. I tasti standard assegnati non sono riprogrammabili quando un apparecchio non funge più da posto di rinvio.
Linee S_0	L'analisi delle linee S_0 avviene solo se non è stato configurato alcun posto di rinvio giorno/notte.
Servizio notte	Per raggiungere la stessa destinazione sia da linee DID che da linee HKZ mentre il servizio notte è attivo, il numero della stazione notte inserito in Rinvio > PO deve corrispondere al numero inserito in **Nr. tel. Notte** in **Assegnazione linea**.

17.5.1 Come configurare il posto e i criteri di rinvio

La procedura guidata **Posto operatore** consente di configurare i numeri di telefono per il posto e i criteri di rinvio.

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Posto operatore**.
4) Nelle aree **Posto operatore** e **Codice di posto** specificare i numeri di telefono desiderati (2 posizioni) per il posto di rinvio.
5) Nell'area **Criteri di rinvio** specificare i valori desiderati.
6) Fare clic su **OK & Avanti**, quindi su **Fine**.

17.5.2 Come configurare il posto di rinvio centrale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu, fare clic su **Impostazioni di base** > **Sistema** > **Rinvio/PO/Hotline**.
4) Nell'area **Posto di rinvio centrale** selezionare la voce desiderata nell'elenco a discesa **Fascio**.
5) Nell'area **Posto di rinvio centrale** indicare il **Numero di telefono** desiderato per **Giorno** e **Notte**.
6) Fare clic su **Applica**, quindi su **OK**.

17.5.3 Come configurare il rinvio con chiave elettronica

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu, fare clic su **Impostazioni di base** > **Sistema** > **Rinvio/PO/Hotline**.
4) Nell'area **Rinvio con chiave elettronica** selezionare la voce desiderata nel menu a tendina **Numero di telefono**.
5) Fare clic su **Applica**, quindi su **OK**.

17.5.4 Come configurare il rinvio con annuncio

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Click **Server** in the menu tree.
4) Click on the **General Settings** tab.
5) Enter the call number for the Intercept position in the **Target Number** field of the **Call number of intercept position** area.
6) Click **Save** and close the window.

18 Contact Center multimediale

Il Contact Center è una potente soluzione per la distribuzione e l'elaborazione di chiamate in arrivo, fax e e-mail. Il sistema di distribuzione intelligente, basato sulle competenze, fa sì che ogni chiamante venga messo in contatto con l'agente del Contact Center più qualificato, indipendentemente dalla modalità di contatto scelta. Tramite l'applicazione myAgent, sono a disposizione di tutti gli agenti del Contact Center pratiche funzioni per l'elaborazione e la post-elaborazione di chiamate, fax e e-mail. myReports fornisce diversi modelli di rapporto per l'analisi dell'attività del Contact Center.

Il Contact Center multimediale è completamente integrato nel software della UC Suite. Comprende tutti i componenti software necessari. Anche le funzioni di Contact Center vengono abilitate tramite licenze.

Il Contact Center utilizza le risorse del sistema di comunicazione, ad esempio le code d'attesa per le chiamate in entrata e le funzioni di comunicazione unificata per la registrazione e la riproduzione da annunci.

La componente centrale software del Contact Center gestisce tutte le funzioni di routing per chiamate in entrata, fax ed e-mail; inoltre gestisce le postazioni di lavoro PC, collegate tramite LAN, degli agenti e delle code d'attesa.

Sulle postazioni di lavoro PC degli agenti viene installata l'applicazione myAgent. Facoltativamente è possibile installare anche l'applicazione myReports per la generazione e l'invio di rapporti. Il software necessario può essere scaricato direttamente dall'area download del sistema di comunicazione e installato sul PC client.

La configurazione delle funzioni di base del Contact Center, delle pianificazioni e delle regole di distribuzione nonché degli agenti viene eseguita tramite il WBM. Le impostazioni per il funzionamento quotidiano del Contact Center, quali ad esempio l'assegnazione di agenti alle code d'attesa, possono anche essere effettuate direttamente tramite myAgent.

In caso di mancata disponibilità del Contact Center in seguito a problemi (crash di sistema, problemi di connessione e simili), è possibile implementare una soluzione secondaria tramite la funzione UCD del sistema di comunicazione. In fase di configurazione dei gruppi UCD nell'ambito della configurazione iniziale del Contact Center, si deve tener conto delle regole di distribuzione per le emergenze.

Suggerimento: Per informazioni sulla UC Suite e le funzioni di comunicazione unificata, consultare il capitolo UC Suite.

18.1 Client del Contact Center

Tramite l'applicazione myAgent, sono a disposizione di tutti gli agenti del Contact Center pratiche funzioni per l'elaborazione e la post-elaborazione di chiamate, fax e e-mail. Tramite l'applicazione integrata myReports, è possibile creare rapporti relativi alle chiamate, code d'attesa, agenti, prestazioni, livelli di servizio e codici post-elaborazione del Contact Center. Sono disponibili oltre 100 modelli di rapporti predefiniti.

18.1.1 myAgent

myAgent mette a disposizione di tutti gli agenti pratiche funzioni per l'elaborazione e la post-elaborazione di chiamate, fax e e-mail.

myAgent offre le seguenti funzioni:

- Elaborazione di
  - Esegui chiamata
  - Fax
  - E-mail
- Funzione Richiamata automatica per gli agenti
- Visualizzazione e modifica dello stato agente
- Visualizzazione e modifica dello stato presenza degli utenti interni del sistema di comunicazione
- Presentazione in tempo reale delle code
- Registrazione di chiamate, se attivata nel sistema di comunicazione
- Invio messaggi immediato
- Richiesta di assistenza tramite
  - Ascolto delle chiamate (disponibile in base al paese)
  - Inclusione in chiamate
  - Invio messaggi immediato
- Integrazione della rubrica interna, della rubrica esterna e della rubrica esterna non in linea (LDAP) per cercare i Contatti Outlook per nome
- Creazione di rapporti basati su modelli di rapporti predefiniti

In base al livello di autorizzazione assegnato, un agente di myAgent può disporre di funzioni standard (agente) o di funzioni avanzate (supervisore o amministratore) (vedere Funzioni degli agenti basate sul livello di autorizzazione).

L'assegnazione degli agenti alle code viene eseguita tramite l'applicazione myAgent. L'assegnazione può essere eseguita solo da un agente con il livello di autorizzazione Supervisore o Amministratore. È possibile assegnare all'agente le seguenti proprietà (assegnazione agente), che influiscono sulla distribuzione di chiamate, fax e e-mail in una coda:

- **Agente primario** o **Agente di overflow**

  Le chiamate vengono distribuite in modo uniforme agli agenti primari. Un agente di overflow riceve una chiamata solo se le chiamate hanno superato un numero o un tempo di attesa predefiniti.
- **Attiva richiamata automatica agente**

  Richiamata automatica agente consente a un chiamante in coda di lasciare un messaggio vocale per gli agenti. Non appena un agente idoneo si libera, riceverà la chiamata, ascolterà il messaggio vocale lasciato dal chiamante e potrà richiamarlo.
- **Livello interfaccia**

  Il livello interfaccia controlla la distribuzione delle chiamate agli agenti nelle code delle chiamate: gli agenti con un livello interfaccia più alto hanno la priorità nella distribuzione delle chiamate. Se tutti gli agenti hanno lo stesso livello interfaccia, l'agente che è libero da più tempo riceve la chiamata.

- **Orario lavorativo**

  L'orario lavorativo consente all'agente di eseguire ad esempio alcune operazioni di gestione al termine della chiamata, prima di passare alla chiamata successiva.
- **Overflow dopo chiamate in coda**

  Le chiamate che superano questo numero massimo vengono deviate su un agente di overflow.
- **Overflow dopo secondi in coda**

  Le chiamate che superano questo tempo di attesa vengono deviate su un agente di overflow.

L'area **Elenco di associazioni agente** mostra gli agenti con il livello di autorizzazione Supervisore o Amministratore, nonché gli agenti assegnati alle varie code. Gli agenti con il livello di autorizzazione Agente potranno vedere solo le code d'attesa a loro assegnate.

18.1.2 Requisiti richiesti per l'uso di myAgent

Per poter utilizzare myAgent, il PC client dell'utente deve disporre di una dotazione hardware e software adeguata.

Suggerimento: Rispettare scrupolosamente le istruzioni correnti contenute nel file `Readme first` che si trova nella stessa cartella dei file di installazione.

Telefoni

myAgent può essere utilizzato in combinazione con i seguenti telefoni:

- OpenStage HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/410/710 HFA
- OpenStage T
- Openscape Personal Edition HFA
- OpenStage M3 (OpenScape Business Cordless)
- OpenScape DECT Phone S6/SL6/R6 (OpenScape Business Cordless)

Sono supportati i dispositivi precedenti (ad esempio, optiPoint 410/420/500 e Gigaset M2/SL3/S4/SL4/S5). I telefoni Optiset E non possono essere utilizzati. myAgent non può essere utilizzato con gli utenti SIP, gli utenti Mobility, gli utenti virtuali, i gruppi o gli utenti MULAP. Per i dispositivi testati e approvati, consultare le rispettive release note.

Sistemi operativi

myAgent può essere utilizzato in combinazione con i seguenti sistemi operativi:

- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bit o 64 bit)
- Microsoft Windows Vista (32 bit)

Suggerimento: Il sistema operativo utilizzato richiede sempre lo stato attuale di tutti gli aggiornamenti disponibili (service pack e patch).

Il supporto di myReports per Microsoft Windows XP e Microsoft Windows Server 2003 termina in concomitanza con il termine del supporto da parte di Microsoft. Il prodotto sarà ancora supportato, ma non testato nei dettagli.

Software aggiuntivo

- Occorre installare Oracle Java 8 o superiore o, in alternativa, OpenJDK 8 (vedere **Centro assistenza** > **Software**)
- Adobe Reader 9 o successivo (per rapporti in formato PDF)

Requisiti hardware minimi

- 2 GHz CPU
- RAM: 2 GB
- LAN 100 Mbit/s
- Risoluzione del monitor XGA (1024x768), myPortal per Outlook: Risoluzione del monitor SVGA (800x600)

Microsoft Terminal Server, Citrix XenApp Server

myAttendant può essere utilizzato in ambienti Microsoft Terminal Server/Citrix Server se vengono soddisfatti i requisiti riportati di seguito.

Suggerimento: Gli ambienti Terminal Server e Citrix Server, ivi compresi i servizi ospitati e gli ambienti virtuali, sono esclusi dall'ambito della fornitura.

Suggerimento: Gli ambienti Citrix Server possono decodificare non correttamente alcune lettere regionali (ad esempio l'umlaut tedesco).

Sistemi operativi:

- Microsoft Windows Server 2015 (32 bit / 64 bit) come Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) come Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) come Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 ((64 bit) con Citrix XenApp 6.5 Server (modalità Desktop)

Il supporto di myAgent per Microsoft Windows XP e Microsoft Windows Server 2003 termina in concomitanza con il termine del supporto da parte di Microsoft. Il prodotto sarà ancora supportato, ma non testato nei dettagli.

Requisiti hardware: il numero di client installabili dipende dalle prestazioni del server e dalla disponibilità di memoria. Se sul server sono utilizzate altre applicazioni, è necessario prendere in considerazione il relativo consumo di memoria.

Ulteriori informazioni sulla configurazione con Citrix XenApp Server sono reperibili sul sito Web:

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

File di installazione

Per mettere a disposizione degli utenti i file di installazione, sono disponibili le seguenti opzioni:

- L'amministratore scarica i file di installazione dal **Centro assistenza** e li mette a disposizione degli utenti, ad esempio tramite un'unità di rete.

Osservare le indicazioni contenute nel file `ReadMe first`, che si trova nella cartella di archiviazione dei file di installazione.

Suggerimento: Non è supportata la distribuzione automatica del file MSI tramite servizio di installazione con Microsoft Windows Server.

18.1.3 myReports

Gli agenti con il livello di autorizzazione Supervisore o Amministratore possono utilizzare myReports per creare rapporti sugli agenti e sulla relativa attività, nonché su chiamate, code d'attesa, prestazioni, livello di servizio e codici di elaborazione.

myReports offre i seguenti servizi:

- Più di 100 modelli predefiniti e suddivisi per temi (gruppi di rapporti) da utilizzare per la creazione di rapporti
- Pianificazioni per la creazione di rapporti programmabili nel tempo
- Invio immediato e programmabile di rapporti tramite e-mail
- Esportazione di rapporti pianificati
- Output formats for report previews, sent e-mails and exported reports: Excel, PDF, and Word
- Anteprima rapporto, per la verifica del rapporto da creare nel formato di output desiderato.

Funzioni utente

myReports dispone di una propria gestione degli utenti che controlla l'accesso alle funzioni di MyReports assegnando ruoli agli utenti. In questo modo è possibile distinguere tra utenti di myReports (utenti standard) e amministratori di myReports.

La funzione corrente di un utente viene definita al suo accesso a myReports.

Le differenze tra le diverse funzioni utente sono riassunte nella seguente tabella.

myReports:	**Funzione utente**	
Attività	myReports User	myReports Amministratore
Rapporti		

myReports: Attività	Funzione utente	
	myReports User	myReports Amministratore
Anteprima rapporto	X	X
Inviare immediatamente il rapporto tramite e-mail	X	X
Aggiungere modelli di rapporto	X	X
Eliminazione dei modelli di rapporto aggiunti	X	X
Definire nuovi modelli di rapporto		X
Aggiornare i modelli di rapporto predefiniti		X
Pianificazioni		
Aggiungere pianificazioni	X	X
Visualizzare i dettagli di una pianificazione	X	X
Modifica pianificazione	X	X
Elimina pianificazione	X	X
Configuration		
Modificare la lingua dell'interfaccia utente	X	X
Modificare i colori interfaccia utente	X	X
Configurare il modello e-mail	X[7]	X
Modificare l'indirizzo del server	X	X
Modificare la password amministratore		X
Configurazione dei prefissi per i numeri di telefono esterni		X
Come attivare/disattivare la protezione dei dati		X
Come configurare il percorso per l'esportazione dei rapporti pianificati		X
Configurazione lingua		X[8]
Configurare la lingua predefinita		X[8]

7 The administrator password must be entered to configure the e-mail template

8 Per la configurazione della lingua e della lingua predefinita è necessario accedere come amministratore di myReports con una password speciale.

18.1.3.1 Come reimpostare la password amministratore di myReports

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**.
4) Click on **Maintenance**.
5) Click on **Reset Password**, under the **Reports** area.

Passaggi successivi

Inform the myReports administrator(s) that you have reset the administrator password to the default password `reports`.

18.1.4 Requisiti richiesti per l'uso di myReports

Per poter utilizzare myReports, il PC client dell'utente deve disporre di una dotazione hardware e software adeguata.

Suggerimento: Rispettare scrupolosamente le note contenute nel file `ReadMe first`, che si trova nella stessa cartella dei file di installazione.

Sistemi operativi

myReports può essere utilizzato in combinazione con i seguenti sistemi operativi:

- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bit o 64 bit)
- Microsoft Windows Vista (32 bit)

Suggerimento: Il sistema operativo utilizzato richiede sempre lo stato attuale di tutti gli aggiornamenti disponibili (service pack e patch).

Il supporto di myReports per Microsoft Windows XP e Microsoft Windows Server 2003 termina in concomitanza con il termine del supporto da parte di Microsoft. Il prodotto sarà ancora supportato, ma non testato nei dettagli.

Software aggiuntivo

- Oracle Java 8 o versioni successive oppure, in alternativa, OpenJDK 8 (vedere **Centro assistenza** > **Software**)
- Adobe Reader 9 o successivo (per rapporti in formato PDF)
- Microsoft Excel 16/2013/2010 (per rapporti in formato Excel)
- Microsoft Word 16/2013/2010 (per report in formato Word)

Requisiti hardware minimi

- CPU 2 GHz
- RAM: 2 GB
- LAN 100 Mbit/s (consigliato: LAN 1 Gbit/s)
- Risoluzione dello schermo XGA (1024x768), myPortal for Outlook: Risoluzione dello schermo SVGA (800x600)

PC multiutente

In Microsoft Windows 7 e Microsoft Windows Vista con PC multiutente, ciascun utente locale può utilizzare myReports con impostazioni personalizzate, se il primo utente locale ha installato il client con diritti di amministratore locale. Solo il primo utente locale con diritti di amministratore locale può eseguire gli aggiornamenti con la funzione aggiornamento automatico.

Microsoft Terminal Server, Citrix XenApp Server

myReports può essere utilizzato in ambienti Microsoft Terminal Server/Citrix Server se vengono soddisfatti i requisiti riportati di seguito.

Suggerimento: Gli ambienti Terminal Server e Citrix Server, ivi compresi i servizi ospitati e gli ambienti virtuali, sono esclusi dall'ambito della fornitura.

Suggerimento: Gli ambienti Citrix Server possono decodificare non correttamente alcune lettere regionali (ad esempio l'umlaut tedesco).

Sistemi operativi:

- Microsoft Windows Server 2015 (32 bit / 64 bit) come Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) come Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) come Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 ((64 bit) con Citrix XenApp 6.5 Server (modalità Desktop)

Requisiti hardware: il numero di client installabili dipende dalle prestazioni del server e dalla disponibilità di memoria. Se sul server sono utilizzate altre applicazioni, è necessario prendere in considerazione il relativo consumo di memoria.

Ulteriori informazioni sulla configurazione con Citrix XenApp Server sono reperibili sul sito Web:

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

File di installazione

Per mettere a disposizione degli utenti i file di installazione, sono disponibili le seguenti opzioni:

- L'amministratore scarica i file di installazione dal **Centro assistenza** e li mette a disposizione degli utenti, ad esempio tramite un'unità di rete.

Osservare le indicazioni contenute nel file `ReadMe first`, che si trova nella cartella di archiviazione dei file di installazione.

Suggerimento: Non è supportata la distribuzione automatica del file MSI tramite servizio di installazione con Microsoft Windows Server.

18.1.5 Note sull'utilizzo simultaneo di myAgent e client UC Suite

In caso di utilizzo simultaneo di myAgent e di altri client UC Suite mediante un account utente UC Suite, non è possibile escludere la possibilità di interazioni reciproche.

In questa sezione, il termine "myPortal" si riferisce a myPortal for Desktop, myPortal for Outlook, myPortal @work e myPortal to go.

Esempi di interazioni reciproche:

- Modifica dello stato presenza tramite myPortal

  Gli esempi si applicano all'impostazione **Casella vocale** predefinita per tutte le destinazioni di inoltro.

  – myAgent: l'agente è connesso.

    myPortal: la funzione di reimpostazione automatica dello stato presenza su Ufficio è disattivata.

    Modificando lo stato presenza tramite myPortal si avrà l'immediata disconnessione dell'agente dalla coda/dalle code. Dopo la disconnessione dell'agente tramite myAgent, lo stato presenza in myPortal viene reimpostato su **Ufficio**.

    Il cambio dello stato agente tramite myAgent (ad esempio **Pausa**) viene registrata da myPortal, ma non viene applicata a **Connetti**, **Disconnetti** e **Orario lavorativo**.

  – myAgent: l'agente è connesso.

    myPortal: la funzione di reimpostazione automatica dello stato presenza su Ufficio è attivata.

    Se l'agente cambia il suo stato in **Pausa** tramite myAgent, allo scadere del tempo di pausa ritornerà automaticamente disponibile.

    Cambiando lo stato presenza tramite myPortal in **Pausa**, si avrà l'immediata disconnessione dell'agente dalla coda/dalle code.

  – myAgent: l'agente è connesso.

    Cambiando lo stato presenza tramite myPortal in **Non disturbare**, si avrà l'immediata disconnessione dell'agente dalla coda/dalle code.

- Chiamate in uscita tramite myPortal

  Lo stato presenza dell'utente è visibile tramite myAgent.

  Le chiamate vengono visualizzate solo nel diario di myPortal. Non verranno incluse nelle statistiche del Contact Center, in quanto non sono chiamate del Contact Center.

- Chiamate in entrata al numero di telefono dell'agente

  Lo stato presenza dell'utente è visibile tramite myAgent.

  Le chiamate vengono visualizzate solo nel diario di myPortal. Non verranno incluse nelle statistiche del Contact Center, in quanto non sono chiamate del Contact Center.
- Registrazione di una chiamata

  La registrazione di chiamate tramite myPortal non viene registrata da myAgent. myAgent offre questa funzione anche quando la registrazione di una chiamata è già eseguita da myPortal.

18.2 Agenti

Gli agenti (utenti) di una coda d'attesa formano un gruppo di lavoro che può essere impostato ad esempio nelle Hotline tecniche o nel reparto di acquisizione/registrazione degli ordini. Le chiamate in arrivo, i fax e le e-mail vengono distribuiti in modo uniforme tra gli agenti disponibili.

Per poter utilizzare un utente del sistema di comunicazione come agente, è necessario che l'utente sia configurato come agente. I diritti degli agenti vengono quindi definiti selezionando i livelli di autorizzazione definiti (agente, supervisore o amministratore). I supervisori e gli amministratori possiedono un livello di autorizzazione superiore (vedere Funzioni degli agenti basate sul livello di autorizzazione).

Un agente può essere impostato come agente sempre disponibile. L'agente rimane disponibile per chiamate, fax e e-mail, anche se non ha risposto a una chiamata, fax o e-mail.

18.2.1 Funzioni degli agenti indipendenti dal livello di autorizzazione

Quando si importa un utente come agente, vengono definiti i diritti di agente selezionando livelli di autorizzazione (agente, supervisore o amministratore). Gli agenti con livello di autorizzazione Supervisore o Amministratore possiedono privilegi elevati.

Le differenze tra i vari livelli di autorizzazione sono riassunte nella seguente tabella.

myAgent:	**Livello di autorizzazione (classe di servizio)**		
Attività	**Agente**	**Supervisore**	**Amministratore**
Assegnare un agente a una coda	–	X	X
Spostare un agente in un'altra coda	–	X	X
Eliminare un agente dalla coda	–	X	X
Cambiare lo stato di un agente	–	X	X
Visualizzare / nascondere l'elenco associazioni dell'agente	Code d'attesa assegnate	Tutte le code	Tutte le code
Modificare l'associazione di un agente	–	X	X

myAgent: Attività	Livello di autorizzazione (classe di servizio)		
	Agente	**Supervisore**	**Amministratore**
Visualizzare l'elenco delle chiamate in tempo reale	Code d'attesa assegnate	Tutte le code	Tutte le code
Attivare automaticamente la schermata popup myAgent per gli allarmi	–	X	X
Attivare il tono di allarme	–	X	X
Visualizzare la bacheca	Code d'attesa assegnate	Tutte le code	Tutte le code
Visualizzare il grafico Grado di servizio	Code d'attesa assegnate	Tutte le code	Tutte le code
Visualizzare il grafico Media oraria	Code d'attesa assegnate	Tutte le code	Tutte le code
Spostare la chiamata nella prima posizione di una coda	–	X	X
Registrare una chiamata	Chiamata corrente	Tutte le chiamate	Tutte le chiamate
Registrazioni: salvataggio come file WAV o invio tramite e-mail	–	X	X
Salvataggio di un fax come file TIFF o invio del fax tramite e-mail	–	X	X
Salvataggio di e-mail o invio di e-mail tramite e-mail come file EML	–	X	X
Ascolto di una chiamata (secondo i paesi)	–	X	X
Inclusione in una chiamata	–	X	X
Accettare una richiesta di assistenza	–	X	X
Creare rapporti	–	X	X
Aprire WBM	–	X	X

18.2.2 Agenti preferiti

A ogni chiamante (ad esempio a ogni cliente che chiama), è possibile assegnare uno o più agenti preferiti di una coda d'attesa. In questo caso, il sistema di comunicazione tenta innanzitutto di inoltrare le chiamate e le prenotazioni di chiamata del cliente a un agente preferito. Se sono definiti più agenti preferiti, è possibile definire una priorità (sequenza) in base alla quale il chiamante verrà connesso agli agenti preferiti.

Se non è disponibile nessuno degli agenti preferiti, la chiamata verrà inoltrata a uno qualsiasi degli agenti disponibili.

18.2.3 Agente in più code d'attesa

Un agente può essere assegnato a più code d'attesa e con un livello di competenza diverso in ognuna di esse. A tale fine, è necessario definire se l'agente deve agire come agente primario o di overflow.

18.2.4 Pause del Contact Center

Per prevedere pause definite per ciascun agente, è possibile impostare pause del Contact Center di diversa durata (ad esempio, pausa pranzo, pausa caffè). Le pause del Contact Center sono impostate nel sistema e possono all'occorrenza essere selezionate da un agente tramite myAgent.

18.2.5 Accesso/Disconnessione agente tramite telefono

La procedura di accesso/disconnessione al Contact Center è supportata anche tramite telefono, senza dover utilizzare myAgent per avvalersi delle funzioni del Contact Center. Se un agente ha effettuato l'accesso tramite telefono vengono gestite solo le chiamate vocali. In questo caso le immissioni tramite finestra popup e codice di post-elaborazione non sono supportate. Ciò avviene anche se myAgent è attivo e l'agente accede al Contact Center utilizzando il telefono. Per ripristinare le funzionalità complete di myAgent, l'agente deve disconnettersi tramite il telefono, quindi accedere nuovamente mediante myAgent.

Premesse e vincoli

- Le funzioni di OpenScape Business Contact Center accessibili tramite telefono sono operative solo per gli agenti ai quali è stata assegnata una licenza di myAgent in OpenScape Business
- Il supporto di tutte le funzioni è disponibile solo sui telefoni rilasciati per l'uso con OpenScape Business Contact Center
- Quando l'accesso tramite telefono viene effettuato correttamente e il client myAgent associato non è attivo, all'agente vengono instradate solo chiamate vocali
- Quando l'accesso tramite telefono viene effettuato correttamente e il client myAgent associato è attivo, se l'agente accede tramite telefono non riceve messaggi e-mail/fax e richiamate. In tal caso, le finestre popup e la post-elaborazione funzionano normalmente ma l'agente riceve solo chiamate vocali. Per utilizzare funzionalità complete, l'agente deve prima disconnettersi tramite telefono, quindi accedere mediante myAgent.

Accesso al Contact Center tramite telefono

Quando l'agente accede a OpenScape Business Contact Center tramite telefono, indipendentemente dallo stato di attività del client myAgent e del Contact Center:

- Le funzioni di accesso UCD vengono utilizzate mediante il telefono
- La funzione di accesso è eseguibile tramite un codice funzione o un tasto programmato

- L'agente accede a tutte le code a cui è assegnato nell'ambito della configurazione del Contact Center
- Il display del telefono visualizza lo stato di accesso per l'agente
- Solo le informazioni sulla coda UCD (ad es. le informazioni sulle chiamate in coda) vengono visualizzate su richiesta

L'agente può utilizzare le seguenti funzioni:

- Accesso / Disconnessione (tramite l'ID agente UCD)
- Post- elaborazione
- Disponibile / Non disponibile
- Visualizzazione delle chiamate nella coda UCD alla quale l'ID agente UCD è stato assegnato

Nota: L'agente non può utilizzare il Servizio notturno UCD.

Nota: Il flag permanente disponibile di myAgent è supportato per l'accesso tramite telefono. Ciò significa che nel caso in cui un agente abbia effettuato l'accesso con il proprio telefono e una chiamata sia stata persa, questo agente rimane disponibile per la chiamata successiva. Lo stesso comportamento avviene con l'utilizzo del client myAgent.

Se il Contact Center si arresta mentre l'agente è connesso, quest'ultimo rimane connesso all'UCD e le chiamate vocali vengono instradate in base alla configurazione del routing UCD. Se l'agente non è connesso, può accedere all'UCD tramite telefono.

Disconnessione dal Contact Center tramite telefono

Quando l'agente si disconnette da OpenScape Business Contact Center tramite telefono, indipendentemente dallo stato di attività del client myAgent e del Contact Center:

- Le funzioni di disconnessione UCD vengono utilizzate mediante il telefono
- La funzione di disconnessione è eseguibile tramite un codice funzione o un tasto programmato
- L'agente viene disconnesso da tutte le code a cui è assegnato nell'ambito della configurazione del Contact Center
- Il display del telefono visualizza lo stato di disconnessione per l'agente
- Nessun'altra informazione sul Contact Center / UCD (ad es. le informazioni sulle chiamate in coda) viene visualizzata

Impostazione tramite telefono dello stato agente disponibile / non disponibile

Quando un agente imposta il proprio stato come disponibile / non disponibile per l'instradamento di contatti di OpenScape Business Contact Center, indipendentemente dallo stato di attività di myAgent e del Contact Center:

- Il display del telefono visualizza lo stato di accesso per l'agente
- Se myAgent non è attivo vengono instradate all'agente solo le chiamate vocali

Impostazione/Reimpostazione della post-elaborazione delle chiamate tramite telefono

Quando un agente imposta il proprio stato su "Post-elaborazione", tramite telefono, indipendentemente dallo stato di attività di myAgent e del Contact Center, non vengono instradate chiamate a tale agente finché l'intervallo di post-elaborazione corrispondente, configurato in OpenScape Business Contact Center, non scade o la post-elaborazione non viene reimpostata dall'agente stesso mediante il telefono.

Mappatura dello stato

La modifica dello stato dell'agente effettuata tramite telefono viene mappata come segue nello stato dell'agente in myAgent:

Dispositivo telefonico			myAgent			
Codice funzione	**Codice funzione**	**Descrizione**	Testo visualizzato dal telefono	**Stato**	**Testo aggiuntivo**	Nota
*401	ID agente UCD	Effettuare il login degli operatori	Disponibile	Disponibile	-	L'agente è impostato come disponibile in tutte le code assegnate
#401	–	UCD - log of operatore	Non disponibile	Non disponibile	-	L'agente è impostato come non disponibile in tutte le code assegnate
*402	–	UCD - operatore disponibile	Disponibile	-	-	Disponibile (fine di tempo di attività)
#402	–	UCD - operatore non disponibile	Non disponibile	Orario lavorativo	conto alla rovescia da 999.999 secondi	-
*403	–	Elaborazione UCD on	Post-elaborazione	Orario lavorativo	conto alla rovescia del tempo di attività configurato	Il tempo di attività deve essere esaurito prima di poter iniziare nuovamente. Non è possibile cumulare tempi di attività come in myAgent. Una volta esaurito il tempo di attività, l'agente ritorna disponibile automaticamente.

Dispositivo telefonico			myAgent			
Codice funzione	**Codice funzione**	**Descrizione**	Testo visualizzato dal telefono	**Stato**	**Testo aggiuntivo**	Nota
#403	–	Elaborazione UCD off	Disponibile	Disponibile	-	-
*404	destinazione del servizio notturno	Servizio notte UCD on	–	Supporto non disponibile	-	Non utilizzare il Servizio notturno UCD
#404	–	Servizio notte UCD off	–	Supporto non disponibile	-	Non utilizzare il Servizio notturno UCD
*405	–	Controllo stato coda chiam.UCD	-	-	-	Viene visualizzata solo la coda alla quale l'ID agente UCD è stato assegnato, indipendentemente dal fatto che l'agente sia assegnato a varie code nel Contact Center

18.3 Code d'attesa e pianificazioni

Le code d'attesa sono alla base del Contact Center. Le chiamate, i fax e le e-mail di una coda d'attesa vengono gestiti in base al livello di competenza degli agenti, alla priorità e al tempo d'attesa. Per le chiamate in attesa è possibile riprodurre annunci. Le pianificazioni definiscono come devono essere trattate le chiamate, in giorni e in orari specifici.

18.3.1 Code d'attesa

Di norma la distribuzione delle chiamate avviene in modo che una chiamata entrante, un fax o un'email venga inoltrata alla coda di attesa dell'utente (agente) del gruppo da più tempo inattivo. È comunque possibile definire altre regole di distribuzione (ad esempio tramite i diversi livelli interfaccia degli agenti). Se tutti gli agenti sono occupati, le successive chiamate, i fax e le e-mail in arrivo verranno inseriti in posizione di attesa e in seguito, in base alla priorità e al tempo di attesa, distribuite agli agenti che nel frattempo si sono liberati.

Con l'aiuto delle pianificazioni e delle regole ivi contenute (= CCV, Call Control Vector), è possibile definire come una chiamata verrà gestita in una coda d'attesa in un momento o in un giorno specifici. Le regole determinano, ad esempio, quale annuncio riprodurre per i chiamanti o dove inoltrare la chiamata.

Fax, e-mail e richiamate degli agenti vengono assegnati alle code d'attesa direttamente dalle pianificazioni.

Quando si assegnano agenti alle code d'attesa, è anche possibile assegnare agli agenti diverse proprietà (associazione agente), che influiscono sulla distribuzione delle chiamate in una coda d'attesa (ad esempio, agente primario, agente di overflow, livello interfaccia). L'assegnazione di agenti alle code d'attesa può avvenire:

- da un amministratore con il profilo **Advanced**, tramite il WBM.
- con l'applicazione myAgent tramite un agente con il livello di autorizzazione Supervisore o Amministratore.

Se un agente è assegnato a più code d'attesa, tramite la priorità delle code d'attesa è possibile definire se le chiamate per una coda d'attesa con priorità più alta devono essere inoltrate a questo agente come le chiamate di altre code d'attesa.

Il WBM consente di eseguire le seguenti importanti impostazioni per le code d'attesa:

- Attivazione, disattivazione ed eliminazione di code d'attesa

  Nota: dopo l'eliminazione di una coda d'attesa, non è possibile creare rapporti sui periodi passati. Le code d'attesa non più necessarie devono essere disattivate.
- Configurazione degli allarmi coda d'attesa

  Le opzioni disponibili sono:

  – Conteggio allarmi coda (Soglia di allarme): se il numero qui indicato supera il numero di chiamate in coda d'attesa, l'icona della coda d'attesa visualizzata dall'agente passa da verde ad arancione. Gli agenti con il livello di autorizzazione "Supervisore" o "Amministratore" possono definire comportamenti del sistema quali l'emissione o meno di un tono di allarme e il richiamo o meno di myAgent in primo piano.
  – Ora allarme coda (Soglia di allarme): se il tempo in coda d'attesa per una chiamata qui indicato viene superato, la corrispondente voce nell'elenco di chiamate del Contact Center dell'agente diventa rossa. Gli agenti con il livello di autorizzazione "Supervisore" o "Amministratore" possono definire comportamenti del sistema quali l'emissione o meno di un tono di allarme e il richiamo o meno di myAgent in primo piano.
- Come definire il timeout per fax, e-mail e chiamate persi

  Se entro il tempo qui specificato una chiamata, un fax o un'e-mail non riceve risposta da parte dell'agente, tale comunicazione verrà inoltrata al successivo agente libero.
- Definizione della soglia chiamate abbandonate

  Sulla base del tempo qui indicato, viene definito se una chiamata abbandonata dovrà essere registrata nelle statistiche (rapporti) o meno. Verranno incluse nelle statistiche le chiamate che vengono abbandonate una volta trascorso il tempo indicato.
- Configurazione della profondità della coda

  Questa procedura permette di controllare il numero massimo di chiamate attive e in attesa in una coda specifica. Il Contact Center indica al sistema che è stata raggiunta la soglia definita per le dimensioni della coda. Di conseguenza, il sistema rifiuta qualsiasi nuova chiamata in entrata per la

coda corrispondente, prima che tale chiamata venga connessa al sistema, finché il numero di chiamate non scende nuovamente sotto la soglia.

Le dimensioni massime della coda dipendono dai seguenti parametri:

– Numero massimo di posizioni di attesa nella coda. (WLS = Waiting Loop Size, Dimensioni del loop di attesa)
– Numero massimo di chiamate attive e in attesa della coda (Dimensioni di profondità coda).

- Configurazione dei piloti fax in arrivo

  Se configurata, è possibile selezionare numeri di telefono per i messaggi fax in arrivo. I fax destinati a questi numeri vengono inseriti nella coda d'attesa e trattati come una chiamata in arrivo.
- Configurazione del servizio e-mail in arrivo

  Per ogni coda d'attesa, è possibile configurare più indirizzi e-mail. Le e-mail a questi indirizzi vengono inserite nella coda d'attesa e trattate come una chiamata in arrivo.
- Configurazione dell'indirizzo e-mail del mittente

  Indirizzo e-mail della coda d'attesa visibile al destinatario in caso di invio di un'email da parte di un agente.
- Attivazione del routing chiamate intelligente

  Una chiamata in arrivo viene inoltrata all'ultimo agente connesso con quel chiamante. Ciò avviene solo se per il chiamante in questione non è stato definito alcun agente preferito.

18.3.2 Pianificazioni

Le pianificazioni e le regole ivi contenute (Call Control Vector, CCV) consentono di definire per ogni coda d'attesa come le chiamate in arrivo verranno gestite in giorni o orari specifici.

Ad esempio, è possibile definire una regola per i giorni lavorativi per il primo turno (dalle 6:00 alle 14:00), una per il secondo turno (dalle 14:00 alle 22:00) e una per il turno notturno (dalle 22:00 alle 06:00). Per i weekend, è possibile definire una regola specifica. Per ciascuna di queste regole, è possibile indicare se è necessario riprodurre un annuncio e/o dove devono essere inoltrate le chiamate.

Le pianificazioni sono il fulcro della configurazione del Contact Center. La configurazione di un Contact Center non può considerarsi conclusa senza aver definito almeno una pianificazione. A ogni coda di attesa deve essere assegnata almeno una pianificazione. Può trattarsi anche di una stessa pianificazione.

A una pianificazione deve essere assegnata almeno una regola (Call Control Vector CCV). Le regole determinano, per il periodo di validità di una pianificazione, come vengono gestite le chiamate in entrata di una coda di attesa. Le regole si applicano solo alle chiamate e non ai fax e alle e-mail.

Le regole vengono create con l'Editor regole grafico (Editor CCV) collegando oggetti CCV predefiniti; dopo la definizione possono essere memorizzate con un nome a libera scelta.

Le regole memorizzate possono essere assegnate a una o più pianificazioni come regola predefinita (CCV predefinito) o regola eccezione (CCV eccezione).

L'apertura, la modifica e il risalvataggio sono possibili in qualsiasi momento tramite l'Editor regole.

Se a una pianificazione è stata assegnata una regola predefinita (CCV predefinito), tale pianificazione può essere memorizzata con un nome a libera scelta. Una pianificazione con una regola predefinita diventa valida dopo l'assegnazione a una coda di attesa di 24 ore al giorno e 365 giorni all'anno. Se in occasioni e orari specifici (pausa, fine settimana, giorno festivo, vacanza ecc.) sono valide altre regole, è possibile assegnarvi una pianificazione corrispondente sotto forma di regole eccezione (CCV eccezione). In questo modo, è possibile definire come devono essere gestite ad esempio le chiamate in arrivo durante il periodo di vacanza. In questo caso le pianificazioni vacanze hanno la priorità rispetto alle altre pianificazioni e regole di una coda d'attesa.

Editor regole (Editor CCV)

Con l'Editor regole è possibile creare delle regole sulla base di oggetti CCV predefiniti. L'ordinamento degli oggetti CCV e delle relative proprietà definisce come le chiamate in arrivo verranno gestite.

Nota: Una regola ha un limite superiore di 500 oggetti CCV.

Sono disponibili i seguenti oggetti CCV predefiniti:

Suggerimento: Per tutti gli oggetti CCV indicati valgono inoltre le due seguenti proprietà generali:

Descrizione: possibilità opzionale di descrivere l'oggetto CCV, ad esempio Annuncio di benvenuto.

Elabora dopo digitazione: indicazione del numero di cifre richieste senza spazi, virgole o altri caratteri. Questa indicazione si riferisce all'oggetto CCV precedente. Se in tale oggetto è stato inserito 9 in Cifre accettate, è necessario inserire un 9 anche qui.

- **Riproduci messaggio**

  Determina la riproduzione dell'annuncio desiderato. È possibile selezionare un qualsiasi file audio nella UC Suite. Inoltre, è possibile importare un nuovo file audio nella UC Suite o registrare un nuovo messaggio e successivamente importarlo come file audio nella UC Suite.

  La riproduzione dell'annuncio occupa sempre un Media Stream Channel.

  Proprietà:

  – **Nome file**: scelta di un annuncio (file audio nel formato WAV)
  – **Interrompi digitazione**: Indicazione di un tasto o combinazione di tasti su tastiera con la quale un chiamante può interrompere la riproduzione dell'annuncio.
  – **Gestione file**: tramite questo pulsante è possibile caricare un file audio in formato wav o creare un nuovo file vocale con il registratore.

- **Musica su Attesa**

  Determina la riproduzione della musica su attesa (Music On Hold MOH del sistema di comunicazione) per chiamante esterno per un tempo impostabile

  Proprietà:

  – **Valore ora**: tempo (in secondi), durante il quale verrà riprodotta la musica su attesa.
- **Disconnetti chiamante**

  Determina l'interruzione della connessione

  Dopo questo oggetto CCV non può essere inserito alcun altro oggetto CCV.
- **Riproduci posizione in coda**

  Determina la notifica del chiamante sulla sua attuale posizione nella coda d'attesa
- **Tempo di attesa previsto**

  Determina la notifica del chiamante sul tempo di attesa previsto.

  Il calcolo del tempo di attesa previsto si basa su:

  1) Tempo medio in coda storico di tutte le code d'attesa
  2) Tempo medio in coda storico della coda d'attesa in particolare
  3) Tempo medio di conversazione storico dell'agente in particolare
- **Vai a CCV**

  Crea un loop a un altro oggetto CCV

  Proprietà:

  – **CCV di destinazione**: scelta dell'oggetto CCV
- **Registra richiamata**

  Consente a un chiamate in una coda d'attesa di attivare la richiamata agente (registrazione di un messaggio vocale). La richiamata agente rimane in coda d'attesa al posto del singolo chiamante. Gli agenti con la proprietà **Attiva richiamata agente** visualizzeranno la richiamata agente nell'elenco di chiamate del Contact Center.

  Dopo questo oggetto CCV non può essere inserito alcun altro oggetto CCV.

  Proprietà:

  – **Tipo**: scelta tra **Richiamata automatica semplice** o **Richiamata automatica senza limitazioni**.

    Diversamente dalla richiamata automatica semplice, con una richiamata automatica senza limitazioni, il chiamante ha a disposizione diverse opzioni e informazioni (conferma o modifica del numero di telefono al quale essere richiamato, conferma del messaggio vocale).
  – **Lunghezza massima messaggi (sec.)**: tempo espresso in secondi a disposizione per la registrazione di un messaggio vocale.

- **Elabora dopo digitazione**

  Determina l'esecuzione di uno o più oggetti CCV successivi, in base alle cifre qui indicate (Elabora dopo digitazione).

  Proprietà:

  – **Nome file**: scelta di uno o più annunci (file audio in formato WAV)
  – **Lista di riproduzione**: elenco di tutti gli annunci selezionati (file audio in formato WAV) in una sequenza di riproduzione
  – **Timeout digitazione**: tempo espresso in secondi per il quale il sistema di comunicazione rimane in attesa dell'immissione della cifra.

    Se entro tale tempo non viene immessa alcuna cifra, il messaggio viene riprodotto di nuovo.
  – **Collegamento a**: elenco di cifre con destinazione.

    Le cifre e le destinazioni possono essere aggiunte, modificate ed eliminate.
  – **Gestione file**: tramite questo pulsante è possibile caricare un file audio in formato wav o creare un nuovo file vocale con il registratore.

  Il contenuto della lista di riproduzione viene visualizzato nell'Editor regole mediante una descrizione che compare quando si posiziona il puntatore del mouse sull'oggetto CCV.
- **Trasferimento a passaggio singolo**

  Questa funzione dipende dall'impostazione **SST AutoAttendant normale** (WBM, **Modalità esperti**: **Applicazioni** > **OpenScape Business UC Suite** > **Server** > **Impostazioni generali**):

  – **SST AutoAttendant normale** attivato (impostazione predefinita, non per USA): determina il trasferimento della chiamata indipendentemente che la destinazione sia libera, occupata o non disponibile.

    Suggerimento: Se l'utente ha attivato il rifiuto dell'avviso di chiamata in attesa, la chiamata viene inoltrata quando l'utente di destinazione è libero. L'avviso di chiamata in attesa su occupato non viene inviato.

  – **SST AutoAttendant normale** disattivato (impostazione predefinita, solo per USA): determina il trasferimento della chiamata se la destinazione è libera.

    Se la destinazione è occupata, e il rifiuto dell'avviso di chiamata è disattivato o se la destinazione non è disponibile, viene riprodotto un messaggio per il chiamante. Il chiamante può scegliere se lasciare un

messaggio nella casella vocale dell'utente o se comporre il numero di telefono di un'altra destinazione.

Se la destinazione è occupata e il rifiuto dell'avviso di chiamata è stato attivato, la chiamata non viene trasmessa.

Dopo questo oggetto CCV non può essere inserito alcun altro oggetto CCV.

Proprietà:

– **Interno di destinazione**: indicazione del numero interno o di selezione passante esterno con il numero della linea impegnata. Non sono consentiti spazi, virgole o altri caratteri.

Il numero di telefono dell'interno di destinazione viene visualizzato nell'oggetto CCV.

Nota: Dopo il trasferimento a passaggio singolo, il sistema scollega la chiamata dopo aver squillato per 5 minuti.

- **Trasferisci in coda**

  Determina il trasferimento della chiamata a una coda d'attesa

  Dopo questo oggetto CCV non può essere inserito alcun altro oggetto CCV.

  Proprietà:

  – **Coda**: scelta della coda d'attesa
- **Registra nella casella postale**

  Devia la chiamata alla casella vocale desiderata di un utente o di un gruppo casella vocale

  Dopo questo oggetto CCV non può essere inserito alcun altro oggetto CCV.

  Proprietà:

  – **Casella postale utente**: indicazione del numero di telefono della casella vocale di un utente o di un gruppo casella vocale

  Il numero di telefono e il nome della casella vocale o del gruppo casella vocale vengono visualizzati nell'Editor regole mediante una descrizione che compare quando si posiziona il puntatore del mouse sull'oggetto CCV.
- **Trasferimento supervisionato (noto anche come trasferimento consultazione)**

  Determina il trasferimento della chiamata a una destinazione interna. Durante il trasferimento, viene riprodotta musica su attesa per il chiamante (Music On Hold, MOH, della UC Suite).

  A differenza del trasferimento a passaggio singolo dell'oggetto CCV, in questo caso è necessario aggiungere altri due oggetti CCV. In altre parole, è necessario definire come deve comportarsi il sistema di comunicazione quando la destinazione di chiamata è occupata o la chiamata non viene

risposta. Di norma in questi casi viene riprodotto un annuncio per il chiamante.

Proprietà:

– **Interno di destinazione**: indicazione del numero interno.

  Nel proprio nodo sono supportati solo numeri interni. L'inoltro a destinazioni esterne, stazioni virtuali, altri AutoAttendant, utenti mobili e destinazioni esterne CallMe non è consentito!

  Per questi scenari, deve essere utilizzato l'SST (Single Step Transfer). Per trasferire una chiamata a un altro UCD che fa parte di Contact Center, è necessario utilizzare l'oggetto CCV **Trasferisci in coda**.

– **Trasferimento squilli**: tempo espresso in secondi entro il quale è necessario rispondere alla chiamata.

  Se la chiamata non viene risposta entro tale tempo, passerà di nuovo al sistema di comunicazione, che utilizzerà l'oggetto CCV successivo.

  Suggerimento: Il tempo qui indicato deve essere più breve di quello configurato per l'inoltro di chiamata (tempo predefinito per l'inoltro di chiamata = 15 secondi). Vedere Come configurare un inoltro di chiamata.

– **Ritira chiamata se inoltrata / deviata dall'apparecchio di destinazione**: opzione (vale solo per un numero interno).

  Se questa opzione viene attivata, viene eseguito un test della destinazione di chiamata. Se per la destinazione di chiamata è stato attivato un inoltro chiamate o una deviazione di chiamata, la chiamata ritorna al sistema di comunicazione che utilizzerà l'oggetto CCV successivo.

– **Quando si trasferisce una chiamata, verificare lo stato di presenza**: opzione

  Se questa opzione è attivata, viene eseguito un test dello stato di presenza della destinazione di chiamata. Se viene rilevato uno stato diverso da Ufficio, la chiamata viene restituita al sistema di comunicazione e si utilizza l'oggetto CCV successivo.

• **Componi per nome**

Determina la richiesta al chiamante di inserire le prime tre lettere del cognome dell'utente desiderato tramite la tastiera.

Se esiste un utente corrispondente alle lettere iniziali specificate, viene stabilita la connessione.

Se vi sono più utenti con le lettere iniziali specificate, al chiamante vengono annunciati i nomi di questi utenti (massimo 10 utenti). Se un utente non ha registrato un annuncio col nome, viene annunciato invece il numero di telefono. Una volta scelto l'utente desiderato, viene stabilita la connessione.

Se nessun utente corrisponde alle lettere iniziali indicate, il chiamante riceve il messaggio corrispondente.

Suggerimento: I tasti della tastiera reagiscono alla prima pressione del tasto. Ad ogni pressione del tasto viene

verificato se esistono cognomi di utenti con le lettere assegnate al tasto.

Esempio: nella rubrica interna sono presenti i seguenti cinque cognomi con le lettere iniziali T, U e V: Taylor, Taler, Ullrich, Vasquez e Volterra. Per creare un abbinamento con l'utente Taylor, si devono premere i tasti seguenti: 8 2 9

Dopo questo oggetto CCV non può essere inserito alcun altro oggetto CCV.

Proprietà:

– **Metodo**: scelta tra **Trasferisci a interno** o **Registra nella casella postale**.

  In base al metodo selezionato viene realizzata una connessione all'utente desiderato o alla relativa casella vocale. Sono supportati solo gli utenti interni che sono registrati con nome e cognome nella rubrica interna.

- **Componi interno**

  Determina la richiesta al chiamante di inserire il numero di telefono dell'utente desiderato tramite la tastiera.

  Se il chiamante compone il numero di telefono di un utente virtuale, gli viene richiesto di inserire il numero di un altro utente. Successivamente viene stabilita una connessione. Se l'utente desiderato non risponde, la chiamata viene accettata dalla sua casella vocale.

  Dopo questo oggetto CCV non può essere inserito alcun altro oggetto CCV.

  Proprietà:

  – **Metodo**: scelta tra **Trasferisci a interno** o **Registra nella casella postale**.

    In base al metodo selezionato viene realizzata una connessione all'utente desiderato o alla relativa casella vocale. Sono supportati solo gli utenti interni della rete per i quali è registrato il numero di telefono nella rubrica interna.

- **Imposta lingua**

  Determina la selezione della lingua per i singoli messaggi predefiniti, in base al numero di telefono del chiamante. Occorre notare che vengono considerati solo gli annunci predefiniti (annunci di sistema) e nessun annuncio personale.

  È ad esempio possibile impostare il sistema in modo che per un numero di telefono con il prefisso internazionale +49 venga riprodotto un annuncio

in tedesco, mentre per un numero con il prefisso internazionale +39 un messaggio in italiano.

Proprietà:

– **Lingua predefinita**: elenco a discesa per la scelta di una lingua.

  La scelta qui selezionata viene applicata a tutti i numeri di telefono per i quali non è stata definita una propria lingua.
– **Motivo**: indicazione del numero di telefono che deve essere assegnato a una lingua specifica.

  È possibile utilizzare i seguenti segnaposto: * = qualsiasi cifra, ? = qualsiasi cifra.
– **Lingua**: elenco a discesa per la scelta della lingua che deve essere assegnata ai numeri di telefono (**Motivo**).

È possibile assegnare a una lingua tanti numeri di telefono quanti lo si desidera (**Motivo**).

• **Istradamento CLI**

Determina l'inoltro di una chiamata a uno o più oggetti CCV consecutivi mediante il numero di telefono del chiamante.

È ad esempio possibile impostare il sistema in modo che per un numero di telefono con il prefisso internazionale +49 venga riprodotto un annuncio in tedesco (oggetto CCV **Riproduci messaggio**) e successivamente venga inoltrata la chiamata a un interno (oggetto CCV **Trasferimento a passaggio singolo**). È inoltre possibile utilizzare il prefisso interurbano (es. 089 per Monaco di Baviera).

Nel contesto di UC Suite e CLI Routing, gli utenti devono considerare scenari specifici, come le chiamate in entrata da MS Teams Native SIP Trunk. Se si intende inviare verso OpenScape Business i numeri dei chiamanti in formato canonico, compreso il prefisso internazionale, è necessario stabilire regole CLI Routing aggiuntive.

Ad esempio, se i chiamanti da MS Teams hanno numeri nel formato +49777555XXXX, e 777555 è la parte comune di questi numeri, gli utenti

devono creare regole di routing CLI pertinenti che incorporino questa parte comune (777555).

Proprietà:

– **Predefinito**: elenco a discesa per la scelta dell'oggetto CCV.

  L'oggetto CCV qui selezionato viene utilizzato per tutti i numeri di telefono per cui non è definita alcuna destinazione.
– **Motivo**: indicazione del numero di telefono a cui occorre assegnare uno specifico oggetto CCV.

  È possibile utilizzare i seguenti segnaposto: * = qualsiasi cifra, ? = qualsiasi cifra.
– **Descrizione**

  Fornitura di una spiegazione.

  Per il **Motivo** +49 (=prefisso internazionale tedesco) è ad esempio possibile inserire Germania.

  Il testo qui inserito viene visualizzato nell'Editor regole.
– **Destinazione**: elenco a discesa per la selezione dell'oggetto CCV che dovrà essere assegnato al numero di telefono (**Motivo**) come destinazione.

A un oggetto CCV è possibile assegnare come destinazione tanti numeri di telefono quanti lo si desidera (**Motivo**).

• **Diramare se variabile**

Determina l'inoltro di una chiamata a uno o più oggetti CCV consecutivi mediante una condizione.

È ad esempio possibile definire se per i chiamanti deve essere riprodotto un annuncio ("si prega di richiamare più tardi..."), non appena in una coda d'attesa sono presenti più di 20 chiamate.

Proprietà:

– **Variabile**: selezione di **Chiamate** o **Agenti disponibili**.

  A seconda delle variabili selezionate, il numero di chiamate in attesa in una coda o il numero di agenti disponibili (compresi gli agenti impegnati in post-elaborazioni) viene usato come condizione predefinita. Nel relativo elenco a discesa, selezionare la condizione (**minore di** ,

maggiore di , **minore o uguale a**, **maggiore o uguale a**, **uguale a**) e nel relativo campo di input, inserire il valore comparativo.

– **Condizione soddisfatta**: elenco a discesa per la selezione dell'oggetto CCV che deve essere utilizzato come destinazione se la condizione viene soddisfatta.
– **Condizione non soddisfatta**: elenco a discesa per la selezione dell'oggetto CCV che deve essere utilizzato come destinazione se la condizione non viene soddisfatta.

Il numero di agenti disponibili in una coda d'attesa dipende dai seguenti cambiamenti di stato degli agenti:

– Accesso di un agente alla coda di attesa tramite "Connetti/Login": --> +1
– Disconnessione di un agente dalla coda di attesa tramite "Disconnetti/Logout": --> -1
– Agente allo stato "Pausa": --> -1
– Agente allo stato "Disponibile dopo la pausa": --> +1

Il numero di agenti disponibili in una coda d'attesa **non** dipende dai seguenti cambiamenti di stato degli agenti:

– Agente allo stato "Squilla"
– Agente allo stato "Conversazione"
– Agente allo stato "Post-elaborazione"
– Agente allo stato "Chiamata persa"
– Agente allo stato "Scaduta"

• **Diramare se dati**

Determina l'inoltro di una chiamata a uno o più oggetti CCV consecutivi mediante una condizione.

È ad esempio possibile definire se per i chiamanti deve essere riprodotto un annuncio ("si prega di richiamare più tardi..."), non appena in una coda d'attesa sono presenti più di 20 chiamate.

Proprietà:

– **Variabile**: scelta di **LDAP data1 (xmpp)** o **LDAP data2 (cercapersone)**.

  L'interrogazione dei dati viene eseguita tramite LDAP o direttamente su un database con funzionalità LDAP o indirettamente tramite Directory Service (ODS) su un database SQL/ODBC. I risultati dell'interrogazione vengono assegnate tramite la mappatura campi LDAP di UC Suite ai criteri appropriati del Contact Center. Nel relativo elenco a discesa, selezionare la condizione (**minore di** , **maggiore di** , **minore o uguale a**, **maggiore o uguale a**, **uguale a**) e nel relativo campo di input, inserire il valore comparativo. È necessario mappare le parole chiave "cercapersone" e "info".
– **Timeout**: tempo in secondi prima che si verifichi un timeout.
– **Condizione timeout**: elenco a discesa per la selezione dell'oggetto CCV che deve essere utilizzato come destinazione quando si verifica un timeout.
– **Condizione soddisfatta**: elenco a discesa per la selezione dell'oggetto CCV che deve essere utilizzato come destinazione se la condizione viene soddisfatta.
– **Condizione non soddisfatta**: elenco a discesa per la selezione dell'oggetto CCV che deve essere utilizzato come destinazione se la condizione non viene soddisfatta.

– **Descrizione**: Fornitura di una spiegazione.

18.3.3 Elaborazione

Mediante l'uso dei motivi per l'elaborazione, è possibile assegnare alle chiamate in arrivo argomenti specifici (ad esempio ordine, reclamo, assistenza, ecc.). L'assegnazione a un'agente della fine della conversazione (entro il tempo di lavoro) tramite myAgent, selezionando il codice di elaborazione corrispondente.

I motivi per l'elaborazione possono essere definiti singolarmente per ogni coda di attesa.

Viene operata una distinzione tra

- Elaborazione semplice

  Per le code d'attesa con la modalità elaborazione "Elaborazione semplice", è possibile definire uno o più motivi per l'elaborazione.

  Esempio: Per una coda d'attesa vengono definiti i due motivi per l'elaborazione Problema hardware e Problema software. Durante il tempo di lavoro, un agente assegna a ogni chiamata uno di questi motivi per l'elaborazione. In questo modo è ad esempio possibile generare un rapporto che presenta un riepilogo di tutte le chiamate con l'argomento Problema hardware.

- Elaborazione multipla

  Per le code d'attesa con la modalità elaborazione "Elaborazione multipla", è possibile definire uno o più motivi per l'elaborazione e riunirli in gruppi o sottogruppi.

  Sotto ogni gruppo o sottogruppo (se presente) deve essere configurato almeno un elemento, per consentire all'agente di elaborare una chiamata. L'elaborazione di una chiamata non è possibile se un gruppo o un sottogruppo è vuoto. Questo vale solo per le code che hanno la configurazione Elaborazione multipla abilitata.

  Esempio: Per una coda d'attesa è stato definito un gruppo hardware con il motivo per l'elaborazione schede madri e alimentatori e un gruppo software con il motivo per l'elaborazione sistema operativo e driver. Durante il tempo di lavoro, un agente assegna a ogni chiamata uno di questi motivi per l'elaborazione. È quindi possibile ad esempio generare un rapporto con un riepilogo di tutte le chiamate per problemi hardware o anche solo per problemi hardware alla scheda madre.

18.3.4 Livello di servizio

Sulla base del livello di servizio, è possibile eseguire valutazioni sulla qualità di risposta in una coda d'attesa. Questo è possibile tramite il confronto dei tempi di attesa dei chiamanti in una coda d'attesa con i valori soglia che possono essere definiti singolarmente per ogni coda d'attesa.

I valori soglia per il grado di servizio (Grade of Service o GoS) possono essere liberamente definiti in base al tempo di attesa del chiamante nella coda d'attesa. Per di ogni chiamata alla rispettiva coda di attesa, al termine della chiamata

viene rilevato il grado di servizio e acquisito nella database. L'analisi del livello di servizio può essere eseguita dagli agenti con il livello di autorizzazione "Supervisore" o "Amministratore" tramite l'applicazione myAgent.

18.3.5 Display a parete

Tramite myAgent è possibile richiamare i dettagli della coda d'attesa. La visualizzazione contiene una tabella con le informazioni statistiche sulla coda di attesa in tempo reale per le ultime 24 ore. I dati possono essere visualizzati ad esempio su un grande monitor LCD o su un proiettore da parete.

Un agente con il livello di autorizzazione Agente riceve informazioni sulle code d'attesa a cui è assegnato. Un agente con il livello di autorizzazione Supervisore o Amministratore riceve informazioni su tutte le code.

Per la visualizzazione a parete, è necessario configurare un utente separato. A tale scopo è necessaria una licenza apparecchio (utente IP o utente TDM) e una licenza myAgent.

18.3.6 Richiamata agente

Se per un chiamante il tempo in coda d'attesa è eccessivo e se la relativa pianificazione contiene l'oggetto CCV **Registra richiamata**, questi ha la possibilità di chiedere di essere richiamato. La richiesta così generata mantiene la posizione del chiamante originale nella coda d'attesa e viene recapitata a un agente sotto forma di un messaggio vocale. Dopo l'ascolto del messaggio vocale, l'agente può richiamare il chiamante tramite una finestra popup.

Se per un chiamante viene definito un agente preferito, il sistema tenta innanzitutto di trasmettere le richieste di richiamata di tale chiamante all'agente preferito. Se l'agente preferito non è disponibile, la prenotazione di chiamata verrà inoltrata a uno qualsiasi degli agenti disponibili.

18.4 Trattamento VIP

Per ogni coda d'attesa è possibile definire in modo individuale se un chiamante specifico (o un chiamante corrispondente a un modello di numero telefonico configurabile) deve ricevere un trattamento preferenziale e quindi essere messo in connessione più rapidamente con l'agente disponibile.

Se tutti gli agenti di una coda di attesa sono occupati, i chiamanti VIP verranno connessi in modo prioritario al primo agente libero.

18.4.1 Priorità chiamante VIP

Sulla base della priorità chiamante VIP, è possibile definire in modo indipendente per ciascuna coda d'attesa se i chiamanti contenuti nell'Elenco chiamate VIP (clienti, ad esempio) devono essere trattati con priorità.

I valori per la Priorità chiamante VIP possono essere liberamente definiti in base al tempo di attesa del chiamante nella coda d'attesa. In questo modo, si determina il livello di priorità di chiamanti VIP rispetto ai chiamanti normali.

Se un chiamante VIP attiva una richiamata agente (registrazione di un messaggio vocale con richiesta di richiamata), la richiamata agente prende il posto del chiamante VIP nella coda d'attesa. Non viene quindi trasmessa la priorità chiamante VIP.

I chiamanti VIP devono essere registrati nell'elenco chiamate VIP (vedere Elenco chiamate VIP).

18.4.2 Elenco chiamate VIP

I chiamanti (rubrica esterna) già registrati nel sistema di comunicazione possono essere inseriti nell'Elenco chiamate VIP. È possibile effettuare selezioni multiple o utilizzare la funzione "**Seleziona tutto**". Oltre a ciò, è possibile l'inserimento di tipi di numeri di telefono. I tipi di numeri di telefono sono costituiti da una sequenza specifica di cifre e caratteri jolly (segnaposto). In questo modo è ad esempio possibile inserire tutti i collaboratori di un'azienda nell'elenco chiamate VIP.

Per ogni coda d'attesa, tramite la priorità chiamante VIP, è possibile definire se

- i chiamanti contenuti nell'elenco chiamate VIP
- i chiamanti che corrispondono al tipo di numero di telefono contenuto in un elenco chiamate VIP riceveranno un trattamento preferenziale.

Non è possibile l'inserimento di tipi di numeri di telefono in formato canonico. Non è consentito neanche l'uso di prefissi internazionali abbreviati (ad esempio +49 anziché 0049). I tipi di numeri di telefono sono sempre privi di codice di linea urbana.

Esempi di tipi di numero di telefono:

- 089 7577* (089 = Prefisso interurbano di Monaco, 7577 = numero di sistema di un'azienda, * = carattere jolly per qualsiasi cifra). Digitando questo tipo di numero di telefono nell'elenco chiamate VIP tutti i chiamanti di Monaco il cui numero inizia con 7577 vengono trattati in modo preferenziale.
- 0039* (0039 = prefisso internazionale italiano, * = carattere jolly per qualsiasi cifra). Digitando questo tipo di numero di telefono nell'elenco chiamate VIP tutti i chiamanti dall'Italia vengono trattati in modo preferenziale.

I seguenti caratteri possono essere utilizzati in un tipo di numero di telefono come carattere jolly (segnaposto):

- * = carattere jolly per qualsiasi numero
- ? = carattere jolly per qualsiasi cifra

18.5 Soluzione secondaria (soluzione fallback)

In caso di mancata disponibilità del Contact Center in seguito a problemi (crash di sistema, problemi di connessione e simili), il sistema di comunicazione commuta automaticamente sul servizio "Uniform Call Distribution, UCD". Questo servizio funge da soluzione secondaria, sostitutiva del Contact Center.

In caso di interruzione del servizio del Contact Center, le chiamate in arrivo verranno distribuite secondo la soluzione secondaria. Non è possibile distribuire fax ed e-mail.

In base alle esigenze, è possibile configurare una delle soluzioni secondarie descritte di seguito.

Soluzione secondaria standard

In questo caso la soluzione secondaria si basa sugli ID UCD (ID Agente) degli agenti:

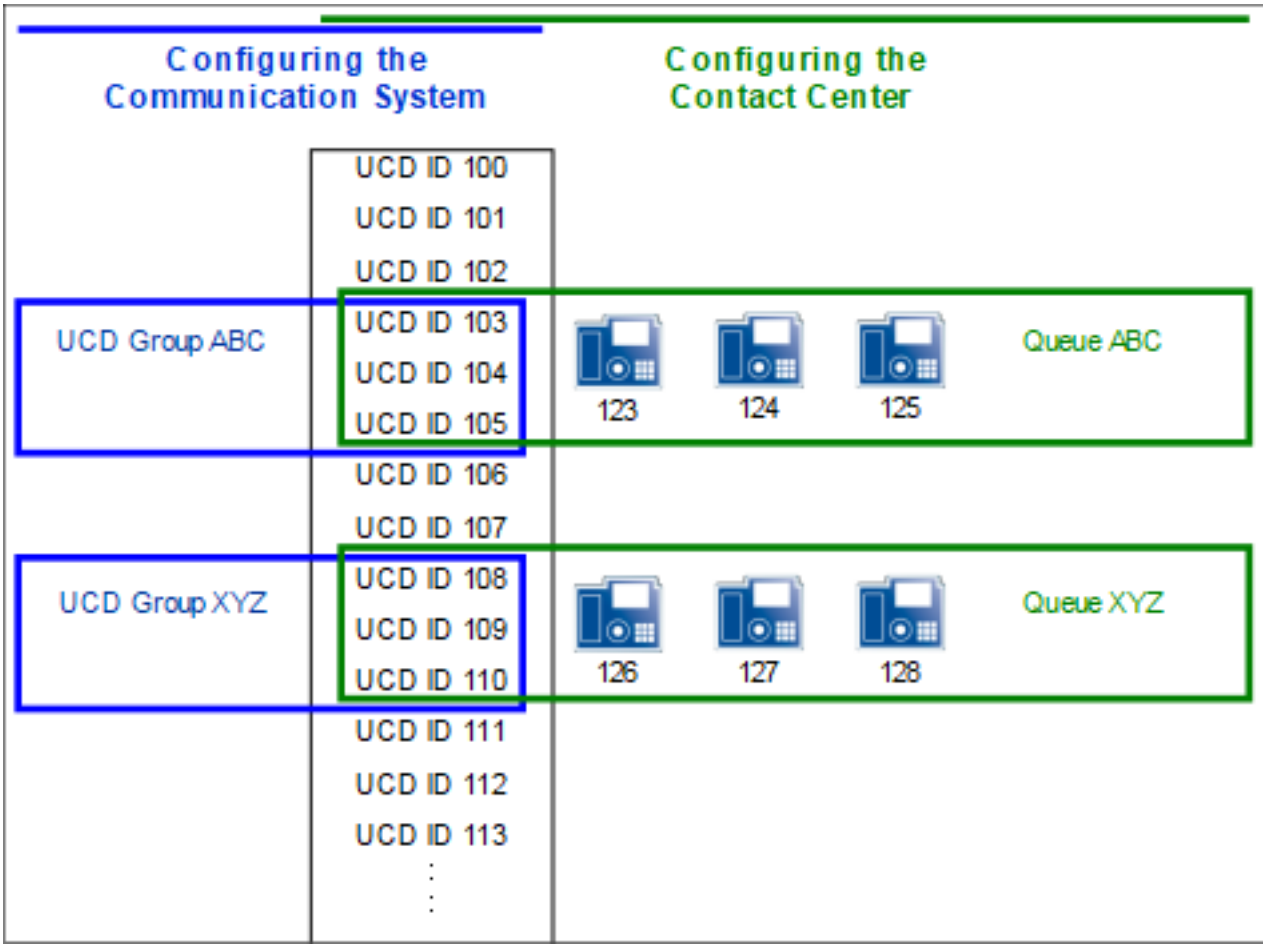
- Ai gruppi UCD del sistema di comunicazione vengono assegnati degli agenti in base agli ID UCD. L'ID UCD definisce a quale gruppo UCD apparterrà l'agente in caso di interruzione del servizio del Contact Center.

Per un corretto funzionamento della soluzione secondaria standard, a ogni coda di attesa devono essere assegnati gli agenti Contact Center con gli ID UCD assegnati ai corrispondenti gruppi UCD.

In caso di interruzione del servizio del Contact Center, le chiamate in arrivo tramite diversi gruppi UCD verranno distribuite agli agenti registrati.

Esempio:

- Al gruppo UCD ABC vengono assegnati gli ID UCD 103, 104 e 105. Al gruppo UCD XYZ vengono assegnati gli ID UCD 108, 109 e 110.
- Le stazioni 123, 124 e 125 sono configurate come agenti con gli ID UCD 103, 104 e 105. Le stazioni 126, 127 e 128 sono configurate come agenti con gli ID UCD 108, 109 e 110.
- Nell'assegnazione degli agenti alle code d'attesa gli utenti 123, 124 e 125 devono essere assegnati alla coda di attesa ABC e gli utenti 126, 127 e 128 alla coda di attesa XYZ.



Soluzione secondaria di base

In questo caso, tutti gli agenti del Contact Center vengono assegnati solo a un gruppo UCD di supporto in base al loro ID UCD. Grazie all'assegnazione ai rispetti agenti, questi ID UCD vengono poi utilizzati anche nelle code d'attesa del Contact Center. Ciò garantisce che in caso di interruzione del servizio del Contact Center gli agenti non debbano registrarsi di nuovo manualmente con un altro ID sul loro telefono. Per tutti i gruppi UCD del sistema di comunicazione, questo gruppo UCD di supporto viene configurato come destinazione di inoltro.

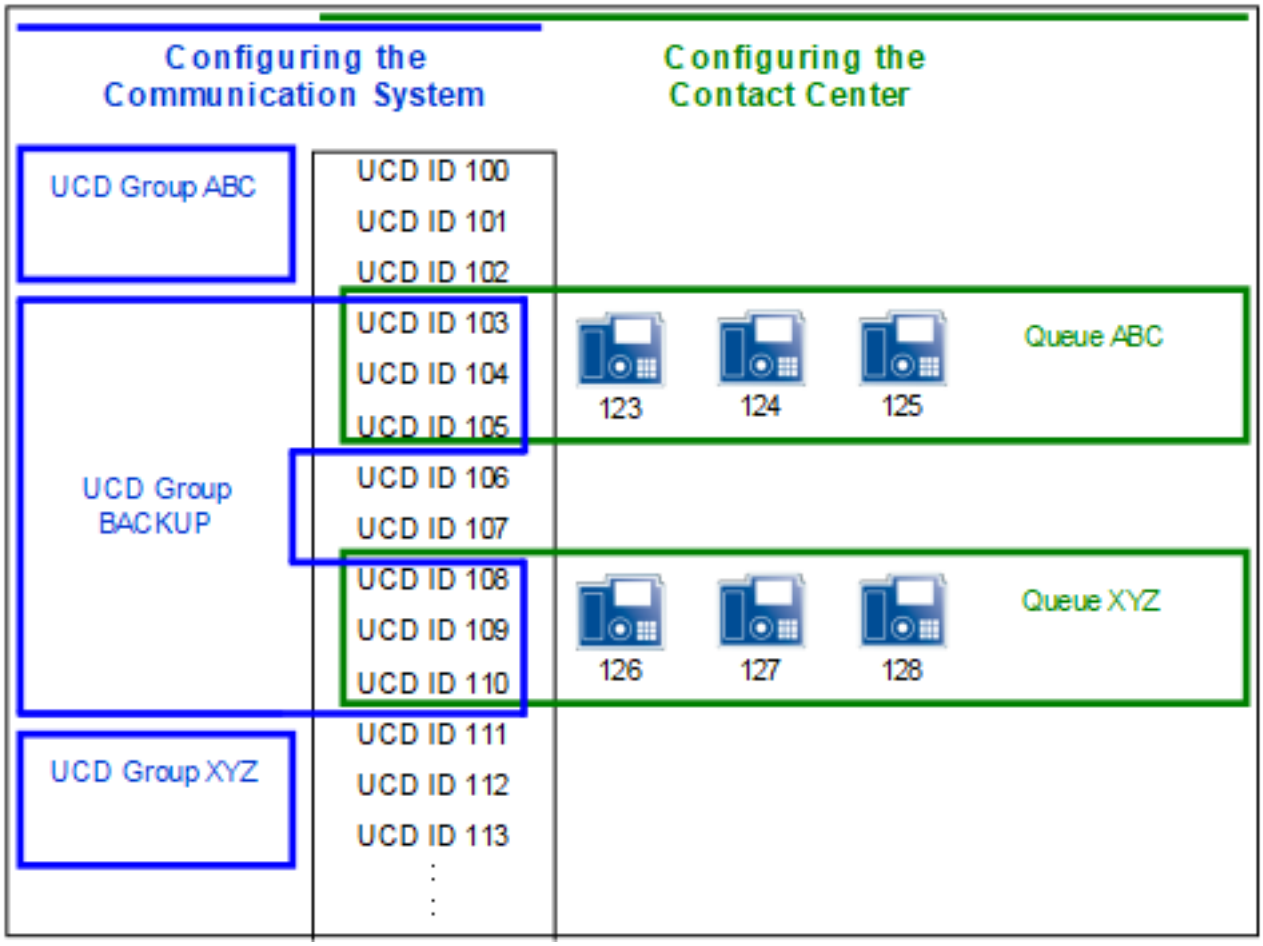
Nota: Anche il gruppo UCD di backup configurato deve essere configurato come gruppo nel Contact Center. In questo modo ci si assicura che venga monitorato anche questo gruppo.

In caso di interruzione del servizio del Contact Center, le chiamate in arrivo verranno distribuiti a tutti gli agenti del gruppo UCD di supporto.

Esempio:

- Al gruppo UCD ABC e XYZ non sono stati assegnati ID UCD. Al gruppo UCD BACKUP vengono assegnati gli ID UCD da 103 a 105 e da 108 a 110.
- Le stazioni 123, 124 e 125 sono configurate come agenti con gli ID UCD 103, 104 e 105. Le stazioni 126, 127 e 128 sono configurate come agenti con gli ID UCD 108, 109 e 110.

- Nell'assegnazione degli agenti alle code d'attesa gli utenti 123, 124 e 125 vengono essere assegnati alla coda di attesa ABC e gli utenti 126, 127 e 128 alla coda di attesa XYZ.



Soluzione secondaria personalizzata

In questo caso viene riprodotta la configurazione del Contact Center personalizzata con più gruppi UCD.

In caso di interruzione del servizio del Contact Center ne verrà quindi riprodotto il comportamento tramite la soluzione secondaria.

Per informazioni sulla configurazione della distribuzione delle chiamate tramite il servizio "Uniform Call Distribution, UCD" del sistema di comunicazione consultare UCD (Uniform Call Distribution).

Un importante vantaggio della soluzione secondaria personalizzata è la possibilità di riprodurre esattamente lo schema del Contact Center su tale soluzione.

Lo svantaggio della soluzione secondaria personalizzata è l'elevata complessità della configurazione. Oltre a ciò, tutte le modifiche alla configurazione del Contact Center dovranno essere riprodotte anche nella soluzione secondaria, per garantire un comportamento simile in termini di distribuzione delle chiamate.

Un importante vantaggio della soluzione secondaria standard e di base è la semplicità della configurazione.

18.6 Configurazione del Contact Center

Quando si configura il Contact Center, occorre innanzitutto definire i gruppi UCD. Le code d'attesa del Contact Center sono gruppi di lavoro basati sui gruppi UCD del sistema di comunicazione. Successivamente è possibile passare alla configurazione del Contact Center vero e proprio (pianificazioni, code d'attesa, ecc.).

Prima di configurare il Contact Center, i processi per la distribuzione delle chiamate (sia per le chiamate normali che per quelle di emergenza) devono venire concordati con il cliente.

Suggerimento: La configurazione del Contact Center deve essere eseguita solo una volta conclusa la configurazione del sistema di comunicazione e della UC Suite.

Se vengono eseguite modifiche alla configurazione di gruppi UCD, è necessario successivamente riavviare la UC Suite tramite il Centro assistenza di WBM.

Per l'uso del Contact Center, sono necessarie le seguenti licenze:

- Un numero di licenze corrispondente al numero degli agenti (myAgent)
- Licenza fax Contact Center (per la ricezione e l'invio di fax), se richiesto
- Licenza e-mail Contact Center (per la ricezione e l'invio di e-mail), se richiesto

18.6.1 Esempio per la configurazione di un Contact Center

Illustreremo con un esempio il principio su cui si basa il Contact Center con OpenScape Business. La struttura e la configurazione dell'esempio sono basate su uno scenario fittizio relativo a un sistema installato presso un cliente, comprendente le funzioni standard del Contact Center.

scenario di esempio per un Contact Center

La Società XYZ utilizza un Contact Center con due i seguenti numeri telefonici (code d'attesa):

- Numero di telefono 440 per il Servizio Assistenza Tecnica
- Numero di telefono 444 per l'Area Vendite
- Numero di telefono 456 per le chiamate gratuite (Hotline). Viene trasmesso un annuncio e i chiamanti possono mettersi in contatto con il Servizio Assistenza Tecnica o l'Area Vendite digitando la cifra corrispondente.

Il Contact Center è formato da sei collaboratori (agenti); tre sono addetti al Servizio Assistenza Tecnica e tre all'Area Vendite.

Le code d'attesa per le aree Servizio e Vendite devono essere direttamente raggiungibili negli orari di ufficio (dalle 09.00 alle 17.00). Entrambe le code d'attesa dispongono di una casella fax e di un indirizzo e-mail.

Se tutti gli agenti sono impegnati in conversazioni o non sono disponibili, il chiamante sarà informato e sentirà musica d'attesa. Se dopo un tempo prestabilito nessun agente è in grado di rispondere al chiamante, quest'ultimo potrà lasciare una richiesta di richiamata o digitare cifre specifiche per essere

messo in comunicazione con il posto operatore. Se non viene digitata alcuna cifra, il chiamante verrà automaticamente riportato in coda d'attesa.

Al di fuori dell'orario di ufficio, verrà riprodotta una registrazione con la possibilità di lasciare una richiesta di richiamata (richiamata agente).

Nota: È possibile riprodurre gli annunci solo tramite linee. Per riprodurre l'annuncio, la chiamata deve provenire da una linea o il chiamante deve essere monitorato da OpenScape Contact Center.

Durante la pausa pranzo, dalle 12.00 alle 13.00, per le code d'attesa dell'area Servizio e Vendite verrà riprodotta una registrazione con la possibilità di lasciare una richiesta di richiamata.

Soluzione secondaria (soluzione fallback) tramite il gruppo UCD di supporto: In caso di mancata disponibilità del Contact Center in seguito a problemi (crash di sistema, problemi di connessione e simili), si deve passare automaticamente al servizio "Uniform Call Distribution, UCD" del sistema di comunicazione. A tal scopo tutti gli agenti del Contact Center devono essere assegnati a un singolo gruppo UCD di supporto. Per tutti i gruppi UCD del sistema di comunicazione, questo gruppo UCD di supporto deve essere configurato come destinazione di inoltro. In caso di interruzione del servizio del Contact Center, le chiamate in arrivo verranno distribuite agli agenti del gruppo UCD di supporto.

Configurazione di scenari di esempio

Per lo scenario di esempio si dovranno eseguire le seguenti attività:

- Configurazione di gruppi UCD

  Le code d'attesa del Contact Center sono gruppi di lavoro basati sui gruppi UCD del sistema di comunicazione. Prima di procedere all'effettiva configurazione del Contact Center, è necessario definire i gruppi UCD.

  Per il presente esempio sul Contact Center della società XYZ devono essere configurati tre gruppi UCD (Service, Sales, Hotline).
- Configurazione della soluzione secondaria (soluzione fallback)

  Per il presente esempio si dovrà configurare un gruppo UCD di supporto e definirlo come destinazione di inoltro di tutti i gruppi UCD del sistema di comunicazione.
- Configurazione di utenti come agenti

  Per il presente esempio si dovranno configurare sei utenti come agenti.
- Registrazione di annunci personalizzati

  Per il presente esempio si dovranno registrare alcuni annunci. Può trattarsi, ad esempio, di annunci per quando nessun agente è disponibile, oppure per informare un chiamante sulle opzioni possibili (**Elabora digitazione**).
- Caricamento di annunci personalizzati

  Per il presente esempio gli annunci registrati dovranno essere caricati nel sistema di comunicazione.

- Definizione di pianificazioni

  Per ogni periodo di una pianificazione viene definito tramite regole (Call Control Vector CCV) come le chiamate in arrivo verranno gestite in giorni o orari specifici.

  Per il presente esempio occorre definire una pianificazione (Standard Schedule XYZ) con una regola per gli orari al di fuori dell'orario di ufficio ed eccezioni per gli orari di ufficio e la pausa pranzo. Inoltre occorre definire una seconda pianificazione (Standard Schedule Hotline) con una regola per chiamate gratuite (Hotline).

Pianificazione	Regola (CCV)	
Standard Schedule XYZ	Fuori sede	Orari al di fuori dell'orario di ufficio
	Open	Orari di ufficio dalle 08.00 alle 11.59 = Open1
		Orari di ufficio dalle 13.00 alle 17.00 = Open2
	Pausa pranzo	Pausa pranzo dalle 12.00 alle 12.59
Standard Schedule Hotline	Hotline	24 ore

- Aggiunta di tre code d'attesa

  Per il presente esempio occorre configurare una coda di attesa per il Servizio Assistenza Tecnica e una per l'Area Vendite. Un'altra coda di attesa (Hotline) deve essere configurata per le chiamate gratuite.
- Assegnazione degli agenti alle code d'attesa

  Per il presente esempio devono essere assegnati tre agenti alla coda di attesa Servizio e tre agenti alla coda di attesa Vendite.

Per informazioni sulla configurazione di tutte le funzioni del Contact Center, consultare Procedura di configurazione .

18.6.1.1 Come configurare i gruppi UCD per il Contact Center di esempio

Con la procedura guidata **Distribuzione delle chiamate** definire i tre gruppi UCD (Service, Sales, Hotline) con i numeri di telefono 440, 444 e 456 per il Contact Center di esempio della società XYZ.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **UCD**. Viene visualizzata una lista di tutti i gruppi UCD disponibili.

4) Per configurare un gruppo UCD, fare clic su **Modifica** nella riga del gruppo UCD desiderato.
5) Nel campo **Numero di telefono** indicare il numero di telefono `440` del gruppo UCD Service.
6) Nel campo **Interno** indicare il numero di interno `440` del gruppo UCD Service.
7) Nel campo **Nome** indicare il nome `Service`.
8) Fare clic su **OK & Avanti**. Viene visualizzata la finestra **Assegnazione agenti UCD**.
9) Fare clic su **OK & Avanti**, in quanto per il gruppo UCD Service non è possibile assegnare un ID UCD.

   Poiché per il Contact Center di esempio della società XYZ occorre configurare una soluzione secondaria con un gruppo UCD di supporto, ai tre gruppi UCD Service, Sales e Hotline non può essere assegnato alcun ID UCD.
10) Fare clic su **OK & Avanti**. Viene visualizzata la finestra **Modifica annuncio/overflow**.
11) Fare clic su **OK**, in quanto i parametri visualizzati non sono rilevanti per la configurazione del gruppo UCD.
12) Ripetere i passi da 4 fino a 11 per il gruppo UCD Sales assegnando il numero di telefono 444 e per il gruppo UCD Hotline assegnando il numero di telefono 456.
13) Fare clic su **OK & Avanti**, quindi su **Fine**.

18.6.1.2 Come configurare la soluzione secondaria (soluzione fallback) per il Contact Center di esempio

La procedura guidata **UCD** consente di configurare il gruppo UCD di supporto assegnando il numero di telefono 400 per il Contact Center di esempio della società XYZ. Per l'esempio vengono utilizzati gli ID UCD da 101 fino a 106. Oltre a ciò, è necessario definire il gruppo UCD di supporto come destinazione di inoltro di tutti i gruppi UCD del Contact Center di esempio della società XYZ.

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

Occorre configurare il gruppo UCD di supporto con il numero di telefono 400 nelle code d'attesa del Contact Center di UC Suite.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **UCD**. Viene visualizzata una lista di tutti i gruppi UCD disponibili.
4) Per configurare un gruppo UCD, fare clic su **Modifica** nella riga del gruppo UCD desiderato.
5) Nel campo **Numero di telefono**, indicare il numero di telefono `400` del gruppo UCD Backup.

6) Nel campo `Interno` indicare il numero di interno **400** del gruppo UCD di supporto.
7) Nel campo **Nome** indicare il nome `Backup`.
8) Fare clic su **OK & Avanti**. Viene visualizzata la finestra **Assegnazione agenti UCD**.
9) Selezionare gli ID degli agenti UCD desiderati in **Scelta** e assegnarli al gruppo UCD di supporto, facendo clic su **Aggiungi**.
10) Fare clic su **OK & Avanti**. Viene visualizzata la finestra **Assegna a utente**.
11) Assegnare a tutti gli ID agente UCD l'utente desiderato.
12) Fare clic su **OK & Avanti**. Viene visualizzata la finestra **Modifica annuncio/overflow**.
13) Fare clic su **OK**, in quanto i parametri visualizzati non sono rilevanti per la configurazione del gruppo UCD di supporto.
14) Per configurare il nuovo gruppo UCD di supporto come destinazione di inoltro, nella riga del gruppo UCD Service, fare clic su **Modifica**.
15) Fare clic su **OK & Avanti** finché non viene visualizzata la finestra **Modifica annuncio/overflow**.
16) Nell'elenco a discesa **Destinazione di overflow**, selezionare il gruppo UCD di supporto con il numero di telefono 400 come destinazione di inoltro.
17) Fare clic su **OK**.
18) Ripetere i passi da 14 a 17, per configurare il nuovo gruppo UCD di supporto come destinazione di inoltro dei gruppi UCD Sales e Hotline.
19) Fare clic su **OK & Avanti**, quindi su **Fine**.

18.6.1.3 Come configurare un utente come agente per il Contact Center di esempio

Con la procedura guidata **Rubrica utente** è possibile configurare gli utenti come agenti per il Contact Center di esempio della società XYZ. Per l'esempio vengono configurati come agenti gli utenti con i numeri di telefono da 101 fino a 106. Gli utenti con i numeri di telefono 101 e 104 otterranno il livello di autorizzazione **Supervisore**, gli altri il livello **Agente**.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Rubrica utente**.
4) Selezionare l'utente con l'**Interno** 101 e fare clic su **Modifica**.
5) Nella struttura dei menu fare clic su **Dati personali** > **Livello utente**.
6) Selezionare la casella di controllo **Agente sempre disponibile**. L'agente rimane disponibile per chiamate, fax e e-mail, anche se non ha risposto a una chiamata, fax o e-mail.
7) Nell'elenco a discesa **Livello**, selezionare il livello di autorizzazione **Supervisore**.
8) Fare clic su **Salva**.

9) Ripetere i passi da 4 fino a 8 per configurare come agenti gli utenti con i numeri di telefono da 102 fino a 106.

18.6.1.4 Come registrare annunci per il Contact Center di esempio

You can record announcements for the sample Contact Center of company XYZ with the **Recorder** wizard. Un annuncio è necessario anche nel caso in cui nessuno degli agenti sia raggiungibile.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Click on **Edit** to start the **File Upload** wizard.
4) Enable the **Recorder** radio button
5) Select the station number of the phone to be used for recording from the **Extension** drop-down list.
6) Click on **Make a Call**. Il numero composto viene chiamato.
7) Pick up the handset and enter the name for your announcement in the **Filename** field.
8) Click on **Record** to start recording the announcement.
9) Click on **Stop** as soon as you have finished recording the entire announcement.
10) If you want to listen to your new announcement, click on **Play**.
11) Click on **Close** to save the announcement.

Suggerimento:

Dopo la registrazione e il salvataggio non è più possibile cancellare un annuncio. Tuttavia, utilizzando lo stesso nome file, è possibile sovrascriverlo. For example, saving an audio file named `announcement1.wav` would overwrite any existing `announcement1.wav` file.

---

12) Repeat steps 3 through 10 to record further announcements for the sample Contact Center of company XYZ.

18.6.1.5 Come caricare annunci per il Contact Center di esempio

You can upload announcements for the sample Contact Center of company XYZ with the **File Upload** wizard.

Prerequisiti

È disponibile un file audio in formato wav con le seguenti proprietà: mono, velocità campione audio 8 kHz, dimensioni campione audio 16 bit, dimensione del frame 2.

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Click on **Edit** to start the **File Upload** wizard.
4) Click on the **Audio Files Manager** tab.
5) Select the destination **Auto Attendant** in the **Upload Destination** drop-down list.
6) Select the **Uploader** radio button and click on **Choose File**, navigate to the desired storage location of the audio file and click on **Open**.
7) Click on **Upload**.

Suggerimento:

Dopo il caricamento del file audio, non sarà più possibile eliminarlo. Tuttavia, utilizzando lo stesso nome del file audio caricato, è possibile sovrascriverlo. For example, uploading an audio file named `announcement1.wav` would overwrite any existing `announcement1.wav` file.

---

8) Repeat steps 4 through 7 to load further announcements for the sample Contact Center of company XYZ.

18.6.1.6 Come aggiungere una pianificazione XYZ per il Contact Center di esempio

Con la procedura guidata **Contact Center** è possibile definire la pianificazione con regole per gli orari di ufficio e della pausa per il Contact Center di esempio della società XYZ. A tal scopo deve essere definita una pianificazione (Standard Schedule XYZ) con una regola per gli orari al di fuori dell'orario di ufficio (Out Of The Office) ed eccezioni per gli orari di ufficio (dalle 08.00 alle 11.59 = Open1, dalle 13.00 alle 17.00 = Open2) e per la pausa pranzo (dalle 12.00 alle 12.59 = Lunch Break).

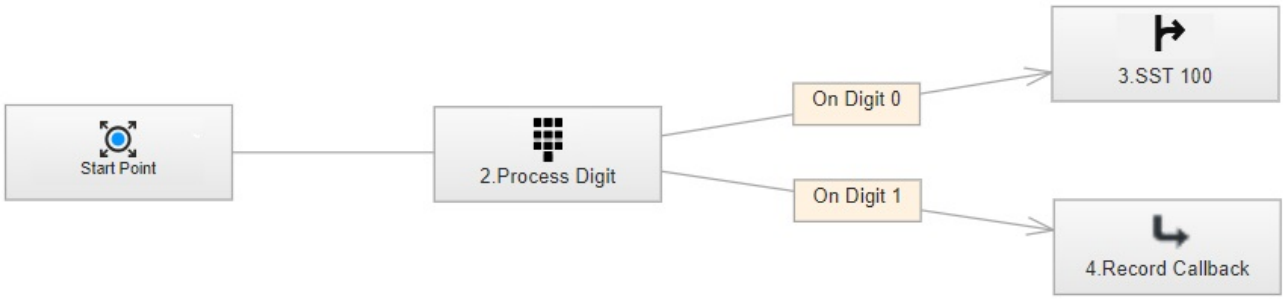
Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Pianificazione**. Vengono visualizzate tutte le pianificazioni disponibili.
5) Fare clic su **Aggiungi**.
6) Fare clic su **Aggiungi** nell'area **Pianificazione**.

7) Definire la regola illustrata per gli orari al di fuori dell'orario di ufficio.



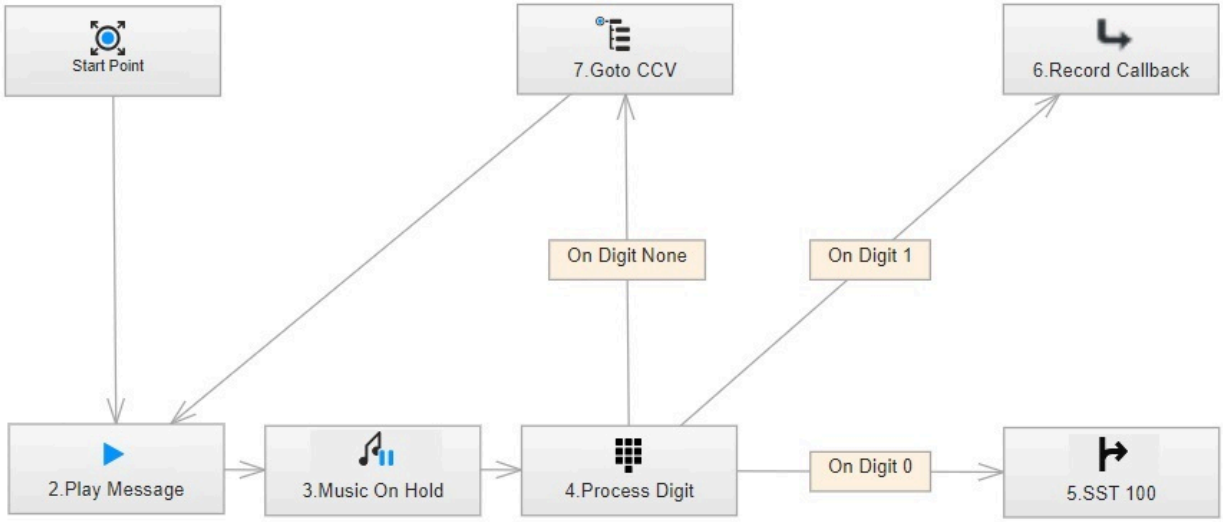
Nell'elenco Strumenti CCV, fare clic su uno degli oggetti CCV contenuti nella regola mostrata e trascinarlo nell'Editor regole. Si aprirà la finestra dell'oggetto CCV in cui inserire le proprietà indicate di seguito. Una volta terminato, confermare facendo clic su **Salva**. Ripetere la procedura per tutti gli oggetti CCV. Collegare due oggetti CCV, facendo clic col pulsante destro del mouse sul primo dei due. Dal menu a tendina **Link To**, selezionare il secondo dei due oggetti CCV collegati. Ripetere la procedura per tutti gli altri oggetti CCV da collegare.

Proprietà		Valore
1° oggetto CCV: **Elabora digitazione**		
	Lista di riproduzione	File audio in formato wav
	Timeout digitazione	5
	Descrizione	Annuncio: "Premere 0 per ...; Premere 1 per ...
2ª oggetto CCV: **Trasferimento a passaggio singolo**		
	Interno di destinazione	100
	Descrizione	Procedi alla console posto operatore
	Elabora dopo digitazione	0
3°oggetto CCV: **Registra richiamata**		
	Tipo	Richiamata automatica senza limitazioni
	Lunghezza massima messaggi (sec.)	20
	Descrizione	Richiesta di richiamata (richiamata agente)
	Elabora dopo digitazione	1

Fare clic su **Salva ...**. Inserire `Orario lavorativo` come **Nome CCV** per la regola, quindi fare clic su **Salva**. Se la nuova regola è errata, non sarà possibile salvarla. Gli oggetti CCV errati vengono contrassegnati in rosso nell'Editor regole. Chiudere la finestra che conferma il salvataggio della regola.

Dall'elenco a discesa **CCV predefinito**, scegliere la regola `Out Of The Office`.

8) Nel campo **Nome pianificazione** indicare il nome `Standard Schedule XYZ`.
9) Fare clic su **Salva**.
10) Fare clic su **Aggiungi** nell'area **Pianificazione**.
11) Definire la regola illustrata per l'orario di ufficio.



Nell'elenco Strumenti CCV, fare clic su uno degli oggetti CCV contenuti nella regola mostrata e trascinarlo nell'Editor regole. Si aprirà la finestra dell'oggetto CCV in cui inserire le proprietà indicate di seguito. Una volta terminato, confermare facendo clic su **Salva**. Ripetere la procedura per tutti gli oggetti CCV. Collegare due oggetti CCV, facendo clic col pulsante destro del mouse sul primo dei due. Dal menu a tendina **Link To**, selezionare il secondo dei due oggetti CCV collegati. Ripetere la procedura per tutti gli altri oggetti CCV da collegare.

Proprietà		Valore
1° oggetto CCV: **Riproduci messaggio**		
	Nome file	File audio in formato wav
	Interrompi digitazione	5
	Descrizione	Annuncio: Agenti non disponibili
2ª oggetto CCV: **Musica su Attesa**		
	Valore ora	30
	Descrizione	Musica su attesa per 30 secondi
3° oggetto CCV: **Elabora digitazione**		
	Lista di riproduzione	File audio in formato wav
	Timeout digitazione	5
	Descrizione	Annuncio: "Premere 0 per ...; Premere 1 per ...
4° oggetto CCV **Trasferimento a passaggio singolo**		

Proprietà		Valore
	Interno di destinazione	100
	Descrizione	Procedi alla console posto operatore
	Elabora dopo digitazione	0
5° oggetto CCV: **Registra richiamata**		
	Tipo	Richiamata automatica senza limitazioni
	Lunghezza massima messaggi (sec.)	20
	Descrizione	Richiesta di richiamata (richiamata agente)
	Elabora dopo digitazione	1
6ª oggetto CCV: **Vai a CCV**		
	CCV di destinazione	1. Riproduci messaggio
	Descrizione	Torna all'annuncio

Fare clic su **Salva ...**. Inserire `Open` come **Nome CCV** per la nuova regola, quindi fare clic su **Salva**. Chiudere la finestra che conferma il salvataggio della regola.

Nell'elenco a discesa per l'eccezione Open1, selezionare la regola `Open`.

12) Nel riquadro **Eccezioni**, fare clic su **Aggiungi** per definire la prima eccezione relativa agli orari di ufficio.

13) Nel campo `Descrizione`, inserire **Open1**.

14) Definire l'orario di validità di questa eccezione Open1:

Selezionare il pulsante di opzione **Entro l'intervallo di ore**. Nel menu a discesa `Ora inizio` selezionare l'ora iniziale **08:00** e in `Ora fine` l'ora finale **11:59** dell'intervallo temporale.

Nella finestra **Seleziona i giorni**, selezionare i giorni della settimana in cui dovrà essere applicata la regola. Fare quindi clic su **Salva**.

15) Nel riquadro **Eccezioni**, fare clic su **Aggiungi** per definire la seconda eccezione relativa agli orari di ufficio.

16) Nel campo **Descrizione**, inserire `Open2`.

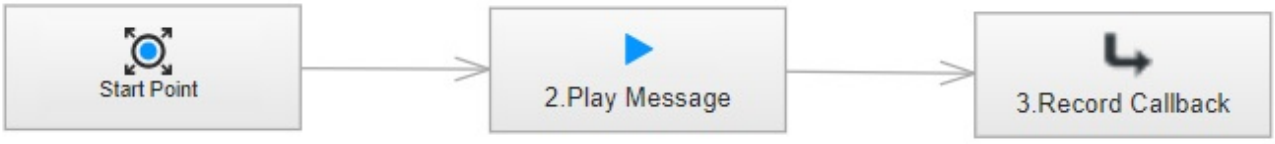
17) Nell'elenco a discesa per l'eccezione Open2, selezionare la regola `Open`.

18) Definire l'orario di validità di questa eccezione Open2:

Nell'elenco a discesa **Tipo**, selezionare l'opzione **Entro l'intervallo di ore**. Nel menu a discesa `Ora inizio` selezionare l'ora iniziale **13:00** e in `Ora fine` l'ora finale **17:00** dell'intervallo temporale.

Nella finestra **Seleziona i giorni**, selezionare i giorni della settimana in cui dovrà essere applicata la regola. Fare quindi clic su **Salva**.

19) Definire la regola illustrata per la pausa pranzo.



Nell'elenco Strumenti CCV, fare clic su uno degli oggetti CCV contenuti nella regola mostrata e trascinarlo nell'Editor regole. Si aprirà la finestra dell'oggetto CCV in cui inserire le proprietà indicate di seguito. Una volta terminato, confermare facendo clic su **Salva**. Ripetere la procedura per tutti gli oggetti CCV. Collegare due oggetti CCV, facendo clic col pulsante destro del mouse sul primo dei due. Dal menu a tendina **Link To**, selezionare il secondo dei due oggetti CCV collegati. Ripetere la procedura per tutti gli altri oggetti CCV da collegare.

Proprietà		Valore
1° oggetto CCV: **Riproduci messaggio**		
	Nome file	File audio in formato wav
	Interrompi digitazione	Selezionare Assistenza
	Descrizione	Annuncio: Agenti non disponibili
2°oggetto CCV: **Registra richiamata**		
	Tipo	Richiamata automatica senza limitazioni
	Lunghezza massima messaggi (sec.)	20
	Descrizione	Richiesta di richiamata (richiamata agente)
	Elabora dopo digitazione	1

Fare clic su **Salva ...**. Inserire la `Lunch Break` come **Nome CCV** della regola. Chiudere la finestra che conferma il salvataggio della regola.

Nell'elenco a discesa per l'eccezione Lunch Break, selezionare la regola `Lunch Break`.

20) Nel riquadro **Eccezioni**, fare clic su **Aggiungi** per definire l'eccezione relativa alla pausa pranzo.

21) Nel campo `Descrizione`, inserire **Lunch Break**.

22) Definire l'orario di validità di questa eccezione Lunch Break:

Nell'elenco a discesa **Tipo**, selezionare l'opzione **Entro l'intervallo di ore**. Nel menu a discesa **Ora inizio** selezionare l'ora iniziale `12:00` e in **Ora fine** l'ora finale `12:59` dell'intervallo temporale.

Nella finestra **Seleziona i giorni**, selezionare i giorni della settimana in cui dovrà essere applicata la regola. Fare quindi clic su **Salva**.

23) Se si desidera testare quale regola (CCV) della pianificazione verrà eseguita in un particolare momento, fare clic su **Test pianificazione**. Nel menu a discesa **Data**, selezionare il giorno desiderato e nell'elenco **Ora** selezionare l'ora desiderata, quindi fare clic su **Test pianificazione**. Successivamente verrà visualizzata la regola (CCV) che sarà attiva al

giorno e all'ora indicati. Fare clic su **Chiudi**, per chiudere la finestra **Test pianificazione**.

24) Fare clic su **Salva**.

25) Chiudere la finestra.

18.6.1.7 Come aggiungere una pianificazione Hotline per il Contact Center di esempio

Con la procedura guidata **Contact Center** è possibile definire la pianificazione con una regola per le chiamate gratuite (Hotline) per il Contact Center di esempio della società XYZ.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.

2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.

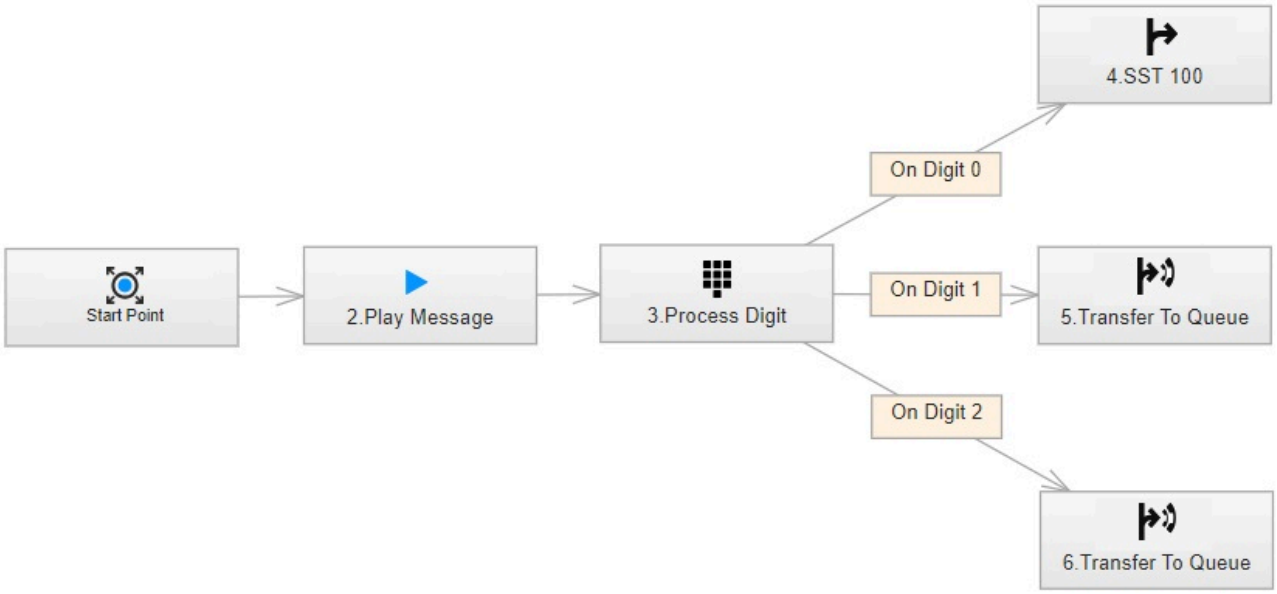
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.

4) Fare clic su **Pianificazione**. Vengono visualizzate tutte le pianificazioni disponibili.

5) Fare clic su **Aggiungi**.

6) Fare clic su **Aggiungi** nell'area **Pianificazione**.

7) Definire la regola raffigurata per le chiamate gratuite (Hotline).



Nell'elenco Strumenti CCV, fare clic su uno degli oggetti CCV contenuti nella regola mostrata e trascinarlo nell'Editor regole. Si aprirà la finestra dell'oggetto CCV in cui inserire le proprietà indicate di seguito. Una volta terminato, confermare facendo clic su **Salva**. Ripetere la procedura per tutti gli oggetti CCV. Collegare due oggetti CCV, facendo clic col pulsante destro del mouse sul primo dei due. Dal menu a tendina **Link To**, selezionare il

secondo dei due oggetti CCV collegati. Ripetere la procedura per tutti gli altri oggetti CCV da collegare.

Proprietà	Valore
1° oggetto CCV: **Riproduci messaggio**	
Nome file	File audio in formato wav
Interrompi digitazione	5
Descrizione	Annuncio: messaggio di saluto
2ª oggetto CCV: **Elabora digitazione**	
Lista di riproduzione	File audio in formato wav
Timeout digitazione	5
Descrizione	Annuncio: "Premere 0 per ...; Premere 1 per ...
3° oggetto CCV: **Trasferimento a passaggio singolo**	
Interno di destinazione	100
Descrizione	Procedi alla console posto operatore
Elabora dopo digitazione	0
4° oggetto CCV **Trasferisci in coda**	
Coda	440
Descrizione	Procedi alla coda di attesa Service
Elabora dopo digitazione	1
5° oggetto CCV **Trasferisci in coda**	
Coda	444
Descrizione	Procedi alla coda di attesa Sales
Elabora dopo digitazione	2

Fare clic su **Salva ...**. Inserire `Hotline` come **Nome CCV** per la regola, quindi fare clic su **Salva**. Se la nuova regola è errata, non sarà possibile salvarla. Gli oggetti CCV errati vengono contrassegnati in rosso nell'Editor regole. Chiudere la finestra che conferma il salvataggio della regola.

Dall'elenco a discesa `CCV predefinito`, scegliere la regola **Hotline**.

8) Nel campo **Nome pianificazione** indicare il nome `Standard Schedule Hotline`.
9) Fare clic su **Salva pianificazione**.

18.6.1.8 Come aggiungere code d'attesa per il Contact Center di esempio

This example shows you how to use the **Contact Center** wizard to configure queues for the sample Contact Center of company XYZ. Per il presente esempio occorre configurare una coda di attesa per il Servizio Assistenza Tecnica (Numero di telefono 440) e una per l'Area Vendite (Numero di telefono 444). Un'altra coda di attesa (Hotline) deve essere configurata per le chiamate gratuite (Numero di telefono 456).

Prerequisiti

The UCD groups **Service**, **Sales** and **Hotline** for the sample Contact Center have been configured.

The schedules **Standard Schedule XYZ** and **Standard Schedule Hotline** have already been created for the sample Contact Center.

È disponibile almeno un account e-mail per la ricezione di e-mail.

Nel sistema di comunicazione è configurato l'invio di e-mail.

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Click on **Queue**.
5) Fare clic su **Aggiungi**.
6) Click on the **General Settings** tab.
7) Enter the name `Service` in the **Queue Name** field.
8) In the **Queue Active** drop-down list, select the item **Active**.
9) Enter the number **440** in the `Hunt Group` field.
10) Select the item **CSP** in the **Phone Switch** drop-down list.
11) Select the item **Standard Schedule XYZ** in the **Schedule** drop-down list.
12) In the field **Queue Alarm Count**, enter the value `20`, for example.

    Se le chiamate in attesa sono oltre 20, l'icona della coda d'attesa visualizzata dall'agente passa da verde ad arancione.
13) In the **Queue Alarm Time** field, enter the value `300`, for example.

    Se il tempo in coda d'attesa di 300 secondi di una chiamata viene superato, la corrispondente voce nell'elenco di chiamate del Contact Center dell'agente diventa rossa.
14) In the field **Missed Call Timeout**, enter the value `100`, for example, so that any call not answered within 100 seconds is forwarded to the next free agent.
15) Enter a number in the **Abandoned Call Threshold** field, e.g., `120`. In questo modo, le chiamate vengono raccolte in statistiche (rapporto) entro 120 secondi.
16) Select the check box **Screen Pop Enabled**. per visualizzare una finestra popup per la visualizzazione e l'inserimento dei dati del cliente all'arrivo di una chiamata in myAgent.
17) Activate the **No Wrapup** option.
18) Select the item **Static** in the **Queue depth mode** drop-down list.
19) Enter a number in the **Queue depth size** field, e.g., `5`.
20) Click on the **Queue Pilots** tab.
21) In the **Inbound Fax Pilots** drop-down list, select the appropriate option or options of the desired pilot/s (phone number/s) so that the faxes are queued.

    I fax a questo(i) numero(i) vengono inseriti nella coda d'attesa e trattati come una chiamata in arrivo.

22) Select one of the following options in the **Inbound Email Service**, area so that e-mails are placed in the queue:

- If you want to set up a new e-mail address, click on **Add**. The **Add** window is displayed.

  Select the authentication method for your e-mail server from the **Auth Method** drop-down list. You can choose between **Basic** and **OAuth 2.0**.

  Enter the designation of the e-mail server to be used for retrieving e-mails in the **Server** field (e.g., `pop3.web.de`).

  Enter the port number of the e-mail server in the **Port** field (e.g., `110`, the default port number for POP3).

  If the authentication method selected is **Basic**, enter the access data for the e-mail server in the **User Name** field and **Password** fields.

  If the authentication method selected is **OAuth 2.0**, enter the user name for accessing the e-mail server in the **User Name**, **Tenant ID**, **Application ID** and **Client Secret** fields. The Tenant ID, Application ID and Client Secret corresponds to the application that has been registered in Azure AD for E-mail Queues. They can be obtained from your Azure AD administrator. Enter the scope for the application in the **Scope** field (default value: https://outlook.office365.com/.default).

  Definire se l'invio di e-mail deve avvenire tramite una connessione SSL (Secure Socket Layer): If you want to use an SSL connection, select the **Use SSL connection** check box. (in questo caso si può eventualmente modificare il numero di porta del server di posta elettronica. Il numero predefinito per POP3 via SSL = 995). If you do not want to use an SSL connection, clear the **Use SSL connection** check box.

  Fare clic su **Salva**. The new e-mail address will then appear in the **Inbound Email Service** area.
- If you want to edit an existing e-mail address, mark the desired e-mail address and click **Edit**. The **Edit** window is displayed.

  Change the required parameters and then lick **Save**.
- If you want to delete an existing e-mail address, mark the desired e-mail address and click **Remove Email**.

23) Click on the **Miscellaneous** tab.

24) In the field **Return Email Address**, enter the e-mail address that is to be displayed as the sender's address (for the recipient) when an e-mail is sent by an agent.

25) If you enable the **Intelligent Call Routing** checkbox , incoming calls are automatically forwarded to the agent with whom the caller was last connected.

26) Fare clic su **Salva**.

27) Repeat steps 5 through 23 to configure the Sales queue. Repeat steps 5 through 17 and step 23 to configure the Hotline queue.

18.6.1.9 Come assegnare gli agenti alle code d'attesa del Contact Center di esempio

Con la procedura guidata **Contact Center** è possibile assegnare gli agenti alle code d'attesa per il Contact Center di esempio della società XYZ. Nell'esempio

tre agenti dovranno essere assegnati alla coda di attesa Servizio e tre alla coda di attesa Vendite.

Prerequisiti

Le code d'attesa **Servizio** e **Vendite** per il Contact Center di esempio sono state configurate.

Sei agenti per il Contact Center di esempio sono stati configurati.

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Associazioni coda**. Le code **Servizio** e **Vendita** vengono visualizzate.
5) Selezionare la coda di attesa alla quale assegnare un agente e fare clic su **Modifica**. Vengono visualizzati tutti gli agenti assegnati.
6) Selezionare il primo agente per la coda **Servizio** dalla tabella e fare clic su **Modifica**. Viene visualizzata la finestra **Modifica**.
7) Selezionare una delle seguenti opzioni:
   - Se l'agente deve ricevere chiamate indipendentemente dal carico sulla coda **Servizio**, selezionare **Agente primario** dall'elenco a discesa **Tipo**.
   - Se l'agente deve ricevere chiamate solo in caso di overflow della coda **Servizio**, selezionare **Agente di overflow** dall'elenco a discesa **Tipo**.
8) Se è stato selezionato **Agente di overflow**:
   a) Nel campo **Overflow dopo secondi in coda** indicare il tempo trascorso il quale una chiamata verrà inoltrata a un agente di overflow.
   b) Nel campo **Overflow dopo chiamate in coda** inserire il numero massimo di chiamate. Un agente di overflow riceverà le chiamate eccedenti tale numero massimo.
9) Inserire un valore percentuale per il **Livello interfaccia** dell'agente.

   Il livello di competenza consente di gestire la distribuzione delle chiamate agli agenti nella coda di attesa **Servizio**. Gli agenti con un livello di competenza più alto hanno la priorità nella distribuzione delle chiamate. Se tutti gli agenti hanno lo stesso livello interfaccia, l'agente che è libero da più tempo riceve la chiamata.
10) Selezionare una delle seguenti opzioni:
    - Se si desidera che l'agente riceva prenotazioni per richiamate sotto forma di messaggi vocali, selezionare la casella di controllo **Attiva richiamata agente**.
    - Se non si desidera che l'agente riceva prenotazioni per richiamate, deselezionare la casella di controllo **Attiva richiamata agente**.
11) Nel campo **Orario lavorativo** indicare l'orario lavorativo automatico in secondi per l'agente della coda **Servizio**.
12) Fare clic su **OK**.
13) Ripetere i passi 5 - 12 per assegnare tutti gli agenti alle code d'attesa del Contact Center di esempio.

18.6.2 Procedura di configurazione

In questa sezione viene fornita una panoramica sulle operazioni da eseguire durante la configurazione del Contact Center.

- Configurazione di gruppi UCD

  Le code d'attesa del Contact Center sono gruppi di lavoro basati sui gruppi UCD del sistema di comunicazione. Prima di procedere all'effettiva configurazione del Contact Center, è necessario definire i gruppi UCD.
- Configurazione di una soluzione secondaria (soluzione fallback)

  In caso di mancata disponibilità del Contact Center in seguito a problemi (crash di sistema, problemi di connessione e simili), il sistema di comunicazione commuta automaticamente sul servizio "Uniform Call Distribution, UCD". Questo servizio funge da soluzione secondaria, sostitutiva del Contact Center (vedere Soluzione secondaria (soluzione fallback)).
- Configurazione di utenti come agenti
- Registrazione di singoli annunci per il Contact Center
- Caricamento di singoli annunci per il Contact Center

  Nota: È possibile riprodurre gli annunci solo tramite linee. Per riprodurre l'annuncio, la chiamata deve provenire da una linea o il chiamante deve essere monitorato da OpenScape Contact Center.
- Aggiunta di pianificazioni
- Aggiunta di code d'attesa
- Definizione di valori soglia per il livello di servizio
- Definizione di priorità chiamante VIP
- Modifica dell'elenco chiamate VIP
- Definizione degli agenti preferiti
- Aggiunta delle pause del Contact Center
- Aggiunta dei codici post-elaborazione
- Assegnazione degli agenti alle code d'attesa

18.6.2.1 Come configurare i gruppi UCD per il Contact Center

Con la procedura guidata **Distribuzione delle chiamate**, è possibile configurare i gruppi UCD per il Contact Center.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **UCD**. Viene visualizzata una lista di tutti i gruppi UCD disponibili.

4) Per configurare un gruppo UCD, fare clic su **Modifica** nella riga del gruppo UCD desiderato.
5) Nel campo **Numero di telefono** indicare il numero di telefono del gruppo UCD.
6) Nel campo **Interno** indicare il numero di interno del gruppo UCD.
7) Nel campo **Nome** indicare il nome del gruppo UCD.
8) Fare clic su **OK & Avanti**. Viene visualizzata la finestra **Assegnazione agenti UCD**.
9) Selezionare gli ID degli agenti UCD desiderati in **Scelta** e assegnarli al gruppo UCD facendo clic su **Aggiungi**.
10) Fare clic su **OK&Avanti**. Viene visualizzata la finestra **Assegna a utente**.
11) Assegnare a tutti gli ID agente UCD l'utente desiderato.
12) Fare clic su **OK&Avanti**. Viene visualizzata la finestra **Modifica annuncio/ overflow**.
13) Fare clic su **OK**, in quanto i parametri visualizzati non sono rilevanti per la configurazione del gruppo UCD.
14) Se si desidera configurare un altro gruppo UCD per il Contact Center, ripetere i passi da 4 a 11.
15) Fare clic su **OK & Avanti**, quindi su **Fine**.

18.6.2.2 Come configurare un utente come agente

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Rubrica utente**.
4) Selezionare l'utente desiderato nell'indice utenti e premere **Modifica**.
5) Nella struttura dei menu fare clic su **Dati personali** > **Livello utente**.
6) Selezionare una delle seguenti opzioni:

   Se l'agente deve essere permanentemente disponibile, selezionare la casella di controllo **Agente sempre disponibile**. L'agente rimane disponibile per chiamate, fax e e-mail, anche se non ha risposto a una chiamata, fax o e-mail.

   Se l'agente non deve essere permanentemente disponibile, deselezionare la casella di controllo **Agente sempre disponibile**. L'agente riceve lo stato non disponibile se non ha risposto a una chiamata, fax o e-mail.
7) Nell'elenco a discesa **Livello**, selezionare il livello di autorizzazione.
8) Fare clic su **Salva**.
9) Se si desidera configurare altri utenti come agenti, ripetere il passo da 4 a 8.

18.6.2.3 Come registrare singoli annunci per il Contact Center

You can record custom announcements for the Contact Center with the **Recorder** wizard.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Click on **Edit** to start the **File Upload** wizard.
4) Enable the **Recorder** radio button
5) Select the station number of the phone to be used for recording from the **Extension** drop-down list.
6) Click on **Make a Call**. Il numero composto viene chiamato.
7) Pick up the handset and enter the name for your announcement in the **Filename** field.
8) Click on **Record** to start recording the announcement.
9) Click on **Stop** as soon as you have finished recording the entire announcement.
10) If you want to listen to your new announcement, click on **Play**.
11) Click on **Close** to save the announcement.

Suggerimento:

Dopo la registrazione e il salvataggio non è più possibile cancellare un annuncio. Tuttavia, utilizzando lo stesso nome file, è possibile sovrascriverlo. For example, saving an audio file named `announcement1.wav` would overwrite any existing `announcement1.wav` file.

18.6.2.4 Come caricare singoli annunci per il Contact Center

You can load custom announcements for the Contact Center with the **File Upload** wizard.

Prerequisiti

È disponibile un file audio in formato wav con le seguenti proprietà: mono, velocità campione audio 8 kHz, dimensioni campione audio 16 bit, dimensione del frame 2.

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Click on **Edit** to start the **File Upload** wizard.
4) Click on the **Audio Files Manager** tab.

5) Select the destination **Auto Attendant** in the **Upload Destination** drop-down list.
6) Select the **Uploader** radio button and click on **Choose File**, navigate to the storage location of the desired audio file and click on **Open**.
7) Click on **Upload**.

Suggerimento: Dopo il caricamento del file audio, non sarà più possibile eliminarlo. Tuttavia, utilizzando lo stesso nome del file audio caricato, è possibile sovrascriverlo. For example, uploading an audio file named `announcement1.wav` would overwrite any existing `announcement1.wav` file.

18.6.2.5 Come aggiungere pianificazioni

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Pianificazione**. Vengono visualizzate tutte le pianificazioni disponibili.
5) Fare clic su **Aggiungi**.
6) Per la scelta della regola (CCV), selezionare una delle seguenti opzioni:
   - Se si vuole assegnare alla pianificazione una regola già definita, nell'elenco a discesa **CCV predefinito**, selezionare la regola desiderata.
   - Se si vuole assegnare alla pianificazione una nuova regola non ancora definita, fare clic su **Modifica** nell'area **Pianificazione** e procedere come segue:

     Nell'elenco Strumenti CCV, fare clic su un oggetto CCV e trascinarlo nell'Editor regole. Inserire le proprietà desiderate nella finestra dell'oggetto CCV che si apre, quindi fare clic su **Salva**. Nel caso sia necessario, trascinare altri oggetti CCV nell'Editor regole e definire le relative proprietà. Per collegare due oggetti CCV, fare clic col pulsante destro del mouse sul primo dei due. Dal menu a tendina **Link To**, selezionare il secondo dei due oggetti CCV collegati.

     Se si desidera eliminare un oggetto CCV dell'Editor regole, fare clic col pulsante destro del mouse sull'oggetto CCV in questione e dal menu a tendina, selezionare **Rimuovi**.

     Fare clic su **Salva ...**. Inserire un nome per la nuova regola, quindi fare clic su **Salva**. Chiudere la finestra che conferma il salvataggio della

regola. Se la nuova regola è errata, non sarà possibile salvarla. Gli oggetti CCV errati vengono contrassegnati in rosso nell'Editor regole.

Dall'elenco a discesa **CCV predefinito**, scegliere la nuova regola appena salvata.

- Se si vuole assegnare alla pianificazione una nuova regola basata su una già definita, procedere come segue:

  Nell'elenco a discesa **CCV predefinito**, selezionare la regola desiderata, quindi premere **Modifica**. La regola viene visualizzata nell'Editor regole. Modificare la regola.

  Nell'elenco Strumenti CCV, fare clic su un oggetto CCV e trascinarlo nell'Editor regole. Inserire le proprietà desiderate nella finestra dell'oggetto CCV che si apre, quindi fare clic su **Salva**. Nel caso sia necessario, trascinare altri oggetti CCV nell'Editor regole e definire le relative proprietà. Per collegare due oggetti CCV, fare clic col pulsante destro del mouse sul primo dei due. Dal menu a tendina **Link To**, selezionare il secondo dei due oggetti CCV collegati.

  Fare clic su **Salva ...**. Inserire un **Nome CCV** per la nuova regola, quindi fare clic su **Salva**. Chiudere la finestra che conferma il salvataggio della regola. Se la nuova regola è errata, non sarà possibile salvarla. Gli oggetti CCV errati vengono contrassegnati in rosso nell'Editor regole.

  Dall'elenco a discesa **CCV predefinito**, scegliere la nuova regola appena salvata.

7) Quando si stampa la regola o la si invia per e-mail, è possibile salvarla come file PDF. A tal fine, fare clic su **Stampa**. Viene visualizzata la finestra **Stampa**.

Inserire il nome e il file, quindi selezionare la cartella in cui salvare il file. Fare clic su **Salva**.

8) Nel campo **Nome pianificazione** indicare il nome della nuova pianificazione.

9) Fare clic su **Salva**.

10) Se si desidera assegnare a un periodo specifico all'interno della pianificazione un'altra regola (CCV), nell'area della finestra **Eccezioni**, fare clic su **Aggiungi**. Successivamente vengono visualizzati i campi per questa eccezione.

11) Nel campo **Descrizione** inserire un nome dell'eccezione.

12) Per la scelta della regola (CCV), selezionare una delle seguenti opzioni:

- Se si vuole assegnare a un periodo all'interno della pianificazione una regola già definita, nell'elenco a discesa di questa eccezione, selezionare la regola desiderata.
- Se si vuole assegnare al periodo all'interno della pianificazione una nuova regola non ancora definita, procedere come segue:

  Fare clic su **Aggiungi** nell'area **Pianificazione**.

  Nell'elenco Strumenti CCV, fare clic su un oggetto CCV e trascinarlo nell'Editor regole. Inserire le proprietà desiderate nella finestra dell'oggetto CCV che si apre, quindi fare clic su **Salva**. Nel caso sia necessario, trascinare altri oggetti CCV nell'Editor regole e definire le relative proprietà. Per collegare due oggetti CCV, fare clic col pulsante

destro del mouse sul primo dei due. Dal menu a tendina **Link To**, selezionare il secondo dei due oggetti CCV collegati.

Se si desidera eliminare un oggetto CCV dell'Editor regole, fare clic col pulsante destro del mouse sull'oggetto CCV in questione e dal menu a tendina, selezionare **Rimuovi**.

Fare clic su **Salva ...**. Inserire un nome per la nuova regola, quindi fare clic su **Salva**. Chiudere la finestra che conferma il salvataggio della regola. Se la nuova regola è errata, non sarà possibile salvarla. Gli oggetti CCV errati vengono contrassegnati in rosso nell'Editor regole.

Dall'elenco a discesa per questa eccezione, scegliere la nuova regola appena salvata.

- Se si vuole assegnare al periodo all'interno della pianificazione una nuova regola basata su una già definita, procedere come segue:

  Nell'elenco a discesa di questa eccezione, selezionare la regola desiderata, quindi premere **Modifica**. La regola viene visualizzata nell'Editor regole. Modificare la regola.

  Nell'elenco Strumenti CCV, fare clic su un oggetto CCV e trascinarlo nell'Editor regole. Inserire le proprietà desiderate nella finestra dell'oggetto CCV che si apre, quindi fare clic su **Salva**. Nel caso sia necessario, trascinare altri oggetti CCV nell'Editor regole e definire le relative proprietà. Per collegare due oggetti CCV, fare clic col pulsante destro del mouse sul primo dei due. Dal menu a tendina **Link To**, selezionare il secondo dei due oggetti CCV collegati.

  Fare clic su **Salva ...**. Inserire un nome per la nuova regola, quindi fare clic su **Salva**. Chiudere la finestra che conferma il salvataggio della regola. Se la nuova regola è errata, non sarà possibile salvarla. Gli oggetti CCV errati vengono contrassegnati in rosso nell'Editor regole.

  Dall'elenco a discesa per questa eccezione, scegliere la nuova regola appena salvata.

13) Selezionare una delle seguenti opzioni per definire in quale momento applicare l'eccezione:

- Se l'applicazione dell'eccezione non è limitata a un particolare periodo dell'anno, selezionare **Entro l'intervallo di ore** dal menu a discesa **Tipo**. Nel menu a discesa **Ora inizio** selezionare l'ora iniziale e in **Ora fine** l'ora finale dell'intervallo temporale.

  Selezionare i giorni della settimana in cui dovrà essere applicata l'eccezione. Fare quindi clic su **Salva**.
- Se l'applicazione dell'eccezione è limitata a un particolare periodo dell'anno, selezionare **Entro l'intervallo di ore** dal menu a discesa **Tipo**. Nel campo **Data inizio** inserire la data di inizio mentre in **Data fine** inserire la data finale del periodo dell'anno (nel formato gg.mm.aaaa). Nel menu a discesa **Ora inizio** selezionare l'ora esatta iniziale e in **Ora fine** l'ora esatta finale. L'eccezione viene applicata tra data/ora di inizio e data/ora di fine del periodo coperto.

  Selezionare i giorni della settimana in cui dovrà essere applicata l'eccezione. Fare quindi clic su **Salva**.
- Se l'eccezione deve essere applicata nei giorni festivi, selezionare **Pianificazioni vacanze** dall'elenco a discesa **Tipo**. Nel campo **Data inizio** inserire la data di inizio e nel campo **Data fine** inserire la data finale del periodo di vacanza. Nell'elenco **Ora inizio**, selezionare l'ora

del giorno di inizio e in **Ora fine** l'ora del giorno finale del periodo di vacanza.

Suggerimento: In questo caso le pianificazioni vacanze hanno la priorità rispetto alle altre pianificazioni e regole di una coda d'attesa.

- Se l'eccezione deve essere applicata ogni anno, selezionare **Ricorrenza annuale** dall'elenco a discesa **Tipo**. Nel campo **Data inizio** inserire la data di inizio e nel campo **Data fine** inserire la data finale della ricorrenza annuale. Nella casella **Ora inizio**, selezionare l'ora del giorno di inizio e nella casella **Ora fine** l'ora del giorno finale della ricorrenza annuale.

14) Fare clic su **Salva**.

15) Ripetere i passi da 10 a 14 se si desidera definire altre eccezioni per periodi specifici.

16) Se si desidera testare quale regola (CCV) della pianificazione verrà eseguita in un particolare momento, fare clic su **Test pianificazione**. Nel menu a discesa **Data**, selezionare il giorno desiderato e nell'elenco **Ora** selezionare l'ora desiderata, quindi fare clic su **Test pianificazione**. Successivamente verrà visualizzata la regola (CCV) che sarà attiva al giorno e all'ora indicati. Fare clic su **Chiudi**, per chiudere la finestra **Test pianificazione**.

17) Se si desidera assegnare questa pianificazione a una o più code, selezionare la/e casella/e di controllo della/e coda/e desiderata/e nell'area **Code**.

Nota: Una coda selezionata può essere assegnata a una sola pianificazione, ma a una pianificazione selezionata possono essere assegnate più code diverse.

18) Chiudere la finestra.

18.6.2.6 Come modificare la pianificazione

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.

2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.

3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.

4) Fare clic su **Pianificazione**. Vengono visualizzate tutte le pianificazioni disponibili.

5) Selezionare la pianificazione da modificare e fare clic su **Modifica**.

6) Modificare le impostazioni desiderate per il CCV predefinito:

- Se si vuole assegnare una regola (CCV) diversa da quella visualizzata nell'elenco a discesa **CCV predefinito**, selezionare la regola desiderata nell'elenco a discesa **CCV predefinito**.
- Se si desidera modificare la regola (CCV) visualizzata nell'elenco a discesa **CCV predefinito**, fare clic su **Modifica** nell'area **Pianificazione**. La regola viene visualizzata nell'Editor regole. Modificare la regola. Fare clic su **Salva ...**. Inserire un nome per la nuova regola, quindi fare clic su **Salva**. Chiudere la finestra che conferma il salvataggio della regola.

  Dall'elenco a discesa **CCV predefinito**, scegliere la nuova regola appena salvata.

7) Fare clic su **Salva**.

8) Nell'area **Eccezioni**, modificare le impostazioni come desiderato:

- Se si desidera assegnare a un periodo specifico all'interno della pianificazione un'altra regola (CCV), nell'area **Eccezioni**, fare clic su **Aggiungi**. Nell'elenco a discesa, selezionare l'eccezione desiderata. Selezionare mediante i pulsanti di opzione e gli elenchi a discesa, in quale periodo di tempo l'eccezione dovrà essere applicata. Nel campo **Descrizione** inserire un nome dell'eccezione. Fare clic su **Salva**.
- Se si desidera modificare questa eccezione o una delle eccezioni visualizzate, fare clic su **Modifica** nell'area **Eccezione** dopo aver selezionato l'eccezione desiderata, quindi usare i pulsanti di opzione, gli elenchi a discesa e i campi per specificare quando l'eccezione deve essere applicata e su quale regola (CCV). Inoltre, è possibile fare clic su **Modifica CCV** al di sotto dell'area **Eccezione** area per modificare la regola (CCV) associata. La regola viene visualizzata nell'Editor regole. Modificare la regola. Fare clic su **Salva ...**. Inserire un nome per la nuova regola, quindi fare clic su **Salva**. Chiudere la finestra che conferma il salvataggio della regola.

  Dall'elenco a discesa scegliere la nuova regola appena salvata. Mediante i pulsanti di opzione e gli elenchi a discesa, selezionare a quale periodo di tempo la regola (CCV) dovrà essere applicata. Fare clic sull'icona verde del salvataggio.
- Se si desidera cancellare questa eccezione o una delle visualizzate, fare clic su **Elimina** dopo aver selezionato l'eccezione desiderata.

9) Se si desidera testare quale regola (CCV) della pianificazione verrà eseguita in un particolare momento, fare clic su **Test pianificazione**. Nel menu a discesa **Data**, selezionare il giorno desiderato e nell'elenco **Ora** selezionare l'ora desiderata, quindi fare clic su **Test pianificazione**. Successivamente verrà visualizzata la regola (CCV) che sarà attiva al giorno e all'ora indicati. Fare clic su **Chiudi**, per chiudere la finestra **Test pianificazione**.

10) Se si desidera assegnare questa pianificazione a una o più code, selezionare la/e casella/e di controllo della/e coda/e desiderata/e nell'area **Code**.

Nota: Una coda selezionata può essere assegnata a una sola pianificazione, ma a una pianificazione selezionata possono essere assegnate più code diverse.

---

11) Chiudere la finestra.

18.6.2.7 Come eliminare le pianificazioni

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Pianificazione**. Vengono visualizzate tutte le pianificazioni disponibili.
5) Selezionare la pianificazione desiderata e fare clic su **Rimuovi**.

Suggerimento: Non è possibile eliminare una pianificazione se a questa è assegnata una coda di attesa. Prima dell'eliminazione, è necessario rimuovere l'assegnazione della pianificazione alle code d'attesa.

18.6.2.8 Come salvare una regola (CCV) come file PDF

The **Contact Center** wizard enables you to save rules (CCV) as a PDF file. Il file PDF può successivamente essere ad esempio stampato o inviato per e-mail.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Pianificazione**. Vengono visualizzate tutte le pianificazioni disponibili.
5) Select the schedule that contains the desired rule and click **Edit**.
6) Select the desired rule from the drop-down list and click **Edit**. La regola viene visualizzata nell'Editor regole.
7) Click on **Print**. Viene visualizzata la finestra Salva.
8) Inserire il nome e il file, quindi selezionare la cartella in cui salvare il file.
9) Fare clic su **Salva**.
10) Chiudere la finestra e confermare la chiusura selezionando **Sì**.

18.6.2.9 How to Download a Rule (CCV) as a Backup File

The **Contact Center** wizard enables you to download rules (CCV) as a backup file.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Pianificazione**. Vengono visualizzate tutte le pianificazioni disponibili.
5) Select the schedule that contains the desired rule and click **Edit**.
6) Select the desired rule from the **CCV** drop-down list and click **Edit** under the **Schedule** area. La regola viene visualizzata nell'Editor regole.
7) Click on **Download**.

The desired rule (CCV) is now downloaded as a backup file.

18.6.2.10 How to Upload a Downloaded Rule (CCV) in a Backup File Format

The **Contact Center** wizard enables you to upload rules (CCV) which are previous downloaded in a backup file format.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Download a rule (CCV) in a backup file format.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Pianificazione**. Vengono visualizzate tutte le pianificazioni disponibili.
5) Select the schedule that contains the desired rule and click **Edit**.
6) Select the desired rule from the **CCV** drop-down list and click **Edit** under the **Schedule** area. La regola viene visualizzata nell'Editor regole.
7) Click on **Choose File**, navigate to the storage location of the desired rule's backup file and click on **Open**.

   If you choose a file which is not in a backup format an error occurs.
8) Click on **Restore Backup**.

The desired rule (CCV) is now uploaded on the system.

18.6.2.11 Come aggiungere una coda d'attesa

Prerequisiti

Deve essere configurato almeno un gruppo UCD.

Deve essere configurata almeno una pianificazione.

È disponibile almeno un account e-mail per la ricezione di e-mail (se nella coda d'attesa vengono accettate le e-mail).

Per consentire agli agenti delle code di attesa di inviare e-mail, è necessario configurare la funzione Invio e-mail nel sistema di comunicazione.

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Click on **Queue**.
5) Fare clic su **Aggiungi**.
6) Click on the **General Settings** tab.
7) Enter the name of the queue in the **Queue Name** field.

   Suggerimento: Use the name of one of your configured UCD groups.

   Suggerimento: Affinché il nome della coda di attesa venga visualizzato per intero in un'analisi (rapporto), scegliere una descrizione breve, senza unire le parole. Esempio: Domestic Sales Group 1 (not: DomesticSalesGroup 1)

   ---

8) Selezionare una delle seguenti opzioni per lo stato della coda d'attesa:
   - If you want to activate the new queue, select the item **Active** in the **Queue Active** drop-down list.
   - If you want to deactivate the new queue, select the item **Not active** in the **Queue Active** drop-down list.

     La disattivazione di una coda di attesa determina l'attivazione della soluzione secondaria da parte del relativo gruppo UCD. Se nessun agente è connesso al gruppo UCD e non è impostata alcun'altra destinazione di inoltro per il gruppo UCD, alle chiamate viene inviata la segnalazione di occupato.
9) Enter the call number of a UCD group that you set up during the basic configuration of the Contact Center in the **Hunt Group** field.
10) Select the item **CSP** in the **Phone Switch** drop-down list.
11) Select the desired schedule in the **Schedule** drop-down list.
12) Enter the alarm threshold value in the **Queue Alarm Count** field.

    Se il numero qui indicato supera il numero di chiamate in coda d'attesa, l'icona della coda d'attesa visualizzata dall'agente passa da verde ad arancione.
13) Enter the alarm threshold value in seconds in the **Queue Alarm Time** field.

    Se il tempo in coda d'attesa per una chiamata qui indicato viene superato, la corrispondente voce nell'elenco di chiamate del Contact Center dell'agente diventa rossa.
14) Enter the time in seconds after which an unanswered call should be forwarded to the next free agent in the **Missed Call Timeout** field.

15) Enter the time in seconds that determines whether or not an abandoned call should be included in the statistics (i.e., in a report) in the **Abandoned Call Threshold** field.

Verranno incluse nelle statistiche le chiamate che vengono abbandonate una volta trascorso il tempo indicato.

16) Selezionare una delle seguenti opzioni per la visualizzazione di finestre popup nell'applicazione myAgent:

Suggerimento: Le finestre popup sono necessarie per accettare ed eseguire richiamate, nonché per accettare fax e e-mail.

- If you want a screen pop for displaying and entering customer data to appear in myAgent on inbound calls, select the check box **Screen Pop Enabled**.
- If you do not want a screen pop to appear in myAgent on inbound calls, clear the **Screen Pop Enabled** check box.

17) Selezionare una delle seguenti opzioni per la modalità elaborazione:

Le code di attesa con modalità elaborazione possono essere ordinate dall'agente in base a motivi specifici (ordine, reclamo, assistenza, ecc.) utilizzando il codice post-elaborazione.

- If you want to set up a queue with the wrapup mode Simple Wrapup, select the **Simple Wrapup** option.
- If you want to set up a queue with the wrapup mode Multiple Wrapup, select the **Multiple Wrapup** option.
- If you want to set up a queue without wrapup mode, select the option **No Wrapup**.

18) If you want to change the priority of the queue, click on **Priorities**.

Click on and drag the red dots in the **Queue Priority Over Time** area to the desired positions. L'asse orizzontale mostra il tempo di attesa in coda, l'asse verticale la priorità della coda d'attesa selezionata rispetto alle altre. If an agent is assigned to multiple queues, the queue priority can be used to define whether calls for a queue with higher priority should be forwarded to this agent with precedence over calls for other queues.

Drag the scroll bars in the **Call Type Priorities** area to the desired position. In questo modo si definisce la priorità per i tipi di chiamata nella coda d'attesa selezionata. Higher priorities are assigned by moving the scroll bars incrementally to the right.

Suggerimento: Per le chiamate vocali è necessario selezionare una priorità maggiore rispetto agli altri tipi di chiamata. In caso contrario, le chiamate in attesa potrebbero venire precedute da richiamate, fax o e-mail.

---

19) Select one of the following options for the Queue depth mode:

Queue Depth can be set for each queue individually within the queue configuration dialog

- In case the **Queue depth mode** is set to **Static**, **WLS** and **Queue depth size** parameters can be configured.
- In case the **Queue depth mode** is set to **None**, the **WLS** parameter can be configured nevertheless and affects also the UCD configuration but parameter **Queue depth size** cannot be set.

20) Enter the time Waiting Loop Size in the **WLS** field. The **WLS** value which is the number of the voice calls waiting to be connected to an agent, affects directly the configuration of the parameter Queued Calls of the assigned UCD group.

21) If **Queue depth mode** is set to **Static**, enter the quantity of the queue depth in the **Queue depth size** field. The queue depth size is the summary of the waiting loop size (WLS) and the calls on agent.

22) Click on the **Queue Pilots** tab.

23) If faxes are to be queued, select the appropriate option or options of the desired pilot/s (phone number/s) in the **Inbound Fax Pilots** area.

I fax a questo(i) numero(i) vengono inseriti nella coda d'attesa e trattati come una chiamata in arrivo.

24) Select one of the following options in the **Inbound Email Service**, area so that e-mails are placed in the queue:

- If you want to set up a new e-mail address, click on **Add**. The **Add** window is displayed.

  Select the authentication method for your e-mail server from the **Auth Method** drop-down list. You can choose between **Basic** and **OAuth 2.0**.

  Enter the designation of the e-mail server to be used for retrieving e-mails in the **Server** field (e.g., `pop3.web.de`).

  Enter the port number of the e-mail server in the **Port** field (e.g., `110`, the default port number for POP3).

  If the authentication method selected is **Basic**, enter the access data for the e-mail server in the **User Name** field and **Password** fields.

  If the authentication method selected is **OAuth 2.0**, enter the user name for accessing the e-mail server in the **User Name**, **Tenant ID**, **Application ID** and **Client Secret** fields. The Tenant ID, Application ID and Client Secret corresponds to the application that has been registered in Azure AD for E-mail Queues. They can be obtained from your Azure AD administrator. Enter the scope for the application in the **Scope** field (default value: https://outlook.office365.com/.default).

  Definire se l'invio di e-mail deve avvenire tramite una connessione SSL (Secure Socket Layer): If you want to use an SSL connection, select the **Use SSL connection** check box. (in questo caso si può eventualmente modificare il numero di porta del server di posta elettronica. Il numero

predefinito per POP3 via SSL = 995). If you do not want to use an SSL connection, clear the **Use SSL connection** check box.

Fare clic su **Salva**. The new e-mail address will then appear in the **Inbound Email Service** area.

- If you want to edit an existing e-mail address, mark the desired e-mail address and click **Edit**. The **Edit** window is displayed.

  Change the required parameters and then lick **Save**.
- If you want to delete an existing e-mail address, mark the desired e-mail address and click **Remove**.

25) Click on the **Miscellaneous** tab.

26) In the field **Return Email Address**, enter the e-mail address that is to be displayed as the sender's address (for the recipient) when an e-mail is sent by an agent.

27) Selezionare una delle seguenti opzioni per l'inoltro intelligente alle code d'attesa:

- If incoming calls are to be forwarded automatically to the agent who was last connected with the caller, enable the check box **Search for last agent customer if no preferred agent is found**. Ciò è possibile se per il chiamante non è stato definito alcun agente preferito.
- If incoming calls are not to be forwarded automatically to the agent who was last connected with the caller, clear the check box **Search for last agent customer if no preferred agent is found**.

28) Fare clic su **Salva**.

18.6.2.12 Come modificare la coda d'attesa

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.

2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.

3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.

4) Click on **Queue**.

5) Mark the desired queue and click **Edit**.

6) Click on the **General Settings** tab.

7) Modificare le impostazioni desiderate.

8) Selezionare una delle seguenti opzioni per lo stato della coda d'attesa:

- If you want to activate the queue, select the item **Active** in the **Queue Active** drop-down list.
- If you want to deactivate the queue, select the item **Not active** in the **Queue Active** drop-down list.

  La disattivazione di una coda di attesa determina l'attivazione della soluzione secondaria da parte del relativo gruppo UCD. Se nessun agente è connesso al gruppo UCD e non è impostata alcun'altra destinazione di inoltro per il gruppo UCD, alle chiamate viene inviata la segnalazione di occupato.

9) Selezionare una delle seguenti opzioni per la visualizzazione di finestre popup nell'applicazione myAgent:

> **Suggerimento:** Le finestre popup sono necessarie per accettare ed eseguire richiamate, nonché per accettare fax e e-mail.

- If you want a screen pop for displaying and entering customer data to appear in myAgent on inbound calls, select the check box **Screen Pop Enabled**.
- If you do not want a screen pop to appear in myAgent on inbound calls, clear the **Screen Pop Enabled** check box.

10) Selezionare una delle seguenti opzioni per la modalità elaborazione:

Le code di attesa con modalità elaborazione possono essere ordinate dall'agente in base a motivi specifici (ordine, reclamo, assistenza, ecc.) utilizzando il codice post-elaborazione.

- If you want to set the wrapup mode Simple Wrapup for the queue, select the **Simple Wrapup** option.
- If you want to set the wrapup mode Multiple Wrapup for the queue, select the **Multiple Wrapup** option.
- If you do not want to set any wrapup mode for the queue, select the **No Wrapup** option.

11) If you want to change the priority of the queue, click on **Priorities**.

Click on and drag the red dots in the **Queue Priority Over Time** area to the desired positions. L'asse orizzontale mostra il tempo di attesa in coda, l'asse verticale la priorità della coda d'attesa selezionata rispetto alle altre. If an agent is assigned to multiple queues, the queue priority can be used to define whether calls for a queue with higher priority should be forwarded to this agent with precedence over calls for other queues.

Drag the scroll bars in the **Call Type Priorities** area to the desired position. In questo modo si definisce la priorità per i tipi di chiamata nella coda d'attesa selezionata. Higher priorities are assigned by moving the scroll bars incrementally to the right.

> **Suggerimento:** Per le chiamate vocali è necessario selezionare una priorità maggiore rispetto agli altri tipi di chiamata. In caso contrario, le chiamate in attesa potrebbero venire precedute da richiamate, fax o e-mail.

12) Click on the **Queue Pilots** tab.

13) Select the desired settings in the **Inbound Fax Pilots** area:

- If faxes are to be queued, select the appropriate check box or check boxes of the desired pilot/s (phone number/s) in the **Inbound Fax Pilots** area.
- If faxes are not to be queued, clear the **Inbound Fax Pilots** check box(es).

14) Select the desired settings in the **Inbound Email Service** area:

- If you want to set up a new e-mail address, click on **Add**. The **Add** window is displayed.

  Select the authentication method for your e-mail server from the **Auth Method** drop-down list. You can choose between **Basic** and **OAuth 2.0**.

  Enter the designation of the e-mail server to be used for retrieving e-mails in the **Server** field (e.g., `pop3.web.de`).

  Enter the port number of the e-mail server in the **Port** field (e.g., `110`, the default port number for POP3).

  If the authentication method selected is **Basic**, enter the access data for the e-mail server in the **User Name** field and **Password** fields.

  If the authentication method selected is **OAuth 2.0**, enter the user name for accessing the e-mail server in the **User Name**, **Tenant ID**, **Application ID** and **Client Secret** fields. The Tenant ID, Application ID and Client Secret corresponds to the application that has been registered in Azure AD for E-mail Queues. They can be obtained from your Azure AD administrator. Enter the scope for the application in the **Scope** field (default value: https://outlook.office365.com/.default).

  Definire se l'invio di e-mail deve avvenire tramite una connessione SSL (Secure Socket Layer): If you want to use an SSL connection, select the **Use SSL connection** check box. (in questo caso si può eventualmente modificare il numero di porta del server di posta elettronica. Il numero predefinito per POP3 via SSL = 995). If you do not want to use an SSL connection, clear the **Use SSL connection** check box.

  Fare clic su **Salva**. The new e-mail address will then appear in the **Inbound Email Service** area.
- If you want to edit an existing e-mail address, mark the desired e-mail address and click **Edit**. The **Edit** window is displayed.

  Change the required parameters and then lick **Save**.
- If you want to delete an existing e-mail address, mark the desired e-mail address and click **Remove**.

15) Click on the **Miscellaneous** tab.

16) Modificare le impostazioni desiderate.

17) Fare clic su **Salva**.

18.6.2.13 Come attivare o disattivare la coda di attesa

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Coda**.
5) Fare clic su **Modifica**.
6) Fare clic sulla scheda **Impostazioni generali**.

7) Selezionare una delle seguenti opzioni per lo stato della coda d'attesa:
   - Se si desidera attivare la coda d'attesa, nell'elenco **Coda attiva**, selezionare la voce **Attiva**.
   - Se si desidera disattivare la coda d'attesa, nell'elenco **Coda attiva**, selezionare la voce **Non attiva**.

     La disattivazione di una coda di attesa determina l'attivazione della soluzione secondaria da parte del relativo gruppo UCD. Se nessun agente è connesso al gruppo UCD e non è impostata alcun'altra destinazione di inoltro per il gruppo UCD, alle chiamate viene inviata la segnalazione di occupato.
8) Fare clic su **Salva**.

18.6.2.14 Come configurare un pilota per i fax in arrivo nella coda di attesa

Prerequisiti

È disponibile almeno un numero di fax pe la ricezione di fax.

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Server telefonia** > **Utente**.
3) Nella struttura dei menu fare clic su **Utente** > **Applicazioni UC** > **Fax del centro contatti**. Vengono visualizzati i numeri di porta logici impostati per le caselle fax.
4) Nella struttura dei menu fare clic sul numero di porta desiderato.
5) Fare clic sulla scheda **Modifica parametri dell'utente**.
6) Nel campo **Numero di telefono** indicare il numero di telefono del nuovo pilota per i fax in arrivo.
7) Nel campo **Nome** indicare il nome del nuovo pilota per i fax in arrivo.
8) Nel campo **Selezione passante** indicare il numero di selezione passante del nuovo pilota per i fax in arrivo.
9) Fare clic su **Applica**, quindi su **OK**.

È ora possibile attivare il pilota per i fax in arrivo per la coda d'attesa desiderata.

18.6.2.15 Come definire i valori soglia per il livello di servizio

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Livello di servizio**.
5) Selezionare la coda d'attesa desiderata e premere **Modifica**.

6) Selezionare e trascinare i punti rossi sulla posizione desiderata.

   L'asse orizzontale mostra il tempo di attesa nella coda a intervalli di 10 secondi, l'asse verticale la soglia per il livello di servizio espressa in valori percentuali.

   A tal scopo, inserire la soglia per la qualità di commutazione nella coda d'attesa. Confrontando i valori soglia con i tempi d'attesa effettivi dei chiamanti, è possibile valutare la qualità.

7) Fare clic su **Salva**.

18.6.2.16 Come definire la priorità del chiamante VIP

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Priorità chiamante VIP**.
5) Selezionare la coda d'attesa desiderata e premere **Modifica**.
6) Selezionare e trascinare i punti rossi sulla posizione desiderata.

   Questa funzione consente di definire la priorità tra chiamanti normali e chiamanti VIP.

   L'asse orizzontale mostra il tempo di attesa nella coda a intervalli di 30 secondi, l'asse verticale la priorità normale del chiamante che non appartiene all'Elenco chiamate VIP.

   È ad esempio possibile impostare i punti rossi in modo che dopo 180 secondi si raggiunga una priorità del 100 percento. In questo caso i chiamanti normali con un tempo di attesa superiore a 180 secondi vengono trattati con gli stessi diritti dei chiamanti VIP. Le chiamate in arrivo di chiamanti VIP giunte da più tempo vengono trattate con priorità nella coda d'attesa.

   In alternativa è possibile inserire il valore per i singoli intervalli di attesa anche nel campo di input a destra accanto al grafico.

7) Fare clic su **Salva**.

18.6.2.17 Come modificare l'elenco chiamate VIP

Prerequisiti

Il chiamante incluso nell'Elenco chiamate VIP è presente nella rubrica esterna.

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.

4) Fare clic su **Elenco chiamate VIP**.
5) Selezionare la coda d'attesa desiderata e premere **Modifica**.
6) Selezionare una delle seguenti opzioni:
   - Se si desidera copiare un chiamante nell'elenco chiamate VIP, nella parte superiore della finestra, fare clic su **Aggiungi**. Selezionare la voce desiderata. Definire la priorità di questo chiamante VIP rispetto agli altri chiamanti VIP, spostando la barra di scorrimento sulla posizione desiderata. Spostando verso destra si aumenta la priorità.
   - Se si desidera copiare un tipo di numero di telefono nell'elenco chiamate VIP, nella parte inferiore della finestra, fare clic su **Aggiungi**. Nel campo Motivo inserire il tipo di numero di telefono (ad esempio `089 7577*`). Definire la priorità di tutti i chiamanti VIP di questo tipo di numero di telefono rispetto agli altri chiamanti VIP, spostando la barra di scorrimento sulla posizione desiderata. Spostando verso destra si aumenta la priorità.

     Non è possibile l'inserimento di tipi di numeri di telefono in formato canonico. Non è consentito neanche l'uso di prefissi internazionali abbreviati (ad esempio +49 anziché 0049). I tipi di numeri di telefono sono sempre privi di codice di linea urbana.

     Esempio per il tipo di numero di telefono: `089 7577*`(089 = prefisso interurbano di Monaco, 7577 = numero di sistema di un'azienda, * = carattere jolly per qualsiasi cifra). Digitando questo tipo di numero di telefono nell'elenco chiamate VIP tutti i chiamanti di Monaco il cui numero inizia con 7577 vengono trattati in modo preferenziale.

     I seguenti caratteri possono essere utilizzati in un tipo di numero di telefono come carattere jolly (segnaposto):

     – * = carattere jolly per qualsiasi numero
     – ? = carattere jolly per qualsiasi cifra
   - Se si desidera modificare una voce nell'elenco chiamate VIP, selezionare la voce desiderata e fare clic su **Modifica**. Modificare le impostazioni desiderate.
   - Se si desidera eliminare una voce dall'elenco chiamate VIP, selezionare la voce desiderata e fare clic su **Rimuovi**.
7) Fare clic su **Salva**.

18.6.2.18 Come impostare l'agente preferito

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Click on **Preferred Agents**.
5) Mark the desired queue and click **Edit**.
6) Mark the desired caller in the **Customers** area, which is the upper of the two tables.
7) Click on **Add Agent**.

8) Select the desired agent and click **Save**.

   The name of the selected agent is then shown in the **Preferred Agents** area.

9) If you want to define another agent as a preferred agent, repeat steps 7 and 8.

10) Nel caso vengano definiti più agenti preferiti, occorre definire le priorità dei singoli agenti. Sono disponibili le seguenti opzioni:

    - If you want to assign a higher priority, mark the desired agent and move that agent to a higher position in the list by using the **Move Up** button.
    - If you want to assign a lower priority, mark the desired agent and move that agent to a lower position in the list by using the **Move Down** button.

18.6.2.19 Come eliminare l'agente preferito

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Agenti preferiti**.
5) Selezionare la coda d'attesa desiderata e premere **Modifica**.
6) Nell'area **Agenti preferiti**, selezionare l'agente da eliminare.
7) Fare clic su **Rimuovi agente**.

18.6.2.20 Come aggiungere una pausa Contact Center

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Click on **Contact Center Breaks**.
5) Fare clic su **Aggiungi**.
6) Enter the name of the Contact Center break in the **Name** field.
7) Enter the duration of the Contact Center break in minutes in the **Duration (Minutes)** field.
8) Select the **Active** check box to activate the new Contact Center break system-wide.
9) Fare clic su **Salva**.
10) If you want to add another Contact Center break, repeat steps 5 through 9.

18.6.2.21 Come modificare una pausa del Contact Center

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Pause del Contact Center**.
5) Selezionare la pausa del Contact Center desiderata e fare clic su **Modifica**.
6) Modificare i parametri desiderati.
7) Selezionare una delle seguenti opzioni:
   - Se occorre mettere le pause a disposizione degli agenti del Contact Center, selezionare la casella di controllo **Attivo**.
   - Se non si desidera mettere le pause a disposizione degli agenti del Contact Center, deselezionare la casella di controllo **Attivo**.
8) Fare clic su **Salva**.

18.6.2.22 Come eliminare una pausa del Contact Center

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Click on **Contact Center Breaks**.
5) Mark the desired Contact Center Break and click **Remove**.

18.6.2.23 Come aggiungere il motivo per l'elaborazione per "Elaborazione semplice"

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Contact Center - Codici post-elaborazione**. Vengono visualizzate tutte le code d'attesa per le quali è stato definito un motivo per l'elaborazione per "Elaborazione semplice".
5) Fare clic su **Aggiungi**.

6) Selezionare dall'elenco a discesa **Coda** la coda d'attesa alla quale si vuole aggiungere un motivo per l'elaborazione.
7) Nel campo **Descrizione** specificare una descrizione per il nuovo motivo per l'elaborazione.
8) Fare clic su **Salva**.
9) Se si desidera aggiungere un altro motivo per l'elaborazione, ripetere i passi da 5 a 8.

18.6.2.24 Come modificare il motivo per l'elaborazione per "Elaborazione semplice"

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Contact Center - Codici post-elaborazione**. Vengono visualizzate tutte le code d'attesa per le quali è stato definito un motivo per l'elaborazione per "Elaborazione semplice".
5) Selezionare la voce desiderata e fare clic su **Modifica**.
6) Se si vuole assegnare il motivo per l'elaborazione a un'altra coda d'attesa, nell'elenco a discesa **Coda**, selezionare la nuova coda d'attesa.
7) Se si desidera modificare la descrizione del motivo per l'elaborazione, nel campo **Descrizione** inserire la nuova descrizione.
8) Fare clic su **Salva**.

18.6.2.25 Come eliminare il motivo per l'elaborazione per "Elaborazione semplice"

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Click on **Contact Center Wrapup Codes**. Vengono visualizzate tutte le code d'attesa per le quali è stato definito un motivo per l'elaborazione per "Elaborazione semplice".
5) Mark the desired entry and click **Remove**.

18.6.2.26 Come aggiungere il motivo per l'elaborazione per "Elaborazione multipla"

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Codice multielaborazione**.
5) Nell'elenco a discesa **Coda d'attesa Contact Center**, selezionare la coda d'attesa desiderata. Vengono visualizzati i gruppi e i sottogruppi già definiti per questa coda d'attesa.

   Nota: Sotto ogni gruppo o sottogruppo (se presente) deve essere configurato almeno un elemento, per consentire all'agente di elaborare una chiamata. L'elaborazione di una chiamata non è possibile se un gruppo o un sottogruppo è vuoto.

6) Se si desidera inserire il nuovo motivo per l'elaborazione in un gruppo con altri motivi per l'elaborazione, selezionare una delle seguenti opzioni:
   - Se si desidera assegnare il nuovo motivo per l'elaborazione a un gruppo o sottogruppo esistente, selezionare il gruppo o sottogruppo desiderato, quindi premere **Aggiungi elemento**. Nel campo **Nuovo elemento di elaborazione** immettere un nome per il nuovo motivo per l'elaborazione e fare clic su **OK**.
   - Se si desidera assegnare il nuovo motivo per l'elaborazione a un nuovo gruppo, fare clic su **Aggiungi gruppo**. Nel campo **Nome gruppo** immettere un nome per il nuovo gruppo e fare clic su **OK**.

     Selezionare il nuovo gruppo e fare clic su **Aggiungi elemento**. Nel campo **Nuovo elemento di elaborazione** immettere un nome per il nuovo motivo per l'elaborazione e fare clic su **OK**.
   - Se si desidera assegnare il nuovo motivo per l'elaborazione a un nuovo sottogruppo, selezionare il gruppo desiderato, quindi premere **Aggiungi gruppo**. Nel campo **Nome gruppo** immettere un nome per il nuovo sottogruppo e fare clic su **OK**.

     Selezionare il nuovo sottogruppo e fare clic su **Aggiungi elemento**. Nel campo **Nuovo elemento di elaborazione** immettere un nome per il nuovo motivo per l'elaborazione e fare clic su **OK**.
7) Se si desidera aggiungere un altro motivo per l'elaborazione, ripetere i passi da 5 a 6.

18.6.2.27 Come modificare il motivo per l'elaborazione per "Elaborazione multipla"

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Codice multielaborazione**.

5) Nell'elenco a discesa **Coda d'attesa Contact Center**, selezionare la coda d'attesa desiderata. Vengono visualizzati i gruppi e i sottogruppi già definiti per questa coda d'attesa.
6) Selezionare il gruppo o sottogruppo assegnato al motivo per l'elaborazione da modificare. Vengono visualizzati tutti i motivi per l'elaborazione (elementi), assegnati a questo gruppo.
7) Selezionare il motivo per l'elaborazione da modificare e fare clic su **Rinomina elemento**.
8) Nel campo **Rinomina codice elaborazione** immettere una descrizione per il motivo per l'elaborazione e fare clic su **OK**.
9) Se si desidera modificare la descrizione del gruppo o sottogruppo, fare clic su **Rinomina gruppo**.
10) Nel campo **Nome gruppo** immettere un nuovo nome per il gruppo o sottogruppo e fare clic su **OK**.

18.6.2.28 Come eliminare il motivo per l'elaborazione per "Elaborazione multipla"

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Codice multielaborazione**.
5) Nell'elenco a discesa **Coda d'attesa Contact Center**, selezionare la coda d'attesa desiderata. Vengono visualizzati i gruppi e i sottogruppi già definiti per questa coda d'attesa.
6) Selezionare il gruppo o sottogruppo assegnato al motivo per l'elaborazione da eliminare. Vengono visualizzati tutti i motivi per l'elaborazione (elementi), assegnati a questo gruppo.
7) Selezionare il motivo per l'elaborazione da eliminare e fare clic su **Rimuovi elemento**.
8) Se si desidera eliminare il gruppo o sottogruppo, fare clic su **Rimuovi gruppo**.

18.6.2.29 Come assegnare un agente alla coda di attesa

Con la procedura guidata **Contact Center** è possibile assegnare gli agenti a una o più code d'attesa.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.

3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.
4) Fare clic su **Associazioni coda**. Vengono visualizzate tutte le code d'attesa disponibili.
5) Selezionare la coda di attesa alla quale assegnare un agente e fare clic su **Modifica**. Vengono visualizzati tutti gli agenti assegnati.
6) Fare clic su **Aggiungi** per aggiungere l'agente appropriato alla coda desiderata. Viene visualizzata la finestra **Aggiungi**.
7) Selezionare una delle seguenti opzioni:
   - Se l'agente deve ricevere chiamate indipendentemente dal carico sulla coda, selezionare **Agente primario** dall'elenco a discesa **Tipo**.
   - Se l'agente deve ricevere chiamate solo in caso di overflow della coda d'attesa, selezionare **Agente di overflow** dall'elenco a discesa **Tipo**.
8) Se è stato selezionato **Agente di overflow**:
   a) Nel campo **Overflow dopo secondi in coda** indicare il tempo trascorso il quale una chiamata verrà inoltrata a un agente di overflow.
   b) Nel campo **Overflow dopo chiamate in coda** inserire il numero massimo di chiamate. Un agente di overflow riceverà le chiamate eccedenti tale numero massimo.
9) Inserire un valore percentuale per il **Livello interfaccia** dell'agente.

   Con il livello di competenza è possibile controllare la distribuzione delle chiamate agli agenti in una coda di attesa. Gli agenti con un livello di competenza più alto hanno la priorità nella distribuzione delle chiamate. Se tutti gli agenti hanno lo stesso livello interfaccia, l'agente che è libero da più tempo riceve la chiamata.
10) Selezionare una delle seguenti opzioni:
    - Se si desidera che l'agente riceva prenotazioni per richiamate sotto forma di messaggi vocali, selezionare la casella di controllo **Attiva richiamata agente**.
    - Se non si desidera che l'agente riceva prenotazioni per richiamate, deselezionare la casella di controllo **Attiva richiamata agente**.
11) Nel campo **Orario lavorativo** indicare l'orario lavorativo automatico in secondi per l'agente in questa coda d'attesa.
12) Fare clic su **Salva**.
13) Se si desidera assegnare altri agenti alle code d'attesa, ripetere i passi da 5 a 12.

18.6.2.30 Come eliminare un agente dalla coda di attesa

Con la procedura guidata **Contact Center** è possibile rimuovere gli agenti da una o più code d'attesa.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Contact Center**.

4) Fare clic su **Associazioni coda**. Vengono visualizzate tutte le code d'attesa disponibili.
5) Selezionare la coda di attesa dalla quale rimuovere un agente e fare clic su **Modifica**. Vengono visualizzati tutti gli agenti assegnati.
6) Selezionare l'agente desiderato e premere **Rimuovi**.
7) Se si desidera rimuovere altri agenti dalla coda d'attesa, ripetere i passi 5 e 6.

18.7 Istruzioni per l'uso del Contact Center

Vengono fornite informazioni sulle particolarità e sulle possibili limitazioni nell'uso del Contact Center.

18.7.1 Limitazioni sull'uso del Contact Center

Per l'uso del Contact Center si applicano le seguenti condizioni. Oltre a ciò, si applicano alcune limitazioni di utilizzo dei servizi del sistema da parte degli agenti.

Condizioni per l'uso del Contact Center

Per l'uso del Contact Center, è necessario rispettare le seguenti condizioni:

- Linee

  Il Contact Center non supporta le linee urbane analogiche (HKZ). Tutte le connessioni esterne del Contact Center devono avvenire tramite ISDN o telefonia IP. Occorre notare che l'integrazione tramite telefonia IP è possibile solo mediante provider di servizi di telefonia Internet (ITSP) certificati.
- Rete

  In una rete, tutti gli agenti devono essere connessi al sistema di comunicazione in cui è configurato il Contact Center.
- Telefoni degli agenti

  Gli agenti possono utilizzare tutti i telefoni del sistema (telefoni IP, (HFA), ad esempio OpenStage 40 o $U_{P0/E}$, quali il telefono OpenStage 40 T) e i telefoni DECT. Occorre notare che possono essere utilizzati esclusivamente i telefoni DECT attualmente approvati per l'uso con OpenScape Business Cordless.

  Non è possibile utilizzare i telefoni analogici, ISDN o SIP.

  Gli agenti non possono essere membri di un gruppo (chiamata di gruppo, gruppo di ricerca) o di un MULAP. Queste limitazioni si applicano anche ai servizi di sistema "Configurazione team (Gruppo Team)", "Direttore/ Segretaria (Gruppi Top)" e "Mobility Entry" utilizzati in combinazione con MULAP.
- myAgent

  myAgent non può essere utilizzato simultaneamente ad altri client UC, in quanto non si può escludere la possibilità di interferenze reciproche dello stato presenza (vedere Note per l'utilizzo contemporaneo di client myAgent e UC Suite). Durante il normale funzionamento del Contact Center, gli agenti utilizzano esclusivamente myAgent per modificare il proprio stato (accesso, disconnetti, disponibile, ecc.).

- Connessione di applicazioni tramite l'interfaccia CSTA

  È possibile la connessione di applicazioni mediante l'interfaccia CSTA, a condizione che vengano rispettate le seguenti condizioni:

  – L'applicazione non può aggiungere alcun carico di lavoro significativo all'interfaccia CSTA.

    Di conseguenza, non è consentita la connessione di soluzioni di comunicazione unificata o distribuzione delle chiamate, CTI Power Dialer o soluzioni CTI con molti client CTI singoli, a uso intensivo.
  – Tramite l'interfaccia CSTA, l'applicazione non può controllare i telefoni degli agenti o configurare le linee di tali telefoni.

    Di conseguenza non è consentita la connessione di applicazioni CTI per agenti, procedure guidate regole o assistenti personali.

  In linea di principio, la connessione di TAPI 120/170 è consentita. Per il carico di lavoro del sistema di comunicazione, si applicano le stesse condizioni del collegamento delle altre applicazioni tramite interfaccia CSTA. In combinazione con il Contact Center, TAPI 120/170 può essere utilizzato per la connessione a sistemi CRM (Customer Relationship Management) e ERP (Enterprise Ressource Planning), a condizione che questi supportino TAPI.

Limitazioni nell'uso dei servizi di sistema

I servizi di sistema indicati di seguito non sono disponibili per gli agenti o lo sono solo con limitazioni. Tuttavia, questi servizi non sono strettamente necessari per gli agenti, in quanto nel Contact Center l'assegnazione delle chiamate avviene normalmente. L'assegnazione dipende dalle regole impostate e dalla disponibilità degli agenti.

- Servizi bloccati

  L'attivazione delle funzioni del sistema tramite myAgent e il telefono dell'agente associato non è supportata dagli agenti del Contact Center. Gli agenti possono attivare i servizi del sistema solo tramite myAgent.

  Le seguenti funzioni del sistema non sono compatibili con myAgent:

  – Avviso di chiamata in attesa
  – Seconda chiamata
  – Parcheggio
  – Chiamata di gruppo
  – Non disturbare (per gli agenti connessi)
  – Inclusione nella conversazione di un agente (eccezione: agente con il livello di autorizzazione Supervisore o Amministratore)
  – Servizi relativi al routing delle chiamate e connessioni di chiamate attive

- Servizi con effetti sul routing delle chiamate

  I seguenti servizi possono produrre modifiche del routing delle chiamate nel Contact Center, pertanto non devono essere utilizzati dagli agenti.

  – Deviazione di chiamata

    Se un agente connesso attiva una deviazione di chiamata, si verifica una disconnessione.

    La deviazione di chiamata viene disattivata non appena un agente si connette a una coda d'attesa.
  – Non disturbare

    Se un agente connesso attiva la funzione Non disturbare su un client di comunicazione unificata, si verifica una disconnessione.

    La funzione Non disturbare viene disattivata non appena un agente si connette a una coda d'attesa.
  – Trasferimento

    Con lo spostamento di un telefono, viene modificata l'assegnazione logistica dei numeri di telefono. La nuova assegnazione dei numeri di telefono viene trasmessa al successivo avvio del Contact Center.
  – Servizio notturno

    In fase di configurazione del servizio notturno nel sistema di comunicazione, occorre assicurarsi che la configurazione dei parametri rilevanti per il Contact Center (agenti, code d'attesa ecc.) del servizio diurno e notturno siano impostati sugli stessi valori.
- Servizi con effetti sui rapporti

  L'esecuzione dei seguenti servizi dal telefono di un agente può portare a un'alterazione dei rapporti.

  – Risposta per assente delle chiamate del Contact Center da parte di non agenti
  – Trasferta (ad esempio tramite il tasto chiamata diretta) delle chiamate del Contact Center a non agenti
  – Conferenza
  – Richiamata alternata
  – Parcheggio

  Suggerimento: Il servizio "consultazione" è neutro ai fini della rappresentazione delle chiamate del Contact Center nei rapporti, può quindi essere utilizzato dagli agenti, indipendentemente dalla destinazione per consultazione.
- Funzioni non utili per gli agenti

  Le seguenti funzioni non sono utili per gli agenti, poiché per questi ultimi il servizio "Avviso di chiamata in attesa" è bloccato.

  – Posto operatore
  – Destinazione hotline

18.8 Note per l'uso dei telefoni DECT

I telefoni DECT possono essere utilizzati come telefoni per gli agenti del Contact Center. Occorre rispettare le differenze nella procedura operativa rispetto agli apparecchi telefonici fissi.

Requisiti per l'utilizzo di telefoni DECT

- Possono essere utilizzati solo i telefoni DECT attualmente approvati per l'uso con HiPath Cordless Office e OpenScape Business Cordless.
- L'area nella quale si trovano gli agenti del Contact Center deve assicurare una completa copertura wireless.
- Il numero della stazione base deve essere tale che siano disponibili canali B in quantità sufficiente per i telefoni DECT degli agenti del Contact Center.
- Ove possibile, un agente del Contact Center non dovrebbe uscire dalla portata del segnale wireless mentre è connesso a una coda d'attesa del Contact Center.

Differenze nella procedura operativa rispetto agli apparecchi telefonici fissi

- L'accesso a una coda d'attesa del Contact Center è possibile esclusivamente tramite myAgent.
- Nel display di un telefono DECT non vengono visualizzati messaggi quali **Disponibile** o **Pausa**.
- Non è possibile controllare un telefono DECT tramite myAgent (ad esempio tramite l'area **Telefonia** o la finestra popup delle chiamate in arrivo di myAgent).
- La risposta a una chiamata in arrivo è possibile esclusivamente tramite il telefono DECT.
- Una chiamata in uscita deve essere eseguita tramite telefono DECT.

Aspetti da considerare quando si utilizzano i telefoni DECT:

- Tempo di ricerca

  All'arrivo di una chiamata, il tempo richiesto per l'individuazione del telefono DECT (quindi precedente alla segnalazione della chiamata sul telefono DECT stesso), può essere di svariati secondi, fino a 20 secondi. Durante il tempo di ricerca, per il chiamante viene riprodotto il tono di chiamata.

  Il Contact Center considera questo arco di tempo come periodo precedente alla risposta alla chiamata. Il tempo effettivo prima dell'accettazione della chiamata da parte di un agente del Contact Center è composto dal tempo di ricerca e da quello di avviso.

  Se un agente del Contact Center esce dalla portata del segnale wireless con il suo telefono DECT, ciò può incrementare i tempi di ricerca.
- Impossibile trovare il telefono DECT

  Se una chiamata del Contact Center supera il tempo previsto per la risposta a una chiamata da parte dell'agente (ad esempio perché l'agente del Contact Center non si trova entro la portata del segnale), l'agente viene automaticamente disconnesso dalla coda o code d'attesa in questione. Il successivo accesso è possibile solo tramite myAgent.

18.9 Rapporti

I rapporti consentono di rilevare lo stato attuale del Contact Center e di analizzare i punti di forza e di debolezza dei componenti associati. Ciò consente ad esempio una configurazione ottimizzata del Contact Center e un uso più efficiente delle risorse del Contact Center. Il Contact Center fornisce agli utenti sia rapporti in tempo reale sia rapporti storici.

Rapporti in tempo reale

I rapporti in tempo reale vengono aggiornati continuamente. Forniscono informazioni importanti, ad esempio sul carico di lavoro degli agenti, sul grado di servizio, sui tassi di interruzione e sui tempi medi di elaborazione. Sulla base delle liste delle chiamate, costantemente aggiornate e filtrabili, è possibile consultare la cronologia di un contatto cliente. Inoltre è possibile esaminare l'attività di tutti gli agenti. Queste informazioni possono essere utili ad esempio per attività di formazione nonché verifica e tracciamento dei contatti.

Gli agenti con il livello di autorizzazione Supervisore o Amministratore possono ricevere un avviso acustico o visivo quando vengono superate delle grandezze definibili. È possibile determinare i valori di soglia individualmente per ogni coda di attesa.

Rapporti storici

Scegliendo degli elementi di dati e dei parametri rapporto specifici dell'utente è possibile configurare rapidamente rapporti storici e richiamarli in formato grafico o tabellare.

L'applicazione myAgent mette a disposizione oltre 20 modelli di rapporti predefiniti per i rapporti predefiniti.

L'applicazione opzionale myReports amplia le possibilità di creazione di rapporti storici grazie a oltre 100 modelli di rapporti predefiniti. È possibile pianificare la generazione di rapporti singolarmente e i rapporti creati possono essere inviati automaticamente a intervalli configurati nei formati di esportazione più diffusi a destinatari e-mail preconfigurati o salvati in un percorso configurato dall'amministratore di myReports.

Suggerimento: I rapporti si basano sulla cronologia chiamate salvata nel sistema di comunicazione. Il massimo tempo di conservazione della cronologia chiamate corrisponde a 365 giorni (impostazione predefinita). Un amministratore con il profilo **Expert** può definire il tempo di conservazione della cronologia chiamate a livello di sistema.

Esempio: il tempo di conservazione è stato impostato su 100 giorni. Per la creazione di rapporti, è pertanto possibile accedere ai dati storici relativi al massimo ai 100 giorni precedenti.

Protezione dei dati

Se per la configurazione di myReports, l'amministratore di myReports ha attivato la protezione dei dati, in tutti i rapporti le ultime quattro cifre del numero di telefono (colonna CLI) verranno sostituite da ****.

Se un utente ha impostato il proprio numero abitazione, numero cellulare, numero di telefono esterno 1 e/o numero di telefono esterno 2 come non visibile, nei rapporti non verranno mostrati tali numeri.

18.9.1 Modelli di rapporti predefiniti

myReports mette a disposizione oltre 100 modelli di rapporti predefiniti per la creazione di rapporti.

Questi modelli sono suddivisi nei seguenti temi (gruppi di rapporti):

- **Attività agente**
- **Agenti**
- **CLI**
- **Cronologia chiamate**
- **Chiamate**
- **Fax/e-mail**
- **Altri**
- **Prestazioni**
- **Code d'attesa**
- **Stato presenza utente**
- **Codici post-elaborazione**

19 Mobilità

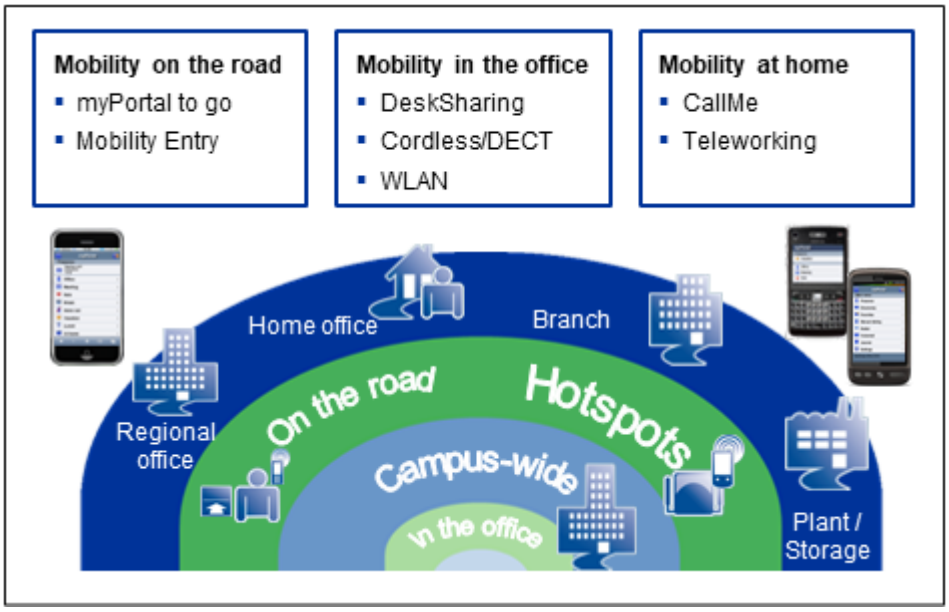
OpenScape Business offre soluzioni di mobilità integrata per ogni azienda. Tali soluzioni comprendono ad esempio l'integrazione di cellulari/smartphone, l'uso di telefoni cordless/DECT e WLAN, nonché funzionalità di desk sharing e telelavoro. Le funzioni di mobilità sono disponibili in tre ambiti: in viaggio, in ufficio e a casa.

Concetti correlati

Utenti alla pagina 419

19.1 Soluzioni di mobilità integrata

Le soluzioni per la mobilità integrate nel sistema di comunicazione offrono funzioni di comunicazione efficienti, sia in generale che con i terminali più diversificati.



19.2 Mobilità in viaggio

Per assicurare la mobilità durante i viaggi è possibile sfruttare funzioni quali l'integrazione nel sistema del cellulare tramite myPortal to go o Mobility Entry. Con il servizio One Number l'utente è raggiungibile in tutto il mondo con un solo numero di telefono. Inoltre, la telefonia dual mode consente di risparmiare sui costi quando l'utente si trova in una zona coperta da una rete WLAN.

La mobilità in viaggio è data da una combinazione di:

- Telefono dell'ufficio e smartphone (myPortal to go)
  - Reperibilità con un solo numero di telefono (servizio One Number)
  - Controllo delle funzioni tramite client Web
  - Funzioni UC quali il controllo dello stato presenza

- Telefono dell'ufficio e cellulare (Mobility Entry)
  - Reperibilità con un solo numero di telefono (servizio One Number
  - Controllo delle funzioni tramite codici DTMF

Oltre alla combinazione di telefono cellulare e telefono dell'ufficio, è anche possibile configurare il solo telefono cellulare (ovvero, senza telefono dell'ufficio in parallelo) rendendolo raggiungibile tramite un numero di rete fissa.

Tutte le funzionalità sono disponibili con i telefoni di sistema (HFA). I telefoni SIP possono essere utilizzati con alcune limitazioni.

19.2.1 myPortal to go

myPortal to go è un'applicazione potente di comunicazione unificate per smartphone e tablet PC che offre al partecipante l'accesso ai servizi Unified Communications del sistema di comunicazione. Oltre ai pratici ausili per la composizione dei numeri di telefono, quali rubriche, Preferiti e informazioni sullo stato presenza degli utenti, consente ad esempio l'accesso ai messaggi vocali.

myPortal to go è disponibile in tre versioni:

- As a Mobile UC App for the Android operating system (version 5.0 or higher)
- As a Mobile UC App for the Apple iOS operating system (version 12.5 or higher)
- come Web Edition per i browser Web mobili con supporto per HTML5, ad esempio per i sistemi operativi di Windows Phone (versione 8.0 o successiva) o Blackberry (versione 10 o successiva):

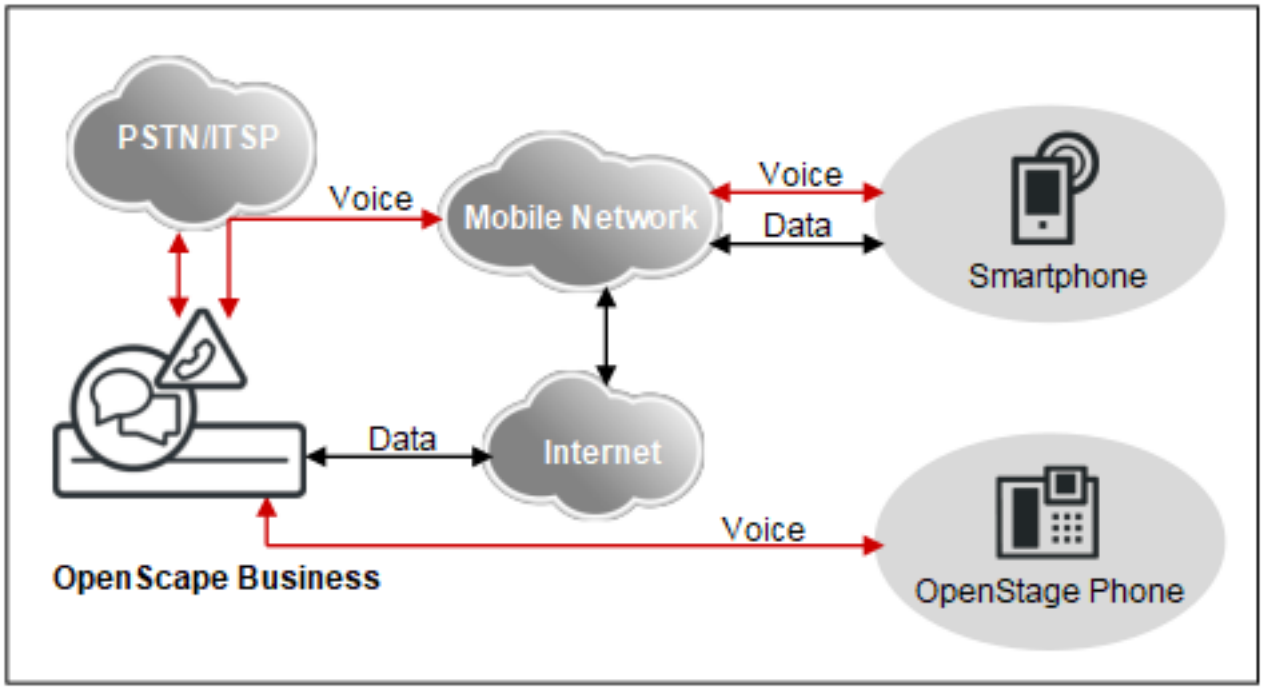
  `http://<Indirizzo IP del sistema di comunicazione>:8801`

  `https://<Indirizzo IP del sistema di comunicazione>:8802`

  Per motivi di sicurezza, si consiglia di utilizzare esclusivamente https. A tale fine è necessario configurare nel router l'inoltro della porta da TCP/443 esterno verso TCP/8802 interno.

  Nota: Utilizzando myPortal to go Web Edition in modalità Telefono scrivania non è possibile telefonare dal client. È possibile effettuare chiamate ma il payload passa attraverso il telefono da scrivania collegato.

myPortal to go può essere utilizzato con telefoni cellulari GSM puri e con telefoni dual mode. Per l'uso di myPortal to go è necessario disporre di un contratto di telefonia mobile con l'opzione dati (si consiglia una tariffa flat).



I servizi offerti sono gli stessi per tutte e tre le versioni, con piccole eccezioni (ad esempio l'accesso ai dati dei contatti nel telefono cellulare).

myPortal to go supporta i servizi seguenti:

- Stato presenza
- Deviazione di chiamata basata sullo stato
- Servizio CallMe (solo con UC Suite)
- Rubriche
- Elenco dei Preferiti
- Diario
- Ricerca del numero di telefono e del nome
- Funzioni chiamata
- One Number Service (ONS)
- Casella vocale
- Messaggi di testo

Servizi CTI durante una conversazione:

- Consultazione
- Richiamata alternata
- Commutazione
- Conferenze
- Disconnetti

myPortal to go può essere utilizzato sia con le soluzioni UC Smart che UC Suite. L'offerta dei servizi può variare leggermente in base alla soluzione UC e alle licenze assegnate.

myPortal to go supporta i seguenti tipi di servizi:

- Mobility:

  Accesso illimitato ai servizi di telefonia e UC, indipendentemente dalla località (incl. One Number Service).

- Utente Office:

  Utilizzo dei servizi UC come un comodo ausilio per la composizione sui telefoni dell'ufficio (senza One Number Service).

Con i client UC (ad esempio myPortal for Desktop) sono disponibili anche altri servizi

myPortal to go stabilisce una connessione crittografata (HTTPS) con OpenScape Business UC Server. Se la connessione viene interrotta (modalità offline) è ancora possibile selezionare un numero dalle voci salvate temporaneamente del diario e dall'elenco dei Preferiti in base al GSM, quindi comporre manualmente il numero tramite GSM.

Nota: A supporto della mobilità, è prima necessario registrare myPortal to go come utente VoIP (HFA), in modo da attivare la porta appropriata sul sistema Openscape Business.

Tipo di selezione per myPortal to go

Per le chiamate in uscita, l'utente di uno Smartphone può scegliere tra più modalità di composizione, in base al tipo di servizio:

- Call through (solo nella modalità Mobility)
- Richiamata automatica preferita (solo per la modalità utente mobile)
- Selezione associata (solo nella modalità Telefono scrivania)

  myPortal to go controlla la connessione del telefono nella postazione di lavoro. Se tramite la composizione associata viene controllato un telefono SIP o un soft client SIP, alcuni servizi CTI, ad esempio la consultazione e la conferenza, non sono disponibili.

19.2.1.1 Requisiti richiesti permyPortal to go

Per poter utilizzare myPortal to go, lo smartphone deve disporre di una dotazione hardware e software adeguata.

Sono validi i seguenti requisiti:

- myPortal to go come UC Mobile App: Sistema operativo Android (versione 5.0 o successive) o Apple iOS (versione 12.5 o successive)
- myPortal to go (Web Edition): per i browser Web mobili con supporto per HTML5, ad esempio per i sistemi operativi di Windows Phone (versione 8.1 o successiva) o Blackberry (versione 10 o successiva). I browser Web senza supporto di TLS 1.2 non sono più compatibili.

  Per l'accesso è necessario configurare nel router l'inoltro della porta da TCP/443 esterno verso TCP/8802 (https) interno o TCP/8801 (http). Per motivi di sicurezza, si consiglia di utilizzare esclusivamente https.
- Client iOS myPortal to go:
  - È necessario configurare un server DNS appropriato e concedere l'accesso a Internet in modo che i nomi dei domini pubblici possano essere risolti e i messaggi di notifica push possano essere inviati al dispositivo iOS tramite i server APNS di Apple.
  - Se il firewall aziendale limita l'accesso a Internet in uscita, verificare che il firewall sia aperto per APNS sulla porta TCP/443.

  - Per le notifiche push iOS, è obbligatorio mantenere aggiornato il software di sistema, dato che i certificati obbligatori per la comunicazione con il servizio APNS di Apple verranno aggiornati frequentemente con le versioni principali/secondarie del sistema e le versioni di correzione.
  - Le ultime versioni di myPortal to go (iOS) supportano l'API CallKit di Apple. CallKit è un framework che mira a migliorare l'esperienza VoIP consentendo a myPortal to go (iOS) di integrarsi con le funzionalità di chiamata native del dispositivo. La versione minima del software di sistema richiesta è V3R2.

    Gli attuali client myPortal to go (iOS) non saranno in grado di accedere alle versioni precedenti di OpenScape Business.
  - Quando si esegue la connessione al server di comunicazione, si applicano i requisiti di sicurezza iOS. Il certificato autofirmato corrente generato automaticamente da Openscape Business non è sufficiente se l'app si connette al server di comunicazione utilizzando un nome di dominio anziché un indirizzo IP del server. Apple ha rivisto i propri requisiti di sicurezza per i certificati server TLS https://support.apple.com/it-it/103769.

    Per evitare problemi quando myPortal to go (iOS) non riesce a stabilire una connessione con il server di comunicazione, si consiglia di connettersi al server di comunicazione tramite l'indirizzo IP o di installare un certificato SSL affidabile sul lato server.
- Touch-screen (consigliato per un impiego confortevole)
- Risoluzione per smartphone di almeno 240 pixel x 320 pixel (consigliata: 320 pixel x 480 pixel o superiore)
- Risoluzione per PC tablet di almeno 800 pixel x 480 pixel (consigliata: 1024 pixel x 600 pixel o superiore)
- Accesso a Internet
- Supporto della trasmissione simultanea di voce e dati tramite cellulare e rete mobile
- Una connessione dati 3G/4G/5G stabile. Tenere presente che le connessioni lente, in particolare 2G/EDGE/GPRS, possono portare a un'esperienza utente scadente e a limitazioni funzionali (VoIP).

  In alternativa: connessione WLAN pura con client SIP per la telefonia.
- Si consiglia vivamente un piano dati a tariffa fissa.

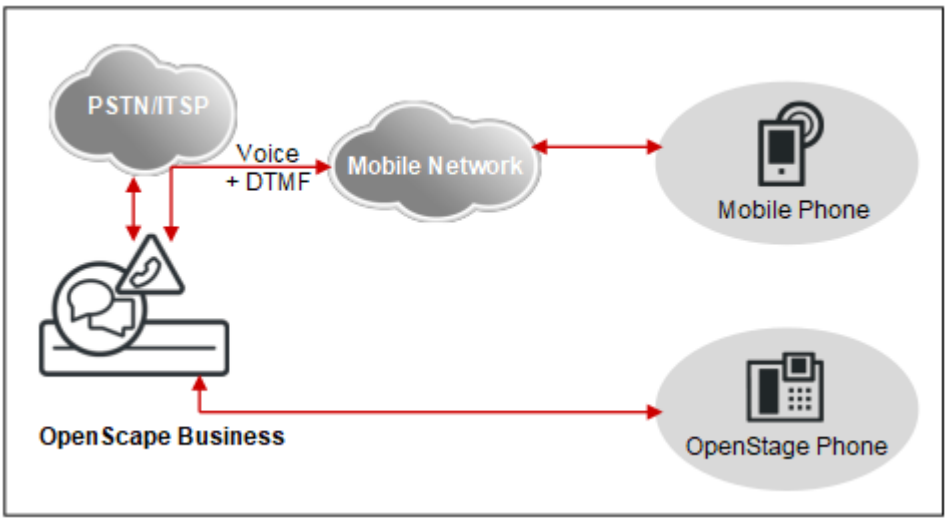
La app Mobile UC può essere scaricata gratuitamente da Google Play Store o dall'App Store di Apple.

A seconda del dispositivo utilizzato e del sistema operativo, è possibile influenzare il funzionamento ed ottimizzare l'impiego. L'assistenza è assicurata solo se il problema con il dispositivo di riferimento è dimostrabile. Per ulteriori informazioni su dispositivi di riferimento, browser e sistemi operativi, consultare le note sulla versione e gli Experts Wiki alla pagina `https://wiki.unify.com/wiki/myPortal_to_go`.

19.2.2 Mobility Entry

Grazie a Mobility Entry è possibile integrare i telefoni cellulari. In questo modo, l'utente ha accesso a servizi specifici del sistema tramite il cellulare.

Mobility Entry consente agli utenti, dopo l'accesso, il controllo di connessioni voce tramite DTMF.



Tipo di selezione di Mobility Entry

Per le chiamate in uscita, l'utente di un cellulare può scegliere tra più modalità di composizione.

Mobility Entry offre il seguente tipo di selezione:

- Richiamata automatica
- Call-through

Se un utente di un cellulare del sistema di comunicazione chiama un numero DISA speciale con una richiamata automatica, la chiamata viene automaticamente terminata prima di stabilire la connessione e la richiamata viene eseguita immediatamente. Dopo la richiamata automatica, non è necessaria alcuna ulteriore autorizzazione. L'utente con numero di cellulare può eseguire chiamate interne ed esterne e utilizzare tutti i servizi Mobility tramite il sistema di comunicazione.

Requisiti richiesti per la richiamata automatica:

- Il numero di telefono esterno del chiamante è registrato e configurato nel sistema di comunicazione. In caso contrario, la chiamata viene interrotta e non viene eseguita alcuna richiamata.
- Il numero DISA è configurato.
- Il numero di telefono esterno dell'utente mobile viene importato nel sistema di comunicazione (informazione CLIP).

Servizi in stato di riposo

- Composizione del numero di telefono
- Programmazione o cancellazione della deviazione di chiamata
- Attivazione/disattivazione funzione Non disturbare
- Invio Info
- Reset di tutti i servizi
- Attivazione/disattivazione della visualizzazione del numero di telefono (CLIR)

Servizi durante una conversazione

- Consultazione
- Richiamata alternata
- Conferenza

- Interruzione e ritorno alla chiamata in attesa
- Attiva richiamata
- Consentire la post-selezione DTMF

Per la segnalazione delle funzioni vengono utilizzati dei codici di sistema (ad esempio *1 si riferisce alla programmazione del trasferimento di chiamata).

Nota: Per gli utenti Mobility Entry, il flag utente **Autorizzazione Disa** deve essere attivato.

Con OpenScape Business X sono disponibili un massimo di 16 risorse DTMF code receiver, ovvero è possibile riservare contemporaneamente un massimo di 16 utenti (analogici, Mobility ecc.). Gli utenti che hanno selezionato il flag **Funzione di attivazione basata su DTMF**, riservano ciascuno un code receiver per la durata della chiamata.

Con OpenScape Business S, è supportato il controllo delle funzioni tramite codici DTMF se le cifre DTMF vengono trasmesse secondo RFC 2833. Se la rete utilizza un Session Border Controller (SBC), non è possibile alcun rilevamento DTMF.

Nota: La voce Mobility deve essere configurata solo sui nodi con accesso CO diretto.

Concetti correlati

Servizio One Number alla pagina 953
Confronto tra client mobile e Mobility Entry alla pagina 950
Dipendenze per Mobility Client e Mobility Entry alla pagina 952

19.2.3 Confronto tra client mobile e Mobility Entry

I client mobili myPortal for Mobile, myPortal to go e Mobility Entry supportano servizi diversi.

Servizio	**myPortal to go**	Mobility Entry
Funzioni generali		
Contratto di telefonia mobile con opzione dati	sì (tariffa flatrate consigliata)	No
Segnalazione della chiamata in parallelo al telefono di sistema e al cellulare (Twinning)	Sì	Sì
Trasmissione del numero di telefono del chiamante al cellulare (se la rete trasmette i numeri di telefono esterni come CLIP, CLIP no screening)	Sì	Sì
Servizio One Number (se la rete trasmette i numeri di telefono esterni come CLIP, CLIP no screening))	Sì	Sì
Non disturbare/Inoltro di chiamata disattivabile	No	Sì

Servizio	**myPortal to go**	Mobility Entry
Visualizzazione del numero di telefono attivabile/disattivabile	No	Sì
Identificazione automatica degli utenti registrati	Sì	Sì
Uso senza telefono d'ufficio (come utente virtuale)	Sì	Sì
Utile con il sistema OpenScape Business S	Sì	Sì
Stato presenza, diario, casella vocale		
Modifica del proprio stato presenza	Sì	No
Visualizzazione dello stato presenza di altri utenti	Sì	No
Diario	Nuove, Tutte, Perse, Accettate, In arrivo, Messaggi vocali	No
Casella vocale comune, può essere controllata anche in viaggio	Sì	Sì
Visualizzazione dei messaggi vocali ricevuti	Visualizzazione di messaggi vocali nuovi, ascoltati e salvati	No
Componi		
Accesso ai contatti sul telefono cellulare	Sì	Sì
Accesso ai contatti nel sistema di comunicazione	Rubrica esterna (UC Suite), rubrica interna, contatti personali e rubrica di sistema	No
Preferiti	Sì	No
Composizione manuale	Sì	Sì
Ripetizione della selezione	Sì	No
Tipo di selezione	Richiamata automatica, Call-through, Selezione associata	Richiamata automatica, Call-through
Durante la chiamata		
Consultazione	sì (non con telefono SIP)	Sì
Richiamata alternata	sì (non con telefono SIP)	Sì
Commutazione	sì (non con telefono SIP)	Sì
Conferenza	sì (non con telefono SIP)	Sì

Servizio	myPortal to go	Mobility Entry
Richiamata automatica su libero e su occupato	No	Sì
Risposta alle chiamate del cellulare sul telefono di sistema	Sì	Sì
Segnalazione di occupato anche in caso di con chiamate al cellulare (con servizio One Number)	Sì	Sì

Concetti correlati

Mobility Entry alla pagina 948

19.2.4 Dipendenze per Mobility Client e Mobility Entry

myPortal to go e Mobility Entry presentano dipendenze da altri servizi (ad esempio, DISA).

Dipendenza	myPortal to go	Mobility Entry
DID Mobility Callback	Con la modalità di composizione Callback Mobility, è necessario configurare il numero DID di richiamata automatica Mobility.	
Numero telefonico di destinazione esterno	La composizione di numeri telefonici di destinazione esterna per gli utenti mobili viene attivata sulla base della configurazione LCR. È possibile utilizzare la rete fissa ISDN, la rete fissa analogica o un ITSP.	
Attivazione CLIP no screening	Per poter visualizzare il numero del chiamante sul display degli apparecchi mobili, questo deve essere fornito come non verificato dal provider di rete.	
CLIP dell'utente mobile	Il CLIP dell'utente mobile deve essere trasmesso al sistema di comunicazione. Tale servizio deve essere messo a disposizione dal provider di rete.	
Amministrazione LCR	Poiché alcuni provider di rete (fissa o ITSP) non accettano numeri telefonici di destinazione con un proprio prefisso internazionale, il sistema abbrevia tali numeri eliminando il prefisso. Questo aspetto viene gestito dal Least Cost Routing (LCR).	
Canali B/connessioni esterne	Il numero di canali B dipende dalla durata della connessione o dal numero degli utenti mobili. Tutte le chiamate esterne in arrivo per un apparecchio mobile avvengono su 2 canali voce del sistema. Se non è disponibile un numero sufficiente di canali voce aggiuntivi, la raggiungibilità dell'utente mobile non è garantita e l'utente mobile stesso non può effettuare chiamate senza il servizio One Number.	
Numeri di emergenza	Quando un utente mobile compone un numero di emergenza tramite il sistema di comunicazione, non è possibile trasmettere la località del suo telefono cellulare. È quindi consigliabile comporre direttamente un numero di emergenza.	
Composizione di un numero interno	Per selezionare numeri interi tramite un apparecchio mobile in formato internazionale (ad es. 00039029100) deve essere stato configurato il numero della sede del sistema di comunicazione. Diversamente, le destinazioni interne verrebbero chiamate tramite la linea urbana, quindi generando costi.	

Dipendenza	myPortal to go	Mobility Entry
Manutenzione delle rubriche	Per assicurare la reperibilità degli interlocutori con tutte le modalità di selezione quando si compone un numero a partire dalla rubrica, è importante che i numeri di telefono siano stati inseriti in formato canonico (ad es.:. +49 89 100).	-
Firewall	Viene stabilita una connessione su un canale dati al server Web integrato del sistema di comunicazione. A tal fine è necessario che nel firewall venga configurato l'inoltro alla porta 8801 (HTTP) o 8802 (HTTPS). Tuttavia, si raccomanda di non configurare alcun inoltro per la porta 8803 (https) per l'accesso a UC Smart Assistant.	-
Connessione dati	Si consiglia di stipulare un contratto di telefonia mobile con una tariffa dati flat. Se si utilizzano tariffe basate sul volume, è opportuno disattivare l'opzione "Aggiornamento automatico" nelle impostazioni di myPortal to go.	-
Chiamate parallele	Per alcuni servizi sono necessarie connessioni vocali e dati in contemporanea. Questa caratteristica deve essere supportata sia dall'operatore di rete che dai terminali mobili.	-
Creazione della connessione dal sistema di comunicazione all'utente mobile su	Tutti i tipi di linee	Tutti i tipi di linee che supportano la trasmissione DTMF.

Concetti correlati

Mobility Entry alla pagina 948

19.2.5 Servizio One Number

Con il servizio One Number (ONS), un numero di cellulare viene utilizzato come un numero di rete fissa. L'utente può essere raggiunto e identificato in tutto il mondo con un unico numero, ovvero il proprio numero di rete fissa.

Mediante l'impostazione di una configurazione team, è possibile usare il servizio One Number, consente di disporre di un numero di telefono unico per l'ufficio (telefono di sistema) e il cellulare. Il chiamante compone il numero del telefono del sistema (rete fissa). Le chiamate in uscita eseguite dal cellulare vengono segnalate all'utente chiamato con il numero di rete fissa. Un ulteriore vantaggio del servizio One Number è la visualizzazione di occupato per gli utenti mobili.

Concetti correlati

Mobility Entry alla pagina 948

19.2.6 Telefonia dual mode

I telefoni cellulari dual mode supportano sia reti GSM/UMTS che WLAN. La registrazione presso il sistema di comunicazione è possibile tramite una WLAN, sia come utente SIP che come client di sistema (utente HFA).

Se il telefono cellulare dual mode si trova entro la portata della WLAN, questo verrà automaticamente chiamato come client di sistema (utenti HFA) o come utente SIP. Al di fuori della portata della WLAN, tale telefono potrà essere chiamato tramite GSM/UMTS (è possibile utilizzare la funzionalità di integrazione con il numero di cellulare).

Nota: Dual mode per HFA è supportata solo quando si utilizza il client myPortal to go e non con altri dispositivi o client.

L'inoltro automatico al numero di telefono GSM funziona solo se il relativo utente HFA o SIP è registrato nel sistema come terminale telefono cellulare (integrazione telefono cellulare). Di conseguenza, se l'utente di telefonia HFA o SIP è registrato, viene chiamato come utente di telefonia HFA o SIP e se non lo è, viene chiamato tramite il numero di telefono GSM assegnato nella configurazione Integrazione cellulare. Le funzioni di chiamata CTI per client SIP non sono disponibili in myPortal to go. Per il controllo è eventualmente possibile utilizzare il client HFA o SIP (vedere anche la release note e `http://wiki.unify.com`).

All'interno dell'area aziendale, le conversazioni avvengono tramite WLAN. Telefonando mediante WLAN, i telefoni cellulari non generano addebiti sulla bolletta. Le funzioni di handover (passaggio) e roaming sono supportate entro la portata della WLAN (se tale infrastruttura è di tipo adatto), tuttavia tali servizi non sono utilizzabili da WLAN a GSM e viceversa.

19.2.7 Konfiguration von myPortal to go und Mobility Entry

myPortal to go (Web Edition) e Mobility Entry sono configurati con la procedura guidata **Integrazione con il numero di cellulare**.

La procedura guidata **Integrazione con il numero di cellulare** consente all'amministratore quanto segue:

- Configurazione del servizio One Number
- Configurazione di myPortal to go (Web Edition)
- Configurazione di Mobility Entry
- Configurazione di telefoni dual mode

L'integrazione dei telefoni portatili con i telefoni GSM viene eseguita tramite gli utenti virtuali. In questo modo è possibile trasferire i servizi all'utente mobile. A ciascun utente dotato di una corrispondente licenza (Mobility User) può essere assegnato un solo utente mobile

Modalità di funzionamento dei telefoni cellulari

Sono implementate le seguenti modalità funzionamento per telefoni cellulari:

- **Modalità GSM**

  Una chiamata del numero di telefono mobile interno viene segnalata sul cellulare GSM.
- **Modalità WLAN**

  Se il telefono cellulare WLAN è accessibile tramite WLAN, la chiamata avviene tramite WLAN. Se la WLAN non è accessibile, la chiamata avviene tramite GSM.

Twinning

Una chiamata viene segnalata in parallelo al telefono mobile e al cellulare GSM (Twinning). Per realizzare funzioni Twinning, è necessario definire una configurazione team dopo la configurazione dell'**Integrazione telefono cellulare**. A tal fine, utilizzare la procedura guidata **Configurazione team** e selezionare come primo telefono il numero telefonico per il quale deve avvenire la segnalazione parallela. Per l'utilizzo di myPortal to go (Web Edition) l'ultimo passaggio della procedura guidata **Integrazione telefono cellulare** consiste nel riconfigurare il nome utente con il gruppo Team. Nel telefono di sistema, è possibile programmare un tasto diretto per richiamare l'utente Mobility per consentire la risposta di chiamate da cellulari senza interruzione. Tutte le funzionalità sono disponibili con i telefoni di sistema (HFA). I telefoni SIP possono essere utilizzati con alcune limitazioni, ad esempio non è supportato il tasto MULAP.

Concetti correlati

Impostazione di funzioni Configurazione team / Gruppo Team e Direttore/ Segretaria / Gruppi Top tramite procedure guidate alla pagina 709

Requisiti per l'uso di Application Launcher alla pagina 1188

19.2.7.1 Come integrare un cellulare GSM

Con la procedura guidata **Integrazione con il numero di cellulare** è possibile integrare i telefoni cellulari nel sistema di comunicazione.

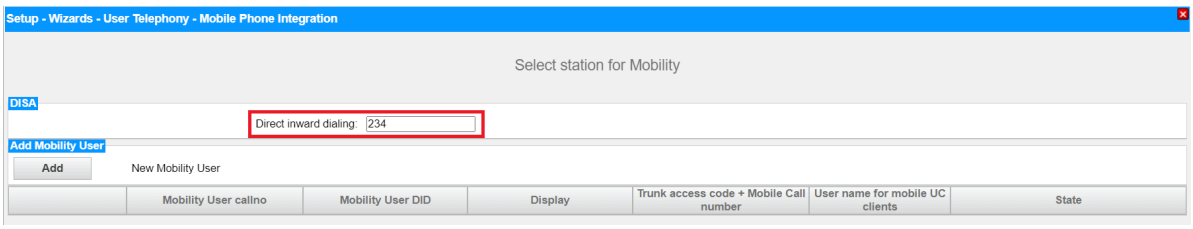
Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Integrazione con il numero di cellulare**. Viene visualizzata la finestra **Seleziona utente per Mobility**.

4) In **Porta DISA**, selezionare o inserire il numero di **Selezione passante** con cui gli utenti mobili possono accedere al sistema di comunicazione.



Nota: DISA è necessario per l'uso di Mobility Entry (controllo del sistema mediante DTMF) e di myPortal for Mobile (solo con la funzione Call-through).

5) Fare clic su **Aggiungi** o **Modifica** in corrispondenza dell'utente di cui si desidera integrare il numero di cellulare GSM nel sistema di comunicazione. Viene visualizzata la finestra **Assegnazione utente Mobility**.

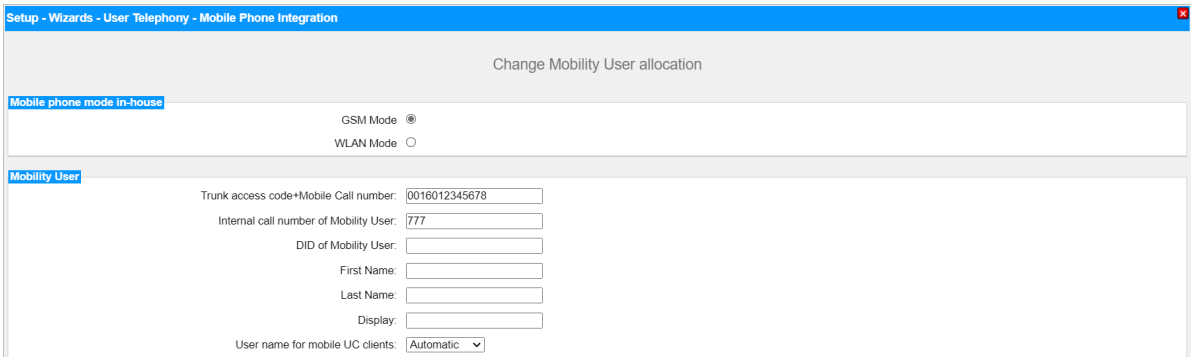
6) Selezionare **Modalità GSM** come modalità di funzionamento del cellulare.

7) Nei campi **Codice di accesso alla linea esterna+Numero di telefono cellulare** inserire il numero del telefono cellulare (ad esempio, 0016012345678).

8) Inserire il **Numero di telefono interno utente Mobility** (ad esempio 777), un **Nome interno** a scelta e il **MSN**. Fare attenzione che il numero interno scelto non sia già stato assegnato.

: Se si desidera utilizzare il numero di interno 879, 890 o 891, occorre configurare l'impostazione tramite Manager E e non tramite WBM.

9) Nell'elenco a discesa **Nome utente per myPortal to go (Web Edition)** selezionare la voce **Non monitorata** (con questa selezione, come nome utente viene assegnato il numero interno dell'utente).



10) Solo con UC Smart: se necessario, assegnare all'utente una casella di posta:
    a) Dal menu a discesa, selezionare **Tipo mailbox UC Smart** se l'utente deve ricevere una mailbox standard o una mailbox posto operatore (AutoAttendant).
    b) Solo con mailbox predefinita: Se un chiamante può lasciare un messaggio nella casella vocale, selezionare la casella di controllo **Registrare**.
    c) Dall'elenco a discesa **Annuncio**, selezionare un annuncio di benvenuto.
    d) Se la password della casella vocale deve essere reimpostata, selezionare la casella di controllo **Reimposta password**.

    Nota: Se una casella vocale viene riconfigurata, la casella di controllo **Reset password** non deve essere selezionata. Consente di reimpostare la password per la casella vocale. In caso di riconfigurazione, l'utente deve cambiare comunque la password iniziale della casella vocale al primo accesso.

11) Fare clic su **OK & Avanti**.
12) Fare clic su **OK & Avanti**, quindi su **Fine**.

19.2.7.2 Come integrare un telefono dual mode (GSM/WLAN) con i client HFA o SIP

Con la procedura guidata **Integrazione con il numero di cellulare**, è possibile configurare un telefono cellulare come telefono dual mode per client di sistema (client HFA) o per client SIP (Modalità WLAN).

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

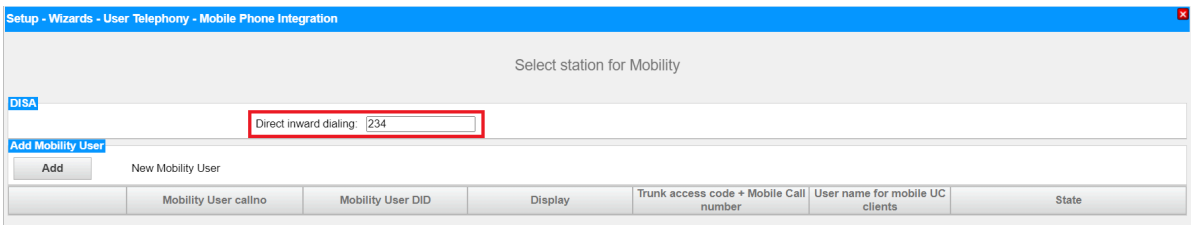
Il dispositivo HFA o l'utente SIP devono essere configurati tramite WBM.

La licenza utente Mobility è stata assegnata all'utente.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Integrazione con il numero di cellulare**. Viene visualizzata la finestra **Seleziona utente per Mobility**.

4) In **Porta DISA**, selezionare o inserire il numero di **Selezione passante** con cui gli utenti mobili possono accedere al sistema di comunicazione.



Nota: DISA è necessario per l'uso di Mobility Entry (controllo del sistema mediante DTMF) e di myPortal for Mobile (solo con la funzione Call-through).

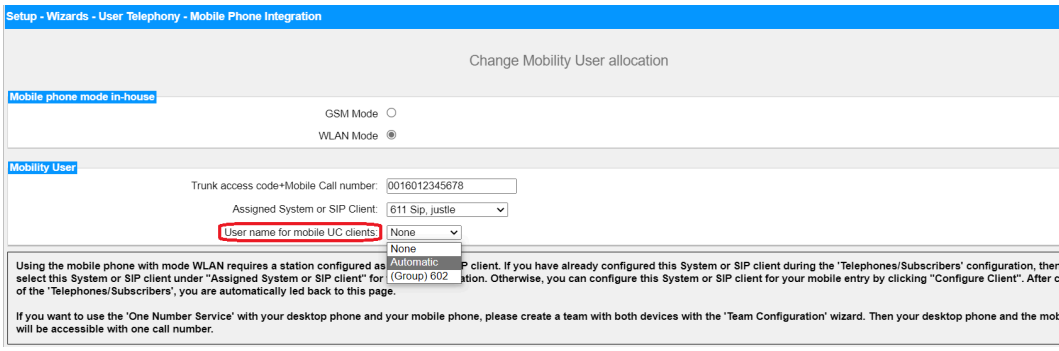
5) Fare clic su **Aggiungi** o **Modifica** in corrispondenza dell'utente di cui si desidera integrare il numero di cellulare GSM nel sistema di comunicazione. Viene visualizzata la finestra **Assegnazione utente Mobility**.

6) Selezionare **Modalità WLAN** come modalità di funzionamento del cellulare.

7) Nei campi **Codice di accesso alla linea esterna+Numero di telefono cellulare** inserire il numero del telefono cellulare (ad esempio, 0016012345678).

8) Selezionare dall'elenco a discesa il **Client di sistema o client SIP assegnato**.

   Se non sono stati ancora configurati i client di sistema (client HFA) o i client SIP, fare clic su **Configura client** e procedere alla configurazione. Dopo la configurazione dell'utente di sistema o dell'utente SIP, si tornerà automaticamente a questa pagina.



9) Nell'elenco a discesa **Nome utente di myPortal to go (Web Edition)**, selezionare il dispositivo SIP o HFA corrispondente. **Se si seleziona Automatico**, il numero interno dell'utente verrà utilizzato come nome utente.

10) Fare clic su **OK & Avanti**.

11) Fare clic su **OK & Avanti**, quindi su **Fine**.

19.2.7.3 Come attivare l'interfaccia Web per telefoni mobili e i client Web

Prerequisiti

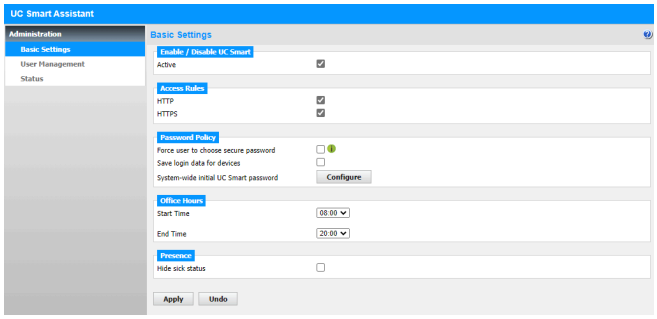
Si è connessi al WBM con il profilo **Expert**.

Selezionare Web Services come requisito per i seguenti servizi:

- Integrazione con il telefono cellulare
- Application Launcher

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Se si utilizza UC Smart, nella struttura di navigazione, fare clic su **Applicazioni** > **UC Smart** > **Impostazione di base**.
3) Verificare se UC Smart è **Attivo**.
4) Se si attiva Web Services nel cellulare, selezionare almeno una delle seguenti opzioni:
   - Se si desidera consentire connessioni crittografate, selezionare la casella di controllo **HTTPS**.
   - Se si desidera consentire connessioni non crittografate, selezionare la casella di controllo **HTTP**.



Nota: Per motivi di sicurezza, si consiglia vivamente di utilizzare solo una connessione crittografata (HTTPS) quando si utilizza myPortal to go (Web Edition) via Internet.

5) Fare clic su **Applica**, quindi su **OK**.

19.2.7.4 Come eliminare l'integrazione numero cellulare

Con la procedura guidata **Integrazione con il numero di cellulare** è possibile eliminare l'integrazione del telefono cellulare.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia utenti**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Integrazione con il numero di cellulare**. Viene visualizzata la finestra **Seleziona utente per Mobility**.
4) Fare clic su **Modifica** per l'utente che si desidera eliminare. Viene visualizzata la finestra **Assegnazione utente Mobility**.

5) Fare clic nella finestra in basso su **Cancella dati**.
6) Fare clic su **OK & Avanti**.
7) Fare clic su **OK & Avanti**, quindi su **Fine**.

19.3 Mobilità in ufficio

È possibile ottimizzare la mobilità in ufficio grazie a funzioni quali desk sharing, uso di telefoni cordless e WLAN. IP Mobility offre servizi di desk sharing per utenti mobili (Mobile Logon e Flex Call), che consentono di utilizzare il telefono di un'altra postazione di lavoro come se fosse il proprio.

19.3.1 Condivisione desk

Con la condivisione desk, più utenti possono condividere un unico telefono di sistema e, quindi, un unico telefono IP (HFA).

Con la condivisione desk, gli utenti non hanno un luogo di lavoro o un telefono d'ufficio fisso. La condivisione desk consente a più utenti mobili del sistema di comunicazione di condividere uno spazio di lavoro d'ufficio e/o il telefono. L'utente accede semplicemente al telefono sul luogo di lavoro in cui attualmente lavora.

Dopo l'accesso, il numero della stazione dell'utente connesso viene trasferito al telefono di sistema usato. Il telefono di sistema usato non può essere più raggiunto al numero della stazione originale. Se l'utente accede a un altro telefono di sistema, il numero della sua stazione viene trasferito a quel nuovo telefono di sistema. Quando l'utente si disconnette, il telefono di sistema si ricollega automaticamente al suo proprio numero non mobile.

Per attivare la funzione, è necessario eseguire uno dei seguenti passaggi sul telefono di sistema:

- Inserire il codice per "accesso mobile" + numero della stazione mobile + password/PIN facoltativo

Se si utilizzano telefoni con diversi numeri di tasti funzione, il trasferimento del layout dei tasti potrebbe essere soggetto a restrizioni.

Se la condivisione desk deve essere implementata per telefoni IP (HFA) in nodi connessi in rete, deve essere installato un DLS (servizio di implementazione) esterno. Per questo scopo si presume che siano state acquisite le competenze necessarie.

Per la condivisione desk possono essere usate le seguenti funzioni:

- Chiamata tramite altoparlante (paging)
- Chiamate in conferenza
- Inclusione
- Richiamata alternata
- Parcheggio
- Consultazione
- Trasferisci
- Ripresa chiamata
- Non disturbare

- Inoltro di chiamata
- Invio messaggio (attesa di messaggio)
- Richiamata
- Soppressione del numero di stazione
- Gruppo suonerie

Nota: Per ogni numero di telefono cellulare è richiesta una licenza Deskshare aggiuntiva. Questa licenza Deskshare deve essere attivata per l'utente e l'utente deve essere configurato come **mobile**. Inoltre, deve essere abilitata la funzione di trasferimento.

Un telefono di sistema usato per la condivisione desk non necessita necessariamente di una licenza. Tuttavia, se non viene attivata nessuna licenza e l'utente della condivisione desk non effettua l'accesso, da quel telefono non saranno possibili neanche le chiamate di emergenza. Il telefono di sistema/ l'utente devono essere configurati come **Non mobile**.

Se un telefono di sistema non verrà utilizzato per la condivisione desk, deve essere configurato come **Non mobile e bloccato**.

Nota: La funzione di condivisione desk non deve essere usata per le prime due stazioni di sistema attive.

19.3.2 Soluzione cordless integrata

OpenScape Business Cordless è una soluzione cordless integrata per l'uso di telefoni cordless (telefoni DECT) tramite il sistema di comunicazione. Con i telefoni DECT collegati è possibile utilizzare le funzionalità HFA di OpenScape Business.

Con la soluzione cordless integrata, i telefoni DECT interni sono gli utenti specifici di sistema, diversamente dai sistemi DECT separati, che sono collegati tramite interfacce standard.

Il collegamento delle stazioni base OpenScape Business per l'uso dei telefoni DECT può essere realizzato mediante:

- OpenScape Business X1/X3/X5: collegamento diretto all'interfaccia $U_{P0/E}$ della scheda madre del sistema di comunicazione (DECT Light)
- Per OpenScape Business X3/X5: collegamento all'interfaccia $U_{P0/E}$ di un modulo SLU8N/SLU8NR (DECT Light)
- Per OpenScape Business X8: collegamento alle interfacce $U_{P0/E}$ di un modulo SLMUC (SLMU + CMAe)

La tecnologia cordless corrisponde allo standard DECT (Digital Enhanced Cordless Telecommunications). L'intera gamma delle frequenze radio gestita dal sistema è utilizzata da stazioni base che formano una rete completa di celle radio che si sovrappongono o singole "isole" di trasmissione radio. La dimensione di una rete di telefonia mobile dipende dalle condizioni strutturali locali.

Modalità ECO

In modalità ECO (modalità risparmio energetico) la potenza di trasmissione dei telefoni DECT può essere ridotta di un valore fisso (statico) oppure ogni telefono DECT regola la sua potenza di trasmissione indipendentemente in base all'intensità del segnale ricevuto (adattivo). La modalità ECO può essere attivata nell'intero sistema di comunicazione per tutti i telefoni DECT (**Modalità esperti** > **Telefonia** > **Cordless** > **Per tutto il sistema**). Non è richiesta alcuna configurazione nei telefoni DECT. Per attivare la funzione con OpenScape Business X1, X3, X5 è necessario eseguire un riavvio manuale.

- Regolazione statica della potenza di trasmissione

  I telefoni DECT e le stazioni base riducono la potenza di trasmissione di un valore fisso.
- Regolazione adattiva della potenza di trasmissione

  A seconda della forza del segnale, i telefoni DECT utilizzano una potenza di trasmissione normale o ridotta. Al momento dell'handover, il telefono passa prima alla potenza di trasmissione elevata, quindi successivamente tale potenza può venire ridotta in base alla potenza del segnale.

Telefoni DECT

La soluzione cordless integrata supporta il collegamento di telefoni cellulari abilitati GAP di altri produttori. L'intera gamma di funzioni HFA disponibili può tuttavia essere utilizzata solo con telefoni DECT approvati.

Configurazione

Per una descrizione della configurazione, vedere Configurazione della soluzione cordless integrata.

Moduli e stazioni base

Per una descrizione dei moduli e delle stazioni base, consultare *OpenScape Business, Documentazione di manutenzione, capitoli Moduli e Stazione base*.

19.3.2.1 Panoramica

Il collegamento delle stazioni base OpenScape Business per OpenScape Business X3/X5 viene eseguita direttamente alle interfacce $U_{P0/E}$ della scheda madre o alle interfacce UP0/E di una scheda SLU8N/SLU8NR (DECT Light) installata. OpenScape Business X8 consente di collegare le stazioni di base ai moduli cordless SLMUC.

Collegamenti diretti (DECT Light)

Le stazioni base possono essere collegate direttamente alle interfacce $U_{P0/E}$ dei sistemi di comunicazione OCCM, OCCMB, OCCMA e OCCMR, OCCMBR, OCCMAR dei sistemi di comunicazione OpenScape Business X3R/X3W e OpenScape Business X5R/X5W o alle interfacce UP0/E di un modulo SLU8N/SLU8NR8.

Utilizzando il sottomodulo CMAe sulle schede madri, vengono rese disponibili le funzioni di conversione ADPCM e cancellazione dell'eco (48 canali per CMAe). Possono essere condotte fino a quattro conversazioni per stazione base. Alle

interfacce $U_{P0/E}$ delle schede madri OCCM, OCCMB, OCCMA e OCCMR, OCCMBR, OCCMAR possono collegate fino a sette stazioni base.

Se non sono installati CMAe, possono essere effettuate massimo due chiamate per stazione base. In questo caso, la conversione ADPCM viene eseguita direttamente dalla stazione base DECT.

Nota: Nel caso in cui non siano installati CMAe, le funzioni di gestione dell'eco non sono disponibili.

Per il collegamento di stazioni base a un modulo SLU8N/SLU8NR occorre assicurare i seguenti requisiti di connessione:

- È possibile utilizzare fino a 15 stazioni base (7 sulla scheda madre e altre 8 su un modulo SLU8N/SLU8NR). Il numero massimo di telefoni DECT collegabili è 64 con un CMAe.
- Per il collegamento alla stazione base è possibile utilizzare solo un modulo SLU8N/SLU8NR.
- Per collegare la stazione base a un'interfaccia U $_{P0/E}$ del modulo SLU8N/SLU8NR può essere utilizzata solo la prima porta della stazione base. Le porte 2 e 3 della stazione base non sono supportate per il collegamento a un'altra interfaccia $U_{P0/E}$.
- Le interfacce U $_{P0/E}$ del modulo SLU8N/SLU8NR possono essere collegate a più tipi di dispositivi (stazioni base o telefoni).

Collegamento di moduli cordless

La stazione base BS5 può essere collegata alle interfacce $U_{P0/E}$ dei seguenti moduli cordless:

- SLMUC (SLMU + CMAe) con OpenScape Business X8 (vedere *Documentazione di servizio, capitolo SLMUC*)

  Il collegamento delle stazioni base può essere eseguito tramite una, due o tre interfacce $U_{P0/E}$. Le ultime 8 interfacce di un SLMUC possono essere utilizzate solo come 2ª o 3ª interfaccia UP0 della stazione base. Il collegamento aggiuntivo di interfacce $U_{P0/E}$ aumenta la capacità di traffico della stazione base e quindi il numero di canali voce disponibili contemporaneamente.

19.3.2.2 Collegamento di moduli cordless

Per la connessione dei moduli, le stazioni base vengono collegate alle interfacce $U_{P0/E}$ del modulo cordless (moduli SLC).

Alle interfacce $U_{P0/E}$ possono essere connessi i seguenti moduli per sistemi cordless:

- SLC16N con OpenScape Business X5W (solo sistemi da parete)
- SLCN con OpenScape Business X8

In OpenScape Business X8 è possibile impostare fino a quattro moduli cordless (SLCN). Tutti e quattro i moduli cordless forniscono funzionalità cordless complete (roaming e la piena funzionalità senza cordone (roaming e Seamless Connection Handover) poiché le aree di trasmissione radio dei moduli cordless vengono sincronizzate all'interno del sistema di comunicazione

tramite connessioni di rete SLC (Multi-SLC). L'handover a livello di rete non è attualmente supportato.

Se non sono disponibili schede SLCN o SLC16N e BS è collegata a $U_{P0/E}$, nel caso di una rete OpenScape Business con roaming CMI sui nodi, nella scheda di controllo è necessario un modulo CMA o CMAe.

19.3.2.3 Configurazione del sistema

A seconda del sistema di comunicazione, è possibile collegare fino a 64 stazioni base e usare fino a 250 telefoni DECT.

La seguente tabella mostra la massima possibile configurazione di sistema per la soluzione cordless integrata e fornisce informazioni sui casi in cui è possibile l'accesso alla linea esterna analogica del sistema di comunicazione.

Nota: Le stazioni base BS4 (S30807-U5491-X), BS3/1 (S30807-H5482-X), BS3/3 (S30807-H5485-X) e BS3/S (X30807-X5482-X100) sono in fine produzione e non possono essere più ordinate. Il collegamento ai sistemi di comunicazione OpenScape Business X è ancora possibile.

Nel caso di guasto, devono essere usate le stazioni base correnti.

Suggerimento: Se non è installato CMA/CMAe, possono essere effettuate massimo due chiamate per utente base. In questo caso, la conversione ADPCM viene eseguita direttamente dall'utente base DECT, ma la riduzione eco non è supportata. Se la riduzione eco è necessaria, occorre una scheda secondaria CMA/CMAe.

Nota: Nella seguente tabella, la combinazione della scheda SLMU con il modulo CMAe viene denominata SLMUC.

OpenScape Business	Numero massimo di moduli				Modulo clock	**Numero max. di BaseStation BS se connesse tramite 1xU $_{P0}$**	Porte / conversaz contempo a BS	**Numero max. di dispositivi registrati**	Max. numero di conversazioni simultanee
	SLC16N	**SLCN**	**SLUN**	**SLMUC**					
X1	–	–	–	–	–	7	1/2	16	14
	–	–	–	–	CMA	7	1/4	16	16
	–	–	–	–	CMAe	7	1/4	16	16

OpenScape Business	Numero massimo di moduli				Modulo clock	Numero max. di BaseStation BS se connesse tramite 1xU $_{P0}$	Porte / conversaz contempo a BS	Numero max. di dispositivi registrati	Max. numero di conversazioni simultanee
	SLC16N	SLCN	SLUN	SLMUC					
X3	–	–	–	–	–	7	1/2	32	16
$U_{P0/E}$ integrato (SLUC)	–	–	–	–	CMA	7	1/4	32	16
	–	–	1	–	CMA	15	1/4	32	16
	–	–	–	–	CMAe	7	1/4	64	28
	–	–	1	–	CMAe	15	1/4	64	48
X5	–	–	–	–	–	7	1/2	32	16
$U_{P0/E}$ integrato (SLUC)	–	–	–	–	CMA	7	1/4	32	16
	–	–	1	–	CMA	15	1/4	32	16
	–	–	–	–	CMAe	7	1/4	64	28
	–	–	1	–	CMAe	15	1/4	64	48
X5W	1	–	–	–	–	16	3/12	64	32*
X8	–	4	–	–	–	64	3/12	250 (128 per SLCN)	128**
	–	–	–	4	CMAe	64	3/12	250 (128 per SLCN)	192***

* Il valore massimo per SLCN16 è 32. In caso di roaming, la conversione ADPCM viene sempre effettuata sulla scheda SLC16N in cui è attualmente presente il portatile. Di conseguenza, il numero di chiamate simultanee per sistema potrebbe essere superiore a 32 se il ricevitore si trova su SLC16N

* Il valore massimo per SLCN è 32. A seconda della posizione dei telefoni in caso di roaming, in teoria tutti i dispositivi registrati (250) potrebbero essere attivi se sono disponibili 4 schede SLCN.

*** È possibile unire SLCN e SLMUC in un unico sistema. Il valore massimo per SLCN è 32, mentre per SLMUC è 48. A seconda della posizione dei telefoni in caso di roaming, in teoria tutti i dispositivi registrati (250) potrebbero essere attivi se sono disponibili in totale 4 SLCN/SLMUC.

19.3.2.4 Cordless/Telefoni DECT

Collegando il modulo SLC e inserendo l'identificativo di sistema DECT, vengono configurati 16 portatili. i codici per portatili (PIN) vengono assegnati e i telefoni portatili possono essere registrati. Altri portatili possono essere utilizzati solo se sono stati approvati.

Se in seguito alla manutenzione viene sostituito un portatile, prima dell'accesso del dispositivo sostitutivo occorre modificare il PIN. Quando si effettua una sostituzione nel sistema di comunicazione è essenziale che all'utente in questione venga assegnato un nuovo PIN. In questo modo, si ha la disconnessione automatica del portatile. Migliora inoltre la sicurezza,

prevenendo l'abuso del vecchio PIN e quindi l'accesso al portatile da parte di utenti non autorizzati di è più possibile.

19.3.2.5 Importanza dei risultati ottenuti dai test della gamma delle frequenze radio

Importante:

I valori registrati con un telefono cellulare non sono molto precisi e servono solo per fornire una valutazione di massima. Inoltre, anche in condizioni ambientali identiche potrebbero essere registrati valori diversi su ciascun telefono cellulare. Se si necessita di risultati più precisi, si consiglia di utilizzare lo strumento Hicom Cordless Service (HCS-DECT).

La figura seguente illustra una visualizzazione di esempio dei risultati di misurazione di un telefono cellulare Gigaset quando è in corso una chiamata:

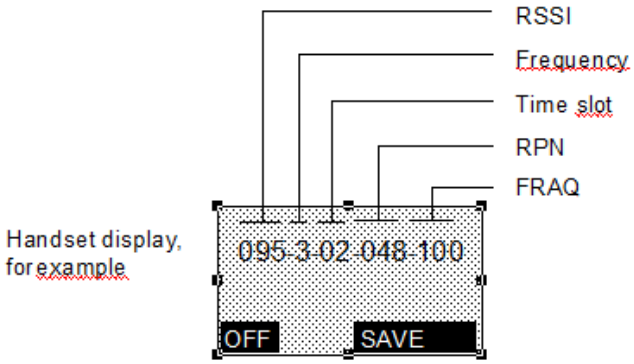


Figura 8: Risultato di misurazione

Capitolo	Descrizione
RSSI (segnale radio)	Potenza di trasmissione dei segnali radio ricevuti dall'utente base, normalizzati fino a un massimo di 100. Se il valore è < 50, il collegamento radio all'utente base non è più garantito. La potenza di trasmissione ammissibile è > 50 (> -60 dBm).
Frequenza	Frequenza (0-9)
Fascia oraria (slot)	Fascia oraria (0-11) del canale ricevente su cui viene eseguita la misurazione.

Capitolo	Descrizione
RPN (numero di porta)	**OpenScape Business X1/X3/X5/ X8** ID utente base, ad esempio, 048, numero di porta nei moduli SLC. Se il ricevitore passa a una cella radio/un utente base che si sovrappone, il numero di porta attuale (in cui è configurato il canale D dell'utente base) viene visualizzato sul display del ricevitore. Formula: A x 16 + B A = numero del modulo SLC (1-127); 16 = fattore B = porta del modulo SLC associato (in cui è configurato il canale D dell'utente base) Esempi: RPN = 1 x 16 + porta 0 = 016 RPN = 2 x 16 + porta 8 = 040. Il numero di porta (PRN) viene visualizzati sui ricevitori Gigaset S3 professional e Gigaset SL3 professional in formato esadecimale con una H aggiunta. Il valore esadecimale viene visualizzato senza H aggiunta, ad esempio "-028-" nel caso dei ricevitori Gigaset S4 professional e OpenStage SL4 professional. Esempio: Se in precedenza veniva visualizzato il valore 040, ora viene visualizzato il valore 028H per Gigaset S3/SL3 professional. La notazione esadecimale si differenzia unicamente in base al suffisso "H". Questo vale anche per i dispositivi OpenScape DECT Phone S5/SL5/S6/SL6/R6 (il prefisso H non è presente).
FRAQ (qualità dei fotogrammi)	Qualità della trasmissione in %. Soddisfacente dal 95% al 100% (dal 90% al 94% non critica per previ periodi), cattiva < 95%.

Per maggiori informazioni sulla lettura del menu delle misurazioni, vedere: *OpenScape Cordless Enterprise, Documentazione di servizio, Capitolo: Test della gamma delle frequenze radio* e *OpenScape Business X3/X5/X8, Documentazione di manutenzione, Capitolo: Controllare la copertura radio.*

19.3.3 Configurazione della soluzione cordless integrata

La configurazione della soluzione cordless integrata comprende la configurazione delle stazioni base e l'accesso dei telefoni DECT/Telefonia mobile al sistema di comunicazione.

Per la configurazione è richiesta la Modalità esperti.

The requisite steps for project planning, lighting, installation and cabling, setting up the system physically and inserting the SLC or CMAe boards have been completed (see also Service Documentation). I telefoni DECT sono carichi. L'identificativo del sistema DECT è noto. Sono disponibili informazioni su utenti, numeri di telefono, nomi ed eventualmente le relative assegnazioni a moduli SLC.

Procedura generale per la configurazione di una soluzione cordless integrata

1) Inserire l'identificativo del sistema DECT e configurare eventuali parametri cordless aggiuntivi
2) Configurazione di un utente base cordless
3) Connettere i telefoni DECT al cordless
4) All'occorrenza aggiungere altri telefoni DECT

Dopo la messa in servizio dei telefoni DECT, è possibile modificare il numero di telefono, il nome e altre impostazioni dell'utente DECT utilizzando il WBM mediante la procedura guidata **Terminali/Utenti**.

Identificativo del sistema DECT

L'ID del sistema DECT viene utilizzato per distinguere i singoli sistemi DECT e quindi i vari segnali radio. In questo modo è possibile la sincronizzazione con il sistema del portatile connesso.

L'ID di sistema DECT è composto da un numero esadecimale a 8 cifre, assegnato all'acquisto del sistema DECT. È valido a livello di sistema (anche in caso di assistenza).

L'identificativo di sistema DECT è composto da:

Cifra	Significato
1° cifra	E/ARC (Access Right Code)
2ª -5ª cifra	EIC (Equipment Installers Code)
6ª -7ª cifra	FPN (Fixed Part Number)
8° cifra	FPS (Fixed Part Subscriber)

19.3.3.1 Come inserire l'identificativo del sistema DECT e configurare eventuali parametri cordless aggiuntivi (dati a livello di sistema)

Prerequisiti

Si è connessi al WBM con il profilo **Expert** o Hipath 3000 Manager. I passaggi seguenti si riferiscono solo a WBM, ma azioni simili possono essere eseguite utilizzando Hipath 3000 Manager.

Al sistema di comunicazione è collegata una stazione di base di OpenScape Business.

È disponibile l'ID DECT di 8 cifre fornito al momento dell'acquisto del sistema DECT.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Cordless**.
3) Fare clic nella struttura ad albero su **Cordless** > **Per tutto il sistema**.
4) In **EIC** digitare l'ID a 8 cifre del sistema DECT.
5) Modificare le impostazioni a livello di sistema in **Gestione eco** e **Modalità ECO** solo all'occorrenza. Per una spiegazione delle impostazioni, vedere Cordless > Per tutto il sistema.
6) Fare clic su **Applica**, quindi su **OK**.

19.3.3.2 Come configurare le stazioni base cordless

Prerequisiti

Si è connessi al WBM con il profilo **Expert** o Hipath 3000 Manager. I passaggi seguenti si riferiscono solo a WBM, ma azioni simili possono essere eseguite utilizzando Hipath 3000 Manager.

Al sistema di comunicazione è collegata una stazione di base di OpenScape Business.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Cordless**.
3) Nella struttura dei menu fare clic su **Cordless** > **Stazione base**. Vengono visualizzate tutti le stazioni base collegate.
4) Se una o più stazioni base sono collegate direttamente (senza modulo SLC) al sistema (SLUC), è possibile attivare o disattivare le stazioni base tramite l'elenco di selezione **Tipo**:
   a) **Stazione base**: la stazione base viene attivata e vengono automaticamente preconfigurati 16 telefoni DECT e una connessione di rete SLC.
   b) **Senza porta**: la stazione base viene disattivata e con essa anche i telefoni DECT e la connessione di rete SLC associati.
5) All'occorrenza modificare in **Nome** il nome preconfigurato della stazione base (ad esempio `Base 1`).
6) In **Livello**, determinare il livello per la stazione base (50% o 100%).
7) Fare clic su **Applica**, quindi su **OK**.

19.3.3.3 Come effettuare la prima configurazione dei telefoni DECT

Prerequisiti

Si è connessi al WBM con il profilo **Expert** o si sta usando HiPath 3000 Manager.

Al sistema di comunicazione è collegata una stazione di base di OpenScape Business.

È necessario eseguire i seguenti passaggi di configurazione prima di registrare i dispositivi DECT nel sistema.

Passo a passo

1) Procedere come segue se si utilizza WBM:
   a) Nella barra di navigazione fare clic su **Modalità esperti**.
   b) Nella struttura di navigazione, fare clic su **Telefonia** > **Cordless**.
   c) Nella struttura dei menu fare clic su **Cordless** > **SLC**. Vengono visualizzati tutti i telefoni DECT già configurati. Quando si collega una stazione base vengono automaticamente preconfigurati 16 telefoni DECT.
   d) Se necessario, in **N° tel.** modificare il numero interno preconfigurato del telefono DECT.
   e) Se necessario, in **DID** modificare il numero di selezione passante preconfigurato del telefono DECT.
   f) Se necessario, in **Nome** modificare il nome preconfigurato del telefono DECT.
   g) Se necessario, in **Codice mobile** modificare il codice cellulare (PIN) preconfigurato del telefono DECT. Tale codice deve essere inserito al momento dell'associazione con la stazione base del telefono DECT.
   h) Fare clic su **Applica**, quindi su **OK**.

2) Procedere come segue se si utilizza Hipath 3000 Manager:
   a) Caricare il controllo del database KDS **Leggere/scrivere CDB** e **Sistema > PC**
   b) Nella struttura dei menu, andare su **Impostazioni > Cordless**.
   c) Nella struttura dei menu, fare clic su **Cordless > SLC**, quindi selezionare tutte le opzioni del parametro **Parti mobili**. Vengono visualizzati tutti i telefoni DECT già configurati. Quando si collega una stazione base vengono automaticamente preconfigurati 16 telefoni DECT.
   d) Se necessario, in **Numero di telefono** modificare il numero interno preconfigurato del telefono DECT.
   e) Se necessario, in **Nome** modificare il nome preconfigurato del telefono DECT.
   f) Se necessario, in **Codice mobile** modificare il codice cellulare (PIN) preconfigurato del telefono DECT. Tale codice deve essere inserito al momento dell'associazione con la stazione base del telefono DECT.
   g) Fare clic su **Applica**, quindi su **OK**.
   h) Trasferire il KDS sul sistema, se sono state apportate modifiche.

Attività correlate

Come configurare gli utenti DECT alla pagina 456

19.3.3.4 Come accedere al cordless di un telefono DECT (portatile OpenStage/Gigaset)

Prima di registrare un telefono DECT è necessario aprire la finestra di registrazione con un telefono di sistema utilizzando il codice di registrazione DECT. Immettere quindi i numeri di telefono dei telefoni DECT da registrare. Possono essere registrati massimo 10 numeri di utenti nella stessa finestra di

registrazione. Una finestra di registrazione resta aperta per un massimo di 10 minuti.

Se non sono disponibili telefoni di sistema, è possibile utilizzare la funzione **Online** di Hipath 3000 Manager ed eseguire le azioni da lì anziché usare un telefono fisico. La procedura di seguito si riferisce al telefono fisico.

La procedura di seguito si riferisce al telefono fisico.

Passo a passo

1) Aprire la finestra di registrazione del sistema di comunicazione:
   a) Sul telefono fisico, inserire il codice *94 2 e poi 19970707.
   b) Inserire i numeri di telefono dei telefoni DECT da registrare.
2) Registrare il telefono DECT:
   a) Dalla schermata iniziale del telefono DECT, premere il **tasto del menu**.
   b) Andare su **Impostazioni > Registrazione > Registra portatile** e selezionare **Base**.
   c) Verrà richiesto di inserire il PIN del sistema telefonico. Inserire il codice a otto cifre del cordless e confermare.

      È necessario attendere una o due chiamate mute, ossia chiamate automatiche brevi (su alcuni dispositivi simili a 2 squilli).

      Se si sta registrando un numero di chiamata inattivo (che non è stato utilizzato in precedenza, visualizzato in nero su WBM e in grigio in KDS), la registrazione viene completata con una chiamata muta. Se si sta registrando un numero di telefono attivo che è stato utilizzato in precedenza (visualizzato in verde su WBM e KDS), la registrazione viene completata con due chiamate mute.

      Non eseguire altre azioni (ad es. avviare chiamate DECT) fino al completamento di questa procedura!

Completata correttamente la registrazione, il numero di telefono verrà visualizzato nella schermata principale e sarà possibile utilizzare il dispositivo.

Esempio: Registrare il cordless (numero di telefono 125) sul sistema di telefoni DECT con il codice cordless (PIN) 11112345 (configurato come codice cordless tramite Manager E o utilizzando WBM come illustrato nel capitolo: Come effettuare la prima configurazione dei telefoni DECT alla pagina 969.)

1) Attivare la finestra di registrazione da un telefono fisico connesso al sistema inserendo *942.
2) Sul display del telefono verrà visualizzato: **Codice**.
3) Inserire 19970707 e sul display del telefono verrà visualizzato: **N. tel.**: Inserire 125.
4) Se necessario, accendere il telefono cordless tenendo premuto per oltre 1 secondo il tasto di fine chiamata. Viene emesso il tono di conferma.
5) Immettere quanto segue entro dieci minuti. Premere il tasto del menu.
6) Andare su **Impostazioni** dal menu del telefono e confermare.
7) Andare su **Registrazione** e confermare la prima scelta: **Registra portatile** (non selezionare la seconda opzione: Seleziona base)
8) Selezionare una base (nell'esempio **Base 2**) e confermare. Al centro del display verranno visualizzati **Registrazione** e **Inserisci PIN di sistema**.
9) Inserire il PIN a otto cifre (codice del cordless; qui **11112345**) e confermare. Se la registrazione va a buon fine, occorre una "chiamata muta", ossia

una breve chiamata automatica (su alcuni dispositivi è simile a 2 squilli). Se si sta registrando un numero di chiamata inattivo (che non è stato utilizzato in precedenza, visualizzato in nero su WBM e in grigio in KDS), la registrazione viene completata con una chiamata muta. Se si sta registrando un numero di telefono attivo che è stato utilizzato in precedenza (visualizzato in verde su WBM e KDS), la registrazione viene completata con due chiamate mute. Non eseguire altre azioni (ad es. avviare chiamate DECT) fino al completamento di questa procedura! Quindi sul lato sinistro dello schermo verrà visualizzato Base 2 (in questo caso). Successivamente, nella schermata principale verrà visualizzato il numero di telefono (125).

10) All'occorrenza, è possibile modificare il nome Base 2. Per farlo, andare su Impostazioni e confermare, andare su Registrazione e confermare e infine selezionare la seconda opzione Seleziona Base. Selezionare il nome della base da rinominare, premere **Nome**e rinominare il nome della base (ad esempio in 125).

19.3.3.5 Come aggiungere altri telefoni DECT

Prerequisiti

Si è connessi al WBM con il profilo **Expert** o Hipath 3000 Manager. I passaggi seguenti si riferiscono solo a WBM, ma azioni simili possono essere eseguite utilizzando Hipath 3000 Manager.

Al sistema di comunicazione è collegata una stazione di base di OpenScape Business.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione, fare clic su **Telefonia** > **Cordless**.

3) Nella struttura dei menu fare clic su **Cordless** > **SLC**.

4) Nella struttura dei menu fare clic sul modulo desiderato.

5) Fare clic sulla scheda **Aggiungi telefoni DECT**.

6) In **Numero di telefoni DECT** indicare il numero dei telefoni DECT appena aggiunti. I telefoni DECT appena aggiunti vengono visualizzati nella scheda **Modifica utente DECT**.

7) Fare clic su **Applica**, quindi su **OK**.

19.3.3.6 Come eliminare i telefoni DECT

Prerequisiti

Si è connessi al WBM con il profilo **Expert** o Hipath 3000 Manager. I passaggi seguenti si riferiscono solo a WBM, ma azioni simili possono essere eseguite utilizzando Hipath 3000 Manager.

Al sistema di comunicazione è collegata una stazione di base di OpenScape Business.

I telefoni DECT sono configurati.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Cordless**.
3) Nella struttura dei menu fare clic su **Cordless** > **SLC**. Vengono visualizzati tutti i telefoni DECT già configurati.
4) Nella colonna **Elimina**, selezionare i telefoni DECT da eliminare.
5) Fare clic su **Applica**, quindi su **OK**.

19.3.3.7 Come configurare i parametri Multi-SLC

Prerequisiti

Si è connessi al WBM con il profilo **Expert** o Hipath 3000 Manager. I passaggi seguenti si riferiscono solo a WBM, ma azioni simili possono essere eseguite utilizzando Hipath 3000 Manager.

There are multiple SLMUC boards inserted in the OpenScape Business X8.

Al sistema di comunicazione è collegata una stazione di base di OpenScape Business.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Cordless**.
3) Nella struttura dei menu, fare clic su **Cordless** > **Multi-SLC**.
4) Edit parameters of the SLMUC board:
   a) If required, edit the preconfigured system-wide unique ID of the SLMUC board under **SLC No.**

      Intervallo di valori: 1-15,17-31,33-47,...,127. I multipli di 16 non sono consentiti.
   b) If required, edit the preconfigured system-wide unique call number of the SLC networking line of the SLMUC board under **SLC number**.

      Nota: Per ogni collegamento in rete SLC viene configurato una stazione S_0 interna. Il numero SLC corrisponde al numero della stazione S_0 interna.
   c) Make sure that the station flag **Call waiting rejection on** is disabled for the internal S_0 station.
5) If necessary, repeat step 4 for the other SLMUC boards.
6) Fare clic su **Applica**, quindi su **OK**.

19.3.3.8 Come richiedere i dati sulle stazioni base

Prerequisiti

Si è connessi al WBM con il profilo **Expert** o Hipath 3000 Manager. I passaggi seguenti si riferiscono solo a WBM, ma azioni simili possono essere eseguite utilizzando Hipath 3000 Manager.

Al sistema di comunicazione è collegata una stazione di base di OpenScape Business.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Cordless**.
3) Nella struttura dei menu fare clic su **Cordless** > **Stazione base**.
4) Nella struttura dei menu fare clic sulla stazione base desiderata. Vengono visualizzati i dati della stazione base. Per ulteriori informazioni sui dati, consultare Cordless > Stazione base.
5) Per una stazione base, è possibile selezionare contemporaneamente fino a 10 canali di frequenza diversi. Per ulteriori informazioni sui canali di frequenza, vedere la tabella riportata in Cordless > Stazione base.
6) Fare clic su **Applica**, quindi su **OK**.

19.3.3.9 Come attivare il tono di avviso dell'indicazione messaggio in attesa (MWI) per i telefoni DECT

Prerequisiti

Si è connessi al WBM con il profilo **Expert** o Hipath 3000 Manager. I passaggi seguenti si riferiscono solo a WBM, ma azioni simili possono essere eseguite utilizzando Hipath 3000 Manager.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazione di base** > **Flag di** > **sistema**.
4) Nel campo **Flag di sistema** selezionare la casella di controllo **Suoneria CMI MWI**.
5) Fare clic su **Applica**, quindi su **OK**.

19.3.3.10 Come controllare lo stato di connessione dei telefoni DECT

Prerequisiti

Si è connessi al WBM con il profilo **Expert** o Hipath 3000 Manager. I passaggi seguenti si riferiscono solo a WBM, ma azioni simili possono essere eseguite utilizzando Hipath 3000 Manager.

Al sistema di comunicazione è collegata una stazione di base di OpenScape Business.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Cordless**.
3) Nella struttura dei menu fare clic su **Cordless** > **SLC**. Vengono visualizzati tutti i telefoni DECT già configurati.

4) Nella colonna **Attivo** viene visualizzato lo stato di registrazione di ogni telefono DECT:
   - Verde: il cellulare è attivo.
   - Rosso: è stato impostato l'interruttore di blocco del modulo per un telefono cellulare registrato.
   - Giallo: il telefono cellulare è stato automaticamente disconnesso a causa della modifica del PIN.
   - Grigio: su questa porta non sono ancora stati registrati telefoni cellulari.
5) Fare clic su **Applica**, quindi su **OK**.

19.3.4 Cordless IP

Cordless IP (DECT IP) è una soluzione cordless opzionale, alternativa alla soluzione cordless integrata o adatta all'uso con OpenScape Business S.

I telefoni IP cordless DECT comunicano tramite la stazione base BSIP con il sistema di comunicazione, come i telefoni SIP. Con Cordless IP si può pertanto utilizzare solo funzionalità SIP. Per ulteriori informazioni su IP cordless, consultare la documentazione di HiPath Cordless IP.

In tutti gli utenti SIP che hanno accesso a un cordless IP è disattivato il parametro utente **Risposta automatica, CSTA**. In caso contrario, è possibile che le chiamate tra utenti SIP tramite IP DECT non vengano realizzate.

19.3.5 Telefoni WLAN e access point

I telefoni WLAN e dual mode consentono la comunicazione mobile. Questi telefoni possono essere integrati in infrastrutture WLAN esistenti. Gli access point WLAN consentono di creare reti senza fili e di utilizzare servizi voce e dati nella stessa infrastruttura. Si consiglia di utilizzare solo access point WLAN ad alte prestazioni (ad esempio, di marca Enterasys).

19.3.5.1 Requisiti per WLAN

Quando si realizzano reti WLAN, occorre accertarsi che tutti i requisiti essenziali per Voice-over-WLAN siano soddisfatti. Prima di implementare la porzione wireless della rete è necessario eseguire una verifica del sito.

Fattori da considerare:

- Le piccole installazioni, fino a 3 AP, possono essere facilmente ed efficacemente definite con una visita sul campo o valutando una planimetria. In questo caso una verifica del sito non è normalmente necessaria.
- Nelle installazioni che presentano 4 o più AP deve comunque essere eseguita la verifica del sito. Ciò si applica in particolare a sistemi che comprendono più edifici o piani di uno stesso edificio.
- La verifica del sito è richiesta, indipendentemente dal numero di AP, quando si tratta di un ambiente particolarmente intenso per quanto riguarda le radiofrequenze o quando la soluzione deve essere implementata accanto a sistemi WLAN esistenti.

19.4 Mobilità a casa

La mobilità a casa si ottiene grazie al telelavoro. Ciò avviene integrando telefoni non locali (come telefoni fissi o cellulari) nella rete di comunicazione OpenScape Business.

Sono disponibili i seguenti tipi di stazioni peri l telelavoro:

- Utenti VPN

  OpenScape Business dispone di una funzionalità VPN integrata. È possibile attivare contemporaneamente un totale di 10 telelavoratori tramite VPN. Ciò può riguardare un PC domestico o un telefono cellulare con sistema operativo Android o iOS. La connessione VPN viene stabilita tra il client VPN nativo del PC o del telefono cellulare e il server OpenVPN di OpenScape Business.

  Gli utenti di UC Suite possono specificare il proprio numero di telefono di casa tramite il client UC e quindi utilizzare il proprio telefono privato come telefono dell'ufficio (CallMe).
- Device@Home: Stazioni SIP@Home o stazioni System Device@Home

  I telefoni SIP abilitati STUN (ad es. Yealink T19) (stazioni SIP Device@Home) o i telefoni HFA (stazioni System Device@Home) possono registrarsi autonomamente sul sistema di comunicazione tramite Internet utilizzando la funzione SBC interna di OpenScape Business. Per farlo, la funzione deve essere abilitata nei dati della stazione per ciascun telefono SIP o telefono HFA tramite il WBM.

  È necessario, inoltre, specificare un server STUN nel WBM solo se non viene utilizzato alcun ITSP o se l'ITSP utilizzato non offre alcun server STUN.

  SIP Device@Home non supporta la trasmissione di segnali video.

  Nota: Quando si utilizzano più dispositivi SIP/HFA @Home dietro lo stesso router, le limitazioni NAT possono causare problemi di payload delle chiamate a causa di conflitti di riutilizzo delle porte; per evitare ciò, configurare ogni dispositivo con una porta sorgente (RTP) univoca.

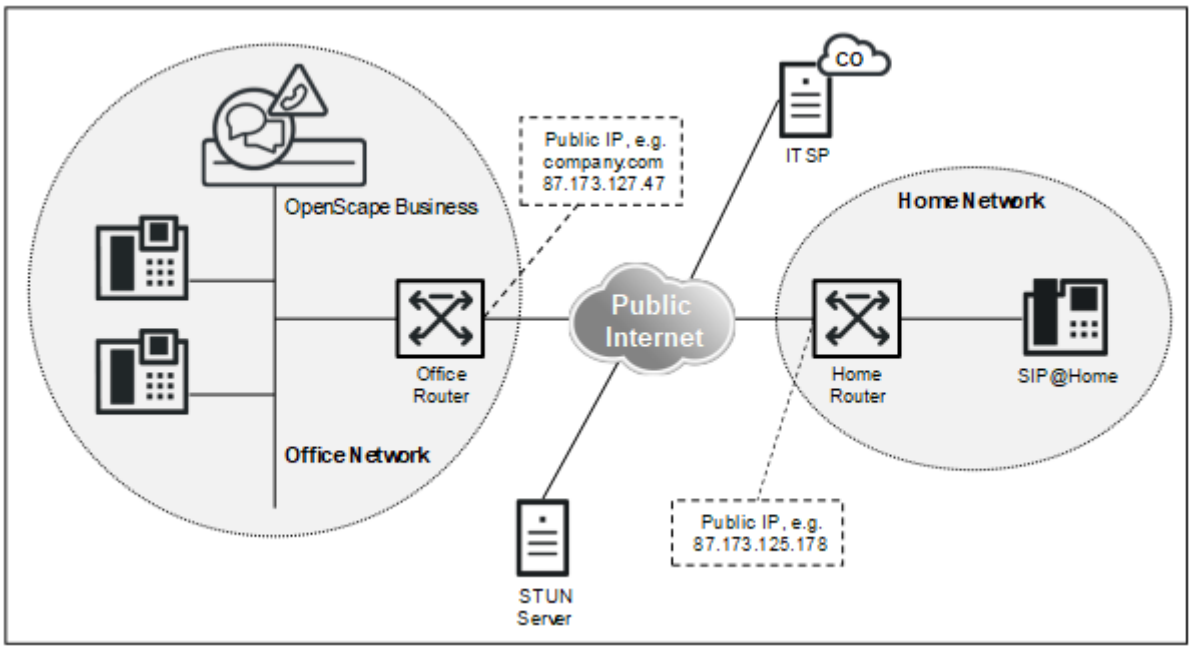


Figura 9: Componenti di Device@Home (SIP Device@Home o System Device@Home)

19.4.1 Configurazione della VPN

Per collegare gli utenti al sistema di comunicazione tramite la funzionalità VPN integrata, è necessario eseguire alcune configurazioni nel sistema OpenScape Business e negli utenti VPN.

Configurazione di OpenScape Business

Per la configurazione VPN del sistema di comunicazione, vedere Come configurare la connessione di operatori remoti tramite VPN .

Configurazione di utenti VPN (client VPN)

Per configurare i client VPN, vedere VPN - Client .

19.4.2 Configurazione del Dispositivo SIP@Home

Per connettersi a OpenScape Business tramite Internet con un telefono SIP compatibile STUN, occorre procedere ad alcune configurazioni.

Configurazione di OpenScape Business

Per registrare un utente SIP nel sistema di comunicazione tramite Internet, è necessario attivare la funzione SBC integrata per l'utente SIP (vedere Come attivare Dispositivo@Home).

Con l'aiuto del protocollo STUN, la funzione SBC integrata rileva l'indirizzo IP pubblico del sistema di comunicazione e la porta utilizzati. Se il sistema di comunicazione è collegato a un ITSP che offre un server STUN, non è necessario eseguire alcuna altra configurazione del sistema di comunicazione. Se tuttavia non viene utilizzato alcun ITSP o se l'ITSP utilizzato non offre alcun

server STUN, occorre configurare un server STUN nel sistema (vedere Come specificare il server STUN per Dispositivo@Home).

Configurazione del router Internet Office

Per consentire al telefono SIP di raggiungere il sistema di comunicazione tramite Internet, è necessario impostare l'inoltro alla porta SIP esterna nel router Internet Office. Per evitare attacchi SIP provenienti da Internet, occorre utilizzare una porta SIP esterna diversa da quelle standard.

Occorre inoltre impostare il protocollo di trasporto sul telefono SIP.

Tabella 9: Configurazione dell'inoltro alla porta nel router Office

Protocollo di trasporto	Porta SIP interna	Porta SIP esterna	Commento
UDP	5070	Acquisizione ad esempio di 5090.	Per configurare l'inoltro alla porta, la porta SIP interna ed esterna non deve essere la stessa. Come porta SIP esterna può essere inserito un valore diverso dalla porta SIP interna standard 5070. Pertanto, si raccomanda l'uso di UDP.
TCP	5070 Passare ad esempio a 5080.	Acquisizione ad esempio di 5080 (= porta SIP interna)	Per configurare l'inoltro alla porta, la porta SIP interna ed esterna deve essere la stessa. Per utilizzare una porta SIP esterna diversa da quella predefinita 5070, è necessario modificare la porta SIP interna. A tal fine è necessario riconfigurare tutti i componenti IP che utilizzano SIP. A tal fine, **non** è consigliato l'uso del TCP.
TLS	5071	Acquisizione di 5071 (= porta SIP TLS interna)	Per configurare l'inoltro alla porta, la porta SIP TLS interna ed esterna deve essere la stessa. Poiché la porta SIP TLS interna è già diversa da quella predefinita, è possibile indicare anche 5071 come porta SIP TLS esterna. A tal fine si raccomanda l'uso di TLS.

Nota: In un sistema aggiornato nessuna modifica delle porte SIP è eseguita automaticamente. Dopo l'aggiornamento le porte sono:

SIP_EXT = 5060

SIP_TLS_SUB_EXT = 5062

Questi valori devono essere modificati manualmente dall'amministratore se Dispositivo@Home è utilizzato in un sistema migrato.

Per l'uso del TLS nel sistema di comunicazione devono essere attivati certificati validi. Sono supportate connessioni TLS per utenti SIP sull'interfaccia LAN del sistema di comunicazione, ma non a livello dell'interfaccia WAN. Il Payload SRTP con la segnalazione SDES non è supportato.

Se il router Internet Office senza un indirizzo IP fisso è connesso a Internet, è necessario configurare il DynDNS del router Internet Office per consentire agli utenti SIP di raggiungere il sistema di comunicazione tramite Internet. L'indirizzo IP corrente viene registrato tramite l'account DynDNS a intervalli regolari. Gli account DynDNS gratuiti che scadono a intervalli regolari possono a volte causare problemi.

Configurazione del telefono SIP

Come esempio della configurazione è possibile ottenere un elenco di tutti i telefoni SIP testati che supportano STUN visitando il sito Internet Unify Experts Wiki. Sono riportati i valori che devono essere inseriti sul telefono SIP.

Configurazione del router Internet Home

Sul router Internet Home non è necessario eseguire alcuna configurazione particolare.

Il router Internet Home deve soddisfare i seguenti requisiti:

- Il router deve disporre di funzionalità VoIP con NAT abilitato (nessun NAT simmetrico).
- La funzione ALG del router deve essere disattivata.

La connessione a Internet deve assicurare una banda sufficiente per il trasferimento delle chiamate. In particolare con le connessioni DSL asimmetriche occorre assicurarsi che la banda in upload sia sufficiente.

Configurazione di myPortal @work

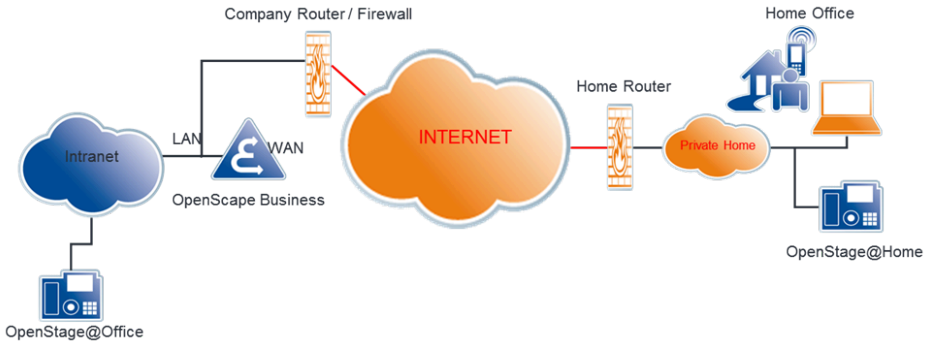
Per attivare myPortal @work e raggiungere il sistema di comunicazione su Internet, eseguire la seguente procedura:

- Configurare il server STUN per il sistema/client.
- Aprire e inoltrare alla porta 8802 (altri inoltri non sono validi).
- Il flag SBC non è necessario. Non è necessaria alcuna autenticazione.

19.4.3 Configurazione del DispositivoSistema@Home

Per connettersi a OpenScape Business tramite Internet con un telefono Dispositivo di Sistema, occorre configurare appositamente OpenScape Business, il router Internet di Office e il telefono Dispositivo di Sistema.

- **Figura 10: Esempio di caso d'uso di DispositivoSistema@Home**



Configurazione di OpenScape Business

Per registrare un utente DispositivoSistema@Home nel sistema di comunicazione tramite Internet, è necessario attivare la funzione SBC integrata per l'utente DispositivoSistema@Home (vedere Come attivare Dispositivo@Home alla pagina 981).

Con l'aiuto del protocollo STUN, la funzione SBC integrata rileva l'indirizzo IP pubblico del sistema di comunicazione e la porta utilizzati. Se il sistema di comunicazione è collegato a un ITSP che offre un server STUN, non è necessario eseguire alcuna altra configurazione del sistema di comunicazione. Se tuttavia non viene utilizzato alcun ITSP o se l'ITSP utilizzato non offre alcun server STUN, al sistema di comunicazione occorre presentare un server STUN (vedere Come specificare il server STUN per DispositivoSistema@Home).

Configurazione del router Internet Office

Per consentire agli utenti DispositivoSistema@Home di raggiungere il sistema di comunicazione tramite Internet, è necessario impostare l'inoltro alla porta DispositivoSistema nel router Internet Office. Per poter registrare da Internet, il router/firewall dell'ufficio deve essere configurato con una regola di inoltro porta:

- Dal TCP/4060 della porta esterna al TCP/4062(HFA) della porta interna, per non-TLS

  Dal TCP/4061 della porta esterna al TCP/4063(HFA) della porta interna, per TLS

  Nota: Durante la migrazione da V2R1 a una versione successiva, è necessario riconfigurare in base a questa regola anche il router internet dell'ufficio.

  Le porte summenzionate sono necessarie solo per i dispositivi di sistema (telefono HFA).

- Intervallo porte RTP in OpenScape Business X:30274-30529RTP intervallo porte in OpenScape Business S: 30528-30887 (valori predefiniti)

  Queste porte sono necessarie anche per i client UC con VoIP attivato, ad esempio myPortal to go, myPortal @work.

- TCP/8802 (HTTPS) (richiesto per il client Unified communications (es. myPortal to Go, myPortal to go Web o VoIP for myPortal to go configurato come DispositivoSistema@Home)

  Nota: La zona interna del firewall deve essere chiusa.

Il protocollo di trasporto è impostato presso l'utente DispositivoSistema@Home.

Se il router Internet Office è connesso a Internet senza un indirizzo IP fisso, è necessario configurare il DynDNS del router Internet Office per consentire agli utenti DispositivoSistema@Home di raggiungere il sistema di comunicazione tramite Internet. L'indirizzo IP corrente viene registrato tramite l'account DynDNS a intervalli regolari. Gli account DynDNS gratuiti che scadono a intervalli regolari possono a volte causare problemi.

Configurazione del router Internet Home

Sul router Internet Home non è necessario eseguire alcuna configurazione particolare.

Il router Internet Home deve soddisfare i seguenti requisiti:

- Il router deve disporre di funzionalità VoIP con NAT abilitato (nessun NAT simmetrico).
- La funzione ALG del router deve essere disattivata.

La connessione a Internet deve assicurare una banda sufficiente per il trasferimento delle chiamate. In particolare con le connessioni DSL asimmetriche occorre assicurarsi che la banda in upload sia sufficiente.

Configurazione del telefono HFA

Il gateway deve essere configurato con il nome DNS (ad esempio miaazienda.net) per consentire al telefono di raggiungere il sistema su Internet. Deve essere inoltre configurato l'IP di DLI. Per l'utente deve essere aggiunto un numero di telefono interno. Occorre inoltre impostare la password del dispositivo.

Limitazioni

- Non è possibile configurare applicazioni XML in OpenStage

19.4.4 Come attivare Dispositivo@Home

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utenti**.
3) Nella struttura dei menu, fare clic su **Utenti** > **Client IP** > **Client SIP** o **Client di sistema**
4) Nella struttura dei menu, fare clic sull'utente SIP o HFA desiderato.
5) Fare clic sulla scheda **Modifica i dati del WorkPoint Client**.

6) Inserire una password. I valori qui riportati devono essere inseriti anche nel telefono SIP o nel dispositivo di sistema.

Nota:

In una connessione a Internet è essenziale utilizzare una password sicura (almeno 8 caratteri comprendenti lettere minuscole, maiuscole, numeri e caratteri speciali).

Nota: La password dei client Deskshare dichiarati come @Home devono contenere esclusivamente caratteri numerici. La password è in realtà il codice PIN per l'attivazione della funzione di mobilità (codice di servizio della funzione: *9419). I dispositivi supportano esclusivamente caratteri numerici per i PIN.

Dopo aver impostato la password, **Registrazione Internet con SBC interna** diventa disponibile per l'attivazione.

Nota: La casella di controllo **Dopo uno speed upgrade o un riavvio del sistema, Autenticazione attiva** viene attivata per tutti gli endpoint SIP e visualizzata in grigio, in modo che l'utente non possa disabilitarla, se per almeno una stazione SIP è attivo il flag **Registrazione Internet con SBC interna**.

19.4.5 Come aggiornare il software per il dispositivo di sistema (HFA) @Home

La normale procedura di aggiornamento SW del DLI per un dispositivo connesso internamente non può essere utilizzata per il dispositivo di sistema (HFA) @Home in quanto ciò richiede l'accesso diretto all'indirizzo IP del dispositivo per il trasferimento del file. Il DLI non è in grado di determinare l'indirizzo IP del Dispositivo Sistema@Home a causa dei seguenti motivi:

- Il Dispositivo@Home si trova in una rete domestica che utilizza indirizzi IP privati. L'accesso a Internet viene eseguito tramite un router domestico con Network Address Translation (NAT).
- Il DLI di OpenScape Business si trova in una rete aziendale/dell'ufficio che utilizza indirizzi IP privati. La rete aziendale è connessa a Internet tramite il router aziendale/dell'ufficio.

Pertanto, la procedura di aggiornamento SW del DLI utilizza una connessione HTTPS aggiuntiva tramite porta 8804 (impostazione predefinita) in combinazione con la porta DLI 18443 (impostazione predefinita) per determinare la versione SW di Device@Home ed eseguire l'aggiornamento SW.

Il controllo della versione SW per Device@Home viene eseguito solo in presenza di una delle condizioni seguenti:

- Riavvio del dispositivo
- Cambio di configurazione a livello locale o in remoto
- Modifiche dell'inventario del dispositivo

- Accesso o disconnessione di un utente mobile da un dispositivo

In questi casi, il DLI controlla la versione del software del dispositivo ed esegue un aggiornamento SW nel caso in cui in OpenScape Business sia disponibile una versione SW più recente.

L'aggiornamento automatico del software di Device@Home da parte del DLI deve essere configurato in OpenScape Business. È disabilitato per impostazione predefinita e deve essere abilitato in modo esplicito.

L'operazione richiede i passaggi indicati di seguito.

Passo a passo

1) Eseguire la connessione al WBM con il profilo Expert.

2) Nella barra di navigazione, fare clic su **Modalità esperti**.

3) Nella struttura di navigazione fare clic su **Server telefonia > Impostazioni di base**.

4) Nella struttura di navigazione fare clic **Impostazioni di base > Implementazione parametri telefoni**.

- Fare clic su **Implementa SW nei dispositivi @Home** per assegnare le autorizzazioni per l'aggiornamento del software tramite DLI per i dispositivi di sistema HFA @Home. Il valore predefinito è "non selezionato".
- Fare clic su **Applica**, quindi su **OK**.

5) Impostazioni firewall

Nessuna impostazione firewall manuale richiesta in OpenScape Business. La porta 8804 viene aperta durante l'avvio del sistema e le richieste indirizzate a questa porta ricevono risposta solo dal sistema se il flag **Implementa SW nei dispositivi @Home** è abilitato.

6) Aprire le porte 18443 e 8804 usate per il DLI con la configurazione appropriata (inoltro porta) nel router aziendale/dell'ufficio.

Limitazioni

I dispositivi HFA@Home risiedono dietro a un firewall (router di casa). Il router o firewall induce un NAT (Network Address Translation) che rende l'indirizzo IP completamente invisibile al mondo esterno. Di conseguenza, i telefoni IP non possono essere visti da remoto per essere amministrati dal DLI.

L'effetto collaterale delle limitazioni di rete indicate in precedenza comporta che tutti gli eventi gestiti da DLI non potranno essere completati poiché vengono inviati all'indirizzo IP locale (non accessibile) del dispositivo.

Il risultato è che non sarà possibile eseguire alcun aggiornamento del software su richiesta. Sarà però possibile eseguire l'aggiornamento del software non appena il dispositivo avvierà uno scambio di messaggi aprendo una sessione HTTPS con il DLI. Le sessioni vengono aperte tramite eventi specifici gestiti da dispositivo, come:

- il riavvio del dispositivo.
- una modifica di configurazione implementata sul dispositivo (tramite visualizzazione locale o gestione basata su Web).
- modifiche dell'inventario del dispositivo.
- accesso o disconnessione di un utente mobile da un dispositivo.

In tutti questi casi, il DLI controllerà il software del dispositivo e, se necessario, il dispositivo verrà aggiornato al software ufficiale supportato da OSBiz.

Nota: L'implementazione del software viene attuata all'avvio del telefono (oppure durante la registrazione in OSBiz o ancora quando il sistema OSBiz entra in servizio).

19.4.6 Come specificare il server STUN per Dispositivo@Home

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Non è utilizzato alcun ITSP o l'ITSP utilizzato non fornisce alcun server STUN.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Gateway voce**.
3) Nella struttura dei menu fare clic su **Provider di servizi di telefonia Internet**.
4) Fare clic sulla scheda **Modifica configurazione STUN**.
5) Nell'area **Server STUN predefinito** in **Indirizzo IP / Nome host** inserire l'indirizzo IP o il nome host del server STUN (ad esempio, `stun.serviceprovider.com`).
6) Nell'area **Server STUN predefinito** in **Porta** indicare la porta del server STUN (ad esempio, `3478`).
7) Fare clic su **Applica**, quindi su **OK**.

20 Sicurezza

L'aspetto della sicurezza si riferisce alla protezione del sistema di sicurezza e dei dati salvati e trasmessi da accesso non autorizzato. Ciò può comprendere tra l'altro la protezione dell'accesso per la rete IP (firewall) e la trasmissione crittografata (SSL, VPN).

Lista di controllo di sicurezza

Nelle impostazioni del sistema di comunicazione è stato preso in considerazione l'aspetto della sicurezza delle comunicazioni. Alla messa in servizio è necessario personalizzare le funzioni in funzione delle esigenze specifiche del cliente e adottare ulteriori misure specifiche dell'ambiente del cliente. Per aumentare la consapevolezza dei rischi legati alla sicurezza e per attuare le misure più opportune, unitamente alla documentazione è disponibile una check list sulla sicurezza. Si consiglia di discutere quanto prima questo elenco con il cliente durante la messa in servizio nonché di documentare tutte le misure implementate.

20.1 Firewall

Un firewall è un insieme di componenti software e hardware che limita l'accesso fra reti diverse, per definire un concetto di sicurezza.

I firewall si trovano sull'interfaccia fra le singole reti e controllano il traffico dati fra le diverse zone, per ridurre il traffico indesiderato e lasciare passare solo il traffico dati richiesto. Le installazioni più frequenti del firewall sono riferite al controllo del traffico fra una rete locale (LAN) e Internet.

In una rete aziendale, il firewall isola la rete LAN interna da Internet.

Il sistema di comunicazione offre funzionalità di sicurezza integrate; a tale riguardo OpenScape Business X presenta delle differenze nelle funzionalità rispetto a OpenScape Business S.

OpenScape Business X offre i seguenti seguenti Servizi:

- Port Firewall/NAT (firewall tra porta WAN e LAN)
- Firewall applicaz. (firewall per l'accesso al sistema di comunicazione)

OpenScape Business S utilizza il firewall di Linux.

20.1.1 Port handling

Il Port handling viene utilizzato per l'attivazione di porte (port mapping, port forwarding) nel firewall del router integrato in OpenScape Business X.

Numeri di porta

Nota: Aprire le porte solo se richiesto per una specifica applicazione!

Le porte (servizi) sono richieste per la comunicazione tramite i protocolli TCP e UDP poiché consentono a più applicazioni di scambiare dati simultaneamente su una sola connessione.

Con il termine firewall si intende solitamente un port firewall con funzionalità di blocco di singoli servizi o porte. Il firewall della porta agisce solo sulla porta WAN di OpenScape Business.

Con OpenScape Business S con Linux è possibile attivare un firewall per le porte tramite LAN. In OpenScape Business X, il firewall è attivo sull'interfaccia WAN al fine di proteggere la rete interna (all'interfaccia LAN) da minacce provenienti da Internet. Tuttavia, se alcune porte/servizi devono essere raggiungibili da Internet, questi devono essere abilitati (vedere Abilitazione della porta). Tutte le porte/i servizi per le funzionalità di OpenScape Business X vengono automaticamente condivisi sulla rete LAN (nella rete interna del cliente).

OpenScape Business S dispone solo di un'interfaccia LAN (nella rete interna del cliente) e la protezione per l'accesso a Internet viene fornita da altri componenti/router in tale rete. È inoltre attivo il firewall Linux interno del server. Per l'uso delle funzionalità OpenScape Business, è necessario che vengano abilitate porte/servizi specifici (ad esempio per consentire ai telefoni di comunicare con OpenScape Business S). Questo avviene in modo automatico, tuttavia, l'amministratore può bloccare singoli servizi.

I numeri di porta accettano valori fra 0 e 65535 e devono essere assegnati alle diverse applicazioni. Fra 0 e 1023 si trovano quelle che vengono definite 'well-known ports' e sono assegnate in modo permanente dalla IANA (Internet Assigned Numbers Authority). Un elenco di queste porte è disponibile all'indirizzo http://www.iana.org/assignments/port-numbers.

20.1.1.1 Abilitazione della porta

Se il sistema definisce l'accesso a Internet (tramite la porta WAN), per impostazione predefinita l'unica comunicazione consentita è dalla rete interna (dalla rete aziendale o dal sistema di comunicazione) a Internet e i pacchetti di risposta associati. Le richieste che originano da Internet vengono bloccate. Questa impostazione di protezione può essere superata ad esempio aprendo la porta in modo selettivo per far funzionare un server Web sulla rete.

Nota: Se il sistema di comunicazione viene utilizzato come router Internet, la porta 5060 deve essere chiusa (impostazione predefinita). Con la telefonia Internet tramite ITSP, il sistema di comunicazione apre le porte corrispondenti e le mantiene aperte.

Anche se si utilizza un router esterno o un firewall, è necessario chiudere la porta 5060. È compito del sistema di comunicazione aprire questa porta quando necessario.

20.1.1.2 Come configurare dell'abilitazione della porta

Con la procedura guidata **Firewall** è possibile abilitare le porte in modo che il sistema di comunicazione o il PC della LAN siano accessibili tramite la porta WAN. L'abilitazione delle porte comporta il rischio di accesso da parte di persone non autorizzate. Pertanto, devono essere aperte solo le porte urgentemente richieste.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Sicurezza**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Firewall**. Viene visualizzata la finestra **Abilitazione della porta**.
4) Nella riga dell'applicazione desiderata/del servizio desiderato, selezionare l'opzione **Regola NAT attiva** per le porte da abilitare.
5) Nei campi **Porta globale**, **Indirizzo IP locale** e **Porta locale** immettere le informazioni per l'abilitazione.
6) Per l'abilitazione della porta di un servizio non impostato, fare clic su **Aggiungi** e compilare i campi **Descrizione**, **Regola NAT attiva**, **Porta globale**, **Indirizzo IP locale** e **Porta locale**.
7) Fare clic su **OK & Avanti**.
8) Fare clic su **Fine**.

20.1.1.3 Gestione della porta

La gestione delle porte consente di modificare le singole porte utilizzate dal sistema di comunicazione. Ciò consente di personalizzare la comunicazione di rete per ogni rete del cliente anche se le porte sono già utilizzate per altri scopi.

Se vengono apportate modifiche alla gestione delle porte, è di norma necessario modificare contemporaneamente anche tutti i componenti (telefoni, impianti, ecc.) per garantirne la funzionalità.

20.1.1.4 Come modificare le impostazioni globali della gestione delle porte

Qui occorre specificare i numeri di porta per le singole funzioni.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Gestione della porta**. Si apre la scheda **Modifica impostazioni globali della gestione delle porte**.
4) In **Numero di porta** indicare la porta per la relativa funzione oppure lasciare invariate le impostazioni.
5) Fare clic su **Applica**, quindi su **OK**.

20.1.2 NAT

NAT (Network Address Translation) è una procedura di conversione di indirizzi che consente di sostituire un indirizzo IP in un pacchetto dati con un altro. In una rete interna i client utilizzano indirizzi IP privati. Poiché questi indirizzi IP privati non possono essere inoltrati alla rete pubblica, NAT consente di convertire gli indirizzi IP privati in indirizzi IP pubblici. In questo modo i client possono accedere alle reti pubbliche e la struttura della rete interna con gli indirizzi IP privati rimane invisibile (nascosta) dalla rete pubblica (ad es. Internet). Per l'abilitazione della porta è necessario NAT o le regole NAT.

La conversione degli indirizzi viene effettuata al passaggio da rete interna a pubblica. NAT può essere eseguita su un router interno, un server dedicato o un altro dispositivo specifico. In questo modo un router grazie a NAT può collegare la rete interna a Internet.

La rete interna presenta a Internet solo l'unico indirizzo IP pubblico assegnato dall'ISP al router. Tutti gli accessi a Internet dalla rete interna vengono gestiti su questo indirizzo IP ufficiale con diversi numeri di porta. Il router sostituisce gli indirizzi IP privati con l'indirizzo IP ufficiale fornito dall'ISP. Quando si ricevono pacchetti di dati l'indirizzo IP ufficiale viene nuovamente convertito negli indirizzi IP privati. Per l'assegnazione si ricorre ai diversi numeri di porta. Solo gli indirizzi IP extra abilitati sono raggiungibili direttamente da Internet.

Regole NAT

Grazie alle regole NAT è possibile definire se gli indirizzi IP privati (locali) devono essere accessibili direttamente da Internet. A tale scopo è necessario definire regole NAT specifiche o utilizzare quelle predefinite per i servizi Server FTP. Nel complesso si possono definire 20 regole NAT. Per utilizzare una regola NAT, occorre immettere i dati di indirizzo locale dei PC client che deve mettere a disposizione il servizio via Internet e attivare la regola NAT. È possibile configurare più regole NAT con il supporto di un editor di tabelle. Le regole NAT non più necessarie possono essere eliminate.

Porte

All'avvio i server richiedono normalmente al sistema operativo porte specifiche per accettare le connessioni. Ad esempio, il server HTTP sulla porta 80, il server FTP sulla porta 21 ecc. Normalmente i client richiedono al sistema operativo una porta casuale per realizzare le connessioni.

20.1.2.1 Come configurare una regola NAT

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Telefonia** > **Routing**.

3) Configurare la regola NAT:
   - Se si desidera definire una nuova regola NAT, nella struttura dei menu, fare clic su **NAT** quindi sulla scheda **Aggiungi NAT**.
   - Se si desidera modificare una regola NAT esistente, nella struttura dei menu, navigare fino a **NAT**, quindi selezionare la regola NAT desiderata.
4) Nel campo **Descrizione** immettere un nome per la regola NAT. Non è possibile modificare il nome di una regola NAT predefinita.
5) Nel campo **Indirizzo IP locale** immettere l'indirizzo IP del client della rete interna che deve essere abilitato.
6) Nel campo **Porta locale** immettere il numero della porta che verrà utilizzata dall'applicazione del client interno.
7) Nel campo **Porta globale** immettere il numero della porta che verrà utilizzata dall'applicazione del partner di comunicazione esterno.
8) Nell'elenco a discesa **Protocollo** immettere il protocollo di trasporto utilizzato dall'applicazione (**TCP** o **UDP**). In una regola NAT predefinita non è possibile modificare il protocollo.
9) Se si desidera utilizzare la regola NAT, selezionare il pulsante di opzione **Regola NAT attiva**.
10) Fare clic su **Applica**, quindi su **OK**. La regola NAT attiva viene segnalata nella voce di menu **NAT** con un simbolo verde.

20.1.2.2 Come configurare più regole NAT con l'Editor tabelle NAT

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella barra di navigazione, fare clic su **Telefonia** > **Routing**.
3) Nella struttura dei menu fare clic su **Routing**.
4) Nella struttura dei menu fare clic su **NAT** quindi sulla scheda **Editor tabelle NAT**.
5) Configurare la regola NAT:
   - Se si desidera definire una nuova regola NAT, compilare i campi nella prima riga come descritto di seguito.
   - Se si desidera modificare una regola NAT disponibile, fare clic nei campi desiderati della regola NAT e compilarli come descritto di seguito.
6) Nella colonna **Indirizzo IP locale** immettere l'indirizzo IP del client della rete interna che deve essere abilitato.
7) Nella colonna **Porta locale** immettere il numero della porta che verrà utilizzata dall'applicazione del client interno.
8) Nella colonna **Porta globale** immettere il numero della porta che verrà utilizzata dall'applicazione del partner di comunicazione esterno.
9) Nell'elenco a discesa **Protocollo** immettere il protocollo di trasporto utilizzato dall'applicazione (**TCP** o **UDP**). In una regola NAT predefinita non è possibile modificare il protocollo.

10) Per utilizzare la regola NAT, selezionare la casella **Attiva** nella colonna.
11) Nella colonna **Descrizione** immettere un nome per la regola NAT. Non è possibile modificare il nome di una regola NAT predefinita.
12) Salvare la regola NAT:
    - Dopo aver configurato una nuova regola NAT, fare clic su **Aggiungi** quindi su **OK**. La nuova regola NAT viene aggiunta in fondo alla tabella.
    - Se è stata modificata una regola NAT esistente, procedere al passo 5.
13) Fare clic su **Applica**. Una regola NAT attiva viene segnalata nella voce di menu **NAT** con un simbolo verde.

20.1.2.3 Come cancellare una regola NAT

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Telefonia** > **Routing**.
2) Nella struttura di navigazione fare clic su **Routing**.
3) Nella struttura dei menu, fare clic su **NAT**.
4) Nella struttura dei menu fare clic sulla regola NAT da eliminare e selezionare la scheda **Cancella NAT**. Le regole NAT predefinite non possono essere eliminate.
5) Confermare l'avviso con **Elimina** quindi fare clic su **OK**. La regola NAT viene eliminata dall'elenco NAT nella voce di menu **NAT**.

20.1.3 Firewall applicaz.

Il firewall delle applicazioni viene utilizzato per limitare l'accesso a servizi specifici come FTP o LDAP. È disabilitato per impostazione predefinita e può essere abilitato definendo le regole appropriate.

I seguenti servizi possono essere bloccati o limitati a specifici indirizzi IP o intervalli di indirizzi IP dal firewall delle applicazioni in OpenScape Business X:

Servizio	Porte
FTP	21, 40000 - 40040
ssh (bloccato per impostazione predefinita)	22
LDAP	389
HTTPS	443
Postgres	5432
Manager E	7000
CSTA	7001 (FP), 7004 (FP), 8800 (CSP)
OBSERVER	Questo servizio consentiva l'accesso da un'applicazione OpenScape Observer, che non è più supportata.

Solo i servizi elencati possono essere bloccati tramite un menu di selezione in modalità Esperto.

Le funzioni telefoniche come SIP, HFA ecc. non possono essere bloccate usando il firewall delle applicazioni.

Un servizio può essere selezionato più volte; ogni volta è possibile specificare restrizioni IP diverse.

Nota: L'attivazione/disattivazione o la modifica dei parametri del firewall può limitare enormemente la funzionalità della scheda (ad esempio, l'amministrazione basata su LAN potrebbe non essere più possibile).

Nota: Se abilitato, il firewall delle applicazioni non blocca i servizi per impostazione predefinita fino a quando non viene aggiunta una regola per quel servizio, a quel punto solo gli indirizzi IP inclusi nella regola possono accedere a quel servizio specifico.

Il firewall delle applicazioni può limitare l'accesso alle funzioni inter-nodo quando il sistema è collegato in rete ad altri sistemi OpenScape Business. Ad esempio, la funzione di sopravvivenza richiede il servizio POSTGRES per funzionare correttamente; in questo caso, se viene aggiunta una regola per il servizio POSTGRES, è necessario aggiungere manualmente gli indirizzi IP degli altri nodi OpenScape Business collegati in rete alla regola POSTGRES per garantire il corretto funzionamento della funzione di sopravvivenza.

20.1.3.1 Come visualizzare la configurazione del Firewall applicazioni

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu, selezionare **Firewall applicaz.**.
4) Fare clic sulla scheda **Display Services** per visualizzare i servizi bloccati.
5) Nel campo **Nome della regola** viene visualizzato il nome della regola.
6) Il segno di spunta in **Regola attivata** indica se la regola è attivata o meno.
7) Nel campo **Limite inferiore dell'intervallo di indirizzi IP di origine**, viene mostrato il limite inferiore degli indirizzi IP bloccati.
8) Nel campo **Limite superiore dell'intervallo di indirizzi IP di origine**, viene mostrato il limite superiore degli indirizzi IP bloccati.

20.1.3.2 Come limitare i servizi tramite il Firewall applicazioni

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu, selezionare **Firewall applicaz.**.
4) Fare clic sulla scheda **Add Service** (Aggiungi servizio) per bloccare un intervallo di indirizzi IP e/o un servizio.
5) In **Nome regola** immettere un nome per questo servizio (questa regola).
6) In **Intervallo degli indirizzi** definire il **Limite inferiore** e il **Limite superiore** dell'intervallo consentito di indirizzi IP di origine.

   È possibile bloccare completamente l'accesso digitando 127.0.0.1.

   Suggerimento: Attivare una regola solo dopo essersi assicurati di avere configurato correttamente gli indirizzi IP autorizzati!

7) Fare clic su **Salva**.

20.1.3.3 Come eliminare la configurazione del Firewall applicazioni

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu, selezionare **Firewall applicaz.**.
4) Fare clic sulla scheda **Delete all Services** (Elimina tutti i servizi) per eliminare tutti i servizi.

20.1.4 Gestione dei servizi (OpenScape Business S)

Per impostazione predefinita il firewall interno di Linux è attivato, pertanto l'accesso a OpenScape Business S è impedito. Il sistema di comunicazione fornisce in ogni caso servizi (ad es. il servizio di telefonia) che richiedono l'apertura delle porte (servizi o Services). Dopo l'installazione di OpenScape Business S, queste porte e servizi necessari sono aperti nel firewall. Se i servizi quali ad esempio SNMP non devono essere utilizzati, possono essere bloccati nel firewall Linux.

Nota: Si osservi che il blocco dei servizi utilizzati da OpenScape Business S può provocare, compromettere e/o impedire la funzionalità del sistema di comunicazione stesso.

20.1.4.1 Come aggiungere o bloccare servizi

Passo a passo

1) Nella barra delle applicazioni, fare clic su **Computer**.
2) Nella struttura dei menu fare clic su **Sistema** > **YaST**.
3) Immettere la password dell'utente root e fare clic su **Continue** (Continua).
4) Nella struttura dei menu fare clic su **Security and Users** (Protezione e utenti).
5) Nell'area **Security and Users** (Protezione e utenti), fare clic su **Firewall**.
6) Nella struttura dei menu della finestra **Firewall Configuration: Start-UP** (Configurazione firewall: avvio), fare clic su **Allowed Services** (Servizi abilitati).
7) Nel campo **Allowed Services for Selected Zone** (Servizi abilitati per la zona selezionata), selezionare l'area per cui si desidera modificare i servizi – **External Zone**, **Demilitarized Zone**, **Internal Zona** (Zona esterna, Zona demilitarizzata, Zona interna).
8) Nel campo **Service to allow** (Servizio da abilitare) selezionare i servizi che si desidera abilitare selettivamente, quindi fare clic su **Add** (Aggiungi). Nel menu a discesa vengono visualizzati tutti i servizi attualmente consentiti.
9) Nel campo **Allowed Service** (Servizio abilitato), selezionare i servizi che si desidera bloccare, quindi fare clic su **Delete** (Elimina).
10) Eventualmente selezionare la casella di controllo **Protect Firewall from Internal Zone** (Proteggi firewall da zona interna).
11) Fare clic su **Advanced** (Avanzate) per aggiungere al firewall eventuali porte o protocolli numerici – **Ports TCP**, **UDP Ports**, **RPC Ports** e **IP Protocols** (Porte TCP, Porte UDP, Porte RPC e Protocolli PIP). Fare quindi clic su OK.
12) Fare clic su **Next** (Avanti). Vengono visualizzate le impostazioni effettuate per il firewall. Se necessario, è possibile visualizzare ulteriori informazioni tramite **Show Details** (Mostra dettagli).
13) Fare clic su **Fine**.

20.2 Crittografia segnalazione e payload (SPE)

La funzione SPE serve ad assicurare la protezione nella trasmissione di dati d'uso e segnalazione tra il sistema di telefonia IP e il sistema di comunicazione. Il servizio si basa su una procedura di crittografia asimmetrica, in cui vengono utilizzate chiavi pubbliche e private.

Crittografia dei dati d'uso e segnalazione:

- Crittografia segnalazione: la trasmissione di segnali tra il gateway e i client viene crittografata con una chiave a 128 bit. Per la trasmissione viene utilizzato il protocollo TLS con crittografia AES.
- Crittografia payload: i dati d'uso (detti anche dati voce o payload) vengono trasmessi tramite Secure Reale-time Transport Protocol (SRTP). e vengono crittografati con una chiave a 128 bit (AES). Il protocollo SRTP è utilizzato anche per le connessioni di rete IP. Il metodo di scambio delle chiavi per SRTP è chiamato "multimedia Internet Keying", in sigla MIKEY.

Per l'uso di SPE si deve garantire l'identificazione univoca dei singoli telefoni di sistema e dei sistemi di comunicazione interessati. Ciò si ottiene tramite certificati contenenti anche le chiavi pubbliche.

Le chiavi o i certificati vengono distribuiti dal server DLS (tuttavia non possono essere distribuiti manualmente).

Suggerimento: La funzione SPE non è disponibile per gli utenti SIP e WL2.

Una connessione crittografata sussiste solo nella connessione diretta tra due telefoni di sistema o per le conferenze.

Crittografia SRTCP

SRTCP (Secure Real Time Transport Control Protocol) è un'ottimizzazione del protocollo SRTP e provvede alla protezione dei dati di controllo. L'ottimizzazione prevede tre campi aggiuntivi: un indice SRTCP, un flag di crittografia e un tag di autenticazione.

Conformità SPE

Family / Protocol / Interface		Signalling Encryption								Payload Encryption				
	Column1	HFA Subscriber	SIP Subscriber	TDM Subscriber	Analog Subscriber	SIP-Q Trunking	ISDN CO	FAX (T38, G711)	Column2	HFA Subscriber2	SIP Subscriber2	TDM Subscriber2	Analog Subscriber2	IP-Q Trunking (GW)
OpenScape Office MX/LX														
HFA		s	nv	t	t	s	t	t		y	n	y	y	y
SIP-UA		t*	t*	nv	nv	t*	nv	nv		n	n	n	n	n
SIP-Trunking/ITSP		t*	nv	nv	nv	t*	nv	nv		n	n	n	n	n
SIP-Q Homogenous		s	t*	t	t	s	t	t*		y	n	y	y	y
Media Server / Conference		t	nv	nv	nv	t	nv	nv		n	n	n	n	n
Openscape Business X3/X5/X8														
HFA		s	nv	t	t	s	t	t		y	n	y	y	y
SIP-UA		t*	t*	nv	nv	t*	nv	nv		n	n	n	n	n
SIP-Trunking/ITSP		t*	nv	nv	nv	t*	nv	nv		n	n	n	n	n
SIP-Q Homogenous		s	t*	t	t	s	t	t*		y	n	y	y	y
SIP-Q Heterogenous - H4k		s	t*	t	t	s	t	t*		y	n	y	y	y
SIP-Q Heterogenous - OSV		s	t*	t	t	s	t	t*		y	n	y	y	y
Media Server / Conference		t	nv	nv	nv	t	nv	nv		n	n	n	n	n
MEB / VSL		t	nv	nv	nv	t	nv	nv		n	n	n	n	n

Legenda:

Signaling encryption	
nv	Nessuna sicurezza VoIP
t	Predefinito: TLS sul lato VoIP, senza Secure Payload end-to-end
s	Crittografia segnalazione e payload (SPE)
*	Nessuna crittografia end-to-end della segnalazione (TLS)
Crittografia payload	
y	Secure Payload (SRTP)
n	Non Secure Payload (RTP)

20.2.1 Come attivare o disattivare il supporto SPE

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema** > **Flag di sistema**.
4) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare la funzione SPE (Signaling and Payload Encryption), selezionare la casella di controllo **Supporto SPE**.
   - Se si desidera disattivare la funzione SPE (Signaling and Payload Encryption), deselezionare la casella di controllo **Supporto SPE**.
5) Fare clic su **Applica**, quindi su **OK**.

20.2.2 Come modificare le impostazioni di protezione SPE

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Sicurezza** > **Crittografia segnalazione e payload (SPE)**.
3) Nella finestra **Modifica impostazioni di protezione SPE** in **Lunghezza minima delle chiavi RSA**, selezionare la lunghezza minima delle chiavi del protocollo di sicurezza (512, 1024 o 2048).
4) Selezionare la voce **Convalida certificati con verifica CRL necessaria**, se si desidera procedere a una sincronizzazione con l'elenco CRL (elenco di certificati revocati).
5) Nel campo **Intervallo massimo di rinegoziazione chiavi [ore]** indicare il tempo (in ore) trascorso il quale verrà assegnata una nuova coppia di chiavi.

6) Fare clic su **Applica**.

20.2.3 Come importare il certificato SPE e la chiave privata (file PKCS#12)

Se non è disponibile alcun certificato personalizzato, è possibile generare un certificato CA autofirmato in SSL > Creazione certificati, e con questo creare e memorizzare un certificato server firmato CA (PKCS#12). Questo viene quindi importato per SPE.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Sicurezza** > **Crittografia segnalazione e payload (SPE)**.
3) Nella struttura dei menu, navigare fino a **Certificato SPE**.
4) In **Importa certificato SPE e chiave privata (file PKCS#12)**, nel campo **Password di decrittografia**, inserire la password per la decrittografia creata durante la generazione del file.
5) Nel campo **File con certificato e chiave privata (formato PKCS#12 o PEM)** inserire il file del certificato e con **Sfoglia** scegliere le cartelle.

   Suggerimento: Se si sta installando un certificato per la prima volta e SPE è attivo, il sistema viene resettato automaticamente!

6) Fare clic su **Mostra impronta digitale del certificato** se si desidera verificare l'integrità.

20.2.4 Come importare il certificato CA SPE

Questo passaggio non è necessario con l'uso di certificati autogenerati utilizzando **SSL - Creazione certificati**.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Sicurezza** > **Crittografia segnalazione e payload (SPE)**.
3) Nella struttura dei menu, navigare fino a **Certificati CA di SPE**.
4) Nella finestra **Importa certificato CA attendibile per SPE (file X.509)** nel campo **File con certificato (PEM o binari)**, inserire il nome del file del certificato, quindi premere **Sfoglia** e selezionare il file.
5) In **Protocollo punto di distribuzione CRL (CDP)** selezionare il protocollo per l'elenco CRL (Certificate Revocation List) (**LDAP** o **HTTP**).

6) Nel campo **CDP (senza, ad es., ldap://)**, inserire il server desiderato.
7) Fare clic su **Mostra impronta digitale del certificato**.

20.2.5 Come attivare o disattivare l'abilitazione SPE per un utente

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Navigare nella struttura dei menu in **Utente** > **Utente** > **Client IP**, fino all'utente desiderato (client di sistema)
3) Nella finestra **Utente** scegliere la scheda **Modifica i parametri dell'utente** e quindi la voce **Sicurezza payload**.
4) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare la funzione, in **Sicurezza payload**, scegliere **On**.
   - Se si desidera disattivare la funzione, in **Sicurezza payload**, scegliere **Off**.
5) Fare clic su **Applica**.

20.3 Virtual Private Network, VPN

Una VPN (Virtual Private Network) è una rete di computer che viene utilizzata per il trasporto di dati privati su una rete pubblica (ad es. Internet). Consente quindi una trasmissione protetta su reti non protette. La trasmissione dei dati è crittografata.

Panoramica VPN

VPN offre:

- Connessioni protette tramite supporto non protetto (Internet)
- Protezione dei dati riservati dalla manipolazione
- Integrazione sicure di partner esterni nella rete aziendale
- Accesso a informazioni aziendali per i servizi esterni

Per garantire la sicurezza delle comunicazioni, VPN funziona nel modo seguente: viene creato un tunnel fra i partner di comunicazione. Durante la creazione del tunnel avvengono l'autenticazione e l'autorizzazione. Una volta creato il tunnel vengono trasmessi i dati crittografati.

Una VPN può essere creata fra (almeno) due computer o reti (punti tunnel).

Esistono due tipi di collegamento in rete:

- VPN Site-to-Site

  Qui avviene la crittografia fra i due gateway VPN; i dati vengono trasmessi sulla LAN crittografati.

- VPN End-to-Site

  Remote Access VPN (accesso remoto di collaboratori mobili)

Informazioni specifiche del sistema

L'amministrazione dei parametri VPN avviene principalmente tramite procedura guidata.

Fare attenzione in quanto la connessione al sistema di comunicazione deve avvenire tramite SSL sicuro. Questa può essere realizzata mediante OpenScape e OpenSSL.

Dipendenze

Argomento	Dipendenza
DynDNS	I terminali VPN devono essere accessibili tramite un nome di dominio o un indirizzo IP fisso. In caso contrario, è possibile utilizzare DynDNS.
DynDNS	Se si modifica un indirizzo IP in una VPN, il sistema di comunicazione aggiorna i dati relativi al nome host (indirizzo IP) in DynDNS.
DNS	Ciascun partner VPN può risolvere i nomi host/ gli indirizzi IP tramite il protocollo DNS standard. Tutti i nomi DNS (ad es. nome host) devono essere nomi di dominio completi (FQDN). Durante l'aggiornamento dell'indirizzo IP tramite DNS, non sono possibili connessioni via tunnel IPSec.

20.3.1 Requisiti per VPN

Per garantire la qualità della trasmissione dati e voce, le reti utilizzate devono soddisfare requisiti specifici. Tenuto conto in particolare della crittografia, è necessario prevedere una larghezza di banda maggiore rispetto alle altre reti.

Negli esempi seguenti nelle tabelle si presuppone la modalità di crittografia "Modalità tunnel ESP con autenticazione". Questa modalità offre la massima sicurezza per le reti VPN Site-to-Site.

Struttura di un pacchetto vocale crittografato:

Lunghezza dell'intestazione ESP

Padding

Calcolo della larghezza di banda per l'algoritmo di crittografia AES:

Calcolo della larghezza di banda per l'algoritmo di crittografia DES / 3DES:

Larghezza di banda per fax T.38

Protocollo	Byte	
ESP Trailer	12	
ESP Padding	varia (y)	crittografato
ESP Padding Header	2	crittografato
Voice Payload	varia (x)	crittografato

Protocollo	Byte	
RTP	12	crittografato
UDP	8	crittografato
IP (originale)	20	crittografato
Intestazione ESP	8 + iv	
IP (Tunnel)	20	
802.1Q VLAN Tagging	4	
MAC (incl. Preamble, FCS)	26	
Totale	**112 + iv + x + y**	

La lunghezza dell'intestazione ESP dipende dall'algoritmo di crittografia utilizzato.

È necessaria in caso di Cipher Block Chaining (concatenazione dei blocchi crittografati). L'intestazione ESP include un vettore di inizializzazione (AI). La lunghezza di tale vettore è identica alla lunghezza del blocco crittografato.

Il padding è necessario poiché gli algoritmi di crittografia si basano sulla crittografia a blocchi. Pertanto la parte crittografata totale del pacchetto (intestazione IP/UDP/RTP originale + carico voce + intestazione-padding ESP) deve essere pari a un multiplo intero della lunghezza del blocco crittografato.

Lunghezza dei blocchi nell'algoritmo di crittografia:

Algoritmo di crittografia	Lunghezza del blocco	Lunghezza iv del vettore di inizializzazione
AES	16 byte (128 bit)	16 byte (128 bit)
3DES	8 byte (64 bit)	8 byte (64 bit)

Calcolo dei byte di padding necessari per i pacchetti voce:

(42 + x + y) (byte) = N x (0 oppure 16 (byte)) (N intero)

Codec	Parametri di pacchettizza	Frame - dimensioni (ms)	Payload (byte)	Padding (byte)	Lunghezza del pacchetto Ethernet (byte)	Rapporto overhead payload/ pacchetto	Carico Ethernet (incl. intestazione) (kBit/s)
G.711	20	20	160	6	294	75%	117,6
G.711	30	30	240	6	372	50%	99,2
G.711	40	40	320	6	454	38%	90,8
G.711	60	60	480	6	614	25%	81,9
G.729A	1	20	20	2	150	600%	60,0
G.729A	2	40	40	6	182	300%	36,4
G.729A	3	60	60	2	198	200%	26,4

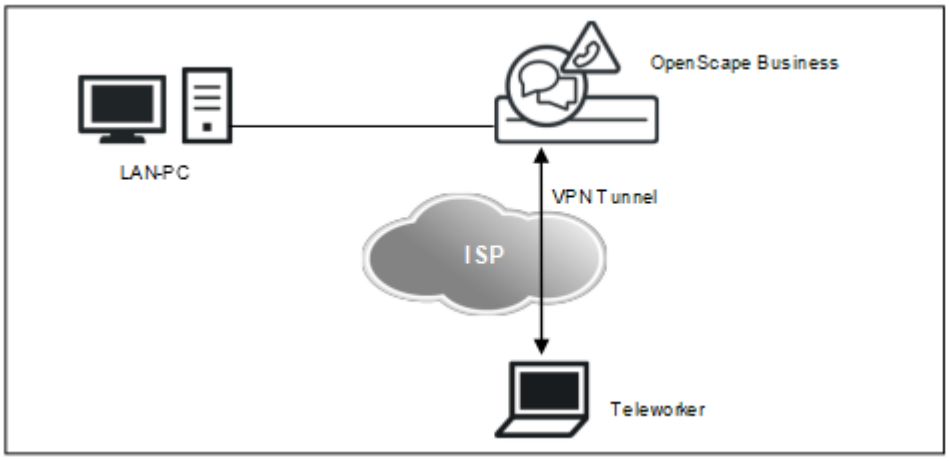
Codec	Parametri di pacchettizza	Frame - dimensioni (ms)	Payload (byte)	Padding (byte)	Lunghezza del pacchetto Ethernet (byte)	Rapporto overhead payload/ pacchetto	Carico Ethernet (incl. intestazione) (kBit/s)
G.711	20	20	160	6	286	75%	114,4
G.711	30	30	240	6	366	50%	97,6
G.711	40	40	320	6	446	38%	89,2
G.711	60	60	480	6	606	25%	80,8
G.729A	1	20	20	2	142	600%	56,8
G.729A	2	40	40	14	166	300%	33,2
G.729A	3	60	60	10	182	200%	24,3

Algoritmo di crittografia	Dimensione del frame (ms)	Payload y (byte)	Padding x (byte)	Lunghezza del pacchetto Ethernet (byte)	Pacchetto Payload (overhead in percentuale)	Carico Ethernet (incl. intestazione) (kBit/s)
DES / 3DES	30	169	1	278	64%	74,1
AES	30	169	9	294	74%	78.3

20.3.2 Connessione di operatori remoti tramite VPN

La rete VPN consente agli operatori remoti di connettersi al sistema di comunicazione tramite una connessione sicura.

Sistema indipendente con collegamento di operatori remoti tramite VPN



Il sistema di comunicazione dispone di funzionalità VPN integrate (configurazione tramite procedura guidata). Tramite VPN possono essere contemporaneamente attivi fino a 10 operatori remoti per sistema di comunicazione.

I seguenti client VPN sono compatibili con OpenScape Business:

- Client NCP VPN
- Client Shrew Soft VPN
- Client Android VPN
- Client iOS VPN
- Client Mac OS X VPN

Esportazione dei dati degli operatori remoti

I dati dell'operatore remoto possono essere esportati in un file ZIP (non crittografato). Nel file ZIP, per ogni client VPN supportato, si trova un file di testo separato con i dati dell'operatore remoto: per il client NCP VPN sotto forma di file `.ini`; per il client Shrew Soft VPN sotto forma di file `.vpn` e per il client OS X VPN sotto forma di file `.networkConnect`. Questi file di testo possono essere importati nel client VPN.

Suggerimento: Eventuali umlaut o accenti non vengono considerati nel file di testo con i dati degli operatori remoti. Gli eventuali spazi vengono sostituiti da caratteri di sottolineatura.

Visualizzazione dello stato delle connessioni VPN

Per la visualizzazione dello stato di tutte le connessioni VPN, utilizzare la procedura guidata **VPN**. Una panoramica dettagliate di tutte le connessioni VPN è disponibile nel **Centro assistenza**, in **Diagnostica** > **Stato** > **Stato VPN**.

VPN con OpenScape Business S

In OpenScape Business S, il tratto VPN viene terminato in corrispondenza di un router esterno. La descrizione delle applicazioni esterne esula dalla presente trattazione.

20.3.2.1 Come configurare la connessione di operatori remoti tramite VPN

La procedura guidata **VPN** consente agli operatori in remoto di accedere alla LAN interna tramite VPN (Virtual Private Network) e di collegare sistemi di com comunicazione tramite VPN. Se il sistema di comunicazione non dispone di indirizzo IP esterno fisso (indirizzo IP pubblico, indirizzo IP globale), è necessario configurare un servizio DynDNS, ad esempio su www.dyndns.org.

Prerequisiti

L'accesso a Internet tramite l'interfaccia WAN è configurato.

Se l'interfaccia WAN non dispone di alcun indirizzo IP fisso (pubblico), è necessario configurare il DynDNS. Perché il test DynDNS abbia successo è necessaria una connessione a Internet.

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.

2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Rete / Internet**.

3) Fare clic su **Modifica**, per avviare la procedura guidata **Configurazione VPN**. L'impostazione predefinita è **VPN è disattivato**.

4) Fare clic su **Configurazione di VPN**.
5) Se si desidera modificare una connessione VPN configurata, nella connessione VPN desiderata fare clic su **Modifica**.
6) Se si desidera creare una nuova connessione VPN, fare clic su **Aggiungere**.
7) Nel campo **Nome del gateway** assegnare un nome alla connessione VPN (ad esempio, `node2mch.dyndns.org`).
8) Inserire un eventuale **Commento** nel campo appropriato.
9) Selezionare la casella di controllo **attivo** (già selezionata per impostazione predefinita).
10) Selezionare la casella di controllo **Utilizza dati del sistema**.
11) Se necessario, selezionare il **Tipo di indirizzo**:
    - Se l'interfaccia WAN dispone di un indirizzo IP fisso (pubblico), selezionare dal menu a discesa **Tipo di indirizzo** la voce **Indirizzo IP** e inserire in **Indirizzo IP globale/ Nome DNS (WAN)** tale indirizzo IP fisso (pubblico).
    - Se l'interfaccia WAN non dispone di un indirizzo IP fisso (pubblico), selezionare dal menu a discesa **Tipo di indirizzo** la voce **Nome DNS**. In **Indirizzo IP globale / Nome DNS (WAN)** immettere il nome DNS del sistema di comunicazione già configurato per il DynDNS.
12) Modificare l'**indirizzo IP locale (LAN)** solo se necessario.
13) Modificare la **Maschera di sottorete locale (LAN)** solo se necessario.
14) Se si desidera modificare un operatore remoto già configurato, nell'area **Operatore remoto**, selezionando l'operatore remoto desiderato, fare clic su **Modifica**.
15) Per configurare un nuovo operatore remoto, nell'area **Operatore remoto**, fare clic su **Aggiungi**.
16) Nel campo **Nome** specificare il nome per la configurazione di questo operatore remoto.
17) Configurare il tipo di client VPN utilizzato:
    - Per operatore remoto IPSec VPN puro (client NCP e Shrew Soft VPN):

      Deselezionare la casella di controllo **L2TP/IPSec**, selezionare come **Tipo di indirizzo** la voce **Indirizzo IP**. Nel campo **Indirizzo IP virtuale / Nome DynDNS** immettere un indirizzo IP virtuale per l'operatore remoto se il client VPN configurato supporta gli indirizzi IP virtuali (indipendentemente dal tipo di accesso a Internet di cui dispone l'operatore remoto: router DSL o modem DSL).
    - Per l'operatore remoto L2TP/IPSec VPN (client VPN iOS, Android e Mac OS X):

      Selezionare la casella di controllo **L2TP/IPSec** e assegnare un **Nome utente** e una **Password** all'operatore remoto.
18) Selezionare la casella di controllo **attivo** (già selezionata per impostazione predefinita).
19) Fare clic su **OK**. Viene nuovamente visualizzata la finestra di panoramica sull'operatore remoto. È possibile aggiungere ulteriori operatori remoti.
20) Una volta configurati tutti gli operatori remoti, fare clic su **OK & Avanti**. Viene visualizzata la finestra **Scegli sistema**.
21) Fare clic su **OK&Avanti**. Viene visualizzata la finestra **Impostazioni di protezione delle connessioni**.

22) Alla connessione VPN appena configurata assegnare una chiave per la connessione VPN sicura nel campo **PreShared Secret**, quindi digitare nuovamente la stessa chiave in **Ripetizione del PreShared Secret**. La chiave deve contenere almeno 20 caratteri.
23) Eventualmente inserire un **Commento**.
24) Fare clic su **OK**. Viene visualizzata la finestra **Informazioni di stato VPN**.
25) Fare clic su **Attiva VPN**.
26) Solo se come tipo di indirizzo è stato utilizzato il nome DNS: controllare i dati già configurati dell'account DynDNS e fare clic su **Test connessione**. I dati di accesso DNS vengono comunicati al provider di servizi. Questo processo dura circa 10 secondi. In caso contrario, verificare i dati di accesso. Se il test ha avuto esito positivo, fare clic su a **OK**.
27) Fare clic su **OK&Avanti**. L'operatore remoto può ora accedere all'interfaccia WAN del sistema di comunicazione.
28) Fare clic su **Fine**.

20.3.2.2 Come esportare i dati degli operatori remoti

Con la procedura guidata **VPN** è possibile esportare i dati dell'operatore remoto.

Prerequisiti

È stata configurata una connessione VPN.

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Rete / Internet**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Configurazione VPN**. L'impostazione predefinita è **VPN è disattivato**.
4) Fare clic su **Esporta/Importa**.
5) Nell'area **Esporta dati operatore remoto dal sistema** fare clic su **Esporta**. Salvare il file ZIP in una posizione di memoria a scelta.

> **Suggerimento:** Nel file ZIP è contenuto un file per ogni client VPN supportato comprendente i dati degli operatori remoti. I dati degli operatori remoti non sono crittografati! Adottare un approccio responsabile con tali dati.

6) Fare clic su **OK & Avanti**, quindi su **Fine**.

20.3.3 Collegamento in rete di sistemi di comunicazione tramite VPN

Più sistemi di comunicazione OpenScape Business possono essere collegati in rete tra loro realizzando una rete VPN sicura site-to-site.

Collegamento tramite rete VPN

In un sistema di comunicazione, è possibile configurare tutti i dati per la connessione in rete di più sistemi, quindi esportare i dati della topologia crittografati e importarli in tutti gli altri sistemi del sistema di reti. In questo modo sarà possibile realizzare rapidamente una configurazione coerente in tutti i sistemi del sistema di reti.

La distinzione tra il proprio sistema e i sistemi stranieri avviene tramite il riconoscimento del proprio nome DynDNS o (se si utilizzano indirizzi IP fissi) tramite il proprio indirizzo Internet.

- Esporta dati topologia dal sistema
  - Tutti i dati sulla struttura della rete VPN vengono raccolti in un file XML crittografato e resi disponibili sotto forma di file ZIP pronto per l'esportazione in un altro sistema.
- Importazione dei dati di topologia nel sistema
  - Tutti i dati relativi alla struttura della rete VPN possono essere importati come file ZIP (contenente il file XML crittografato) e utilizzati per questo sistema.

La chiave (password) per l'esportazione può essere scelta liberamente e deve essere comunicata a ogni altro amministratore che desidera importare tali impostazioni.

Visualizzazione dello stato delle connessioni VPN

Per la visualizzazione dello stato di tutte le connessioni VPN, utilizzare la procedura guidata **VPN**. Una panoramica dettagliate di tutte le connessioni VPN è disponibile nel **Centro assistenza**, in **Diagnostica** > **Stato** > **Stato VPN**.

20.3.3.1 Come configurare la connessione di rete tramite VPN

Con la procedura guidata **VPN** è possibile configurare in un sistema tutti i sistemi di comunicazione della connessione di rete VPN. I dati di questa topologia possono essere esportati e importati in tutti i sistemi del sistema di reti VPN.

Prerequisiti

L'accesso a Internet tramite l'interfaccia WAN è configurato.

Se l'interfaccia WAN non dispone di alcun indirizzo IP fisso (pubblico), è necessario configurare il DynDNS. Perché il test DynDNS abbia successo è necessaria una connessione a Internet.

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Rete / Internet**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Configurazione VPN**. L'impostazione predefinita è **VPN è disattivato**.
4) Fare clic su **Configurazione di VPN**.
5) Fare clic su **Aggiungi**.

6) Nel campo **Nome del gateway** assegnare un nome al primo sistema del sistema di reti VPN (ad esempio, `node1mch.dyndns.org`).
7) Inserire un eventuale **Commento** nel campo appropriato.
8) Selezionare la casella di controllo **attivo** (già selezionata per impostazione predefinita).
9) Selezionare la casella di controllo **Utilizza dati del sistema**. I seguenti campi vengono compilati con i dati del sistema.
10) Se necessario, selezionare il **Tipo di indirizzo** predefinito:
    - Se l'interfaccia WAN dispone di un indirizzo IP fisso (pubblico), selezionare dal menu a discesa **Tipo di indirizzo** la voce **Indirizzo IP** e inserire in **Indirizzo IP globale/ Nome DNS (WAN)** tale indirizzo IP fisso (pubblico).
    - Se l'interfaccia WAN non dispone di un indirizzo IP fisso (pubblico), selezionare dal menu a discesa **Tipo di indirizzo** la voce **Nome DNS**. In **Indirizzo IP globale / Nome DNS (WAN)** immettere il nome DNS del sistema di comunicazione già configurato per il DynDNS.
11) Modificare l'**indirizzo IP locale (LAN)** predefinito solo se necessario.
12) Modificare la **Maschera di sottorete locale (LAN)** predefinita solo se necessario.
13) Fare clic su **OK&Avanti**. Viene visualizzata la finestra **Scegli sistema**.
14) Fare clic di nuovo su **Aggiungere**.
15) Nel campo **Nome del gateway** assegnare un nome al secondo sistema del sistema di reti VPN (ad esempio, `node2mch.dyndns.org`).
16) Inserire un eventuale **Commento** nel campo appropriato.
17) Selezionare la casella di controllo **attivo** (già selezionata per impostazione predefinita).
18) Selezionare il **Tipo di indirizzo** del secondo sistema:
    - Se l'interfaccia WAN dispone di un indirizzo IP fisso (pubblico), selezionare dal menu a discesa **Tipo di indirizzo** la voce **Indirizzo IP** e inserire in **Indirizzo IP globale/ Nome DNS (WAN)** tale indirizzo IP fisso (pubblico).
    - Se l'interfaccia WAN non dispone di un indirizzo IP fisso (pubblico), selezionare dal menu a discesa **Tipo di indirizzo** la voce **Nome DNS**. In **Indirizzo IP globale / Nome DNS (WAN)** immettere il nome DNS del sistema di comunicazione già configurato per il DynDNS.
19) Immettere l'**Indirizzo IP locale (LAN)** del secondo sistema.
20) Immettere la **maschera di sottorete locale (LAN)** del secondo sistema.
21) Fare clic su **OK&Avanti**. Viene visualizzata la finestra **Scegli sistema**.
22) Ripetere i punti da 14 a 21 per gli altri sistemi del sistema di reti VPN.
23) Infine, fare clic su **OK & Avanti**. Viene visualizzata la finestra **Impostazioni di protezione delle connessioni**.
24) Ad ogni connessione VPN di un sistema ad un altro assegnare una propria chiave in **PreShared Secret** e digitare nuovamente la chiave in **Ripetizione del PreShared Secret**. La chiave deve contenere almeno 20 caratteri.
25) Eventualmente inserire un **Commento** per ogni connessione VPN.
26) Fare clic su **OK**. Viene visualizzata la finestra **Informazioni di stato VPN**.

27) Per esportare i dati della topologia, fare clic su **Esporta/Importa**. Viene visualizzata la finestra **Esportazione e importazione dati di configurazione VPN**.
28) Nell'area **Esporta dati topologia dal sistema**, immettere in **Chiave** e **Ripeti chiave** una chiave (min. 7 cifre) per la protezione dei dati e fare clic su **Esporta**. Salvare il file ZIP in una posizione di memoria a scelta.
29) Fare clic su **OK & Avanti**.
30) Fare clic su **Attiva VPN**.
31) Solo se come tipo di indirizzo è stato utilizzato il **Nome DNS**: controllare i dati già configurati dell'account DynDNS e fare clic su **Test connessione**. I dati di accesso DNS vengono comunicati al provider di servizi. Questo processo dura circa 10 secondi. In caso contrario, verificare i dati di accesso. Se il test ha avuto esito positivo, fare clic su **OK**.
32) Fare clic su **OK & Avanti**, quindi su **Fine**.
33) Nella barra di navigazione del WBM del secondo sistema fare clic su **Configurazione** e nella struttura di navigazione su **Procedure guidate** > **Rete / Internet**.
34) Fare clic su **Modifica**, per avviare la procedura guidata **Configurazione VPN**. L'impostazione predefinita è **VPN è disattivato**.
35) Per esportare i dati della topologia, fare clic su **Esporta/Importa**. Viene visualizzata la finestra **Esportazione e importazione dati di configurazione VPN**.
36) Fare clic su **Importa dati topologia sul sistema** per importare i dati della topologia.
37) Immettere la **Chiave** (Password) precedentemente inserita per l'esportazione dei dati del primo sistema.
38) Selezionare il percorso del file zip. Fare quindi clic su **Importa**.
39) Fare clic su **OK&Avanti**. Si visualizzano i sistemi configurati.
40) Fare clic su **Attiva VPN**.
41) Solo se come tipo di indirizzo è stato utilizzato il **Nome DNS**: controllare i dati già configurati dell'account DynDNS e fare clic su **Test connessione**. I dati di accesso DNS vengono comunicati al provider di servizi. Questo processo dura circa 10 secondi. In caso contrario, verificare i dati di accesso. Se il test ha avuto esito positivo, fare clic su **OK**.
42) Fare clic su **OK & Avanti**, quindi su **Fine**.
43) Ripetere i punti da 33 a 42 per i restanti sistemi nel sistema di reti VPN.

20.3.3.2 Come esportare e importare i dati relativi alla topologia di una rete VPN

Con la procedura guidata **VPN** è possibile esportare e importare i dati relativi alla topologia della rete tramite VPN.

Prerequisiti

È stata configurata una connessione VPN.

Per importare i dati della topologia è necessario conoscere la chiave assegnata durante l'esportazione.

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Rete / Internet**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Configurazione VPN**. L'impostazione predefinita è **VPN è disattivato**.
4) Fare clic su **Esporta/Importa**.
5) Se si desidera esportare i dati della topologia, nell'area **Esporta dati topologia dal sistema**, immettere in **Chiave** e **Ripeti chiave** una chiave (min. 7 cifre) per la protezione dei dati e fare clic su **Esporta**. Salvare il file ZIP in una posizione di memoria a scelta.
6) Se si desidera importare i dati della topologia, nell'area **Importa dati topologia sul sistema** in **Chiave** immettere la chiave per decrittografare i dati, quindi selezionare il percorso per il file zip. Infine fare clic su **Importa**.
7) Fare clic su **OK & Avanti**, quindi su **Fine**.

20.3.4 VPN - Meccanismi di protezione

La crittografia dei dati sulle reti VPN avviene tramite diversi meccanismi, come il tunnel IPSec, Security Associations e metodi di autenticazione (Peer-to-Peer, firme digitali).

Tunnel IPSec

IPSec viene utilizzato per la crittografia dei dati e può prevedere o meno l'uso di un tunnel. IPSec è una possibilità per realizzare VPN. Consente infatti di crittografare l'intero pacchetto IP, compresa l'intestazione utilizzando la modalità tunnel.

I tunnel devono sempre essere configurati per entrambi i partner VPN.

Con IPSec è possibile configurare lo scambio automatico delle chiavi Internet (IKE, Internet Key Exchange). Si tratta di un'impostazione predefinita, integrata in IPSec.

Security Associations SA

IKE-SA

Payload-SA

Autenticazione

Una Security Association (SA, ovvero associazione di sicurezza) è un'intesa fra due entità comunicanti in una rete informatica. Descrive come entrambe le parti possano utilizzare i servizi di protezione per poter comunicare fra loro.

Le connessioni VPN richiedono sempre tre Security Associations SA (che vengono gestite in due fasi):

- Fase 1 - Creazione dell'IKE-SA

  una per l'autenticazione reciproca iniziale e per lo scambio delle chiavi di sessione (IKE-SA)

- Fase 2 - Gestione delle Payload-SA

  una per ciascun fascio della connessione, per il traffico payload (Payload-SA)

Il protocollo IKE svolge essenzialmente due funzioni distinte. Per prima cosa crea una SA utilizzata esclusivamente dal protocollo IKE (IKE-SA). Quindi la utilizza per proteggere tutte le trasmissioni successive di dati payload che richiedono SA (Payload-SA). IKE funziona in due fasi consecutive:

Nella creazione della connessione fra due partner VPN è necessario gestire diversi parametri (ad es. la frequenza di generazione delle chiavi o la procedura di crittografia da utilizzare). Questi parametri vengono definiti e gestiti nell'IKE-SA.

La fase 2 IKE consente di gestire tutti i parametri di sicurezza per le Payload-SA fra i partner VPN.

Devono essere sempre create due SA, per la trasmissione e la ricezione.

Essenzialmente, vengono effettuati i seguenti passaggi:

- Gestione degli algoritmi per la crittografia e l'autenticazione
- Gestione dei protocolli di sicurezza utilizzati (ESP e AH)
- Gestione della modalità di funzionamento dei protocolli di protezione
- Gestione della durata delle SA
- Definizione dei materiali di codifica

In una VPN ha luogo la comunicazione Peer-to-Peer. L'autenticazione dei partner VPN può avvenire in due modi:

- Chiavi precondivise

  Nelle VPN vengono prevalentemente utilizzate le chiavi precondivise (Preshared Keys). In questo modo entrambi i partner VPN vengono configurati con una coppia di chiavi. Da queste chiavi si crea per l'autenticazione un cosiddetto valore hash, che verifica ciascun partner.
- Firme digitali

  A ciascun partner VPN viene assegnato un certificato. Affinché l'autenticazione riesca, i partner VPN su entrambi i punti finali del tunnel devono verificare la firma digitale dell'altro partner rispetto a una CA attendibile.

Informazioni specifiche del sistema

L'amministrazione dei parametri VPN avviene principalmente tramite procedura guidata.

Assicurarsi che la connessione dell'amministratore avvenga tramite una connessione protetta SSL.

- Security Associations SA

  Il sistema di comunicazione supporta i gruppi Oakley 1, 2 e 5
- IPSec

  Il sistema di comunicazione utilizza la modalità tunnel IPSec con ESP (Encapsulating Security Payload). Si tratta di un protocollo IPSec che consente di garantire l'integrità e l'autenticità dei pacchetti grazie alla crittografia degli stessi

- Payload SA

  Il sistema di comunicazione supporta gli algoritmi di crittografazione DES, 3DES e AES

  Fra i gruppi noti di algoritmi MAC (MAC=Message Authentication Code) per l'autenticazione di provenienza e integrità dei dati, supporta HMAC-SHA1, HMAC-SHA2 e HMAC-MD5.
- Modalità di funzionamento consigliate
  - IKE in "Main Mode" con Perfect Forward Secrecy
  - Funzione hash con SHA-2
  - Autenticazione con certificati (DSA e RSA)
  - Crittografia con AES (fino a 256 bit)
  - Supporto indirizzi IP dinamici pubblici tramite indirizzi IP virtuali o meccanismo di aggiornamento con DynDNS per il PC dell'operatore remoto

20.3.5 VPN - Certificati

Un certificato lega una chiave pubblica definita a uno specifico client VPN; può trattarsi sia di client del sistema di comunicazione che di client operatore remoto. La combinazione univoca di chiave pubblica e client VPN è la base della procedura di autenticazione.

Certificato e autorità di certificazione

CA Lightweight

CRL, Certificate Revocation Lists (Liste di revoca certificato)

I certificati vengono firmati in modo digitale ed emessi da una cosiddetta autorità di certificazione (CA). IPSec accetta un certificato se è stato emesso da un'autorità di certificazione attendibile.

In un ambiente VPN semplice è sufficiente la definizione di una singola autorità di certificazione; questa CA funge da autorità di certificazione attendibile originale per l'intera VPN e si identifica rispetto a tutti i client VPN in base ai certificati autofirmati.

Ciascun client VPN necessita di un certificato emesso da questa CA.

I certificati conformi allo standard X.509 (quello corrente) contengono i seguenti elementi principali:

- Informazioni sull'identità del proprietario del certificato
- La chiave pubblica del proprietario del certificato
- Informazioni sulla CA che ha firmato il certificato (numero di serie, validità, informazioni sull'identità della CA nonché sulla firma digitale della CA)

Per gli ambienti in cui il cliente non utilizza già una PKI, è disponibile una funzionalità CA Lightweight per la certificazione. Una CA Lightweight consente di:

- Creare coppie di chiavi pubblica/privata
- Firmare e rilasciare i certificati corrispondenti
- Salvare coppie di chiavi e certificati su file

Con PKI (Public Key Infrastructure) in crittografia si identifica un sistema che consente di emettere, distribuire e verificare certificati digitali.

Una situazione critica è quella in cui un certificato diventa noto (o si suppone che lo sia) e non risulta più attendibile per l'autenticazione peer. In questo caso, l'autorità di certificazione deve richiamare il certificato e tutti gli interessati devono essere informati prima possibile di tale richiamo. I tentativi di un utente remoto di autenticare la propria identità per mezzo di un certificato richiamato vengono respinti.

Una CLR fondamentalmente è una visualizzazione di tutti i certificati revocati. Le CRL possono sempre essere generate dalle autorità di certificazione prima dell'emissione del certificato.

Contiene i seguenti elementi principali:

- Presentazione dei certificati revocati; l'identificazione avviene tramite il numero di serie
- Data del prossimo aggiornamento della CRL (validità della CRL)
- Informazioni sulla CA che ha emesso il certificato (informazioni sull'identità della CA nonché sulla firma digitale della CA)

L'amministratore deve provvedere manualmente a un regolare aggiornamento e alla distribuzione della CLR.

Informazioni specifiche del sistema

L'autenticazione avviene sulla base di algoritmi di crittografia con chiavi pubbliche. Il sistema di comunicazione supporta RSA come algoritmo di crittografia con chiavi pubbliche. Il sistema di comunicazione supporta solo certificati conformi allo standard X.509.

Per l'autenticazione, il sistema di comunicazione funge sempre da client VPN.

- CA Lightweight

  Il sistema di comunicazione offre una funzionalità CA limitata (CA Lightweight). L'amministratore predispone il materiale della chiave per un sistema, mentre importa manualmente tramite la connessione SSL di amministrazione le coppie di chiavi pubbliche/private e i certificati in tutti i partner di comunicazione interessati.

- CRL

  Vengono utilizzate le CRL (Certificate Revocation List) per la revoca dei certificati. L'amministratore importa la CRL nel sistema di comunicazione tramite una connessione SSL protetta.

20.3.5.1 VPN - Come generare certificati CA Lightweight

CA Lightweight è una funzione utilizzabile su licenza per la generazione e la gestione di CA e certificati peer.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **CA Lightweight**. Nella finestra **Crea certificato** è possibile creare un proprio certificato CA.
4) In **Nome del certificato** immettere un nome per il certificato richiesto.
5) In **Numero di serie del certificato** immettere un numero di serie per il certificato.

Suggerimento: Un numero di serie utilizzato non può essere riutilizzato per un altro certificato, visto che i numeri di serie di tutti i certificati finora creati devono essere univoci.

---

6) In **Tipo di algoritmo della firma**, immettere il tipo di algoritmo desiderato per il certificato (sha256RSA o sha512RSA).
7) In **Lunghezza della chiave pubblica**, immettere la lunghezza della chiave pubblica (ad es. 2048).
8) Immettere la data e l'ora di inizio del periodo di validità nel campo **Inizio della validità del certificato (GMT)**. La data viene espressa come ora di Greenwich (GMT).
9) In **Fine della validità del certificato (GMT)**, immettere data e ora di fine della validità.
10) In **Richiedente** immettere il **Paese (C)**, l'**Organizzazione (O)**, l'**Unità organizzativa (OU)** ed il **Nome generale (CN)**.
11) In via opzionale, nel campo **Richiedente alternativo** inserire il nome del richiedente alternativo. Una volta completata questa operazione, sarà necessario indicare anche un formato (ad esempio, l'indirizzo IP o il nome DNS). La finestra di immissione dipende dal formato selezionato.
12) Nel campo **Punto di distribuzione del CRL** indicare il punto di distribuzione per l'elenco CRL (viene visualizzato nel menu a discesa).
13) Fare clic su **Crea certificato**.

20.3.5.2 VPN - Gestione certificati - Come visualizzare un certificato

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Gestione certificati**. Viene visualizzata la finestra **Mostra certificato da file**.
4) Eventualmente selezionare la casella di controllo **Formato PKCS#12**.
5) Immettere la **Password di decrittografia**.
6) Nel campo **File con il certificato** immettere il file del certificato o selezionarlo facendo clic su **Sfoglia**.
7) Fare clic su **Carica**.

20.3.5.3 VPN - Come importare un certificato CA attendibile (X.509)

X.509 è uno standard per i certificati. Nel certificato vengono salvati anche il nome e la firma digitale dell'emittente. X.509 è parte integrante del servizio directory X.500 per sistemi aperti, ripartiti, su base internazionale.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Gestione certificati** > **Certificati CA attendibili** > **Certificati configurati**.
4) In **Nome del certificato** immettere un nome per il certificato richiesto.
5) In **File con il certificato** immettere il file del certificato o selezionarlo dal campo **Sfoglia**.
6) Confermare e fare clic su **Attivazione delle tabelle VPN configurate.**

20.3.5.4 VPN - Certificati Peer - Come richiedere un certificato (CSR)

È possibile creare un certificato Peer firmato CA basato su un certificato CA. A tal fine è necessario che sia stato generato almeno un certificato. Il certificato creato viene salvato in un file PKCS#12. I file PKCS#12 (Personal Information Exchange Syntax Standard) memorizzano i certificati con chiave privata. Un file PKCS#12 contiene quindi i dati per la crittografia e la decrittografia personali.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Certificati Peer**.
4) Nella scheda **Crea richiesta del certificato (CSR)** immettere i dati richiesti.
5) Immettere il **Nome della richiesta del certificato**.
6) In **Tipo di algoritmo della firma** indicare l'algoritmo desiderato (sha256RSA o sha512RSA).
7) Inserire la lunghezza della chiave (2048) in **Lunghezza della chiave**.
8) Nei campi relativi al **Richiedente** immettere tutti i dati per il **Paese (C)**, l'**Organizzazione (O)**, l'**Unità organizzativa (OU)** e il **Nome generale (CN)**.
9) In **Richiedente alternativo** inserire il **Formato del nome di DN**, un eventuale **Altro formato** o un **Richiedente alternativo**.
10) Salvare il file *.csr che deve essere firmato da un CA.

20.3.5.5 VPN - Certificati Peer - Come creare un certificato (PKCS#12)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **CA Lightweight**.
4) Fare clic sul certificato CA, quindi su **Crea certificato Peer firmato CA (PKCS#12)**.
5) Immettere la **Password di crittografia**.
6) Immettere un numero di serie a scelta nel campo **Numero di serie del certificato**.
7) In **Lunghezza della chiave** inserire la lunghezza della chiave (1024, 1536 o 2048).
8) Immettere la data e l'ora di inizio del periodo di validità nel campo **Inizio della validità del certificato (GMT)**. La data viene espressa come ora di Greenwich (GMT).

   Nota: La durata di validità del certificato Peer deve essere adeguata ai criteri di protezione in vigore nell'azienda. Poco prima della fine del periodo di validità, il certificato deve essere prorogato oppure va creato un nuovo certificato.

9) Immettere la data e l'ora di fine del periodo di validità nel campo **Fine della validità del certificato (GMT)**.
10) Nei campi relativi al **Richiedente** immettere tutti i dati per il **Paese (C)**, l'**Organizzazione (O)**, l'**Unità organizzativa (OU)** e il **Nome generale (CN)**.
11) In via opzionale, nel campo **Richiedente alternativo** inserire il nome del richiedente alternativo. Una volta completata questa operazione, sarà necessario indicare anche un formato (ad esempio, l'indirizzo IP o il nome DNS). La finestra di immissione dipende dal formato selezionato.
12) Specificare il **Punto di distribuzione del CRL** (opzionale).
13) Fare clic su **Crea certificato**.

20.3.5.6 VPN - Come importare un certificato Peer (PKCS#12)

I file PKCS#12 (Personal Information Exchange Syntax Standard) memorizzano i certificati con chiave privata. Un file PKCS#12 contiene quindi i dati per la crittografia e la decrittografia personali.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.

3) Nella struttura dei menu selezionare **VPN** > **Certificati Peer**.
4) Fare clic sulla scheda **Importa certificato peer (PKCS#12)**.
5) Immettere un nome per il certificato richiesto in **Nome del certificato**.
6) In **Password di decrittografia** immettere la password personale per la decrittografia del certificato.
7) In **File con il certificato** immettere il nome del file o individuare il file utilizzando il pulsante **Sfoglia**.
8) Fare clic su **Mostra impronta digitale del certificato**.
9) Fare clic su **Importa certificato da file**.

20.3.6 VPN - Client

Tramite un tunnel VPN via Internet, un operatore remoto può realizzare una connessione VPN sicura alla rete aziendale. Per questo è necessario installare sul proprio dispositivo (PC, tablet PC, smartphone) un client VPN. Tutti i dati trasmessi tra il client VPN, il firewall aziendale e il server VPN del sistema di comunicazione sono crittografati.

Sono supportati i seguenti client VPN:

- **Client NCP VPN**

  I client NCP possono essere inseriti negli ambienti VPN desiderati tramite IPSec. Questo è importante quando un PC remoto deve accedere a gateway VPN di diversi produttori o nella rete aziendale è già installato un gateway VPN centrale di un altro produttore. In caso di collegamento in rete di filiali, il gateway NCP Secure Enterprise è in grado di comunicare con altri gateway VPN tramite connessioni IPSec.

  Il client NCP è a pagamento, ma fornisce un'interfaccia utente grafica con indicazione dello stato della connessione.
- **Shrew Soft VPN Client**

  Lo Shrew Soft VPN Client è un client VPN gratuito con interfaccia grafica che dalla versione 2.1.5 supporta anche autenticazione ibrida.

  Lo Shrew Soft VPN Client offre, tra l'altro, supporto per ISAKMP, Xauth ed RSA, protocolli di crittografia AES, Blowfish, 3DES e numerose funzionalità che si trovano solo in soluzioni professionali.
- **Client iOS e Android VPN**

  Il sistema operativo iOS o Android dispone del client L2TP/IPSec VPN integrato.

  I client L2TP/IPSec VPN utilizzano l'intervallo di indirizzi IP `10.254.253.x`. Se gli indirizzi IP in questo intervallo sono già utilizzati sulla rete del cliente, è necessario modificarlo nel WBM, selezionando il seguente percorso: **Modalità esperti** > **Manutenzione** > **Diagnostica applicazione** > **Test IPSec: IPSec Test Routine** > **Imposta indirizzo IP per L2TP** (ad esempio da `10.254.253.1` a `10.254.252.1`).
- **Client Mac OS X VPN**

  Il sistema operativo Mac OS X dispone del client Mac OS X VPN integrato.

Informazioni specifiche del sistema

- I dati dell'operatore remoto di un client VPN possono essere esportati sotto forma di file ZIP (non crittografati). Nel file ZIP, per ogni client VPN supportato, si trova un file di testo separato con i dati dell'operatore remoto: per il client NCP VPN sotto forma di file `.ini`; per il client Shrew Soft VPN sotto forma di file `.vpn` e per il client OS X VPN sotto forma di file `.networkConnect`. Questi file di testo possono essere importati nel client VPN.
- Infrastruttura LAN con più sottoreti

  Se in un'infrastruttura LAN con più sottoreti occorre utilizzare il protocollo VPN, è necessario creare delle regole per tali sottoreti. Le regole non possono essere configurate mediante procedura guidata, ma in Modalità esperti.
- Tunnel nel Tunnel

  Non è possibile realizzare un secondo tunnel VPN attraverso un tunnel VPN esistente.

20.3.6.1 Impostazioni del client NCP VPN

Per realizzare manualmente una connessione VPN utilizzando il client NCP VPN è necessario eseguire le seguenti impostazioni. Tramite il sistema di comunicazione esportare un file di testo `ncp_vpn.ini` contenente tutti i dati del client VPN configurato e importarlo in un altro client VPN. Le impostazioni saranno quindi già precompilate.

Impostazioni di base

- Nome profilo

  liberamente selezionabile, si consiglia un nome sensato
- Tipo di connessione

  VPN a IPSec
- Supporto di connessione

  In base alla connessione Internet utilizzata

  ad es. LAN (over IP) o DSL (PPPoE)

Selezione rete

Nessuna configurazione necessaria.

Accesso HTTP

Nessuna configurazione necessaria.

Modem

Nessuna configurazione necessaria.

Gestione linea

- Connessione

  automatica o manuale

  Timeout = 0

  Nota: In questo modo la connessione non viene interrotta nei periodi di inattività!

- Attribuire priorità a Voice over IP (VoIP)

  Selezionare
- Autenticazione EAP

  Nessuna configurazione necessaria
- Autenticazione HTTP

  Nessuna configurazione necessaria

Impostazioni IPSec

- Gateway = indirizzo IP o nome DNS del sistema di comunicazione

  Con questo indirizzo IP o nome DNS, il sistema di comunicazione è raggiungibile via Internet

  Denominazione nella procedura guidata VPN: **Indirizzo IP/nome DynDNS**
- Linea guida IKE = modalità automatica
- Linea guida IPSec = modalità automatica
- Modalità Exchange = modalità Main
- Gruppo PFS = DH-Group 2 (1024 Bit)
- Validità / Durata
  - Linea guida IKE: 000:00:07:00 (7 minuti)
  - Linea guida IPSec: 000:00:08:00 (8 minuti)
- Editor

  Nessuna configurazione necessaria

Opzioni IPSec avanzate

Nessuna configurazione necessaria

Identità

- Tipo = IP Address

  ID = indirizzo IP del PC dell'operatore remoto (vedere anche Assegnazione indirizzi IP)

  Utilizzo di una chiave precondivisa

  Selezionare

  Shared Secret = si tratta della password per la connessione VPN

  Denominazione nella procedura guidata VPN: **PreShared Secret**
- Extended Authentication (XAUTH)

  non utilizzato, nessuna configurazione necessaria

Assegnazione indirizzi IP

- Assegnazione manuale di indirizzo IP

  Indirizzo IP = indirizzo IP del PC dell'operatore remoto

  Denominazione nella procedura guidata VPN: **Indirizzo IP virtuale/Nome DNS**
- DNS / WINS

  Selezionare
- Server DNS = Indirizzo IP del sistema di comunicazione

  Indicazione nella procedura guidata VPN: **Indirizzo IP sottorete locale (LAN)**

Rete IP VPN

Nessuna configurazione necessaria

Verifica del certificato

Nessuna configurazione necessaria

Collegamento Firewall

- Attivazione di Stateful Inspection:

  per connessioni esistenti
- Comunicazione autorizzata solo nel tunnel:

  Selezionare

20.3.6.2 Come configurare un client NCP VPN

Per realizzare una connessione VPN sicura al sistema di comunicazione, è necessario installare e configurare sul dispositivo dell'operatore remoto un client NCP VPN.

Prerequisiti

L'amministratore del sistema di comunicazione ha configurato nel WBM di OpenScape Business l'operatore remoto e ha messo a sua disposizione un file ZIP di esportazione con i relativi dati.

L'amministratore del sistema di comunicazione ha comunicato all'operatore remoto la chiave segreta pre-condivisa necessaria per la connessione VPN.

Sul dispositivo dell'operatore remoto è stato installato il client NCP VPN (client LANCOM Advanced VPN). Per le informazioni necessarie, consultare la documentazione del client NCP VPN.

Il dispositivo dell'operatore remoto dispone di una connessione a Internet esistente e attiva.

Passo a passo

1) Estrarre i file `ncp_readme.txt` e `ncp_vpn.ini` e salvarli in una cartella locale. Le voci del file `ncp_vpn.ini` si riferiscono al profilo `HOOME`.

2) Importare il profilo `HOOME` nel client NCP VPN.

3) Aggiungere al profilo `HOOME` un server DNS. L'indirizzo del server DNS corrisponde all'indirizzo IP privato (LAN) del proprio sistema di comunicazione.
4) Avviare il client NCP VPN
5) Selezionare il profilo `HOOME` e fare clic su **Connetti**.

20.3.6.3 Come configurare un client Shrew Soft VPN

Per realizzare una connessione VPN sicura al sistema di comunicazione, è necessario installare e configurare sul dispositivo dell'operatore remoto un client Shrew Soft VPN.

Prerequisiti

L'amministratore del sistema di comunicazione ha configurato nel WBM di OpenScape Business l'operatore remoto e ha messo a sua disposizione un file ZIP di esportazione con i relativi dati.

L'amministratore del sistema di comunicazione ha comunicato all'operatore remoto la chiave segreta pre-condivisa necessaria per la connessione VPN.

Sul dispositivo dell'operatore remoto è stato installato il client Shrew Soft VPN. I client VPN Shrew Soft possono essere scaricati alla pagina `http://www.shrew.net`.

Il dispositivo dell'operatore remoto dispone di una connessione a Internet esistente e attiva.

Passo a passo

1) Estrarre i file `shrewsoft_readme.txt` e `shrewsoft_openswan.vpn` e salvarli in una cartella locale.
2) Avviare lo **Shrew Soft VPN Client Access Manager** e configurarlo. Salvare le immissioni.
3) Importare il file `shrewsoft_openswan.vpn` nel client Shrew Soft.
4) Al termine, in **Shrew Soft Client VPN Access Manager** la connessione sarà visibile nel campo **Connect** (Connetti a).

20.3.6.4 Come configurare un client iOS o Android VPN

Per realizzare una connessione VPN sicura al sistema di comunicazione, è necessario configurare sul dispositivo dell'operatore remoto una connessione L2TP-VPN.

Prerequisiti

L'amministratore del sistema di comunicazione ha configurato l'operatore remoto nel WBM di OpenScape Business e gli ha comunicato il nome utente, la password e la chiave Pre-Shared Secret per la connessione VPN.

Il dispositivo dell'operatore remoto dispone di una connessione a Internet esistente e attiva.

Passo a passo

1) Nel dispositivo iOS o Android dell'operatore remoto, selezionare il menu **Impostazioni** > **Generale** > **VPN**.
2) Utilizzando **Aggiungi VPN**, aggiungere una nuova connessione VPN.
3) Fare clic sulla scheda **L2TP**.
4) Nel campo **Descrizione** assegnare un nome alla connessione VPN.
5) Nel campo **Server**, inserire l'indirizzo IP pubblico o il nome DNS del sistema di comunicazione.
6) Nel campo **Account**, immettere il nome utente dell'operatore remoto.
7) Nel campo **Password**, inserire la password dell'operatore remoto.
8) Nel campo **PreShared Secret** inserire la chiave (PreShared Secret) del tunnel VPN.
9) Attivare il pulsante **Per tutti i dati**.
10) Nel menu **Impostazioni** attivare il pulsante **VPN**.

20.3.6.5 Come configurare un client VPN Mac OS X

Per realizzare una connessione VPN sicura al sistema di comunicazione, è necessario configurare sul dispositivo dell'operatore remoto una connessione L2TP-VPN.

Prerequisiti

L'amministratore del sistema di comunicazione ha configurato nel WBM di OpenScape Business l'operatore remoto e ha messo a sua disposizione un file ZIP di esportazione con i relativi dati.

L'amministratore del sistema di comunicazione ha comunicato all'operatore remoto il nome utente, la password e la chiave PreShared Secret necessari per realizzare la connessione VPN.

Il dispositivo dell'operatore remoto dispone di una connessione a Internet esistente e attiva.

Passo a passo

1) Estrarre il file `.networkConnect` e salvarlo in una cartella locale.
2) Fare doppio clic sul file `.networkConnect`.
3) Fare clic su **VPN (L2TP)**.
4) Nel campo **Configurazione** selezionare la connessione VPN.
5) Nel campo **Indirizzo del server**, inserire l'indirizzo IP pubblico o il nome DNS del sistema di comunicazione.
6) Nel campo **Nome utente**, immettere il nome utente dell'operatore remoto.
7) Configurare le impostazioni di protezione:
   a) Fare clic su **Impostazioni di autenticazione**.
   b) Nel campo **Password**, inserire la password dell'operatore remoto.
   c) Nel campo **Chiave ("Shared Secret")** inserire la chiave (PreShared Secret) del tunnel VPN.
   d) Fare clic su **OK**.
8) Fare clic su **Altre opzioni** e selezionare la casella di controllo **Invia tutto il traffico tramite la connessione VPN**. Premere quindi **OK**.

9) Fare clic su **Applica**, quindi su **Collega**. Se la connessione a OpenScape Business ha esito positivo, viene visualizzato lo stato **Connesso**.

20.3.7 VPN - Servizi

La funzione Servizi configurati consente di gestire i servizi. Con l'attivazione, i servizi configurati diventano attivi.

20.3.7.1 VPN - Servizi attivi - Come mostrare tutti i servizi IPsec

È possibile visualizzare una lista dettagliata di tutti i servizi IPSec attivi sotto forma di tabella.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Servizi** > **Servizi attivi**.
4) Nella scheda **Mostra servizi IPsec** è possibile visualizzare i dettagli dei servizi IPSec attivi.

20.3.7.2 VPN - Servizi attivi - Come mostrare un servizio IPsec speciale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Servizi** > **Servizi attivi**.
4) Nella struttura dei menu, fare clic sul servizio di cui si desidera visualizzare tutte le informazioni (**Nome del servizio**, **Porta di origine**, **Porta di destinazione**, **Protocollo IP**, **Regola 'PASS'**, **Regola 'DENY'**).

20.3.7.3 VPN - Servizi configurati - Come mostrare tutti i servizi IPsec

È possibile visualizzare una lista dettagliata di tutti i servizi IPSec configurati sotto forma di tabella.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Servizi** > **Servizi configurati**.
4) Nella scheda **Mostra servizi IPsec** è possibile visualizzare i dettagli dei servizi IPSec configurati.

20.3.7.4 VPN - Servizi configurati - Come modificare un servizio IPsec

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Nota: Prima della modifica o attivazione del servizio IPsec, è necessario eseguire un backup. Le regole IPSec si comportano come le voci di un firewall e possono limitare l'accesso al sistema. Nel caso sia stato attivato IPsec senza disporre di accesso al sistema, è possibile ripristinare il sistema utilizzando la funzione **Ricarica**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Servizi** > **Servizi configurati**.
4) Nella struttura dei menu fare clic sul servizio che si desidera modificare.
5) In **Nome del servizio**, modificare il nome del servizio.
6) In **Porta di origine**, modificare la porta di origine.
7) In **Porta di destinazione**, modificare la porta di destinazione.
8) In **Protocollo IP** modificare il servizio (ad esempio UDP).
9) Completata la configurazione VPN, la modifica viene applicata utilizzando **Attiva le tabelle VPN configurate**

20.3.7.5 VPN - Servizi configurati - Come rinominare un servizio IPsec

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Servizi** > **Servizi configurati**.
4) Nella struttura dei menu fare clic sul servizio che si desidera rinominare.
5) In **Nome del servizio**, modificare il nome del servizio.
6) Completata la configurazione VPN, la modifica viene applicata utilizzando **Attiva le tabelle VPN configurate**

20.3.7.6 VPN - Servizi configurati - Come cancellare un servizio IPsec

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Servizi** > **Servizi configurati**.
4) Nella struttura dei menu fare clic sul servizio che si desidera cancellare.
5) Completata la configurazione VPN, la modifica viene applicata utilizzando **Attiva le tabelle VPN configurate**

20.3.8 VPN - Tunnel

Il termine tunnel si riferisce al trasporto di pacchetti di dati crittografati fino a un punto terminale fisso. I tunnel attivi sono tunnel configurati dopo un'attivazione della configurazione. Nel complesso si possono configurare fino a 256 tunnel per gateway.

20.3.8.1 VPN - Tunnel attivi - Come mostrare i dati generici dei tunnel

È possibile visualizzare i dati di tutti i tunnel attivi sotto forma di tabella.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Tunnel** > **Tunnel attivi**.
4) Nella scheda **Mostra dati generici dei tunnel** vengono visualizzati i dettagli specifici per ciascun tunnel attivo. Questo comprende:
   - **Nome del tunnel**
   - **Stato nello stack IP**
   - **Tipo di punto terminale del tunnel locale**
   - **Indirizzo del punto terminale del tunnel locale**
   - **Tipo di punto terminale del tunnel remoto**
   - **Indirizzo del punto terminale del tunnel remoto**
   - **Durata proposta delle chiavi di sessione**
   - **Durata proposta della sessione di scambio delle chiavi**
   - **Regole Regola di invio**
   - **Regole Regola di ricezione**

20.3.8.2 VPN - Tunnel attivi - Come visualizzare le regole di tutti i tunnel

È possibile visualizzare in una finestra le regole di tutti i tunnel attivi.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Tunnel** > **Tunnel attivi**.
4) Nella scheda **Visualizza regole di tutti i tunnel** sono riportate le informazioni dettagliate sui singoli tunnel attivi, quali
   - **Dati del tunnel**
   - **Dati della regola**
   - **Indirizzo di origine**
   - **Indirizzo di destinazione**
   - **Dati del servizio**

20.3.8.3 VPN - Tunnel configurati - Come mostrare i dati generici dei tunnel

È possibile visualizzare tutti i dati per i tunnel configurati sotto forma di tabella

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Tunnel** > **Tunnel configurati**.
4) Nella scheda **Mostra dati generici dei tunnel** vengono visualizzati i dettagli specifici per ciascun tunnel configurato. Questo comprende:
   - **Nome del tunnel**
   - **Tipo di punto terminale del tunnel locale**
   - **Indirizzo del punto terminale del tunnel locale**
   - **Tipo di punto terminale del tunnel remoto**
   - **Indirizzo del punto terminale del tunnel remoto**
   - **Durata proposta delle chiavi di sessione**
   - **Durata proposta della sessione di scambio delle chiavi**
   - **Regole Regola di invio**
   - **Regole Regola di ricezione**

20.3.8.4 VPN - Tunnel configurati - Come visualizzare le regole di tutti i tunnel

È possibile visualizzare in una finestra le regole di tutti i tunnel configurati.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Tunnel** > **Tunnel configurati**.
4) Nella scheda **Visualizza regole di tutti i tunnel** sono riportate le informazioni dettagliate sui singoli tunnel configurati, quali
   - **Dati del tunnel**
   - **Dati della regola**
   - **Dati di origine**
   - **Dati di destinazione**
   - **Dati del servizio**

20.3.8.5 VPN - Come aggiungere un tunnel configurato

È possibile configurare un nuovo tunnel IPSec. Nel complesso si possono configurare fino a 256 tunnel per gateway.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Tunnel** > **Tunnel configurati**.
4) Nella scheda **Aggiungi tunnel** è disponibile la finestra di immissione per il nuovo tunnel.
5) Selezionare **Dati del tunnel**.
6) In **Nome del tunnel** immettere il nome desiderato per il nuovo tunnel.
7) Nell'elenco a discesa **Punto terminale tunnel locale** selezionare il tipo di indirizzo del punto terminale per il lato di invio del tunnel (si possono immettere un nome host o un nome DNS).
8) In **Indirizzo del punto terminale del tunnel locale** immettere l'indirizzo del mittente nel formato appropriato per il tipo di punto terminale.
9) In **Tipo di punto terminale del tunnel remoto** immettere il tipo di indirizzo del punto terminale per il lato destinatario del tunnel (supporta l'immissione di indirizzi IP).
10) In **Indirizzo del punto terminale del tunnel remoto** immettere l'indirizzo del destinatario nel formato appropriato per il tipo di punto terminale. Se si imposta l'indirizzo 0.0.0.0, il punto terminale del tunnel è sconosciuto. In tal caso, la creazione del tunnel deve avvenire sempre dal lato opposto (ad es. operatore remoto).
11) In **Gestione della chiave di sessione** immettere la procedura per lo scambio delle chiavi (opzioni: automaticamente, con il protocollo IKE).
12) In **Algoritmi di crittografazione proposti** definire gli algoritmi utilizzabili (AES o 3DES).

13) In **Algoritmi Hash proposti**, definire gli algoritmi di verifica utilizzabili (MD5, SHA1 o SHA2). Gli algoritmi selezionati vengono offerti dall'iniziatore della negoziazione IKE.
14) In **Durata proposta delle chiavi di sessione** immettere un periodo di validità per le chiavi di sessione (Session Key) da utilizzare. Una volta trascorso questo periodo, non sarà più possibile scambiare informazioni con questa sessione. In sostituzione delle chiavi di sessione non più valide vengono negoziate automaticamente nuove chiavi di sessione.
15) In **Durata proposta della sessione di scambio delle chiavi** immettere un periodo di validità. Una volta scaduta la sessione di scambio delle chiavi, vengono negoziate automaticamente nuove chiavi tramite IKE.
16) In **Volumi di dati proposti delle chiavi di sessione** immettere il volume dati massimo per le chiavi di sessione. Se il volume dati viene superato, vengono negoziate automaticamente nuove chiavi di sessione tramite IKE. Scegliendo **illimitato** la validità delle chiavi di sessione non sarà limitata dal volume di dati.
17) Nella parte superiore della finestra, selezionare la casella di controllo **Dati di scambio delle chiavi**.
18) Immettere tutti i dati di scambio delle chiavi (**Attiva 'Perfect Forward Secrecy', e selezionare il metodo di autenticazione dei Peer di VPN, Pre-Shared-Key** o **Firma digitale**).

Suggerimento: Se come metodo di autenticazione si è scelto **Chiave precondivisa**, è necessario inserire una chiave precondivisa di 20 caratteri (e quindi ripeterla).

Suggerimento: Se in una rete VPN con più nodi come metodo di autenticazione si utilizza **Firme digitali** (CA Lightweight), è necessario completare altri passaggi di configurazione.

---

a) Creare in un nodo un certificato LWCA.
b) Esportare il certificato (.crt) sotto forma di file.
c) Creare ed esportare una Certificate Revocation List (.crl) in un file.
d) Per ogni nodo, creare ed esportare un certificato Peer (.p12), firmato dall'autorità di certificazione.
e) Il certificato (.crt) firmato dall'autorità di certificazione (CA), la Certificate Revocation List (.crl) e i corrispondenti certificati Peer devono essere importati in ogni nodo.

19) Immettere i **Gruppi Diffie Hellman proposti** (Gruppo DH 2, 5 o 14).
20) Completata la configurazione VPN, la modifica viene applicata utilizzando **Attiva le tabelle VPN configurate**

20.3.9 VPN - Regole

Le regole definiscono cosa accade a un pacchetto IP. L'azione regola *Pass* significa che il pacchetto IP continua ad essere trasportato. L'azione regola *DENY* significa che il pacchetto IP non viene più trasportato. È inoltre possibile scegliere se il pacchetto IP deve utilizzare un tunnel VPN (crittografato) o meno.

Il sistema di comunicazione è in grado di gestire 640 regole, tra cui 6 regole predefinite e 634 liberamente assegnabili.

20.3.9.1 VPN - Regole attive - Come mostrare tutte le regole

È possibile visualizzare tutte le regole attive.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Regole** > **Regole attive**.
4) Fare clic sulla scheda **Mostra regole**. Quindi visualizzare le informazioni dettagliate sulle regole attive, ad esempio
   - **Priorità**
   - **Servizio**
   - **Azione per la regola**
   - **Crittografazione necessaria**
   - **Stato della regola**
   - **Stato nello stack IP**
   - **Indirizzo di origine**
   - **Indirizzo di destinazione**
   - **Tunnel per la crittografazione**

20.3.9.2 VPN - Regole attive - Come mostrare una regola speciale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Regole** > **Regole attive**.
4) Nella struttura dei menu, fare clic sulla regola desiderata. Viene visualizzata la finestra **Mostra regola** con tutte le informazioni dettagliate sulla regola (**Priorità**, **Servizio**, **Azione per la regola**, **Crittografia necessaria**, **Stato della regola**, **Indirizzo di origine**, **Indirizzo di destinazione**)

20.3.9.3 VPN - Regole configurate - Come mostrare tutte le regole

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Regole** > **Regole configurate**.
4) Fare clic sulla scheda **Mostra regole**. Quindi visualizzare le informazioni dettagliate sulle regole attive, ad esempio
   - **Priorità**
   - **Servizio**
   - **Azione per la regola**
   - **Crittografazione necessaria**
   - **Attiva regola**
   - **Indirizzo di origine (tipo e indirizzo IP)**
   - **Indirizzo di destinazione (tipo e indirizzo IP)**

20.3.9.4 VPN - Regole configurate - Come aggiungere una regola

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Regole** > **Regole configurate** > **Aggiungi regola**.
4) Eseguire le impostazioni per i seguenti parametri:
   - **Priorità**
   - **Servizio**
   - **Azione per la regola (PASS, PASS_INCOMING, PASS_OUTGOING, DENY)**
   - **Crittografazione necessaria**
   - **Stato regola**
   - **Indirizzo di origine - Tipo**
   - **Indirizzo di origine - Indirizzo (l'ultimo dell'intervallo)**
   - **Indirizzo di origine - Maschera sub-rete (primo indirizzo dell'intervallo)**
   - **Indirizzo di destinazione - Tipo**
   - **Indirizzo destinazione - Indirizzo (l'ultimo dell'intervallo)**
   - **Indirizzo destinazione - Maschera sub-rete (primo indirizzo dell'intervallo)**
   - **Tunnel lato di ricezione**
   - **Tunnel lato invio**
5) Fare clic su **Applica**.

20.3.9.5 VPN - Come modificare una regola

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Regole** > **Regole configurate**.
4) Nella struttura dei menu, evidenziare la regola che si desidera modificare.
5) In **Priorità** immettere la priorità.
6) In **Servizio** immettere il servizio (ad es. DNS).
7) In **Azione per la regola** inserire la regola (**PASS**, **PASS_INCOMING**, **PASS_OUTGOING**, **DENY**).
8) Eventualmente selezionare la casella di controllo **Crittografia**.
9) Selezionare la casella di controllo **Attiva regola**.
10) In **Indirizzo di origine** immettere il **Tipo** e l'**Indirizzo IP** della regola modificata.
11) In **Indirizzo di destinazione** immettere il **Tipo** e l'**Indirizzo IP** della regola modificata.
12) Completata la configurazione VPN, la modifica viene applicata utilizzando **Attiva le tabelle VPN configurate**

20.3.9.6 VPN - Come aggiungere una regola per direzione opposta

Quando si crea una regola IPSec per una direzione di trasmissione, occorre inserire subito dopo anche la regola per la direzione opposta. Con l'opzione "Aggiungi regola per direzione opposta" le voci della regola selezionata vengono copiate scambiando gli indirizzi di origine e destinazione e modificando di conseguenza l'assegnazione del tunnel.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Regole** > **Regole configurate**.
4) Nella struttura dei menu, evidenziare la regola che si desidera modificare.
5) Fare clic sulla scheda **Aggiungi regola per direzione opposta**.
6) Fare clic su **Applica**.
7) Completata la configurazione VPN, la modifica viene applicata utilizzando **Attiva le tabelle VPN configurate**

20.3.9.7 VPN - Come cancellare una regola

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Regole** > **Regole configurate**.
4) Nella struttura dei menu, selezionare la regola che si desidera eliminare.
5) Fare clic sulla scheda **Cancella regola**. Viene visualizzata la regola selezionata con tutti i dati.
6) Fare clic su **Cancella**. Viene visualizzato un avviso di cancellazione della regola.
7) Completata la configurazione VPN, la modifica viene applicata utilizzando **Attiva le tabelle VPN configurate**

20.3.10 Server PKI

Il server PKI si riferisce a un server in grado di rilasciare, distribuire e verificare i certificati digitali. I certificati emessi nell'ambito di una PKI (Public Key Infrastructure)vengono utilizzati per la protezione delle comunicazioni.

Quando si utilizzano certificati (firme digitali), viene eseguito un tentativo di scaricare il CRL tramite l'URL PKI configurato nel server PKI.

20.3.10.1 VPN - Come mostrare il server PKI

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Public Key Infrastructure (PKI)**.
4) Fare clic sulla scheda **Mostra server PKI**. Vengono visualizzati il **Nome del server PKI**, il **Tipo di server PKI** e l'**URL del server PKI**.

20.3.10.2 VPN - Come aggiungere un server PKI

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **VPN** > **Public Key Infrastructure (PKI)**.
4) Fare clic sulla scheda **Aggiungi server PKI**.
5) Immettere il **Nome del server PKI**.
6) Inserire il **Tipo di server PKI** (ad esempio, LDAP).
7) Immettere l'**URL del server PKI**.
8) Confermare e fare clic su **Applica**.

20.4 Gestione dei certificati

La gestione dei certificati (per Secure Sockets Layer, SSL) consente l'amministrazione protetta del sistema di comunicazione. I dati non possono essere letti o manipolati da postazioni non autorizzate. L'autorizzazione è basata su certificati. I certificati si possono generare e gestire.

L'accesso amministrazione è crittografato e utilizza HTTPS e il protocollo TLS 1.2. I certificati consentono di autentificare la connessione. Per impostazione predefinita, viene utilizzato un certificato autofirmato. Per aumentare la sicurezza, è possibile utilizzare un certificato specifico del cliente.

SSL mette a disposizione i seguenti servizi di protezione:

- Autenticità (il partner della comunicazione è quello che sostiene di essere)
- Affidabilità (le informazioni non possono essere lette da terzi)
- Integrità (i dati vengono ricevuti come sono stati inviati)

Questi servizi di protezione richiedono un precedente accordo sul meccanismo di protezione e lo scambio di chiavi crittografate. Questi vengono definiti al momento della connessione.

SSL utilizza certificati e chiavi per consentire una trasmissione dati protetta.

CRL (Certificate Revocation List)

I CRL (Certificate Revocation List) sono file che riportano un elenco di certificati bloccati, con relativo numero di serie e informazioni sul blocco. Inoltre contengono i nomi dei responsabili del rilascio della lista di certificati bloccati e il successivo aggiornamento previsto.

CDP (CRL Distribution Point)

Punto di distribuzione CRL (CRL Distribution Point, CDP) è la directory (il luogo) in cui si trova la versione aggiornata del CRL (ad es. http://sectestcal.microsoft.com/ErtEnvoll/SecTestCAL.crl).

Informazioni specifiche del sistema

In un'amministrazione basata su SSL, la comunicazione è di tipo Client-Server.

Il server si autentica rispetto al client con il supporto di certificati generati dal o importati nel WBM. Nel browser questi certificati possono essere importati come attendibili, per evitare che vengano visualizzati avvisi del browser nelle connessioni al server SSL.

Suggerimento: La generazione del certificato SSL può essere utilizzata anche per SPE.

20.4.1 Introduzione

Cosa sono i certificati SSL?

I certificati TLS/SSL vengono utilizzati per proteggere i dati durante la comunicazione tra server come OpenScape Business e client basati su Web mediante crittografia e per verificare l'identità della società appartenente al sito Web in modo che l'utente possa essere sicuro di stare effettivamente comunicando con il server reale.

OpenScape Business emette un certificato SSL temporaneo ("autofirmato") durante l'installazione iniziale del sistema o al momento della modifica dell'indirizzo IP LAN, ma questo certificato non contiene dati sufficienti per la verifica dell'identità a parte l'indirizzo IP LAN dell'utente.

Tale certificato non è conforme agli attuali standard di sicurezza e deve essere sostituito da un certificato SSL individuale affidabile emesso da un'autorità di certificazione (CA) ufficiale il prima possibile dopo l'installazione iniziale di OpenScape Business. Questo è l'unico modo per soddisfare gli standard minimi degli attuali sistemi operativi client e browser Web per la comunicazione Internet sicura.

Le CA solitamente offrono certificati SSL con diversi livelli di affidabilità: Convalida del dominio (CD), Convalida dell'organizzazione (CO) e Convalida estesa (CE). Per OpenScape Business sono sufficienti i certificati con convalida del dominio. Si tratta solitamente dell'opzione più economica, addirittura gratuita con alcune CA.

Per quali servizi Web OpenScape Business utilizza il certificato SSL?

Il certificato SSL attivo viene utilizzato per l'accesso amministratore tramite il portale di amministrazione nonché per varie altre applicazioni basate su Web (ad esempio la programmazione dei tasti) e client UC basati su WSI come myPortal @work, myPortal to go, Application Launcher, myContacts e myPortal for Teams.

Da dove si può ottenere un certificato SSL affidabile?

Per ottenere un certificato SSL è necessario contattare un'autorità di certificazione. È necessario verificare il nome di dominio utilizzato per raggiungere OpenScape Business per creare una richiesta di firma del certificato (CSR), che viene quindi inviata alla CA per la convalida.

Va notato che i certificati SSL affidabili emessi da CA hanno solo un periodo di validità limitato, che va da pochi mesi ad alcuni anni, per garantire che siano conformi agli attuali standard di sicurezza. È importante tenere d'occhio la data di scadenza e rinnovare i certificati SSL prima che venga raggiunta.

Il mancato rinnovo dei certificati SSL può far sì che l'ambiente client classifichi il sito Web come "non sicuro" e impedisca la comunicazione con il server.

Tenere presente che alcuni ambienti client hanno requisiti speciali per i certificati SSL, che potrebbero non essere soddisfatti da tutte le CA. Più avanti, nella sezione "Considerazioni sul lato client", si riportano i collegamenti a

detti requisiti speciali. Quando si sceglie la propria CA, seguire le istruzioni corrispondenti.

Perché il rilascio dei certificati è diventato così importante?

L'uso di certificati SSL affidabili, specifici del cliente o del server, è estremamente importante e viene sempre più imposto dai principali produttori di sistemi operativi e browser. Sicurezza, professionalità, integrità e riservatezza nel trattamento dei dati personali sono gli argomenti chiave a questo riguardo.

Dato il crescente utilizzo di servizi e client basati su Web, anche tramite Internet, l'uso permanente del certificato SSL predefinito temporaneo, autofirmato (e quindi non sicuro) di OpenScape Business è fuori discussione.

Inoltre, il certificato temporaneo e autofirmato di OSBiz ha una validità pluriennale, mentre alcuni ambienti client hanno iniziato a limitare la validità del certificato, a volte a non più di un anno.

Inoltre, in molte installazioni dei clienti originariamente configurate con versioni software precedenti alla V3R2.1, la validità di questi certificati temporanei e autofirmati scade il 1º gennaio 2024.

Il portale di amministrazione di OpenScape Business fornisce una gamma di strumenti per generare e gestire i certificati SSL e supporta inoltre l'amministratore di sistema nella creazione di richieste di firma dei certificati. Di seguito vengono spiegate le funzioni più importanti a questo riguardo.

20.4.2 Come generare un certificato CA

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu, andare su **SSL** > **Generazione certificati**.
4) Fare clic sulla scheda **Genera certificato CA**.
5) Immettere il **Nome del certificato**.
6) Immettere un numero valido in **Numero di serie del certificato**.
7) Selezionare l'algoritmo in **Tipo di algoritmo della firma** (**sha256RSA**, **sha512RSA**).
8) Selezionare la chiave pubblica in **Lunghezza della chiave pubblica**.
9) Immettere nei campi corrispondenti l'Inizio e la Fine della validità del certificato.
10) Infine, compilare i campi **Nome del soggetto** o **Nome alternativo del soggetto**.
11) Inserire il **Punto di distribuzione del CRL**.
12) Fare clic su **Applica**, quindi su **OK**.

20.4.3 Come creare un certificato autofirmato

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **SSL** > **Creazione certificati**.
4) Fare clic sulla scheda **Crea certificato autofirmato** nella finestra **Creazione certificati**.
5) Nel campo **Nome del certificato** immettere un nome per il certificato generato.
6) Immettere un numero valido in **Numero di serie del certificato**.
7) In **Tipo di algoritmo della firma** selezionare l'algoritmo.
8) In **Lunghezza della chiave pubblica** selezionare la chiave pubblica.
9) Immettere nei campi corrispondenti l'Inizio e la Fine della validità del certificato.
10) Infine compilare i campi **Richiedente** e/o **Nome alternativo del richiedente**.
11) Registrare il **Punto di distribuzione del CRL**.
12) Fare clic su **Applica**, quindi su **OK**.

20.4.4 Come generare una richiesta di firma di un certificato (CSR)

A seconda dell'autorità di certificazione scelta, esistono diverse opzioni per creare richieste di firma di un certificato online (ad esempio tramite il portale Web di una CA) oppure offline. Il portale di amministrazione di OpenScape Business offre un'opzione per creare una CSR da scaricare e trasmettere alla CA.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Nella pagina Genera richiesta di firma certificato (CSR), è necessario compilare i seguenti campi per generare la chiave e i file CSR.

Generale:

Nome della richiesta del certificato: Un nome per la CSR che verrà utilizzato nel nome del file che verrà scaricato.

Tipo di algoritmo della firma: Selezionare tra "sha256RSA" e "sha512RSA"

Lunghezza della chiave pubblica: L'unica opzione è il 2048

Paese (P): Utilizzare un codice paese di due lettere, ad esempio "IT"

Organizzazione (O): denota il nome formale dell'entità o società generale a cui è assegnato il certificato.

Unità organizzativa (UO): designa una sottounità o un reparto specifico all'interno di un'organizzazione, offrendo ulteriore granularità per identificare la struttura organizzativa.

Nome comune (NC): un identificatore vitale, che rappresenta solitamente il nome di dominio per il quale viene emesso il certificato, che fornisce un elemento chiave per verificare l'identità del titolare del certificato.

Nome alternativo del soggetto (facoltativo)

L'estensione del nome alternativo del soggetto (SAN) è una caratteristica dei certificati X.509 utilizzati nel campo della crittografia. X.509 è uno standard che definisce il formato dei certificati a chiave pubblica. L'estensione SAN consente di associare identità aggiuntive, come nomi host, indirizzi IP o indirizzi e-mail, a un singolo certificato X.509. Ciò è particolarmente utile negli scenari in cui è possibile accedere a un server con nomi o indirizzi diversi.

Formato nome distinto: Devono essere compilate informazioni simili al nome del soggetto come Paese (P), Organizzazione (O), Unità organizzativa (UO), Nome comune (NC).

Altro formato:

Estensione del nome alternativo del soggetto: Le opzioni sono Nome DNS, Indirizzo IP, Indirizzo e-mail, indirizzo e-mail, Uniform Resource Indicator, Altro

Nome alternativo del soggetto: L'estensione SAN aiuta a risolvere le limitazioni nei casi in cui un singolo nome comune non è sufficiente o quando è necessario includere più identità all'interno di un singolo certificato. Ciò è importante per i moderni servizi Web, in cui un server potrebbe essere accessibile tramite più nomi di dominio o indirizzi IP.

Ecco un esempio di come potrebbe apparire l'estensione SAN in un certificato:

Nome alternativo del soggetto:

DNS:www.esempio.com

DNS:mail.esempio.com

Indirizzo IP:192.168.1.1

E-mail: admin@esempio.com

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Sicurezza**.
3) Nella struttura dei menu, selezionare **SSL** > **Gestione certificati** > **Certificati server**.
4) Nella scheda **Genera richiesta di firma del certificato (CSR)**:
5) Inserire il nome del certificato nel campo **Nome della richiesta del certificato**.
6) Dal menu a discesa **Tipo di algoritmo della firma**, selezionare**sha256RSA** o **sha512RSA**.
7) **Lunghezza della chiave pubblica** è fisso a **2048** caratteri.
8) Inserire il Paese in **Paese (P)**.
9) Inserire l'organizzazione in **Organizzazione (O)**.
10) Inserire **Unità organizzativa (UO)**.

11) Inserire **Nome comune (NC)**.
12) Fare clic su **Formato nome distinto** o **Altro formato** per selezionare il formato del certificato.
13) Facoltativamente, scegliere uno dei valori per **Estensione del nome alternativo del soggetto**.
14) Facoltativamente, fare clic sul pulsante **Aggiungi** per aggiungere un **Nome alternativo del soggetto** nella CSR.
15) Fare clic su **Applica**, quindi su **OK**.

20.4.5 Come importare un certificato server (PKCS#12)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Sicurezza**.
3) Nella struttura dei menu, selezionare **SSL** > **Gestione certificati** > **Certificati server**.
4) Fare clic sulla scheda **Importa certificati server (PKCS#12)** nella finestra **Certificati server**.

Nota: Se si seleziona un altro formato, è possibile configurare più di una voce SAN.

---

5) Immettere il **Nome del certificato**.
6) Immettere la **Password di crittografia**.
7) In **File con il certificato**, immettere il file del certificato utilizzando il pulsante **Scegli file**.
8) Fare clic su **Importa certificato da file** e successivamente su **OK**.

20.4.6 Come importare i certificati server (PEM)

In alternativa sono supportati i certificati in formato PEM. Ciò è possibile importando il certificato e il file della chiave come due file separati.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu, selezionare **SSL** > **Gestione certificati** > **Certificati server**.

4) Fare clic sulla scheda **Importa certificati server (PKCS#12)** nella finestra **Certificati server**.

Nota: Se si seleziona un altro formato, è possibile configurare più di una voce SAN.

---

5) Alla sezione **Importa file di certificato e chiave**:
6) Immettere il **Nome del certificato**. (È possibile inserire un nome a propria scelta.)
7) Immettere la **Password di crittografia**. (È possibile inserire una passphrase a propria scelta.)
8) In **File di certificato**, scegliere il file del certificato utilizzando il pulsante **Scegli file**.
9) In **File della chiave**, scegliere il file della chiave utilizzando il pulsante **Scegli file**.
10) Fare clic su **Importa certificato e chiave** e successivamente su **OK**.

20.4.7 Come visualizzare i certificati

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **SSL** > **Gestione certificati** > **Certificati server**.
4) Fare clic sul certificato desiderato. Viene visualizzata la finestra **Certificati server**.
5) Fare clic su **Mostra certificato** per visualizzare il certificato corrente.

20.4.8 Come cancellare un certificato

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **SSL** > **Gestione certificati** > **Certificati server**.
4) Fare clic sul certificato desiderato. Viene visualizzata la finestra **Certificati server**.
5) Fare clic sulla scheda **Cancella certificato**. Il nome del certificato valido viene visualizzato con un avviso di cancellazione.
6) Se si desidera cancellare effettivamente il certificato, fare clic su **Cancella**.

20.4.9 Come esportare un certificato (X.509)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **SSL** > **Gestione certificati** > **Certificati server**.
4) Fare clic sul certificato desiderato. Viene visualizzata la finestra **Certificati server**.
5) Fare clic sulla scheda **Esporta certificato (x.509)**. Il certificato può essere aperto o salvato.

20.4.10 Come importare un certificato prorogato (X.509)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **SSL** > **Gestione certificati** > **Certificati server**.
4) Fare clic sul certificato desiderato. Viene visualizzata la finestra **Certificati server**.
5) Fare clic sulla scheda **Importa certificato prorogato (X.509)**. Viene visualizzato il nome del certificato attualmente valido.
6) Nel campo **File con il certificato** immettere il certificato desiderato o selezionarlo nel campo **Sfoglia**.
7) Concludere l'immissione con **Impronta digitale**.

20.4.11 Come attivare un certificato

Con questa funzione è possibile definire il certificato da utilizzare per l'amministrazione basata sul Web.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **SSL** > **Gestione certificati** > **Certificati server**.

4) Fare clic sul certificato desiderato.
5) Fare clic sulla scheda **Attiva certificato**. Viene visualizzato un avviso per informare che l'azione determina l'interruzione di tutte le connessioni HTTP esistenti.
6) Dal menu a tendina **Sistema** selezionare il sistema desiderato (OpenScape Business, UC Booster Server, UC Booster Card) per il quale si desidera attivare il certificato.

Nota: Per l'applicazione corretta in ogni certificato deve essere inserito l'indirizzo IP del sistema nel campo **Nome comune**. Assicurarsi di selezionare il certificato corretto per il sistema selezionato.

---

7) Fare clic su **Attiva subito**.

Nota: Il certificato del server importato deve essere emesso direttamente da una CA root. Non utilizzare CA intermedie.

20.4.12 Gestione dei certificati per Booster Server

Quando all'inizio si installa un Booster Server, viene creato un certificato con l'indirizzo IP del Booster che funge da nome comune. Il certificato ha una validità di 10 anni e viene rilasciato per l'organizzazione "Unify Software and Solutions GmbH & Co. KG", con l'unità organizzativa specificata come "Unify".

È possibile sostituire il certificato predefinito su Booster Server trasferendo un certificato diverso tramite l'interfaccia Web-Based Management (WBM) del sistema. Una volta trasferito, il nuovo certificato può essere attivato, fornendo una configurazione di sicurezza alternativa per Booster Server.

Nota: Allo stesso modo, se il sistema utilizza invece UC Booster Card (OCAB), è possibile scegliere **UC Booster Card** dal menu a discesa al **passaggio 6**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Server telefonia** > **Sicurezza**.
3) Nella struttura dei menu, andare su **SSL** > **Gestione certificati** > **Certificati server**.
4) Scegliere uno dei certificati importati.
5) Andare su **Attiva certificato**.
6) Dal menu a discesa del sistema, selezionare **OpenScape Business UC Booster Server**.
7) Fare clic sul pulsante **Attiva ora** per applicare il certificato selezionato a Booster Server.

20.5 Sicurezza Web

In Sicurezza Web sono riportati i filtri di accesso Web con cui si controllano le abilitazioni dei client e il registro Admin che consente di condurre ricerche sugli accessi e modifiche al sistema di comunicazione.

20.5.1 Collegamenti al server Web

I collegamenti del client (ad esempio myPortal to go) al server Web interno del sistema di comunicazione possono essere crittografati (HTTPS) o non crittografati (HTTP).

Nota: I collegamenti non crittografati al server Web possono consentire a persone non autorizzate di accedere a dati sensibili! Per motivi di sicurezza, si consiglia vivamente di utilizzare solo una connessione crittografata (HTTPS) quando si utilizza myPortal to go (Web Edition) via Internet.

Per myPortal to go (App Edition) è disponibile solo una connessione crittografata al server Web.

20.5.1.1 Come configurare la connessione al server Web (UC Suite)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Sicurezza**.
3) Nella struttura dei menu selezionare **Accesso Web**.
4) Configurare le connessioni al server Web:
   - Se si desidera consentire connessioni crittografate, selezionare la casella di controllo **HTTPS**.
   - Se si desidera consentire connessioni non crittografate, selezionare la casella di controllo **HTTP**.
5) Se necessario, selezionare il campo **Salvare i dati di accesso nel terminale** se si desidera attivare questa funzione. In questo modo, i dati di accesso vengono salvati nel browser Web del cellulare mediante i cosiddetti cookie.
6) Fare clic su **Salva**.

20.5.1.2 Come configurare le connessioni al server Web (UC Smart)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **UC Smart** > **Impostazioni di base**.
3) Verificare se UC Smart è **Attivo**.
4) Configurare le connessioni al server Web:
   - Se si desidera consentire connessioni crittografate, selezionare la casella di controllo **HTTPS**.
   - Se si desidera consentire connessioni non crittografate, selezionare la casella di controllo **HTTP**.
5) Fare clic su **Applica**, quindi su **OK**.

20.5.2 Registro Admin

Il registro Admin consente di definire quando devono essere effettuate particolari modifiche al sistema di comunicazione e da chi.

20.5.2.1 Come caricare il registro Admin

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione**.
3) Nella struttura dei menu selezionare **Registro Admin** > **Dati del registro Admin.**.
4) Nella finestra **Dati del registro Admin.** viene visualizzato il messaggio "Il registro Admin verrà trasferito dal sistema". Confermare".
5) Fare clic su **Carica**.

20.5.2.2 Come modificare la Lingua registro Admin

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Manutenzione**.
3) Nella struttura dei menu selezionare **Registro Admin** > **Configurazione**.
4) Nella finestra **Modifica configurazione**, in **Lingua del registro Admin**, selezionare la lingua desiderata.
5) Fare clic su **Applica**.

20.6 Sicurezza SQL

OpenScape Business salva dati di configurazione del sistema, record di dati sulle chiamate, credenziali di account utente, ecc., in un database SQL interno. L'accesso al database è protetto da apposite credenziali.

Fino alla versione SW V2R2 i dati di accesso utente sono protetti tramite una password non modificabile dall'amministratore di OpenScape Business. Dalla versione SW V2R2, la password può essere modificata. La password viene generata dal sistema e non è visibile all'amministratore. Per la compatibilità negli scenari multinodo che eseguono versioni SW precedenti, è possibile ripristinare il valore precedente delle password modificate. La configurazione della password di accesso a SQL è disponibile in Sicurezza SQL. La configurazione della password di accesso a SQL è utilizzabile sia negli ambienti di rete che nei nodi singoli. Le procedure di gestione di singoli nodi specifici o di scenari multinodo sono riportate nei capitoli seguenti.

20.6.1 Nodo singolo

Upgrade SW da V2R1 o versioni precedenti

Dopo un aggiornamento dalla versione SW V2R1, per il database SQL è attiva la password precedente. La password SQL deve essere modificata dall'amministratore del sistema nella nuova versione software, tramite il Portale Amministrazione (WBM).

Impostazione del nuovo sistema

Quando si imposta la data nel sistema per la prima volta, viene generata una nuova password SQL. La data e l'ora vengono impostate solo la prima volta, quando la password SQL viene modificata automaticamente.

Impostazione di un sistema "a nodo singolo" ricaricato

Dopo ogni ricaricamento del sistema, per il database SQL è attiva la password precedente. Nella nuova versione del software la password SQL deve essere modificata dall'amministratore del sistema, tramite il Portale Amministrazione (WBM).

20.6.2 Multinodo

Il sistema a nodo singolo viene configurato e integrato nella rete secondo la procedura consueta. Dopo l'impostazione del sistema, il nuovo nodo slave sincronizza la propria password SQL con il nodo master. Non sono necessari interventi per adattare la password SQL nel nodo slave.

Ricaricare un nodo V2R2 o versione successiva in una rete V2R2 o versione successiva

Un nodo di rete, dopo il ricaricamento nella rete, deve essere riconfigurato e integrato nuovamente nella rete stessa.

Ricaricamento del nodo master

Nel caso di un nodo master, la password SQL deve essere modificata dall'amministratore del sistema utilizzando il Portale Amministrazione (WBM). Tutti i nodi slave sincronizzano la propria password SQL con quella nuova nel nodo master. Non sono necessari interventi per modificare la password SQL nei nodi slave.

Ricaricamento del nodo slave

Nel caso di un nodo slave, non sono necessari interventi in quanto il nodo slave sincronizza la propria password SQL con quella del nodo master.

Nuovo nodo slave V2R2 o versione successiva in una rete V2R1 (scenario non consigliato)

Il sistema a nodo singolo viene configurato e integrato nella rete secondo la procedura consueta. Dopo l'impostazione del sistema, il nuovo nodo slave rileva che il nodo master usa la password SQL precedente e, di conseguenza, la utilizza anch'esso. Non sono necessari ulteriori interventi per adattare la password SQL nel nodo slave.

Nota: Si consiglia di aggiornare l'intera rete alla versione software più recente.

Nuovo nodo master V2R2 o versione successiva in una rete V2R1 (scenario non consigliato)

Il sistema del nodo master viene configurato e integrato nella rete secondo la procedura consueta. Dopo l'impostazione del sistema, il nuovo nodo master utilizza la password SQL precedente. L'amministratore del sistema non deve modificare la password precedente, in quanto i nodi slave V2R1 non sono in grado di sincronizzarsi con una nuova password SQL nel nodo master. In questo caso il nodo non funzionerebbe nella rete. Se l'amministratore del sistema ha modificato la password SQL per errore, deve ripristinare la password "predefinita" nella configurazione del nodo master.

Nota: Si consiglia di aggiornare l'intera rete alla versione software più recente.

20.6.3 Come configurare password per il database SQL

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Server telefonia** > **Sicurezza**.

3) Nella struttura dei menu selezionare **Sicurezza SQL**.

4) Configurare le password per il database SQL:

- Se si desidera generare una nuova password non nota all'utente, selezionare la casella **Genera nuova**.
- Se si desidera attivare la password predefinita, selezionare la casella **Attiva predefinita**.

Nota: Nell'area delle notifiche della pagina principale viene visualizzato il messaggio seguente se si utilizza la password predefinita SQL (o una password generata con il vecchio algoritmo di generazione delle password):

"`Password SQL predefinita in uso, si consiglia di modificarla nella Modalità esperti`"

Il messaggio è un collegamento URL che porta alla pagina della Sicurezza SQL per la modifica della password.

20.7 Protezione da attacchi SIP

I cosiddetti "attacchi SIP" costituiscono una nuova forma di minaccia per i sistemi di comunicazione basati sulla telefonia IP. Le minacce possono provenire sia dalla LAN che da Internet (tramite un router configurato in modo non corretto). La protezione da attacchi SIP offre un accesso SIP protetto da password.

Per un accesso per utenti SIP, occorre applicare le seguenti regole:

- Autenticazione attiva
- Una password qualificata, di
- – lunghezza compresa tra 8 e 20 caratteri,
  – con una o più lettere maiuscole (dalla A alla Z),
  – con una o più lettere minuscole (dalla a alla Z),
  – con una o più cifre (da 0 a 9),
  – con uno o più caratteri speciali (ad esempio: %),
  – con non più di 3 caratteri ripetuti.
- Definizione di un ID utente SIP che si differenzia dal numero di telefono.

Quando viene configurato un nuovo utente SIP, per impostazione predefinita viene attivata l'autenticazione e viene generata una password casuale. Siccome questa password casuale non è nota, deve essere modificata dall'amministratore.

Nel sistema di comunicazione, le impostazioni corrispondenti vengono eseguite mediante la procedura guidata "Telefonia centrale" in Manager E.

Durante l'avvio del sistema, nel caso in cui sia stato configurato un utente SIP senza password, viene verificato l'elenco di password e viene creata una voce del registro eventi (visualizzazione eventi).

Suggerimento: Se il sistema di comunicazione viene utilizzato come router Internet, la porta 5060 deve essere chiusa (impostazione predefinita). Con la telefonia Internet tramite ITSP, il sistema di comunicazione apre le porte corrispondenti e le mantiene aperte.

Anche se si utilizza un router esterno o un firewall, è necessario chiudere la porta 5060. È compito del sistema di comunicazione aprire questa porta quando necessario.

21 Connessione in rete di OpenScape Business

I sistemi di comunicazione OpenScape Business possono essere connessi in rete fra loro e con i sistemi di comunicazione, OpenScape 4000 (HiPath 4000) e OpenScape Voice. Con una rete omogenea OpenScape Business, gli utenti possono utilizzare servizi quali stato presenza, casella vocale, conferenze e molto altro, in precedenza solo di pertinenza di un singolo sistema di comunicazione OpenScape Business.

Possibili connessioni in rete:

- Connessione voce pura di OpenScape Business X
- Connessione in rete di OpenScape Business X e OpenScape Business S (opzionale con UC Suite o UC Smart).
- OpenScape Business X con OpenScape 4000 (funzionalità UC di OpenScape Business solo se sono soddisfatte determinate condizioni)
- OpenScape Business X con OpenScape Voice (senza funzionalità UC in OpenScape Business)
- Connessione di porte esterne a OpenScape Business tramite interconnessione SIP.
- Connessione in rete tramite ISDN
- Sistema di reti OpenScape Business con attacco di linea urbana ITSP centralizzato

Con la procedura guidata **Configurazione di rete**, i sistemi di comunicazione vengono preparati per la connessione in rete. In questa procedura guidata viene definito se il nodo dovrà agire come master o slave. Inoltre, al fascio 16 (Rete) vengono automaticamente assegnate 16 linee.

Tutte le reti che utilizzano servizi di comunicazione unificata (ad esempio UC Smart o UC Suite), devono essere basati su un piano di numerazione chiuso. Le connessioni in rete senza servizi di comunicazione unificata possono essere basate su un piano di composizione a numerazione aperta o chiusa. Per rispondere in modo flessibile alle necessità di espansione dei clienti, nei sistemi di reti di nuova creazione si consiglia sempre di usare la numerazione chiusa.

Suggerimento: La configurazione di una rete IP è un compito complesso e deve essere eseguito esclusivamente da tecnici dell'assistenza esperti.

Non è possibile realizzare un sistema di reti OpenScape Business X1 puro, poiché un sistema X1 non può essere un sistema master e in un sistema di reti è sempre necessario un sistema master.

Non è supportata la connessione in rete di OpenScape Business con i seguenti sistemi:

- HiPath 3000 SIP-Q, supporta solo la connessione in rete TDM basata su S_0/ S_{2M} con CorNet NQ, vedere Connessione in rete tramite ISDN.
- HiPath 5000 RSM
- OpenScape Office MX
- Openscape Office LX

La migrazione da un sistema HiPath 3000 (incluso HiPath 5000 RSM) a OpenScape Business è descritta nel capitolo Migrazione.

Nota: Per informazioni relative alle licenze e all'aggiornamento o alla migrazione dei sistemi in una rete, vedere la sezione **Rete - Licenze** al capitolo Aggiornamenti.

21.1 Piano di rete

Prima di configurare un sistema di reti, occorre definire un piano di rete di comune accordo col cliente.

Il piano di rete deve comprendere i seguenti dati:

- ID nodo (ID del nodo) e relativi indirizzi IP
- Piano di composizione

21.1.1 Reti omogenee ed eterogenee

In generale, le reti si distinguono in omogenee (tutti i componenti appartengono alla stessa famiglia di sistemi) ed eterogenee (sistemi diversi).

Rete omogenea (rete nativa)

Rete eterogenea (rete ibrida)

Una rete omogenea (nativa) è costituita da componenti della famiglia di sistemi OpenScape Business.

Una rete eterogenea (ibrida) è costituita da componenti della famiglia di sistemi OpenScape Business e ad esempio un OpenScape 4000 o un OpenScape Voice.

Descrizione di tutti i nodi di OpenScape Business presenti nel sistema di reti

Tramite la voce **Collegamento in rete** nella barra di navigazione del WBM, è possibile visualizzare tutti i nodi OpenScape Business di un sistema di reti. Inoltre, tutti gli utenti OpenScape Business del sistema di reti possono essere visualizzati ordinati in base al nodo.

È possibile visualizzare le seguenti informazioni:

- **ID nodo**: ID nodo
- **M**/**S**: l'abbreviazione indica se il nodo è master o slave
- **Nome rete**: nome del nodo
- **Tipo**: tipo di nodo (**OSBiz X**: modello hardware, **OSBiz S**: Softswitch)
- **OSBiz X/OSBiz S**: indirizzo IP del nodo, cliccabile (aprire il WBM del nodo)
- **Server applicazioni**: indirizzo IP del server UC (UC Booster Card o UC Booster Server)
- **Stato registrazione**: stato della registrazione
- **Tempo reale**: indicazione dello stato attivo o no del nodo

21.1.1.1 Come visualizzare una panoramica di tutti i nodi OpenScape Business

Prerequisiti

Più sistemi di comunicazione OpenScape Business sono collegati in rete uno con l'altro.

Passo a passo

1) Nella barra di navigazione fare clic su **Collegamento in rete**.
2) Nella struttura di navigazione fare clic su **Visualizzazione dominio**. Vengono elencati tutti i nodi OpenScape Business presenti nella rete.

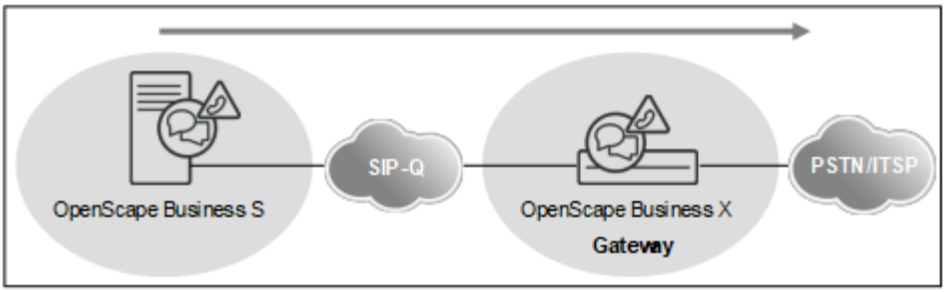
21.1.2 Gateway singolo e multiplo

In una rete omogenea di OpenScape Business, occorre distinguere tra gateway singolo e multiplo: per gateway singolo si intende una connessione con un solo gateway, mentre la connessione con gateway multiplo prevede l'uso di più gateway.

Gateway singolo

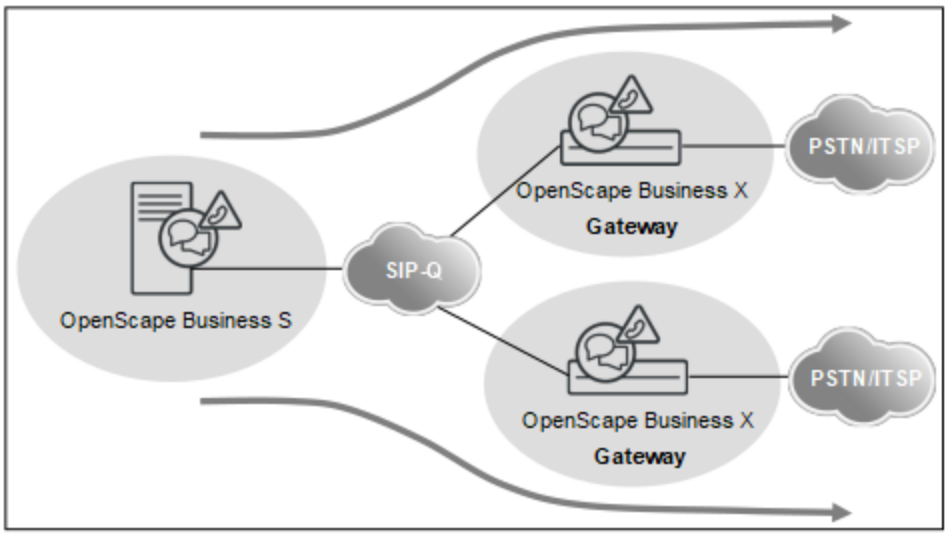
Gateway multiplo

In caso di collegamento in rete a gateway singolo, tutte le chiamate da e per il server vengono istradate tramite un solo gateway. Tutti gli utenti IP registrati sul server utilizzano questo gateway.



- La funzione è supportata se in rete sono presenti uno o più OpenScape Business S.
- Gli utenti IP sono collegati a sistemi di comunicazione diversi.
- OpenScape Business X viene utilizzato come gateway.

In caso di collegamento in rete a gateway multiplo, le chiamate vengono istradate tramite più gateway OpenScape Business.



- Solo 1 provider PSTN o un numero linea esterna per gateway
- Gli utenti di siti diversi sono registrati presso un sistema centrale (OpenScape Business S).
- A ogni utente di OpenScape Business S viene assegnato un gateway specifico (OpenScape Business X).
- In una rete può essere presente un solo OpenScape Business S.
- OpenScape Business e OpenScape Business S si trovano nello stesso fuso orario e nello stesso Paese (stesso prefisso internazionale).
- A livello della rete, è presente un solo codice di linea urbana.
- Nel gateway possono essere configurati ad esempio utenti locali analogici e ISDN.

21.2 Servizi di rete

Le funzioni voce a livello di rete sono essenzialmente determinate dal protocollo di rete SIP-Q. La disponibilità di funzionalità UC a livello di rete è determinata dalla connessione in rete della soluzione UC (UC Suite o UC Smart) e dei relativi client UC.

21.2.1 Servizi a livello di rete delle soluzioni UC

La seguente tabella fornisce una panoramica dei servizi disponibili in rete per le due soluzioni di comunicazione unificata UC Smart e UC Suite.

Non è consentito l'interworking UC con OpenScape 4000 e OpenScape Voice. In un sistema di reti OpenScape Business è necessario utilizzare UC Smart o UC Suite. Non è supportato l'uso di soluzioni di comunicazione unificata miste.

Funzioni UC disponibili a livello di rete	UC Smart		UC Suite		
	myPortal @work	myPortal to go	myPortal for Desktop/ Outlook	myPortal @work	myPortal to go
Visibilità a livello di rete dello stato presenza (gestione presenza)	x	x	x	x	x
Modifica del proprio stato presenza tramite client	x	x	x	x	x
Modifica del proprio stato presenza tramite TUI	x	x	x	x	x
Deviazione di chiamata basata sullo stato	x	x	x	Tramite destinazioni definite in altri client UC Suite	Tramite destinazioni definite in myPortal
Visualizzazione a livello di rete dello stato nei Preferiti	x	x	x	x	x
Visualizzazione a livello di rete dello stato nelle rubriche	x	x	x	x	x
Visualizzazione a livello di rete dello stato nel diario	-	-	x	-	-
Attivazione del servizio CallMe	-	-	x	x	x
Integrazione calendario (Outlook)	-	-	x	-	-
Integrazione calendario, iCal (solo myPortal for Desktop)	-	-	x	-	-
Visualizzazione a livello di rete dello stato di chiamata (libero, occupato, in chiamata)	x	x	x	x	x
Creazione di gruppi a livello di rete	x	x	x	-	-
Visualizzazione compatta dei Preferiti	-	-	x	-	-
Conversazioni	x	-	-	x	-
Rubrica personale	Locale	Locale	Locale	Locale	Locale
Rubrica interna	Locale	Locale	Locale	Locale	Locale
Rubrica esterna	-	-	x	x	x

Funzioni UC disponibili a livello di rete	**UC Smart**		**UC Suite**		
	myPortal @work	**myPortal to go**	**myPortal for Desktop/ Outlook**	**myPortal @work**	**myPortal to go**
Ricerca nelle rubriche a livello di rete	x	x	x	x	x
Accesso al sistema di destinazioni di selezione breve definite (KWZ)	Locale	Locale	-	Locale	Locale
Importazione/Gestione dei contatti personali (CSV/XML)	x	-	x	-	-
Accesso ai contatti di Outlook	x	-	x	-	-
Importazione di contatti personali (Mac OS) (myPortal for Desktop)	-	-	x	-	-
Integrazione server directory esterno tramite LDAP	-	-	x	-	-
Tutte le chiamate	x	x	x	x	x
Chiamate perse	-	x	x	-	-
Chiamate perse	x	x	x	x	x
Chiamate risposte	x	x	x	x	x
Chiamate pianificate	-	-	x	-	-
Chiamate VoIP	x	-	x	x	-
Diario fax	-	-	x	-	-
Composizione manuale	x	x	x	x	x
Dialer sul desktop (clic per chiamare)	-	-	x	-	-
Inoltro chiamate	x	x	x	x	x
In attesa	x	x	x	x	x
Registrazione di chiamate (registrazione vocale)	-	-	x	-	-
Invia e-mail	x	x	x	x	x
Invia SMS	-	x	-	-	x
Popup	x	-	x	x	-
Conferenza AdHoc	x	x	x	x	x
Conferenze pianificate	-	-	x	-	-

Funzioni UC disponibili a livello di rete	UC Smart		UC Suite		
	myPortal @work	myPortal to go	myPortal for Desktop/ Outlook	myPortal @work	myPortal to go
Conferenza permanente e aperta (conferenza Drag&Drop)	x	-	x	-	-
Integrazione di Web Collaboration	x	-	x	x	-
Casella vocale (Voicemail visivo)	x	x	x	x	x
Ascolto messaggi vocali tramite telefono	x	x	x	x	x
Ascolto messaggi vocali tramite scheda audio PC	-	-	x	-	-
Come inviare messaggi vocali tramite e-mail	x	x	x	-	-
Fax (per i sistemi operativi Windows)	-	-	x	-	-
Invio di messaggi istantanei (chat) a livello di rete	x	-	x	-	-

21.2.2 Servizi voce a livello di rete

Il collegamento in rete tramite il protocollo SIP-Q supporta i seguenti servizi voce per OpenScape Business e altri sistemi di comunicazione.

Servizio	SIP-Q (rete IP)
Chiamata di base	Sì
Richiamata automatica su dispositivo occupato	Sì
Richiamata automatica su libero	Sì
Inclusione	Sì
Avviso di chiamata in attesa	Sì
Seconda chiamata	Sì
CLIP (Calling Line Identification Presentation)	Sì
CLIR (Calling Line Identification Restriction)	Sì
COLP (Connected Line Identification Presentation)	Sì
COLR (Connected Line Identification Restriction)	Sì
CNIP (Calling / Connected Name Identification Presentation)	Sì
CNIR (Calling / Connected Name Identification Restriction)	Sì

Servizio	SIP-Q (rete IP)
Non disturbare	Sì
Deviazione di chiamata	Sì
Inoltro di chiamata su occupato	Sì
Inoltro di chiamata su libero	Sì
Deviazione di chiamata	Sì
Avviso di addebito allo stabilimento della connessione	No
Avviso di addebito durante la chiamata	Sì
Avviso di addebito al termine della chiamata	Sì
Ottimizzazione delle rotte	No
Rerouting	No
Indicazione messaggio in attesa / Info	Sì
Identificazione chiamate di disturbo	Sì
In attesa	Sì
Richiamata alternata	Sì
Trasferimento	Sì
Conferenza	Sì
Richiamata	Sì
Chiamata di emergenza	Sì
Rinvio	Sì
PNP (Private Numbering Plan)	No
Risposta per assente	No
Gruppo di ricerca	Sì
SPE (eccetto conferenze e applicazioni)	Sì

21.3 Concessione della licenza di un sistema di reti

Per un sistema di comunicazione connesso in rete può essere utilizzato un sistema di gestione licenze centrale.

Tutte le licenze dei singoli sistemi sono combinate in una licenza a livello di rete sul server licenze. Nel sistema di reti, le licenze possono essere assegnate ai singoli nodi in base alle proprie esigenze utilizzando il WBM.

Per ulteriori informazioni, vedere Concessione della licenza in più sistemi di comunicazione (sistema di reti).

21.4 Requisiti per la connessione in rete

Per garantire la qualità della trasmissione voce, le reti IP utilizzate e il sistema di comunicazione devono soddisfare specifici requisiti. La qualità voce e l'affidabilità della comunicazione dipendono dalla tecnologia di rete implementata.

Parametri di rete, requisiti per LAN e WAN

Parametri	Requisito minimo	Commento
Ritardo (unidirezionale)	50 ms	Valori superiori influenzano negativamente la qualità vocale.
Ritardo (bidirezionale)	100 ms	Valori superiori influenzano negativamente la qualità vocale.
Jitter	20 ms	Valori superiori influenzano negativamente la qualità vocale.
Perdita di pacchetti	3%	Con trasmissioni via fax o modem tramite G.711, la perdita di pacchetti non deve superare quota 0,05% (nel caso in cui non sia possibile T.38).
Perdita di pacchetti consecutivi	3 con G.711	Valori superiori influenzano negativamente la qualità vocale.

Suggerimenti per il calcolo della larghezza di banda

- Nel sistema di reti è necessaria una larghezza di banda di almeno 256 kBit/s (in entrata e in uscita).
- Il calcolo della larghezza di banda deve basarsi su un massimo del 50% riservato ai servizi voce sul totale della banda disponibile, ad esempio, in una WAN con una banda di 1 MBit, ai servizi voce deve essere destinato un massimo di 500 Kbit/s. Se si prende in considerazione ad esempio il codec G.711, ciò corrisponde a un massimo di 5 linee IP.
- Indipendentemente da ciò, occorre osservare anche altri parametri di rete, quali QoS, ritardo, perdita di pacchetti, ecc.

21.4.1 Requisiti della rete LAN

Per garantire la qualità della trasmissione dati e voce, le reti IP utilizzate e il sistema di comunicazione devono soddisfare specifici requisiti della LAN.

Requisiti LAN

La rete dati deve essere di tipo Ethernet:

- Si consiglia di utilizzare almeno cavi di Cat. 5 (schermati/non schermati multipolari da 100 MHz per aree orizzontali e verticali, in conformità a EN 50288).
- Supporto di QoS: IEEE 802.1p, DiffServ (RFC 2474).
- Tutte le porte LAN attive devono supportare la comunicazione full-duplex e 100 / 1000 MBit/s.

Ciascun sistema di comunicazione deve essere collegato tramite uno switch o una porta dedicata di un router. Gli hub e i ripetitori non sono supportati.

Collegamenti Payload con RTP (Realtime Transport Protocol) in ambiente LAN

La larghezza di banda necessaria per la trasmissione voce in una rete IP può essere calcolata sulla base della tabella riportata di seguito:

Tipo Codec	Parametri di pacchettizzazi	Frequenza di campionamen (ms)	Payload (byte)	Lunghezza del pacchetto Ethernet (byte)	Pacchetto Payload (overhead in percentuale)	Carico Ethernet (incl. intestazione) (kBit/s)
G.711	20	20	160	230	44%	92
G.711	30	30	240	310	29%	82,7
G.711	40	40	320	390	22%	78
G.711	60	60	480	550	15%	73,3
G.729A	1	20	20	90	350%	36
G.729A	2	40	40	110	175%	22
G.729A	3	60	60	130	117%	17,3
RTCP		5000		280		0,4

Il carico nella LAN si applica a entrambe le direzioni di trasmissione e ricezione.

Il calcolo include il tagging VLAN secondo IEEE 802 1q. Senza tagging VLAN, la lunghezza di un pacchetto si riduce di 4 byte.

L'overhead viene calcolato come segue:

Protocollo	Byte
Intestazione RTP	12
Intestazione UDP	8
Intestazione IP	20
802.1Q VLAN Tagging	4
MAC (incl. Preamble, FCS)	26
Totale	70

Trasporto Payload in ambiente LAN T.38:

	Frequenza di campionamento (ms)	Payload (byte)	Lunghezza del pacchetto Ethernet (byte)	Pacchetto Payload (overhead in percentuale)	Carico Ethernet (incl. intestazione) (kBit/s)
T.38	30	169	227	34%	60,5

Collegamenti Payload con SRTP (Secure Realtime Transport Protocol) in ambiente LAN:

Tipo Codec	Frequenza di campionamen (ms)	Payload (byte)	Lunghezza del pacchetto Ethernet (byte)	Lunghezza del pacchetto Ethernet SRTP (kBit/s)	Lunghezza del pacchetto Ethernet RTP (kBit/s)	Larghezza di banda aggiuntiva banda per SRTP (%)
G.711	20	160	244	97,6	92	6,1
G.711	30	240	324	86,4	82,4	4,5
G.711	40	320	404	80,8	78	3,6
G.711	60	480	564	75,2	73,3	2,5
G.729A	20	20	104	41,6	36	15,6
G.729A	40	40	124	24,8	22	12,7
G.729A	60	60	144	19,2	17,3	10,8

21.4.2 Piano di composizione per rete

Il piano di composizione è un requisito essenziale per il collegamento in rete. A seconda del piano di composizione, la configurazione della rete può risultare più o meno difficoltosa. In linea generale, OpenScape Business supporta sia la numerazione aperta che quella chiusa sul sistema di reti, tuttavia è possibile sfruttare appieno tutte le funzionalità UC solo con una numerazione chiusa.

Numerazione chiusa

Nella numerazione nascosta (chiusa) un utente del sistema di reti viene identificato in modo univoco grazie al proprio numero di telefono utente. Ciascun utente del sistema di reti può raggiungere gli altri mediante composizione diretta dei rispettivi numeri di telefono.

La numerazione nascosta presenta il vantaggio di non dover comporre alcun numero di telefono del nodo per raggiungere un utente in un altro sistema di comunicazione.

Tabella 10: Esempio di numerazione nascosta

	Nodo 1	Nodo 2	Nodo 3	Nodo 4
Numeri di telefono	100	200	300	400
	101	201	301	401
	102	202	302	402
	103	203	303	403
	104	204	304	404

Numerazione aperta

In caso di numerazione aperta, un utente viene identificato in modo univoco tramite il numero di telefono del nodo e il numero di telefono utente. Con questo approccio, più utenti di sistemi di comunicazione (nodi) compresi nel sistema di reti possono avere lo stesso numero utente.

Nella numerazione aperta occorre sempre selezionare il numero di telefono del nodo oltre al numero di telefono dell'utente. In questo modo è possibile utilizzare più volte le fasce di numeri telefonici e, di conseguenza, la quantità di numeri disponibili è superiore.

Le seguenti funzionalità di comunicazione unificata non sono supportate con una numerazione aperta:

- UC Smart
- UC Suite
- CSP a livello di rete (CSTA Service Provider)
- Server DSS
- CMD (CSTA Message Dispatcher)

Tabella 11: Esempio con numerazione aperta:

	Nodo 1	Nodo 2	Nodo 3	Nodo 4
Numero di telefono del nodo (numero del sistema)	95	96	97	98
Numeri di telefono	100	100	100	100
	101	101	101	101
	102	102	102	102
	103	103	103	103
	104	104	104	104

21.4.2.1 Composizione di numeri di rete pubblica in rete

Indipendentemente dalla numerazione chiusa o aperta, è naturalmente possibile chiamare sia numeri interni del nodo che destinazioni di rete tramite i numeri di telefono di rete pubblica (ad esempio, un client UC che seleziona contatti da rubriche, in formato completamente qualificato).

21.5 Ottimizzazione delle rotte (Path Replacement)

La funzione di ottimizzazione delle rotte (Path Replacement) consente di evitare un impegno doppio delle linee IP nei sistemi di comunicazione collegati in rete.

Se più sistemi OpenScape Business sono collegati in rete, potrebbe verificarsi il problema descritto di seguito: Ipotizziamo che l'utente A chiami l'utente B che a sua volta ha inoltrato tutte le chiamate all'utente C. Gli utenti A e C sono sullo stesso nodo, mentre l'utente B si trova su un nodo di rete diverso. In questo modo, la deviazione di chiamata occupa inizialmente due linee tra i due nodi. Per evitare questo doppio impegno delle linee, occorre attivare la funzione ottimizzazione delle rotte.

Suggerimento: Il flag di sistema per l'ottimizzazione delle rotte deve essere attivato in tutti i sistemi OpenScape Business collegati in rete!

: Si consiglia vivamente di non attivare la funzione di Ottimizzazione delle rotte nelle reti che utilizzano utenti analogici come fax. Questo limite sarà eliminato in una successiva versione software.

L'ottimizzazione delle rotte viene eseguita:

- All'interno del segmento di rete OpenScape Business
- Dopo l'instaurazione della connessione (non in fase di segnalazione della chiamata!)
- Dopo gli scenari di trasferimento
- Dopo l'inoltro di chiamata o la deviazione di chiamata

L'ottimizzazione delle rotte non viene eseguita:

- Con una segnalazione della chiamata o chiamata di gruppo
- Con conferenze
- In caso di attivazione di un altro servizio mentre è in corso l'ottimizzazione delle rotte, quest'ultima viene interrotta.
- In caso di rete non omogenea, i sistemi esterni vengono configurati tramite interconnessione SIP. In questo caso, indipendentemente dalla configurazione del flag, non è possibile alcuna sostituzione del percorso (ad esempio OpenScape 4000, OpenScape Voice, server SIP esterno).

21.5.1 Come attivare o disattivare l'ottimizzazione delle rotte (Path Replacement)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Sistema** > **Flag di sistema**.
4) Selezionare una delle seguenti opzioni:
   - Se si vuole consentire la risposta per assente di richiamate, selezionare la casella di controllo **Ottimizzazione delle rotte**.
   - Se non si vuole consentire la risposta per assente di richiamate, deselezionare la casella di controllo **Ottimizzazione delle rotte**.
5) Fare clic su **Applica**, quindi su **OK**.

21.6 Scenari di connessione in rete

Sono disponibili più scenari per collegare più sistemi OpenScape Business in rete tra loro e con altri sistemi di comunicazione.

- Utilizzo di più OpenScape Business X
- Collegamento in rete di OpenScape Business X e OpenScape Business S (gateway singolo)
- Collegamento in rete di OpenScape Business X e OpenScape Business S (gateway multiplo)
- Collegamento in rete di OpenScape Business S in un ambiente di hosting
- Collegamento in rete di OpenScape Business X e OpenScape 4000
- Collegamento in rete di OpenScape Business X e OpenScape Voice
- Collegamento di porte esterne a OpenScape Business tramite interconnessione SIP
- Numerazione aperta in OpenScape Business X - collegamento in rete
- Collegamento in rete tramite ISDN
- Sistema di reti OpenScape Business con attacco di linea urbana ITSP centralizzato

I dettagli delle chiamate possono essere richiamati solo per nodo di rete, non a livello di nodo.

21.6.1 Dipendenze e limitazioni

Per gli scenari di connessione possibili occorre essere consapevoli di alcune dipendenze e limitazioni.

Dipendenze e limitazioni

- A ogni sistema di un sistema di reti viene assegnato un proprio fuso orario. Pertanto, tutti gli utenti di un sistema presentano lo stesso fuso orario.
- I collegamenti MultiGateway OpenScape Business S sono consentiti solo all'interno di un unico paese (stesso fuso orario, stesso codice di linea esterna).
- In generale, i sistemi di reti con OpenScape Business vengono configurati tramite procedure guidate. OpenScape Voice e OpenScape 4000 in una connessione di rete vengono configurati per nodo tramite la Modalità esperti.
- Il gestore presenze (Presence Manager) (funzionalità server DSS = visualizzazione a livello di rete degli stati di occupato su tasti DSS + risposta per assente) è disponibile nelle reti OpenScape Business.
- Le linee SIP-Q con fascio 16 (ultimo fascio) sono utilizzate per configurare sistemi di comunicazione OpenScape Business omogenei attraverso la procedura **Configurazione di rete**. Le linee esterne SIP (interconnessione SIP) sono utilizzate per il collegamento in rete di OpenScape 4000, OpenScape Voice o altri sistemi di comunicazione, la configurazione viene eseguita in Modalità esperti.
- Se il sistema viene configurato come slave o master tramite la procedura guidata **Configurazione di rete**, viene verificato se le linee sono assegnate al fascio "Rete". In caso contrario, al fascio "Rete" vengono automaticamente assegnate 16 linee. Se il sistema viene eliminato dal sistema di reti, tali associazioni permangono.

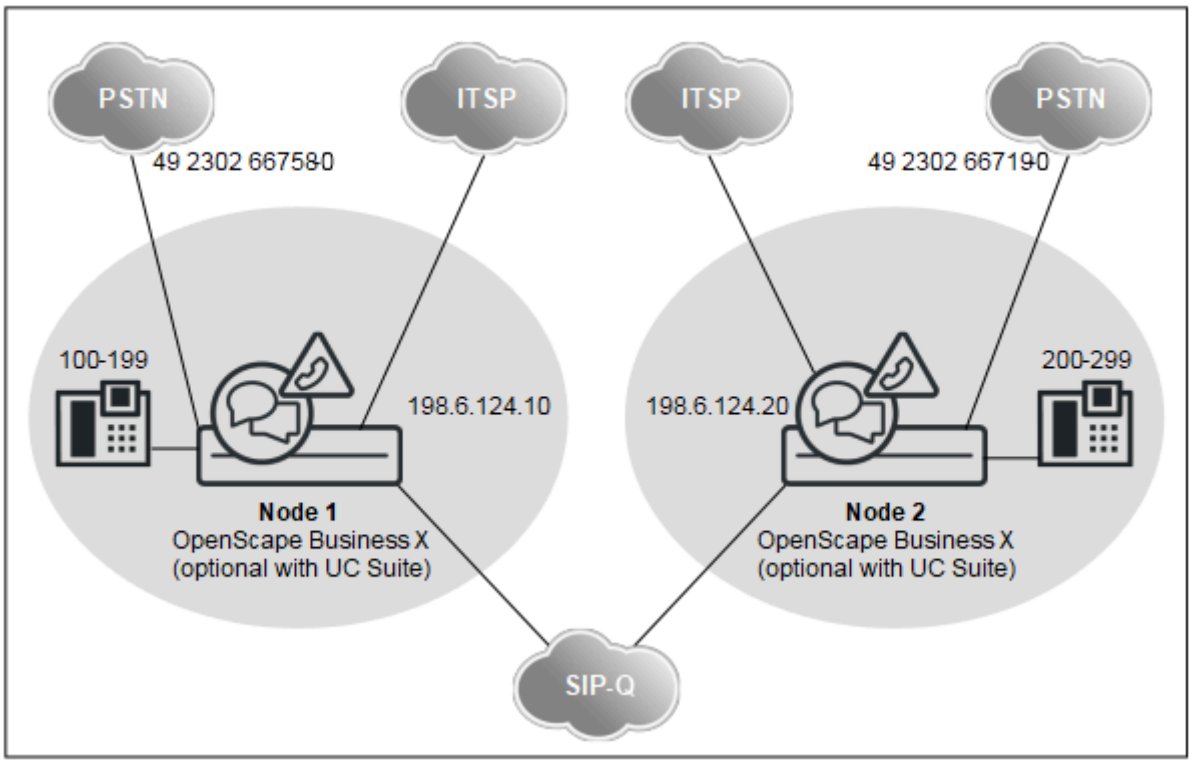
- In ogni nodo, può essere usato solo un sistema Voicemail. In generale, in un sistema di reti OpenScape Business sono consentiti più sistemi Voicemail:
  - Se si utilizza la UC Suite, gli altri sistemi Voicemail disponibili nel sistema di reti devono essere disattivati dall'amministratore.
  - È possibile effettuare la migrazione 1:1 da un sistema di reti HiPath 3000 con più sistemi voicemail a OpenScape Business.
- Per motivi tecnici, i sistemi OpenScape Business X1 non possono essere impostati come master. Poiché un sistema master è necessario in ciascuna rete OpenScape Business, almeno uno dei sistemi deve essere superiore a X1.

Suggerimento: I limiti nella versione venduta possono variare rispetto a questi dati (e di conseguenza anche i seguenti dettagli nei singoli scenari). Prendere nota delle indicazioni contenute nelle informazioni di vendita.

21.6.2 Utilizzo di più OpenScape Business X

Fino a 32 sistemi di comunicazione OpenScape Business X possono essere collegati in rete.

Dati di rete



- Con la soluzione UC (UC Smart o UC Suite): è possibile solo la numerazione chiusa
- Senza soluzione UC: sono possibili sia la numerazione aperta che quella chiusa
- Configurazione tramite WBM (procedure guidate) con numerazione chiusa

- La funzionalità UC Suite si basa sull'UC Booster Server o la UC Booster Card
- Fino a 32 sistemi in rete e 1500 utenti senza soluzione UC
- Fino a 8 sistemi in rete e 1500 utenti con soluzione UC

Servizi di rete

Collegamento in rete UC	Numerazione chiusa	Numerazione aperta
Numero massimo di nodi	8 con soluzione UC e 32 senza soluzione UC	
Numero massimo di utenti in un singolo sistema di comunicazione	a seconda del sistema OpenScape Business X	
Numero massimo di utenti nella rete	1500	

Collegamento in rete UC	Numerazione chiusa	Numerazione aperta
UC Booster Card	UC Smart: 51-150 utenti (0-50 utenti senza UC Booster Card) UC Suite: 0-150 utenti	Supporto non disponibile
UC Booster Server	UC Smart: da 150 utenti UC Suite: da 150 Utenti	Supporto non disponibile

Amministrazione	Numerazione chiusa	Numerazione aperta
WBM	Amministrazione di rete, tramite procedure guidate	Amministrazione di rete, Modalità esperti
Manager E	Amministrazione di rete per attività speciali	Amministrazione di rete per attività speciali
Amministrazione UC Suite (per UC Booster Server e UC Booster Card)	Amministrazione di rete, tramite procedure guidate	Supporto non disponibile
Importazione di dati in blocco tramite file CSV (numeri, numeri interni, nomi)	Separatamente per ogni nodo del sistema di reti	

Concessione della licenza	Numerazione chiusa	Numerazione aperta
Struttura di concessione delle licenze	È necessaria una licenza di rete per ogni nodo	

Configurazione

Questa configurazione (con la numerazione chiusa e la UC Suite) mostra un esempio di quali passaggi occorre eseguire per la configurazione del collegamento in rete.

Requisiti:

- È disponibile un piano di rete. Tramite il piano di rete ci si assicura che ogni numero di telefono interno nel sistema di reti venga assegnato una sola volta con numerazione univoca (chiusa). Sono consentiti numeri di telefono di diversa lunghezza. Solo i numeri di telefono DID possono ricorrere più volte

(ad esempio, i numeri linea esterna 49 2302 66758 100 e 49 2302 66719 100 hanno lo stesso numero DID 100).

Suggerimento: I numeri di telefono devono eventualmente essere modificati. Non è consentito l'uso di una numerazione di tipo aperto!

- La rete IP è configurata e tutti i nodi sono reciprocamente raggiungibili tramite ping
- Tutti i nodi sono dotati della stessa versione del software

Deviazioni di chiamata a livello di nodo: all'arrivo di chiamate su linee IP per le quali è già prevista una deviazione, non verranno eseguite ulteriori deviazioni alla casella vocale. Il motivo è che in caso contrario non è possibile realizzare un'assegnazione univoca alla casella vocale

Nel caso siano necessarie regole di rappresentanza a livello di nodo, queste devono essere configurate nei profili degli apparecchi OpenScape Business o nelle segnalazioni delle chiamate. Le chiamate corrispondenti a livello di nodo non verranno più segnalate come deviate, ma come chiamate dirette. In questo caso, potrà essere eseguita la deviazione di chiamata del rappresentante alla casella vocale.

Tabella 12: Configurazione dei dati località per il nodo 1

Nodo 1		
Località Paese G.		49
Località rete locale G.		2302
Località sistema G.		66758
Prefisso internazionale		00
Prefisso nazionale		0
Fasci		
ISDN	Codice di linea urbana	0
Servizi di rete	2° cod. linea	0
Parametri del fascio		
Fascio	Tipo n., in uscita	Tipo RNR
Servizi di rete	Sconosciuto	int./DID
ISDN	(Nessuna modifica dei dati immessi)	DID

Nelle tabelle di routing vengono inseriti automaticamente i numeri di telefono di tutti gli utenti escluso il nodo 1, in particolare i numeri interni e i numeri DID diversi dai numeri interni.

Tabella 13: Panoramica delle voci LCR per il nodo 1

Piano di composizione		Tabella delle rotte			Regola di composizione		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 2 Internet	0C0049230266719-Z	Servizi di rete	Forzato	2	D49230266719E3A	Corp. Rete	Internazionale
Nodo 2 NAT	0C0230266719-Z						
Nodo 2 Utente	0C66719-Z						
Linea urbana	0CZ	ISDN	No		A	Gestore di rete principale	Sconosciuto
Varie	-Z	Servizi di rete	No		A	Corp. Rete	Sconosciuto

Tabella 14: Configurazione dei dati località per il nodo 2

Nodo 2		
Località Paese G.		49
Località rete locale G.		2302
Località sistema G.		66719
Prefisso internazionale		00
Prefisso nazionale		0
Fasci		
ISDN	Codice di linea urbana	0
Servizi di rete	2° cod. linea	0
Parametri del fascio		
Fascio	Tipo n., in uscita	Tipo RNR
Servizi di rete	Sconosciuto	int./DID
ISDN	(Nessuna modifica dei dati immessi)	DID

Nelle tabelle di routing vengono inseriti automaticamente i numeri di telefono di tutti gli utenti escluso il nodo 2, in particolare i numeri interni e i numeri DID diversi dai numeri interni.

Tabella 15: Panoramica delle voci LCR per il nodo 2

Piano di composizione		Tabella delle rotte			Regola di composizione		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 1 Internet	0C0049230266758-Z	Servizi di rete	Forzato	1	D49230266758E3A	Corp. Rete	Internazionale
Nodo 1 NAT	0C0230266758-Z						

Piano di composizione		Tabella delle rotte			Regola di composizione		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 1 Utente	0C66758-Z						
Linea urbana	0CZ	ISDN	No		A	Gestore di rete principale	Sconosciuto
Varie	-Z	Servizi di rete	No		A	Corp. Rete	Sconosciuto

Come procedere per la configurazione del collegamento di rete:

1) Configurare l'installazione di base per il nodo 1 (master)
2) Configurare il collegamento in rete per il nodo 1
3) Configurare l'installazione di base per il nodo 2 (slave)
4) Configurare il collegamento in rete per il nodo 2
5) Come controllare le funzioni di rete per il master
6) Come verificare i fasci e i relativi parametri (master)
7) Come verificare i fasci e i relativi parametri (fascio 16) (master)
8) Come configurare l'LCR per il collegamento in rete (master)
9) Come verificare i fasci e i relativi parametri (slave)
10) Come configurare l'LCR per il collegamento in rete (slave)

21.6.2.1 Come configurare l'installazione di base per il nodo 1 (master)

Per l'integrazione in un sistema di reti, è necessario indicare il prefisso internazionale e un ID nodo. I numeri di telefono interni devono essere configurati in modo univoco a livello di rete. L'immissione dei numeri di telefono nazionali e locali è importante in quanto questi numeri vengono configurati nella linea ISDN fascio 1 e utilizzati come numeri della sede per la normalizzazione.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Installazione di base**.
4) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. 39 per l'Italia.
5) Inserire l'**Indicativo località** e il **numero di sistema**.
6) Selezionare la casella di controllo **Integrazione rete**.
7) Nel campo **ID nodo** per OpenScape Business, assegnare un ID nodo univoco sul sistema di reti ("**1**" per la configurazione di esempio).
8) Fare clic su **Esegui funzione**. Si apre la finestra **Funzioni centrali per gli utenti**.

9) Siccome in una rete tutti i numeri di telefono interni devono essere univoci, i numeri di telefono predefiniti devono venire cancellati. Selezionare il pulsante di opzione **Cancella tutti numeri di telefono**.
10) Selezionare la casella di controllo **Cancella tutti numeri di telefono dell'utente** e fare clic su **OK & Avanti.**. Si procede alla finestra **Modifica numeri di telefono e funzionali pre-configurati**.

Nota: I codici funzione di un sistema di reti devono essere univoci. Non sono consentiti numeri di telefono doppi!

---

11) Modificare il numero di telefono preconfigurato con il numero di telefono della rete e fare clic su **OK & Avanti**. I numeri di telefono possono essere configurati manualmente tramite procedura guidata o importati da un file CSV contenente i numeri di telefono appositamente preparati.
12) Configurare ora i client IP.
13) Modificare le impostazioni di una Conferenza Incontro. È necessario inserire nel sistema di reti un codice univoco.
14) Configurare ora l'invio di e-mail.
15) Fare clic su **Fine**.

21.6.2.2 Come configurare la rete per il nodo 1 (master)

Il passaggio successivo prevede la configurazione della procedura guidata per il collegamento in rete.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Configurazione di rete**.
4) Selezionare l'impostazione **Rete con OSBiz X / OSBiz S**.
5) Definire il tipo di nodo (**Master**).
6) Nel campo **ID nodo** indicare di numero del nodo dei relativi sistemi OpenScape Business (nella configurazione di esempio, quello dello slave con ID nodo 2).
7) Nel campo **Indirizzo IP** indicare l'indirizzo IP dei relativi sistemi OpenScape Business (nella configurazione di esempio, quello dello slave con l'ID nodo 2).
8) Nel campo **Nome** indicare il tipo corrispondente di sottosistema.

9) Eventualmente selezionare la casella di controllo **Crittografia**.

Suggerimento: La crittografia è basata su SPE e non vale per le applicazioni!

Nota: Selezionando la casella di controllo non viene utilizzata alcuna crittografia. Vedere Crittografia segnalazione e payload (SPE) .

10) Fare clic su **Fine**.

21.6.2.3 Come configurare l'installazione di base per il nodo 2 (slave)

Per l'integrazione in un sistema di reti, è necessario indicare il prefisso internazionale e un ID nodo. I numeri di telefono interni devono essere configurati in modo univoco a livello di rete. L'immissione dei numeri di telefono nazionali e locali è importante in quanto questi numeri vengono configurati nella linea ISDN fascio 1 e utilizzati come numeri della sede per la normalizzazione.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. 39 per l'Italia.
4) Inserire l'**Indicativo località** e il **numero di sistema**.
5) Selezionare la casella di controllo **Integrazione rete**.
6) Nel campo **ID nodo** per OpenScape Business S, assegnare un ID nodo univoco sul sistema di reti ("**2**" per la configurazione di esempio).
7) Fare clic su **Esegui funzione**. Si apre la finestra **Funzioni centrali per gli utenti**.
8) Siccome in una rete tutti i numeri di telefono interni devono essere univoci, i numeri di telefono predefiniti devono venire cancellati. Selezionare il pulsante di opzione **Cancella tutti numeri di telefono**.
9) Selezionare la casella di controllo **Cancella tutti numeri di telefono dell'utente** e fare clic su **OK & Avanti.**. Si procede alla finestra **Modifica numeri di telefono e funzionali pre-configurati**.

Nota: I codici funzione di un sistema di reti devono essere univoci. Non sono consentiti numeri di telefono doppi!

10) Modificare il numero di telefono preconfigurato con il numero di telefono della rete e fare clic su **OK & Avanti**. I numeri di telefono possono essere configurati manualmente tramite procedura guidata o importati da un file CSV contenente i numeri di telefono appositamente preparati.
11) Configurare ora i client IP.

12) Modificare le impostazioni di una Conferenza Incontro. È necessario inserire nel sistema di reti un codice univoco.

13) Configurare ora l'invio di e-mail.

14) Fare clic su **Fine**.

21.6.2.4 Come configurare la rete per il nodo 2 (slave)

Il passaggio successivo prevede la configurazione della procedura guidata per il collegamento in rete.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.

2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.

3) Fare clic su **Modifica** per avviare la procedura guidata **Configurazione di rete**.

4) Selezionare l'impostazione **Rete con OSBiz X / OSBiz S**.

5) In **Tipo nodo**, selezionare la casella **Questo sistema è un nodo SLAVE**.

6) In **Indirizzo IP** immettere l'indirizzo IP del master.

Suggerimento: Dopo aver selezionato **OK & Avanti** non sarà più possibile annullare questa azione!

---

7) Lo **Stato registrazione** viene visualizzato con lo stato **eseguito** (o con il relativo messaggio d'errore). La procedura guidata viene chiusa.

8) Fare clic su **Fine**.

21.6.2.5 Come controllare le funzioni di rete per il master

È possibile controllare lo stato generale della rete e i singoli numeri di telefono.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Rete**.

2) Nella riga di stato, visualizzare lo **Stato sincronizzazione** della rete. Il verde indica nessun problema sulla rete, il rosso presenza di problemi sulla rete.

3) Nella finestra **Rete**, selezionare la scheda **Visualizzazione dominio**, verranno visualizzati tutti i nodi disponibili con **ID nodo**, **Nome**, **Tipo sistema**, **Indirizzo server**, **Stato registrazione** e **Stato disponibilità**.

4) Nella finestra **Rete**, selezionare la scheda **Numeri di telefono**, si apre una finestra con tutte le informazioni su:

- **Numero di telefono**
- **DISA**
- **Nome**
- **Tipo porta**
- **Nodi**

21.6.2.6 Come configurare i fasci e i relativi parametri (linea ISDN per master)

Con i seguenti passaggi, configurare i fasci per il collegamento in rete del master.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Fascio**.
4) Nella finestra **Cambia gruppo di linee**, nel campo **Nome del fascio**, immettere il nome `Fascio 1` per il fascio linee esterne.
5) In **Codici del fascio** digitare `0`.
6) In **Numero del sistema - entrante** , nel campo **Prefisso internazionale** digitare `39`.
7) In **Numero del sistema- entrante**, nel campo **Prefisso interurbano** digitare `02`.
8) In **Numero del sistema- entrante**, nel campo **Numero del sistema** digitare `66758`.
9) Selezionare la casella di controllo in **Numero del sistema - entrante** nel campo **Numero località**.
10) Fare clic su **Applica**, quindi su **OK**.

21.6.2.7 Come configurare i fasci e i relativi parametri (fascio 16) (master)

Per il fascio 16 (rete), è obbligatorio compilare la voce per 2° cod. linea, sia per il master che per lo slave. Il fascio 16 è il fascio predefinito per la connessione in rete di OpenScape Business.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic sull'ultimo **Fascio** (ad es. **Fascio 16**).

4) Nella finestra **Cambia gruppo di linee**, nel campo **Nome del fascio**, immettere un nome (ad es. `Rete`) per il fascio di rete.
5) In **Codici del fascio** non inserire nulla.
6) In **Codice di linea urbana (2° cod. linea)** digitare 0.
7) È possibile accettare le impostazioni predefinite per i parametri del fascio (Tipo nr., in uscita, Tipo di numero di telefono).
8) Fare clic su **Applica**, quindi su **OK**.

21.6.2.8 Come configurare l'LCR per il collegamento in rete (master)

Nel piano di composizione LCR, le voci predefinite nell'indice 32, 33 e 34 devono essere ampliate con altre voci per consentire la composizione dei numeri nei formati "Internazionale, Nazionale e Utenti" per le chiamate al nodi 2. "Internazionale" e "Nazionale" sono sempre richiesti; "Utenti" è necessario per i nodi partner che si trovano nella stessa rete locale. Queste informazioni vengono utilizzate per la composizione dei numeri dalle applicazioni (ad esempio myPortal for Desktop).

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Nella struttura dei menu fare clic su **Piano di composizione**.
4) Inserire i seguenti valori nei punti liberi (in questo caso da 35 a 37) secondo i valori predefiniti:

Piano di composizion	Nome	Cifre selezionate	Tabella delle rotte
32	Predefinito	88CZ	1
33	IP rete	-Z	13
34	COInternat	0C0049-Z	14
35	Nodo 2 Inter	0C0049230266719-Z	16
36	Nodo 2 Nat	0C0230266719-Z	16
37	Nodo 2 Utente	0C66719-Z	16

5) Fare clic su **Applica**, quindi su **OK**.
6) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 2.
   a) Nel campo **Nome della regola**, immettere **Nodo 2**.
   b) In **Formato della regola di selezione** immettere **D49230266719E3A**.
   c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
   d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
   e) Fare clic su **Applica**, quindi su **OK**.
7) Nella struttura dei menu fare clic su **Tabella dei collegamenti**.

8) Fare clic sulla tabella delle rotte 16.
   a) Nel campo **Fascio**, selezionare la voce **Rete**.
   b) In **Regola di composizione**, selezionare la voce **Nodo 2**.
   c) In **Abil. min.**, selezionare la voce **15**.
   d) In **Avviso**, selezionare la voce **Nessuno**.
   e) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
   f) In **ID nodo GW**, selezionare la voce **2**.
   g) Fare clic su **Applica**, quindi su **OK**.

21.6.2.9 Come configurare il fascio e i relativi parametri (slave)

Con i seguenti passaggi, configurare il fascio e i parametri del fascio per il collegamento in rete dello slave.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Fascio**.
4) Nella finestra **Cambia gruppo di linee**, nel campo **Nome del fascio**, immettere il nome `Fascio 1` per il fascio di rete.
5) In **Codici del fascio** digitare `0`.
6) In **Numero del sistema - entrante** , nel campo **Prefisso internazionale** digitare `39`.
7) In **Numero del sistema- entrante**, nel campo **Prefisso interurbano** digitare `02`.
8) In **Numero del sistema** - entrante, nel campo **Numero del sistema** digitare `66719`.
9) Selezionare la casella di controllo in **Numero del sistema - entrante** nel campo **Numero località**.
10) È possibile accettare le impostazioni predefinite per i parametri del fascio (Tipo nr., in uscita, Tipo di numero di telefono).
11) Fare clic su **Applica**, quindi su **OK**.

21.6.2.10 Come configurare l'LCR per il collegamento in rete (slave)

Nel piano di composizione LCR, le voci predefinite nell'indice 32, 33, 34 e 35 devono essere ampliate con altre voci per consentire la composizione dei numeri nei formati "Internazionale, Nazionale e Utenti" per le chiamate al nodo 2. "Internazionale" e "Nazionale" sono sempre richiesti; "Utenti" è necessario per i nodi partner che si trovano nella stessa rete locale. Queste informazioni vengono utilizzate per la composizione dei numeri dalle applicazioni (ad esempio myPortal for Desktop).

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Nella struttura dei menu fare clic su **Piano di composizione**.
4) Inserire i seguenti valori nei punti liberi (in questo caso da 35 a 37) secondo i valori predefiniti:

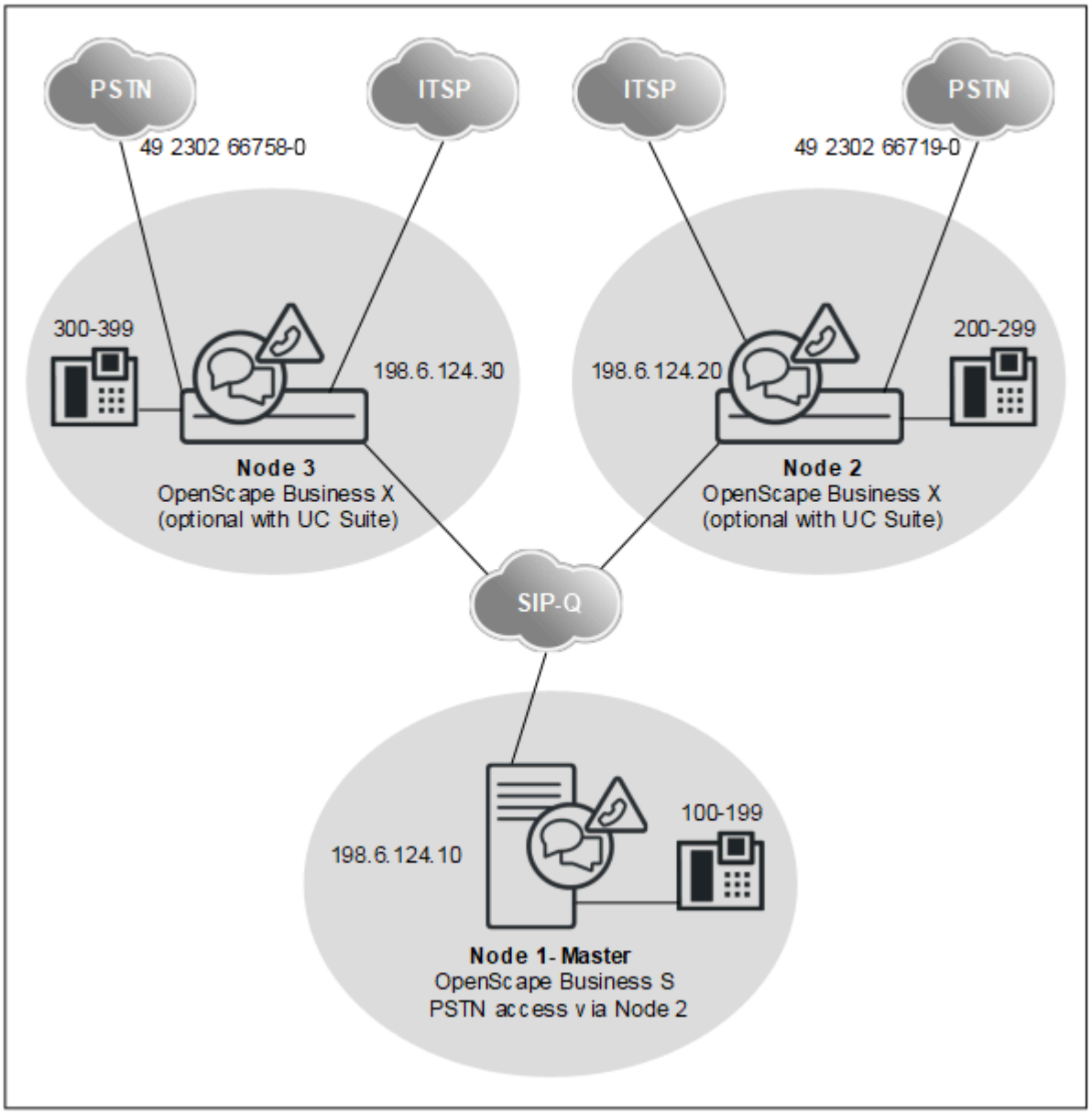
Piano di composizion	Nome	Cifre selezionate	Tabella delle rotte
32	Predefinito	88CZ	1
33	IP rete	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 1 Inter	0C0049230266758-Z	16
37	Nodo 1 Nat	0C00230266758-Z	16
38	Nodo 1 Utente	0C66758-Z	16

5) Fare clic su **Applica**, quindi su **OK**.
6) Nella struttura dei menu fare clic sulla **Regola di composizione** per il **Nodo 2**.
   a) Nel campo **Nome della regola**, immettere **Nodo 1**.
   b) In **Formato della regola di selezione** immettere **D49230266758E3A**.
   c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
   d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
   e) Fare clic su **Applica**, quindi su **OK**.
7) Fare clic sulla tabella delle rotte 16.
   a) Nel campo **Fascio**, selezionare la voce **Rete**.
   b) In **Regola di composizione**, selezionare la voce **Nodo 1**.
   c) In **Abil. min.**, selezionare la voce **15**.
   d) In **Avviso**, selezionare la voce **Nessuno**.
   e) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
   f) In **ID nodo GW**, selezionare la voce **2**.
   g) Fare clic su **Applica**, quindi su **OK**.
8) Nella struttura dei menu fare clic su **Tabella dei collegamenti**.

21.6.3 Collegamento in rete di OpenScape Business X con OpenScape Business S (gateway singolo)

Fino a 32 sistemi di comunicazione OpenScape Business X/S possono essere collegati in rete. In un sistema di reti è consentito l'uso di più OpenScape Business S. Gateway singolo significa che tutti gli utenti IP registrati in OpenScape Business S utilizzano UN solo gateway per accedere alla PSTN o all'ITSP.

Dati di rete



- Numerazione chiusa
- Funzionalità voce e UC a livello di rete con configurazione UC Suite tramite WBM (procedure guidate)
- La funzionalità UC viene realizzata tramite l'UC Booster Server o la UC Booster Card
- Sul sistema di reti sono consentiti più OpenScape Business S.
- Fino a 32 sistemi in rete e 1500 utenti senza soluzione UC
- Fino a 8 sistemi in rete e 1500 utenti con soluzione UC

Servizi di rete

Collegamento in rete UC	Numerazione chiusa	Numerazione aperta
Numero massimo di nodi	8 con soluzione UC e 32 senza soluzione UC	

Collegamento in rete UC	Numerazione chiusa	Numerazione aperta
Numero massimo di utenti in un singolo sistema di comunicazione	a seconda del sistema OpenScape Business X	
Numero massimo di utenti nella rete	1500	

Collegamento in rete UC	Numerazione chiusa	Numerazione aperta
UC Booster Card	UC Smart: 51-150 utenti (0-50 utenti senza UC Booster Card) UC Suite: 0-150 utenti	Supporto non disponibile
UC Booster Server	UC Smart: da 150 utenti UC Suite: da 150 Utenti	Supporto non disponibile

Amministrazione	Numerazione chiusa	Numerazione aperta
WBM	Amministrazione di rete, tramite procedure guidate	Supporto non disponibile
Manager E	Amministrazione dell'intera rete per compiti speciali (non per OpenScape Business S)	Supporto non disponibile
Amministrazione UC Suite (per UC Booster Server e UC Booster Card)	Amministrazione di rete, tramite procedure guidate	Supporto non disponibile
Importazione di dati in blocco tramite file CSV (numeri, numeri interni, nomi)	Separatamente per ogni nodo del sistema di reti	Supporto non disponibile

Concessione della licenza	Numerazione chiusa	Numerazione aperta
Struttura di concessione delle licenze	È necessaria una licenza di rete per ogni nodo	Supporto non disponibile

Configurazione

Questa configurazione (con la numerazione chiusa e la UC Suite) mostra un esempio di quali passaggi occorre eseguire per la configurazione del collegamento in rete.

Requisiti:

- È disponibile un piano di rete. Tramite il piano di rete ci si assicura che ogni numero di telefono interno nel sistema di reti venga assegnato una sola volta con numerazione univoca (chiusa). Sono consentiti numeri di telefono di diversa lunghezza. Solo i numeri di telefono DID possono ricorrere più volte (ad esempio, i numeri linea esterna 49 2302 66758 100 e 49 2302 66719 100 hanno lo stesso numero DID 100).
- La rete IP è configurata e tutti i nodi sono reciprocamente raggiungibili tramite ping

Deviazioni di chiamata a livello di nodo: all'arrivo di chiamate su linee IP per le quali è già prevista una deviazione, non verranno eseguite ulteriori deviazioni alla casella vocale. Il motivo è che in caso contrario non è possibile realizzare un'assegnazione univoca alla casella vocale

Nel caso siano necessarie regole di rappresentanza a livello di nodo, queste devono essere configurate nei profili degli apparecchi OpenScape Business o nelle segnalazioni delle chiamate. Le chiamate corrispondenti a livello di nodo non verranno più segnalate come deviate, ma come chiamate dirette. In questo caso, potrà essere eseguita la deviazione di chiamata del rappresentante alla casella vocale.

In un sistema di reti in cui viene utilizzata la funzione periodo di attivazione, è necessario utilizzare sempre i CLA di OpenScape Business S come CLA centralizzati!

Essendoci due diversi limiti superiori, sono necessari due file del periodo di attivazione, per OpenScape Business e OpenScape Business S. Il file del periodo di attivazione di OpenScape Business S contiene, oltre a OpenScape Business S base anche la Base S per gli scenari di collegamento in rete.

Se, in questo scenario, OpenScape Business presenta una richiesta di licenza durante il periodo di attivazione a un CLA di OpenScape Business S, vengono utilizzati i valori soglia di OpenScape Business S.

Se, al contrario, viene utilizzato il CLA di OpenScape Business, al ricevimento di una richiesta da parte di OpenScape Business S non verrebbe concesso alcun periodo di attivazione, in quanto in questo file non vi sarebbero le basi per OpenScape Business S.

Tabella 16: Configurazione dei dati località per il nodo 1 OpenScape Business S

Nodo 1		
Località Paese G.		49
Località rete locale G.		2302
Località sistema G.		66719
Prefisso internazionale		00
Prefisso nazionale		0
Fasci		
Fsc 1	Codice di linea urbana	0
Servizi di rete	2° cod. linea	0
Parametri del fascio		
Fascio	Tipo n., in uscita	Tipo RNR
Servizi di rete	Sconosciuto	int./DID
ISDN	(Nessuna modifica dei dati immessi)	DID

Nelle tabelle di routing vengono inseriti automaticamente i numeri di telefono di tutti gli utenti escluso il nodo 1, in particolare i numeri interni e i numeri DID diversi dai numeri interni.

Tabella 17: Panoramica delle voci LCR per il nodo 1

Piano di composizione		Tabella delle rotte			Regola di composizione		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 2 Internet	0C0049230266719-2Z	Servizi di rete	Forzato	2	D49230266719E3A	Corp. Rete	Internazionale
Nodo 2 NAT	0C0230266719-2Z						
Nodo 2 Utente	0C66719-2Z						
Nodo 3 Internet	0C0049230266758-3Z	Servizi di rete	Forzato	3	D49230266758E3A	Corp. Rete	Internazionale
Nodo 3 NAT	0C0230266758-3Z						
Nodo 3 Utente	0C66758-3Z						
Linea urbana	0CZ	Servizi di rete	Forzato	2	E1A	Gestore di rete principale	Sconosciuto
Varie	-Z	Servizi di rete	No		A	Corp. Rete	Sconosciuto

Tabella 18: Configurazione dei dati località per il nodo 2 OpenScape Business

Nodo 2		
Località Paese G.		49
Località rete locale G.		2302
Località sistema G.		66719
Prefisso internazionale		00
Prefisso nazionale		0
Fasci		
ISDN	Codice di linea urbana	0
Servizi di rete	2° cod. linea	0
Parametri del fascio		
Fascio	Tipo n., in uscita	Tipo RNR
Servizi di rete	Sconosciuto	int./DID
ISDN	(Nessuna modifica dei dati immessi)	DID

Nelle tabelle di routing vengono inseriti automaticamente i numeri di telefono di tutti gli utenti escluso il nodo 2, in particolare i numeri interni e i numeri DID diversi dai numeri interni.

Tabella 19: Panoramica delle voci LCR per il nodo 2

Piano di composizione		Tabella delle rotte			Regola di composizione		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 1 Internat	0C0049230266719-1Z	Servizi di rete	Forzato	1	D49230266719E3A	Corp. Rete	Internazionale
Nodo 1 NAT	0C0230266719-1Z						
Nodo 1 Utente	0C66719-1Z						
Nodo 3 Internet	0C0049230266758-3Z	Servizi di rete	Forzato	3	D49230266758E3A	Corp. Rete	Internazionale
Nodo 3 NAT	0C0230266758-3Z						
Nodo 3 Utente	0C66758-3Z						
Linea urbana	0CZ	ISDN	No		A	Gestore di rete principale	Sconosciuto
Varie	-Z	Servizi di rete	No		A	Corp. Rete	Sconosciuto

Tabella 20: Configurazione dei dati località per il nodo 3 OpenScape Business

Nodo 3		
Località Paese G.		49
Località rete locale G.		2302
Località sistema G.		66758
Prefisso internazionale		00
Prefisso nazionale		0
Fasci		
ISDN	Codice di linea urbana	0
Servizi di rete	2° cod. linea	0
Parametri del fascio		
Fascio	Tipo n., in uscita	Tipo RNR
Servizi di rete	Sconosciuto	int./DID
ISDN	(Nessuna modifica dei dati immessi)	DID

Nelle tabelle di routing vengono inseriti automaticamente i numeri di telefono di tutti gli utenti escluso il nodo 3, in particolare i numeri interni e i numeri DID diversi dai numeri interni.

Tabella 21: Panoramica delle voci LCR per il nodo 3

Piano di composizione		Tabella delle rotte			Regola di composizione		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 1 Internat	0C0049230266719-1Z	Servizi di rete	Forzato	1	D49230266719E3A	Corp. Rete	Internazionale
Nodo 1 NAT	0C0230266719-1Z						
Nodo 1 Utente	0C66719-1Z						
Nodo 2 Internet	0C0049230266719-2Z	Servizi di rete	Forzato	2	D49230266719E3A	Corp. Rete	Internazionale
Nodo 2 NAT	0C0230266719-2Z						
Nodo 2 Utente	0C66719-2Z						
Linea urbana	0CZ	ISDN	No		A	Gestore di rete principale	Sconosciuto
Varie	-Z	Servizi di rete	No		A	Corp. Rete	Sconosciuto

Come procedere per la configurazione del collegamento di rete:

1) Configurare l'installazione di base per il nodo 1 (master)
2) Configurare il collegamento in rete per il nodo 1
3) Configurare l'installazione di base per il nodo 2 (slave)
4) Configurare il collegamento in rete per il nodo 2
5) Configurare l'installazione di base per il nodo 3 (slave)
6) Configurare il collegamento in rete per il nodo 3 (slave)
7) Come controllare le funzioni di rete per il master
8) Configurare l'LCR per il collegamento in rete (nodo 1, master)
9) Come configurare l'LCR per il collegamento in rete (nodo 2)
10) Come configurare i fasci e i relativi parametri (nodo 3)
11) Come configurare i fasci e i relativi parametri (fascio 16) (nodo 3)
12) Come configurare l'LCR per il collegamento in rete (nodo 3)

21.6.3.1 Come configurare l'installazione di base per il nodo 1 (master)

Per l'integrazione in un sistema di reti, è necessario indicare il prefisso internazionale e un ID nodo. I numeri di telefono interni devono essere configurati in modo univoco a livello di rete. L'immissione dei numeri di telefono nazionali e locali è importante in quanto questi numeri vengono configurati nella linea ISDN fascio 1 e utilizzati come numeri della sede per la normalizzazione.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. 39 per l'Italia.
4) Inserire l'**Indicativo località** e il **numero di sistema**.
5) Selezionare la casella di controllo **Integrazione rete**.
6) Nel campo **ID nodo** per OpenScape Business S, assegnare un ID nodo univoco sul sistema di reti. L'ID nodo deve essere compreso tra "**1**" e "**100**" (inserire "**1**" per la configurazione di esempio).
7) Fare clic su **Esegui funzione**. Si apre la finestra **Funzioni centrali per gli utenti**.
8) Siccome in una rete tutti i numeri di telefono interni devono essere univoci, i numeri di telefono predefiniti devono venire cancellati. Selezionare il pulsante di opzione **Cancella tutti numeri di telefono**.
9) Selezionare la casella di controllo **Cancella tutti numeri di telefono dell'utente** e fare clic su **OK & Avanti.**. Si procede alla finestra **Modifica numeri di telefono e funzionali pre-configurati**.

   Nota: I codici funzione di un sistema di reti devono essere univoci. Non sono consentiti numeri di telefono doppi!

10) Modificare il numero di telefono preconfigurato con il numero di telefono della rete e fare clic su **OK & Avanti**. I numeri di telefono possono essere configurati manualmente tramite procedura guidata o importati da un file CSV contenente i numeri di telefono appositamente preparati.
11) Importare i client IP.
12) Configurare ora la telefonia Internet.
13) Modificare le impostazioni di una Conferenza Incontro. È necessario inserire nel sistema di reti un codice univoco.
14) Configurare ora l'invio di e-mail.
15) Fare clic su **OK & Avanti**.
16) Fare clic su **Fine**.

21.6.3.2 Come configurare la rete per il nodo 1 (master)

Al passaggio successivo, verrà configurato il collegamento di rete del nodo 1 (master), mediante procedura guidata.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Configurazione di rete**.

4) Selezionare l'impostazione **Rete con OSBiz X / OSBiz S**.
5) Definire il tipo di nodo (**Master**).
6) Nel campo **ID nodo** indicare di numero del nodo dei relativi sistemi OpenScape Business (nella configurazione di esempio, quello dello slave con ID nodo 2).
7) Nel campo **Indirizzo IP** indicare l'indirizzo IP dei relativi sistemi OpenScape Business (nella configurazione di esempio, quello degli slave con l'ID nodo 2 e 3).
8) Selezionare la casella di controllo **Gateway**.
9) Nel campo **Nome** indicare il tipo di sistema.
10) Nel campo **Tipo** indicare il tipo di sottosistema.
11) Eventualmente selezionare la casella di controllo **Crittografia**.

Suggerimento: La crittografia è basata su SPE e non vale per le applicazioni!

Nota: Selezionando la casella di controllo non viene utilizzata alcuna crittografia. Vedere Crittografia segnalazione e payload (SPE) .

12) Fare clic su **Fine**.

21.6.3.3 Come configurare l'installazione di base per il nodo 2 (slave)

Per l'integrazione in un sistema di reti, è necessario indicare il prefisso internazionale e un ID nodo. I numeri di telefono interni devono essere configurati in modo univoco a livello di rete. L'immissione dei numeri di telefono nazionali e locali è importante in quanto questi numeri vengono configurati nella linea ISDN fascio 1 e utilizzati come numeri della sede per la normalizzazione.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. 39 per l'Italia.
4) Inserire l'**Indicativo località** e il **numero di sistema**.
5) Selezionare la casella di controllo **Integrazione rete**.
6) Nel campo **ID nodo** per OpenScape Business, assegnare un ID nodo univoco sul sistema di reti ("**2**" e "**3**" per la configurazione di esempio).
7) Fare clic su **Esegui funzione**. Si apre la finestra **Funzioni centrali per gli utenti**.
8) Siccome in una rete tutti i numeri di telefono interni devono essere univoci, i numeri di telefono predefiniti devono venire cancellati. Selezionare il pulsante di opzione **Cancella tutti numeri di telefono**.

9) Selezionare la casella di controllo **Cancella tutti numeri di telefono dell'utente** e fare clic su **OK & Avanti.**. Si procede alla finestra **Modifica numeri di telefono e funzionali pre-configurati**.

Nota: I codici funzione di un sistema di reti devono essere univoci. Non sono consentiti numeri di telefono doppi!

---

10) Modificare il numero di telefono preconfigurato con il numero di telefono della rete e fare clic su **OK & Avanti**. I numeri di telefono possono essere configurati manualmente tramite procedura guidata o importati da un file CSV contenente i numeri di telefono appositamente preparati.
11) Configurare ora gli utenti ISDN e analogici.
12) Modificare le impostazioni di una Conferenza Incontro. È necessario inserire nel sistema di reti un codice univoco.
13) Configurare ora l'invio di e-mail.
14) Fare clic su **OK & Avanti**.
15) Fare clic su **Fine**.

21.6.3.4 Come configurare la rete per il nodo 2 (slave)

Al passaggio successivo, verrà configurato il collegamento in rete del nodo 2, mediante procedura guidata.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Configurazione di rete**.
4) Selezionare l'impostazione **Rete con OSBiz X / OSBiz S**.
5) In **Tipo nodo**, selezionare la casella **Questo sistema è un nodo SLAVE**.
6) **Indicare l'indirizzo IP del nodo master** (nella configurazione di esempio, l'indirizzo IP del nodo 1).

Suggerimento: Dopo aver selezionato **OK & Avanti** non sarà più possibile annullare questa azione!

---

7) Lo **Stato registrazione** viene visualizzato con lo stato **eseguito** (o con il relativo messaggio d'errore). La procedura guidata viene chiusa.
8) Fare clic su **Fine**.

21.6.3.5 Come configurare l'installazione di base per il nodo 3 (slave)

Per l'integrazione in un sistema di reti, è necessario indicare il prefisso internazionale e un ID nodo. I numeri di telefono interni devono essere configurati in modo univoco a livello di rete. L'immissione dei numeri di telefono

nazionali e locali è importante in quanto questi numeri vengono configurati nella linea ISDN fascio 1 e utilizzati come numeri della sede per la normalizzazione.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. 39 per l'Italia.
4) Inserire l'**Indicativo località** e il **numero di sistema** (identico a quello del sistema gateway assegnato).
5) Selezionare la casella di controllo **Integrazione rete**.
6) Nel campo **ID nodo** per OpenScape Business, assegnare un ID nodo univoco sul sistema di reti ("**3**" per la configurazione di esempio).
7) Fare clic su **Esegui funzione**. Si apre la finestra **Funzioni centrali per gli utenti**.
8) Siccome in una rete tutti i numeri di telefono interni devono essere univoci, i numeri di telefono predefiniti devono venire cancellati. Selezionare il pulsante di opzione **Cancella tutti numeri di telefono**.
9) Selezionare la casella di controllo **Cancella tutti numeri di telefono dell'utente** e fare clic su **OK & Avanti.**. Si procede alla finestra **Modifica numeri di telefono e funzionali pre-configurati**.

   Nota: I codici funzione di un sistema di reti devono essere univoci. Non sono consentiti numeri di telefono doppi!

10) Modificare il numero di telefono preconfigurato con il numero di telefono della rete e fare clic su **OK & Avanti**. I numeri di telefono possono essere configurati manualmente tramite procedura guidata o importati da un file CSV contenente i numeri di telefono appositamente preparati.
11) Configurare ora gli utenti ISDN e analogici.
12) Modificare le impostazioni di una Conferenza Incontro. È necessario inserire nel sistema di reti un codice univoco.
13) Configurare ora l'invio di e-mail.
14) Fare clic su **OK & Avanti**.
15) Fare clic su **Fine**.

21.6.3.6 Come controllare le funzioni di rete per il master

È possibile controllare lo stato generale della rete e i singoli numeri di telefono.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Rete**.

2) Nella riga di stato, visualizzare lo **Stato sincronizzazione** della rete. Il verde indica nessun problema sulla rete, il rosso presenza di problemi sulla rete.
3) Nella finestra **Rete**, selezionare la scheda **Visualizzazione dominio**, verranno visualizzati tutti i nodi disponibili con **ID nodo**, **Nome**, **Tipo sistema**, **Indirizzo server**, **Stato registrazione** e **Stato disponibilità**.
4) Nella finestra **Rete**, selezionare la scheda **Numeri di telefono**, si apre una finestra con tutte le informazioni su:
   - **Numero di telefono**
   - **DISA**
   - **Nome**
   - **Tipo porta**
   - **Nodi**

21.6.3.7 Configurare il collegamento in rete per il nodo 3 (slave)

Al passaggio successivo, verrà configurato il collegamento di rete del nodo 3, mediante procedura guidata.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Configurazione di rete**.
4) Selezionare l'impostazione **Rete con OSBiz X / OSBiz S**.
5) In **Tipo nodo**, selezionare la casella **Questo sistema è un nodo SLAVE**.
6) **Indicare l'indirizzo IP del nodo master** (nella configurazione di esempio, l'indirizzo IP del nodo 1).

   Suggerimento: Dopo aver selezionato **OK & Avanti** non sarà più possibile annullare questa azione!

7) Lo **Stato registrazione** viene visualizzato con lo stato **eseguito** (o con il relativo messaggio d'errore). La procedura guidata viene chiusa.
8) Fare clic su **Fine**.

21.6.3.8 Come configurare l'LCR per il collegamento in rete (nodi 3, slave)

Nel piano di composizione LCR, le voci predefinite nell'indice 32, 33, 34 e 35 devono essere ampliate con altre voci per consentire la composizione dei numeri nei formati "Internazionale, Nazionale e Utenti" per le chiamate ai nodi 1 e 2. "Internazionale" e "Nazionale" sono sempre richiesti; "Utenti" è necessario per i nodi partner che si trovano nella stessa rete locale. Devono essere compilate le voci 36, 37 e 39 per la interazione con nodo 1 (numero di telefono 100 > 199) e le voci 39, 40 e 41 per la interazione con nodo 2

(numero di telefono 200 > 299). Queste informazioni vengono utilizzate per la composizione dei numeri dalle applicazioni (ad esempio myPortal for Desktop).

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Nella struttura dei menu fare clic su **Piano di composizione**.
4) Inserire i seguenti valori nei punti liberi (in questo caso da 35 a 40) secondo i valori predefiniti:

Piano di composizior	Nome	Cifre selezionate	Tabella delle rotte
31	Suite applicazioni	-371	12
32	Predefinito	88CZ	1
33	IP rete	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 1 Inter	0C0049230266719-1Z	16
37	Nodo 1 Nat	0C0230266719-1Z	16
38	Nodo 1 Utente	0C66719-1Z	16
39	Nodo 2 Inter	0C0049230266719-2Z	17
40	Nodo 2 Nat	0C0230266719-2Z	17
41	Nodo 2 Utente	0C66719-2Z	17

5) Fare clic su **Applica**, quindi su **OK**.
6) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 1 e 2.
   a) Nel campo **Nome della regola**, immettere **Nodo 1 + 2**.
   b) In **Formato della regola di selezione** immettere **D49230266719E3A**.
   c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
   d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
   e) Fare clic su **Applica**, quindi su **OK**.
7) Nella struttura dei menu fare clic su **Tabella delle rotte** per configurare la tabella delle rotte 16 per i servizi di rete a assegnarla direttamente al nodo 1.
8) Fare clic sulla tabella delle rotte 16.
   a) Nel campo **Fascio**, selezionare la voce **Rete**.
   b) In **Regola di composizione**, selezionare la voce **Nodo 1 + 2**.
   c) In **Abil. min.**, selezionare la voce **15**.
   d) In **Avviso**, selezionare la voce **Nessuno**.
   e) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
   f) In **ID nodo GW**, selezionare la voce **1**.
   g) Fare clic su **Applica**, quindi su **OK**.

9) Nella struttura dei menu fare clic su **Tabella delle rotte**, per configurare la tabella delle rotte 17 per la rete e assegnarla direttamente al nodo 2.

10) Fare clic sulla tabella delle rotte 17.

a) Nel campo **Fascio**, selezionare la voce **Rete**.
b) In **Regola di composizione**, selezionare la voce **Nodo 1 + 2**.
c) In **Abil. min.**, selezionare la voce **15**.
d) In **Avviso**, selezionare la voce **Nessuno**.
e) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
f) In **ID nodo GW**, selezionare la voce **2**.
g) Fare clic su **Applica**, quindi su **OK**.

21.6.3.9 Come configurare l'LCR per il collegamento in rete (nodo 2)

Nel piano di composizione LCR, le voci predefinite nell'indice 32, 33, 34 e 35 devono essere ampliate con altre voci per consentire la composizione dei numeri nei formati "Internazionale, Nazionale e Utenti" per le chiamate ai nodi 1 e 3. "Internazionale" e "Nazionale" sono sempre richiesti; "Utenti" è necessario per i nodi partner che si trovano nella stessa rete locale. Devono essere compilate le voci 36, 37 e 38 per la interazione con nodo 1 (numero di telefono 100 > 199) e le voci 39, 40 e 41 per la interazione con nodo 3 (numero di telefono 300 > 399). Queste informazioni vengono utilizzate per la composizione dei numeri dalle applicazioni (ad esempio myPortal for Desktop).

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.

3) Nella struttura dei menu fare clic su **Piano di composizione**.

4) Inserire i seguenti valori nei punti liberi (in questo caso da 35 a 40) secondo i valori predefiniti:

Piano di composizior	Nome	Cifre selezionate	Tabella delle rotte
31	Suite applicazioni	-271	12
32	Predefinito	88CZ	1
33	IP rete	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 1 Inter	0C0049230266719-1Z	16
37	Nodo 1 Nat	0C0230266719-1Z	16
38	Nodo 1 Utente	0C66719-1Z	16
39	Nodo 3 Inter	0C0049230266758-3Z	17
40	Nodo 3 Nat	0C0230266758-3Z	17
41	Nodo 3 Utente	0C66758-3Z	17

5) Fare clic su **Applica**, quindi su **OK**.

6) Nella struttura dei menu fare clic su **Tabella dei collegamenti**.
7) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 1.
   a) Nel campo **Nome della regola**, immettere **Nodo 1**.
   b) In **Formato della regola di selezione** immettere **D49230266719E3A**.
   c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
   d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
   e) Fare clic su **Applica**, quindi su **OK**.
8) Fare clic sulla tabella delle rotte 16, per configurarla per il collegamento in rete al nodo 1.
   a) Nel campo **Fascio**, selezionare la voce **Rete**.
   b) In **Regola di composizione**, selezionare la voce **Nodo 1**.
   c) In **Abil. min.**, selezionare la voce **1**.
   d) In **Avviso**, selezionare la voce **Nessuno**.
   e) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
   f) In **ID nodo GW**, selezionare la voce **1**.
   g) Fare clic su **Applica**, quindi su **OK**.
9) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 3.
   a) Nel campo **Nome della regola**, immettere **Nodo 3**.
   b) In **Formato della regola di selezione** immettere **D49230266758E3A**.
   c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
   d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
   e) Fare clic su **Applica**, quindi su **OK**.
10) Nella struttura dei menu fare clic su **Tabella dei collegamenti**.
11) Fare clic sulla tabella delle rotte 17, per configurarla per il collegamento in rete al nodo 3.
   a) Nel campo **Fascio**, selezionare la voce **Rete**.
   b) In **Regola di composizione**, selezionare la voce **Nodo 3**.
   c) In **Abil. min.**, selezionare la voce **1**.
   d) In **Avviso**, selezionare la voce **Nessuno**.
   e) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
   f) In **ID nodo GW**, selezionare la voce **3**.
   g) Fare clic su **Applica**, quindi su **OK**.

21.6.3.10 Come configurare i fasci e i relativi parametri (nodo 1, master)

Nel nodo 1 occorre configurare le impostazioni per la linea esterna relativamente a numero località, codice del fascio e parametri del fascio. Qui è necessario inserire il numero del sistema per la definizione della località del gateway. Queste informazioni vengono utilizzate per la composizione dalle applicazioni, quali ad esempio, myPortal.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Fascio**.
4) Nella finestra **Cambia gruppo di linee**, nel campo **Nome del fascio**, immettere il nome `Fascio 1` per il fascio linee esterne.
5) In **Codici del fascio** digitare `0`.
6) In **Numero del sistema - entrante** , nel campo **Prefisso internazionale** digitare `39`.
7) In **Numero del sistema- entrante**, nel campo **Prefisso interurbano** digitare `02`.
8) In **Numero del sistema** - entrante, nel campo **Numero del sistema** digitare `66719`.
9) Selezionare la casella di controllo in **Numero del sistema - entrante** nel campo **Numero località**.
10) È possibile accettare le impostazioni predefinite per i parametri del fascio (Tipo nr., in uscita, Tipo di numero di telefono).
11) Fare clic su **Applica**, quindi su **OK**.

21.6.3.11 Come configurare i fasci e i relativi parametri (fascio 16) (nodo 1)

Per il fascio 16 (rete), è obbligatorio compilare la voce per 2° cod. linea, sia per il master che per lo slave.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic sull'ultimo **Fascio** (ad es. **Fascio 16**).
4) Nella finestra **Cambia gruppo di linee**, nel campo **Nome del fascio**, immettere un nome (ad es. `Rete`) per il fascio di rete.
5) In **Codici del fascio** non inserire nulla.
6) In **Codice di linea urbana (2° cod. linea)** digitare 0.
7) È possibile accettare le impostazioni predefinite per i parametri del fascio (Tipo nr., in uscita, Tipo di numero di telefono).
8) Fare clic su **Applica**, quindi su **OK**.

21.6.3.12 Come configurare l'LCR per il collegamento in rete (nodo 1)

Nel piano di composizione LCR, le voci predefinite nell'indice 32, 33, 34 e 35 devono essere ampliate con altre voci per consentire la composizione dei numeri nei formati "Internazionale, Nazionale e Utenti" per le chiamate ai nodi 2 e 3. "Internazionale" e "Nazionale" sono sempre richiesti; "Utenti" è necessario per i nodi partner che si trovano nella stessa rete locale. Queste informazioni

vengono utilizzate per la composizione dei numeri dalle applicazioni (ad esempio myPortal for Desktop).

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Nella struttura dei menu fare clic su **Piano di composizione**.
4) Inserire i seguenti valori nei punti liberi (in questo caso da 35 a 40) secondo i valori predefiniti:

Piano di composizion	Nome	Cifre selezionate	Tabella delle rotte
16	Predefinito	0CZ	1
17	Predefinito	0C1Z	1
18	Predefinito	0CNZ	1
32	Predefinito	88CZ	1
33	IP rete	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 2 Inter	0C0049230266719-2Z	16
37	Nodo 2 Nat	0C0230266719-2Z	16
38	Nodo 2 Utente	0C66719-2Z	16
39	Nodo 3 Inter	0C0049230266758-3Z	17
40	Nodo 3 Nat	0C0230266758-3Z	17
41	Nodo 3 Utente	0C66758-3Z	17

5) Fare clic su **Applica**, quindi su **OK**.
6) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 2.
   a) Nel campo **Nome della regola**, immettere **Nodo 2**.
   b) In **Formato della regola di selezione** immettere **D49230266719E3A**.
   c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
   d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
   e) Fare clic su **Applica**, quindi su **OK**.
7) Nella struttura dei menu fare clic su **Tabella dei collegamenti**.

8) Fare clic sulla tabella delle rotte 16, per configurarla per il collegamento in rete al nodo 2.
   a) Nel campo **Fascio**, selezionare la voce **Rete**.
   b) In **Regola di composizione**, selezionare la voce **Nodo 2**.
   c) In **Abil. min.**, selezionare la voce **1**.
   d) In **Avviso**, selezionare la voce **Nessuno**.
   e) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
   f) In **ID nodo GW**, selezionare la voce **2**.
   g) Fare clic su **Applica**, quindi su **OK**.

9) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 3.
   a) Nel campo **Nome della regola**, immettere **Nodo 3**.
   b) In **Formato della regola di selezione** immettere **D49230266719E1A**.
   c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
   d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
   e) Fare clic su **Applica**, quindi su **OK**.

10) Nella struttura dei menu fare clic su **Tabella dei collegamenti**.

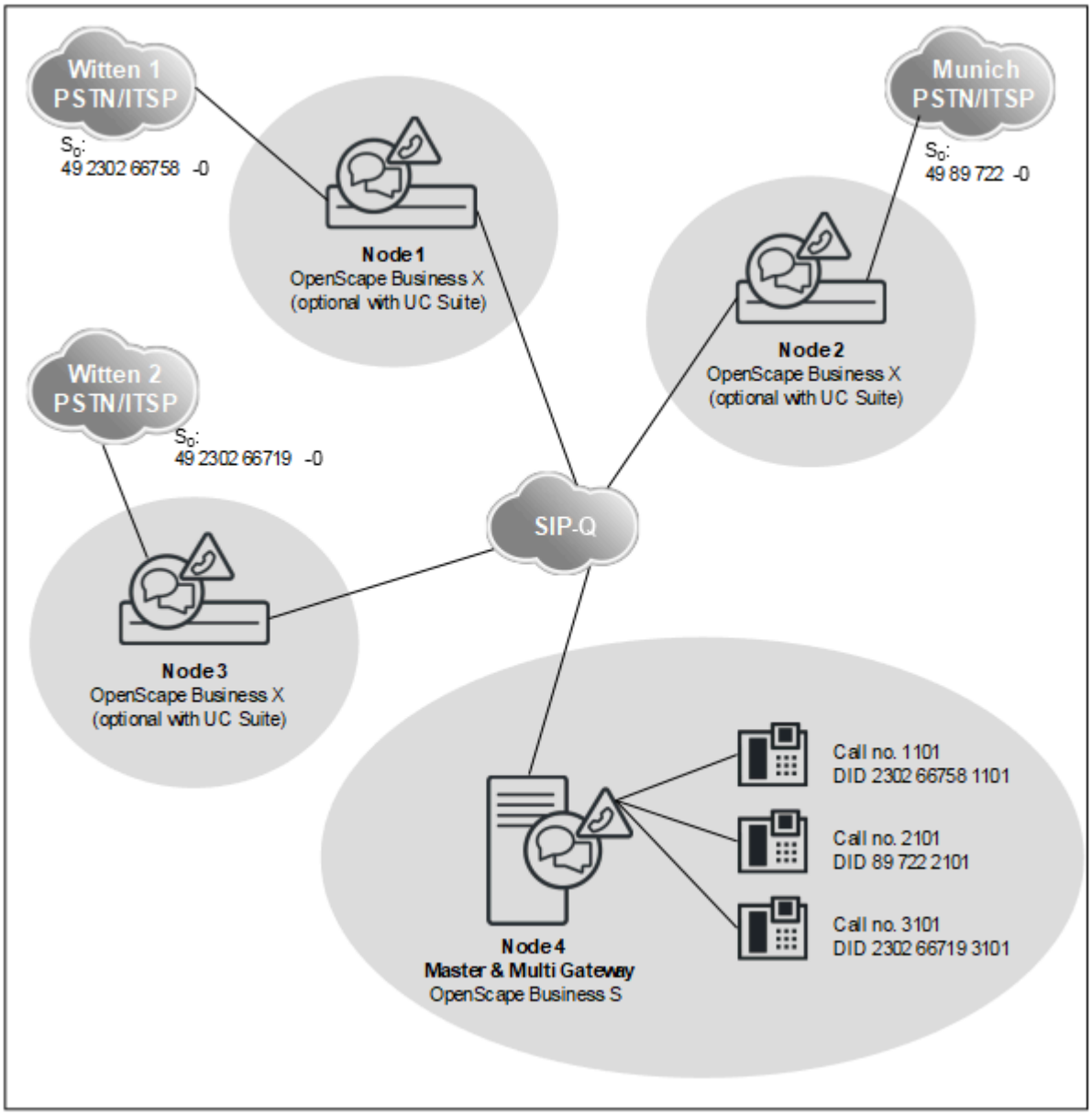
11) Fare clic sulla tabella delle rotte 17, per configurarla per il collegamento in rete al nodo 3.
   a) Nel campo **Fascio**, selezionare la voce **Rete**.
   b) In **Regola di composizione**, selezionare la voce **Nodo 3**.
   c) In **Abil. min.**, selezionare la voce **1**.
   d) In **Avviso**, selezionare la voce **Nessuno**.
   e) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
   f) In **ID nodo GW**, selezionare la voce **3**.
   g) Fare clic su **Applica**, quindi su **OK**.

12) Nella struttura dei menu fare clic su **Tabella dei collegamenti**.

21.6.4 Collegamento in rete di Open Scape Business X e OpenScape Business S (gateway multiplo)

Fino a 32 sistemi di comunicazione OpenScape Business X e OpenScape Business S possono essere collegati in rete. Multi Gateway significa che ogni utente IP registrato in OpenScape Business S è assegnato a uno specifico gateway.

Dati di rete



- Numerazione chiusa
- Funzionalità voce e UC a livello di rete con configurazione UC Suite tramite WBM (procedure guidate)
- La funzionalità UC viene realizzata tramite l'UC Booster Server o la UC Booster Card
- È consentito un solo OpenScape Business S in un sistema di reti.
- Tutti i sistemi devono utilizzare lo stesso prefisso del paese
- Tutti i sistemi devono essere sullo stesso fuso orario
- Sulla rete può essere presente un solo codice linea esterna (ad esempio, 0).
- Fino a 32 sistemi in rete e 1500 utenti senza soluzione UC
- Fino a 8 sistemi in rete e 1500 utenti con soluzione UC

Servizi di rete

Collegamento in rete UC	Numerazione chiusa	Numerazione aperta
Numero massimo di nodi	8 con soluzione UC e 32 senza soluzione UC	
Numero massimo di utenti in un singolo sistema di comunicazione	a seconda del sistema OpenScape Business X	
Numero massimo di utenti nella rete	1500	

Collegamento in rete UC	Numerazione chiusa	Numerazione aperta
UC Booster Card	UC Smart: 51-150 utenti (0-50 utenti senza UC Booster Card) UC Suite: 0-150 utenti	Supporto non disponibile
UC Booster Server	UC Smart: da 150 utenti UC Suite: da 150 Utenti	Supporto non disponibile

Amministrazione	Numerazione chiusa	Numerazione aperta
WBM	Amministrazione di rete, tramite procedure guidate	Supporto non disponibile
Manager E	Amministrazione dell'intera rete per compiti speciali (non per OpenScape Business S)	Supporto non disponibile
Amministrazione UC Suite (per UC Booster Server e UC Booster Card)	Amministrazione di rete, tramite procedure guidate	Supporto non disponibile
Importazione di dati in blocco tramite file CSV (numeri, numeri interni, nomi)	Separatamente per ogni nodo del sistema di reti	Supporto non disponibile

Concessione della licenza	Numerazione chiusa	Numerazione aperta
Struttura di concessione delle licenze	È necessaria una licenza di rete per ogni nodo	Supporto non disponibile

Configurazione

Questa configurazione (con la numerazione chiusa e la UC Suite) mostra un esempio di quali passaggi occorre eseguire per la configurazione del collegamento a gateway multiplo.

Requisiti:

- È disponibile un piano di rete. Tramite il piano di rete ci si assicura che ogni numero di telefono interno nel sistema di reti venga assegnato una sola volta con numerazione univoca (chiusa). Sono consentiti numeri di telefono di diversa lunghezza. Solo i numeri di telefono DID possono ricorrere più volte.
- La rete IP è configurata e tutti i nodi sono reciprocamente raggiungibili tramite ping
- Tutti i nodi sono dotati della stessa versione del software

Deviazioni di chiamata a livello di nodo: all'arrivo di chiamate su linee IP per le quali è già prevista una deviazione, non verranno eseguite ulteriori deviazioni alla casella vocale. Il motivo è che in caso contrario non è possibile realizzare un'assegnazione univoca alla casella vocale

Nel caso siano necessarie regole di rappresentanza a livello di nodo, queste devono essere configurate nei profili degli apparecchi OpenScape Business o nelle segnalazioni delle chiamate. Le chiamate corrispondenti a livello di nodo non verranno più segnalate come deviate, ma come chiamate dirette. In questo caso, potrà essere eseguita la deviazione di chiamata del rappresentante alla casella vocale.

Tabella 22: Configurazione dei dati località per il nodo 1

Nodo 1		
Località Paese G.		49
Località rete locale G.		2302
Località sistema G.		66758
Prefisso internazionale		00
Prefisso nazionale		0
Fasci		
ISDN	Codice di linea urbana	0
Servizi di rete	2° cod. linea	0
Parametri del fascio		
Fascio	Tipo n., in uscita	Tipo RNR
Servizi di rete	Sconosciuto	int./DID
ISDN	(Nessuna modifica dei dati immessi)	DID

Nelle tabelle di routing vengono inseriti automaticamente i numeri di telefono di tutti gli utenti escluso il nodo 1, in particolare i numeri interni e i numeri DID diversi dai numeri interni.

Tabella 23: Panoramica delle voci LCR per il nodo 1

Piano di composizione		**Tabella delle rotte**			**Regola di composizione**		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 2 Internet	0C004989722-Z	Servizi di rete	Forzato	2	D4989722E3A	Corp. Rete	Internazionale
Nodo 2 NAT	0C089722-Z						
Nodo 2 Utente	0C722-Z						
Nodo 3 Internet	0C0049230266719-Z	Servizi di rete	Forzato	3	D49230266719E3A	Corp. Rete	Internazionale
Nodo 3 NAT	0C0230266719-Z						
Nodo 3 Utente	0C66719-Z						

Piano di composizione		Tabella delle rotte			Regola di composizione		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 4 Internet	0C0049230266758-Z	Servizi di rete	NO		D230266758E3A	Corp. Rete	Nazionale
Nodo 4 NAT	0C0230266758-Z						
Nodo 4 Utente	0C66758-Z						
Varie	-Z	Servizi di rete	No		BA	Corp. Rete	Sconosciuto
Linea urbana internazionale	0C0049-Z	ISDN	No		D0E3A	Gestore di rete principale	Sconosciuto
Linea urbana	0CZ	ISDN	No		A	Gestore di rete principale	Sconosciuto

Tabella 24: Configurazione dei dati località per il nodo 2

Nodo 2		
Località Paese G.		49
Località rete locale G.		89
Località sistema G.		722
Prefisso internazionale		00
Prefisso nazionale		0
Fasci		
ISDN	Codice di linea urbana	0
Servizi di rete	2° cod. linea	0
Parametri del fascio		
Fascio	Tipo n., in uscita	Tipo RNR
Servizi di rete	Sconosciuto	int./DID
ISDN	(Nessuna modifica dei dati immessi)	DID

Nelle tabelle di routing vengono inseriti automaticamente i numeri di telefono di tutti gli utenti escluso il nodo 2, in particolare i numeri interni e i numeri DID diversi dai numeri interni.

Tabella 25: Panoramica delle voci LCR per il nodo 2

Piano di composizione		Tabella delle rotte			Regola di composizione		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 1 Internet	0C0049230266758-Z	Servizi di rete	Forzato	1	D492302667E3A	Corp. Rete	Internazionale

Piano di composizione		Tabella delle rotte			Regola di composizione		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 1 NAT	0C0230266758-Z						
Nodo 1 Utente	0C66758-Z						
Nodo 3 Internet	0C0049230266719-Z	Servizi di rete	Forzato	3	D49230266719E3A	Corp. Rete	Internazionale
Nodo 3 NAT	0C0230266719-Z						
Nodo 3 Utente	0C66719-Z						
Nodo 4 Internet	0C004989722-Z	Servizi di rete	NO		D89722E3A	Corp. Rete	Nazionale
Nodo 4 NAT	0C089722-Z						
Nodo 4 Utente	0C722-Z						
Varie	-Z	Servizi di rete	No		BA	Corp. Rete	Sconosciuto
Linea urbana internazionale	0C0049-Z	ISDN	No		D0E3A	Gestore di rete principale	Sconosciuto
Linea urbana	0CZ	ISDN	No		A	Gestore di rete principale	Sconosciuto

Tabella 26: Configurazione dei dati località per il nodo 3

Nodo 3		
Località Paese G.		49
Località rete locale G.		2302
Località sistema G.		66719
Prefisso internazionale		00
Prefisso nazionale		0
Fasci		
ISDN	Codice di linea urbana	0
Servizi di rete	2° cod. linea	0
Parametri del fascio		
Fascio	Tipo n., in uscita	Tipo RNR
Servizi di rete	Sconosciuto	int./DID
ISDN	(Nessuna modifica dei dati immessi)	DID

Nelle tabelle di routing vengono inseriti automaticamente i numeri di telefono di tutti gli utenti escluso il nodo 3, in particolare i numeri interni e i numeri DID diversi dai numeri interni.

Tabella 27: Panoramica delle voci LCR per il nodo 3

Piano di composizione		Tabella delle rotte			Regola di composizione		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 1 Internet	0C0049230266758-Z	Servizi di rete	Forzato	1	D49230266758E3A	Corp. Rete	Internazionale
Nodo 1 NAT	0C0230266758-Z						
Nodo 1 Utente	0C66758-Z						
Nodo 2 Internet	0C004989722-Z	Servizi di rete	Forzato	2	D4989722E3A	Corp. Rete	Internazionale
Nodo 2 NAT	0C089722-Z						
Nodo 2 Utente	0C722-Z						
Nodo 4 Internet	0C004989230266719-Z	Servizi di rete	No		D230266719E3A	Corp. Rete	Nazionale
Nodo 4 NAT	0C0230266719-Z						
Nodo 4 Utente	0C66719-Z						
Varie	-Z	Servizi di rete	No		BA	Corp. Rete	Sconosciuto
Linea urbana internazionale	0C0049-Z	ISDN	No		D0E3A	Gestore di rete principale	Sconosciuto
Linea urbana	0CZ	ISDN	No		A	Gestore di rete principale	Sconosciuto

Configurazione dei dati località per il nodo 4: collegare i dati località per la "pseudo" linea esterna (fascio 1) con codice di linea urbana = 0 e tipo = Linea urbana, in quanto il nodo 4 non dispone di alcuna connessione diretta a una linea.

Tabella 28: Nodo 4, pseudo-linea esterna

Nodo 4	
Località Paese G.	49
Località rete locale G.	
Località sistema G.	
Prefisso internazionale	00

Nodo 4		
Prefisso nazionale		0
Fasci		
ISDN	Codice di linea urbana	0
Servizi di rete	2° cod. linea	0
Parametri del fascio		
Fascio	Tipo n., in uscita	Tipo RNR
Servizi di rete	Sconosciuto	int./DID
ISDN	(Nessuna modifica dei dati immessi)	DID

Nelle tabelle di routing vengono inseriti automaticamente i numeri di telefono di tutti gli utenti escluso il nodo 1, in particolare i numeri interni e i numeri DID diversi dai numeri interni.

Tabella 29: Nodo 4, fascio rete

Nodo 4		
Località Paese G.		
Località rete locale G.		
Località sistema G.		
Prefisso internazionale		00
Prefisso nazionale		0
Fasci		
ISDN	Codice di linea urbana	0
Servizi di rete	2° cod. linea	0
Parametri del fascio		
Fascio	Tipo n., in uscita	Tipo RNR
Servizi di rete	Nazionale	int./DID
ISDN	(Nessuna modifica dei dati immessi)	DID

Tabella 30: Panoramica delle voci LCR per il nodo 4

Piano di composizione		Tabella delle rotte			Regola di composizione		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 1 Internet	0C0049230266758-Z	Servizi di rete	Forzato	1	D49230266758E3A	Corp. Rete	Internazionale
Nodo 1 NAT	0C0230266758-Z						
Nodo 2 Internet	0C004989722-Z	Servizi di rete	Forzato	2	D4989722E3A	Corp. Rete	Internazionale

Piano di composizione		Tabella delle rotte			Regola di composizione		
Nome	**Cifre selezionate**	**Fascio**	**Gateway dedicato**	**ID gateway**	**Regola di composizione**	**Metodo**	**Tipo**
Nodo 2 NAT	0C089722-Z						
Nodo 3 Internet	0C004989230266719-Z	Servizi di rete	Forzato	3	D49230266719E3A	Corp. Rete	Internazionale
Nodo 3 NAT	0C0230266719-Z						
Varie	-Z	Servizi di rete	NO		A	Corp. Rete	Sconosciuto
Linea urbana	0CZ	Servizi di rete	GATEWAY MULTIPLO	1	E1A	Gestore di rete principale	Sconosciuto

Come procedere per la configurazione del collegamento di rete:

1) Come configurare l'installazione di base per il nodo 4 (master)
2) Configurare la rete per il nodo 4 (master)
3) Configurare l'installazione di base per il nodo 1 (slave)
4) Configurare il collegamento in rete per il nodo 1 (slave)
5) Configurare l'installazione di base per il nodo 2 (slave)
6) Configurare il collegamento in rete per il nodo 2 (slave)
7) Configurare l'installazione di base per il nodo 3 (slave)
8) Configurare il collegamento in rete per il nodo 3 (slave)
9) Come controllare le funzioni di rete per il master
10) Come configurare il gateway multiplo per il nodo 4 (master)
11) Come configurare i fasci e i relativi parametri (nodo 1, slave)
12) Configurare l'LCR per il collegamento in rete (nodi 1, slave)
13) Come configurare i fasci e i relativi parametri (nodo 2, slave)
14) Configurare l'LCR per il collegamento in rete (nodi 2, slave)
15) Come configurare i fasci e i relativi parametri (nodo 3 slave)
16) Configurare l'LCR per il collegamento in rete (nodi 3, slave)
17) Come configurare i fasci e i relativi parametri (nodo 4, master)
18) Configurare l'LCR per il collegamento in rete (nodi 4, master)

21.6.4.1 Come configurare l'installazione di base per il nodo 4 (OpenScape Business S, master)

Per l'integrazione in un sistema di reti, è necessario indicare il prefisso internazionale e un ID nodo. I numeri di telefono interni devono essere configurati in modo univoco a livello di rete. L'immissione dei numeri di telefono nazionali e locali è importante in quanto questi numeri vengono configurati nella linea ISDN fascio 1 e utilizzati come numeri della sede per la normalizzazione.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.

2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. 39 per l'Italia.
4) Non inserire nulla nei campi **Indicativo località** e **Numero del sistema**!
5) Selezionare la casella di controllo **Integrazione rete**.
6) Nel campo **ID nodo** per OpenScape Business S, assegnare un ID nodo univoco sul sistema di reti. L'ID nodo deve essere compreso tra "**1**" e "**100**" (utilizzare "**4**" per la configurazione di esempio).
7) Fare clic su **Esegui funzione**. Si apre la finestra **Funzioni centrali per gli utenti**.
8) Siccome in una rete tutti i numeri di telefono interni devono essere univoci, i numeri di telefono predefiniti devono venire cancellati. Selezionare il pulsante di opzione **Cancella tutti numeri di telefono**.
9) Selezionare la casella di controllo **Cancella tutti numeri di telefono dell'utente** e fare clic su **OK & Avanti.**. Si procede alla finestra **Modifica numeri di telefono e funzionali pre-configurati**.

Nota: I codici funzione di un sistema di reti devono essere univoci. Non sono consentiti numeri di telefono doppi!

---

10) Modificare il numero di telefono preconfigurato con il numero di telefono della rete e fare clic su **OK & Avanti**. I numeri di telefono possono essere configurati manualmente tramite procedura guidata o importati da un file CSV contenente i numeri di telefono appositamente preparati.
11) Importare ora i client IP.
12) Configurare i client IP.
13) Modificare le impostazioni di una Conferenza Incontro. È necessario inserire nel sistema di reti un codice univoco.
14) Configurare ora l'invio di e-mail.
15) Fare clic su **Fine**.

21.6.4.2 Come configurare la rete per il nodo 4 (master)

Al passaggio successivo, verrà configurato il collegamento di rete del nodo 3, mediante procedura guidata.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Configurazione di rete**.
4) Selezionare l'impostazione **Rete con OSBiz X / OSBiz S**.
5) Selezionare la casella di controllo **Questo sistema è il nodo MASTER**.

6) Nel campo **ID nodo** indicare il numero del nodo dei relativi sistemi OpenScape Business (nella configurazione di esempio, quello degli slave con l'ID nodo 1, 2 e 3).
7) Nel campo **Indirizzo IP** indicare l'indirizzo IP dei relativi sistemi OpenScape Business (nella configurazione di esempio, quello degli slave con l'ID nodo 1, 2 e 3).
8) Selezionare la casella di controllo **Gateway**.
9) Nel campo **Nome** indicare il tipo di sistema (ad esempio, Slave 1).
10) Nel campo **Tipo** indicare il tipo di sottosistema.
11) Eventualmente selezionare la casella di controllo **Crittografia**.

Suggerimento: La crittografia è basata su SPE e non vale per le applicazioni!

Nota: Selezionando la casella di controllo non viene utilizzata alcuna crittografia. Vedere Crittografia segnalazione e payload (SPE) .

12) Fare clic su **Fine**.

21.6.4.3 Come configurare l'installazione di base per il nodo 1 (slave)

Per l'integrazione in un sistema di reti, è necessario indicare il prefisso internazionale e un ID nodo. I numeri di telefono interni devono essere configurati in modo univoco a livello di rete. L'immissione dei numeri di telefono nazionali e locali è importante in quanto questi numeri vengono configurati nella linea ISDN fascio 1 e utilizzati come numeri della sede per la normalizzazione.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. 39 per l'Italia.
4) Inserire l'**Indicativo località** e il **numero di sistema**.
5) Selezionare la casella di controllo **Integrazione rete**.
6) Nel campo **ID nodo** per OpenScape Business S, assegnare un ID nodo univoco sul sistema di reti ("**1**" per la configurazione di esempio).
7) Fare clic su **Esegui funzione**. Si apre la finestra **Funzioni centrali per gli utenti**.
8) Siccome in una rete tutti i numeri di telefono devono essere univoci, i numeri di telefono predefiniti devono venire cancellati. Selezionare il pulsante di opzione **Cancella tutti numeri di telefono**.

9) Selezionare la casella di controllo **Cancella tutti numeri di telefono dell'utente** e fare clic su **OK & Avanti.**. Si procede alla finestra **Modifica numeri di telefono e funzionali pre-configurati**.

Nota: I codici funzione di un sistema di reti devono essere univoci. Non sono consentiti numeri di telefono doppi!

---

10) Modificare il numero di telefono preconfigurato con il numero di telefono della rete e fare clic su **OK & Avanti**. I numeri di telefono possono essere configurati manualmente tramite procedura guidata o importati da un file CSV contenente i numeri di telefono appositamente preparati.
11) Configurare ora gli utenti ISDN e analogici.
12) Modificare le impostazioni di una Conferenza Incontro. È necessario inserire nel sistema di reti un codice univoco.
13) Configurare ora l'invio di e-mail.
14) Fare clic su **Fine**.

21.6.4.4 Come configurare la rete per il nodo 1 (slave)

Il passaggio successivo prevede la configurazione della procedura guidata per il collegamento in rete.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Configurazione di rete**.
4) Selezionare l'impostazione **Rete con OSBiz X / OSBiz S**.
5) **Inserire l'indirizzo IP del nodo MASTER** (un OpenScape Business viene configurato come nodo slave e viene inserito l'indirizzo IP corrispondente del nodo master, ovvero OpenScape Business S). Master e Gateway multiplo vengono assegnati allo stesso sistema, nella configurazione di esempio di OpenScape Business S).

Suggerimento: Dopo aver selezionato **OK & Avanti** non sarà più possibile annullare questa azione!

---

6) Lo **Stato registrazione** viene visualizzato con lo stato **eseguito** (o con il relativo messaggio d'errore). La procedura guidata viene chiusa.
7) Fare clic su **Fine**.

21.6.4.5 Come configurare l'installazione di base per il nodo 2 (slave)

Per l'integrazione in un sistema di reti, è necessario indicare il prefisso internazionale e un ID nodo. I numeri di telefono interni devono essere

configurati in modo univoco a livello di rete. L'immissione dei numeri di telefono nazionali e locali è importante in quanto questi numeri vengono configurati nella linea ISDN fascio 1 e utilizzati come numeri della sede per la normalizzazione.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. 39 per l'Italia.
4) Inserire l'**Indicativo località** e il **numero di sistema**.
5) Selezionare la casella di controllo **Integrazione rete**.
6) Nel campo **ID nodo** per OpenScape Business S, assegnare un ID nodo univoco sul sistema di reti ("**2**" per la configurazione di esempio).
7) Fare clic su **Esegui funzione**. Si apre la finestra **Funzioni centrali per gli utenti**.
8) Siccome in una rete tutti i numeri di telefono interni devono essere univoci, i numeri di telefono predefiniti devono venire cancellati. Selezionare il pulsante di opzione **Cancella tutti numeri di telefono**.
9) Selezionare la casella di controllo **Cancella tutti numeri di telefono dell'utente** e fare clic su **OK & Avanti.**. Si procede alla finestra **Modifica numeri di telefono e funzionali pre-configurati**.

   Nota: I codici funzione di un sistema di reti devono essere univoci. Non sono consentiti numeri di telefono doppi!

10) Modificare il numero di telefono preconfigurato con il numero di telefono della rete e fare clic su **OK & Avanti**. I numeri di telefono possono essere configurati manualmente tramite procedura guidata o importati da un file CSV contenente i numeri di telefono appositamente preparati.
11) Configurare ora gli utenti ISDN e analogici.
12) Modificare le impostazioni di una Conferenza Incontro. È necessario inserire nel sistema di reti un codice univoco.
13) Configurare ora l'invio di e-mail.
14) Fare clic su **Fine**.

21.6.4.6 Come configurare la rete per il nodo 2 (slave)

Al passaggio successivo, verrà configurato il collegamento in rete del nodo 2, mediante procedura guidata.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.

2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Configurazione di rete**.
4) Selezionare l'impostazione **Rete con OSBiz X / OSBiz S**.
5) In **Tipo nodo**, selezionare la casella **Questo sistema è un nodo SLAVE**.
6) **Inserire l'indirizzo IP del nodo MASTER** (un OpenScape Business viene configurato come nodo slave e viene inserito l'indirizzo IP corrispondente del nodo master, ovvero OpenScape Business S). Master e Gateway multiplo vengono assegnati allo stesso sistema, nella configurazione di esempio di OpenScape Business S).

   Suggerimento: Dopo aver selezionato **OK & Avanti** non sarà più possibile annullare questa azione!

7) Lo **Stato registrazione** viene visualizzato con lo stato **eseguito** (o con il relativo messaggio d'errore). La procedura guidata viene chiusa.
8) Fare clic su **Fine**.

21.6.4.7 Come configurare l'installazione di base per il nodo 3 (slave)

Per l'integrazione in un sistema di reti, è necessario indicare il prefisso internazionale e un ID nodo. I numeri di telefono interni devono essere configurati in modo univoco a livello di rete. L'immissione dei numeri di telefono nazionali e locali è importante in quanto questi numeri vengono configurati nella linea ISDN fascio 1 e utilizzati come numeri della sede per la normalizzazione.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Nel campo **Prefisso internazionale**, immettere il prefisso del paese, ad es. 39 per l'Italia.
4) Inserire l'**Indicativo località** e il **numero di sistema**.
5) Selezionare la casella di controllo **Integrazione rete**.
6) Nel campo **ID nodo** per OpenScape Business, assegnare un ID nodo univoco sul sistema di reti ("**3**" per la configurazione di esempio).
7) Fare clic su **Esegui funzione**. Si apre la finestra **Funzioni centrali per gli utenti**.
8) Siccome in una rete tutti i numeri di telefono interni devono essere univoci, i numeri di telefono predefiniti devono venire cancellati. Selezionare il pulsante di opzione **Cancella tutti numeri di telefono**.

9) Selezionare la casella di controllo **Cancella tutti numeri di telefono dell'utente** e fare clic su **OK & Avanti.**. Si procede alla finestra **Modifica numeri di telefono e funzionali pre-configurati**.

Nota: I codici funzione di un sistema di reti devono essere univoci. Non sono consentiti numeri di telefono doppi!

---

10) Modificare il numero di telefono preconfigurato con il numero di telefono della rete e fare clic su **OK & Avanti**. I numeri di telefono possono essere configurati manualmente tramite procedura guidata o importati da un file CSV contenente i numeri di telefono appositamente preparati.
11) Configurare ora gli utenti ISDN e analogici.
12) Modificare le impostazioni di una Conferenza Incontro. È necessario inserire nel sistema di reti un codice univoco.
13) Configurare ora l'invio di e-mail.
14) Fare clic su **Fine**.

21.6.4.8 Come configurare la rete per il nodo 3 (slave)

Al passaggio successivo, verrà configurato il collegamento di rete del nodo 3, mediante procedura guidata.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Configurazione di rete**.
4) Selezionare l'impostazione **Rete con OSBiz X / OSBiz S**.
5) In **Tipo nodo**, selezionare la casella **Questo sistema è un nodo SLAVE**.
6) **Inserire l'indirizzo IP del nodo MASTER** (un OpenScape Business viene configurato come nodo slave e viene inserito l'indirizzo IP corrispondente del nodo master, ovvero OpenScape Business S). Master e Multi Location vengono sempre assegnati allo stesso sistema, nella configurazione di esempio di OpenScape Business S).

Suggerimento: Dopo aver selezionato **OK & Avanti** non sarà più possibile annullare questa azione!

---

7) Lo **Stato registrazione** viene visualizzato con lo stato **eseguito** (o con il relativo messaggio d'errore). La procedura guidata viene chiusa.
8) Fare clic su **Fine**.

21.6.4.9 Come controllare le funzioni di rete per il master

È possibile controllare lo stato generale della rete e i singoli numeri di telefono.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Rete**.
2) Nella riga di stato, visualizzare lo **Stato sincronizzazione** della rete. Il verde indica nessun problema sulla rete, il rosso presenza di problemi sulla rete.
3) Nella finestra **Rete**, selezionare la scheda **Visualizzazione dominio**, verranno visualizzati tutti i nodi disponibili con **ID nodo**, **Nome**, **Tipo sistema**, **Indirizzo server**, **Stato registrazione** e **Stato disponibilità**.
4) Nella finestra **Rete**, selezionare la scheda **Numeri di telefono**, si apre una finestra con tutte le informazioni su:
   - **Numero di telefono**
   - **DISA**
   - **Nome**
   - **Tipo porta**
   - **Nodi**

21.6.4.10 Come configurare il gateway multiplo per il nodo 4 (master)

Il sistema di reti viene configurato come rete con gateway multiplo al nodo master.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Configurazione di rete**.
3) In **Configurazione di rete**, selezionare l'impostazione **Impostazione multi-posizione**. Nella finestra **Impostazione multi-posizione** viene definita l'assegnazione dell'utente alla località. L'assegnazione del numero di telefono all'ID nodo viene utilizzata ad esempio per l'impegno della linea in uscita nel nodo predefinito assegnato.
4) Nella configurazione di esempio, in **Impostazione multi-posizione**, inserire le seguenti assegnazioni (tutti i telefoni sono registrati in OpenScape Business S):

Numero di telefono	Nome	Node Id
1101	1101KN1	1 slave Witten1
1102	1102KN1	1 slave Witten1
1103	1103KN1	1 slave Witten1
2101	2101KN2	2 slave Monaco
2102	2102KN2	2 slave Monaco
2103	2103KN2	2 slave Monaco

Numero di telefono	Nome	Node Id
3101	3101KN3	3 slave Witten 2
3102	3102KN3	3 slave Witten 2
3103	3103KN3	3 slave Witten 2

5) Fare clic su **Fine**.

21.6.4.11 Come configurare il fascio e i relativi parametri (nodo 1, slave)

Con i seguenti passaggi, configurare il fascio e i parametri del fascio per il collegamento in rete dello slave.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Fascio**.
4) Nella finestra **Cambia gruppo di linee**, nel campo **Nome del fascio**, immettere il nome `Fascio 1` per il fascio linee esterne.
5) In **Codici del fascio** digitare `0`.
6) In **Numero del sistema - entrante** , nel campo **Prefisso internazionale** digitare `39`.
7) In **Numero del sistema- entrante**, nel campo **Prefisso interurbano** digitare `02`.
8) In **Numero del sistema- entrante**, nel campo **Numero del sistema** digitare `66758`.
9) Selezionare la casella di controllo in **Numero del sistema - entrante** nel campo **Numero località**.
10) È possibile accettare le impostazioni predefinite per i parametri del fascio (Tipo nr., in uscita, Tipo di numero di telefono).
11) Fare clic su **Applica**, quindi su **OK**.

21.6.4.12 Come configurare l'LCR per il collegamento in rete (nodi 1, slave)

Nel piano di composizione LCR, le voci predefinite nell'indice 32, 33, 34 e 35 devono essere ampliate con altre voci per consentire la composizione dei numeri nei formati "Internazionale, Nazionale e Utenti" per le chiamate ai nodi 2 e 3 nonché per il nodo 4 (gateway multiplo). "Internazionale" e "Nazionale" sono sempre richiesti; "Utenti" è necessario per i nodi partner che si trovano nella stessa rete locale.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Nella struttura dei menu fare clic su **Piano di composizione**.
4) Inserire i seguenti valori nei punti liberi (in questo caso da 36 a 43) secondo i valori predefiniti:

Piano di composizion	Nome	Cifre selezionate	Tabella delle rotte
31	Suite applicazioni	-171	12
32	Predefinito	88CZ	1
33	IP rete	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 2 Inter	0C004989722-Z	16
37	Nodo 2 Nat	0C089722-Z	16
38	Nodo 3 Inter	0C0049230266719-Z	17
39	Nodo 3 Nat	0C0230266719-Z	17
40	Nodo 3 Utente	0C66719-Z	17
41	Nodo 4 Inter	0C0049230266758-Z	18
42	Nodo 4 Nat	0C0230266758-Z	18
43	Nodo 4 Utente	0C66758-Z	18
44			-

5) Fare clic su **Applica**, quindi su **OK**.
6) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 2.
   a) Nel campo **Nome della regola**, immettere **Nodo 2**.
   b) In **Formato della regola di selezione** immettere **D4989722E3A**.
   c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
   d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
   e) Fare clic su **Applica**, quindi su **OK**.
7) Nella struttura dei menu fare clic su **Tabella delle rotte** per configurare la tabella delle rotte 16 per i servizi di rete a assegnarla direttamente al nodo 2.
   a) Fare clic sulla tabella delle rotte 16.
   b) Nel campo **Fascio**, selezionare la voce **Rete**.
   c) In **Regola di composizione**, selezionare la voce **Nodo 2**.
   d) In **Abil. min.**, selezionare la voce **15**.
   e) In **Avviso**, selezionare la voce **Nessuno**.
   f) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
   g) In **ID nodo GW**, selezionare la voce **2**.
   h) Fare clic su **Applica**, quindi su **OK**.

8) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 3.
   a) Nel campo **Nome della regola**, immettere **Nodo 3**.
   b) In **Formato della regola di selezione** immettere **D49230266719E3A**.
   c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
   d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
   e) Fare clic su **Applica**, quindi su **OK**.

9) Nella struttura dei menu fare clic su **Tabella delle rotte**, per configurare la tabella delle rotte 17 per la rete e assegnarla direttamente al nodo 3.
   a) Fare clic sulla tabella delle rotte 17.
   b) Nel campo **Fascio**, selezionare la voce **Rete**.
   c) In **Regola di composizione**, selezionare la voce **Nodo 3**.
   d) In **Abil. min.**, selezionare la voce **15**.
   e) In **Avviso**, selezionare la voce **Nessuno**.
   f) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
   g) In **ID nodo GW**, selezionare la voce **3**.
   h) Fare clic su **Applica**, quindi su **OK**.

10) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 4.
   a) Nel campo **Nome della regola**, immettere **Nodo 4 ML**.
   b) In **Formato della regola di selezione** immettere **D230266758E3A**.
   c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
   d) Nel campo **Tipo**, selezionare la voce **Nazionale**.
   e) Fare clic su **Applica**, quindi su **OK**.

11) Nella struttura dei menu fare clic su **Tabella delle rotte**, per configurare la tabella delle rotte 18 per la rete e assegnarla direttamente al nodo 4.
   a) Fare clic sulla tabella delle rotte 18.
   b) Nel campo **Fascio**, selezionare la voce **Rete**.
   c) In **Regola di composizione**, selezionare la voce **Nodo 4**.
   d) In **Abil. min.**, selezionare la voce **15**.
   e) In **Avviso**, selezionare la voce **Nessuno**.
   f) Fare clic su **Applica**, quindi su **OK**.

21.6.4.13 Come configurare il fascio e i relativi parametri (nodo 2, slave)

Con i seguenti passaggi, configurare il fascio e i parametri del fascio per il collegamento in rete dello slave.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.

3) Nella struttura dei menu fare clic su **Fascio**.

4) Nella finestra **Cambia gruppo di linee**, nel campo **Nome del fascio**, immettere il nome `Fascio 1` per il fascio linee esterne.
5) In **Codici del fascio** digitare `0`.
6) In **Numero del sistema - entrante** , nel campo **Prefisso internazionale** digitare `39`.
7) In **Numero del sistema** - entrante, nel campo **Prefisso interurbano** digitare 89.
8) In Numero del sistema - entrante, nel campo Numero del sistema digitare `722`.
9) Selezionare la casella di controllo in **Numero del sistema - entrante** nel campo **Numero località**.
10) È possibile accettare le impostazioni predefinite per i parametri del fascio (Tipo nr., in uscita, Tipo di numero di telefono).
11) Fare clic su **Applica**, quindi su **OK**.

21.6.4.14 Come configurare l'LCR per il collegamento in rete (nodi 2, slave)

Nel piano di composizione LCR, le voci predefinite nell'indice 32, 33, 34 e 35 devono essere ampliate con altre voci per consentire la composizione dei numeri nei formati "Internazionale, Nazionale e Utenti" per le chiamate ai nodi 1 e 2. "Internazionale" e "Nazionale" sono sempre richiesti; "Utenti" è necessario per i nodi partner che si trovano nella stessa rete locale. Devono essere compilate le voci 36, 37 e 38 per la interazione con nodo 1 (numero di telefono 100 > 199) e le voci 39, 40 e 41 per la interazione con nodo 3 (numero di telefono 300 > 399). Queste informazioni vengono utilizzate per la composizione dei numeri dalle applicazioni (ad esempio myPortal for Desktop).

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Nella struttura dei menu fare clic su **Piano di composizione**.
4) Inserire i seguenti valori nei punti liberi (in questo caso da 36 a 43) secondo i valori predefiniti:

Piano di composizion	Nome	Cifre selezionate	Tabella delle rotte
31	Suite applicazioni	-171	12
32	Predefinito	88CZ	1
33	IP rete	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 1 Inter	0C0049230266758-Z	16
37	Nodo 1 Nat	0C0230266758-Z	16
38	Nodo 3 Inter	0C0049230266719-Z	17
39	Nodo 3 Nat	0C0230266719-Z	17

Piano di composizior	Nome	Cifre selezionate	Tabella delle rotte
40	Nodo 3 Utente	0C66719-Z	17
41	Nodo 4 Inter	0C004989722-Z	18
42	Nodo 4 Nat	0C089722-Z	18
43	Nodo 4 Utente	0C722-Z	18
44			-

5) Fare clic su **Applica**, quindi su **OK**.

6) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 1.

a) Nel campo **Nome della regola**, immettere **Nodo 1**.
b) In **Formato della regola di selezione** immettere **D49230266758E3A**.
c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
e) Fare clic su **Applica**, quindi su **OK**.

7) Nella struttura dei menu fare clic su **Tabella delle rotte** per configurare la tabella delle rotte 16 per i servizi di rete a assegnarla direttamente al nodo 1.

a) Fare clic sulla tabella delle rotte 16.
b) Nel campo **Fascio**, selezionare la voce **Rete**.
c) In **Regola di composizione**, selezionare la voce **Nodo 1**.
d) In **Abil. min.**, selezionare la voce **15**.
e) In **Avviso**, selezionare la voce **Nessuno**.
f) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
g) In **ID nodo GW**, selezionare la voce **1**.
h) Fare clic su **Applica**, quindi su **OK**.

8) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 3.

a) Nel campo **Nome della regola**, immettere **Nodo 3**.
b) In **Formato della regola di selezione** immettere **D49230266719E3A**.
c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
e) Fare clic su **Applica**, quindi su **OK**.

9) Nella struttura dei menu fare clic su **Tabella delle rotte**, per configurare la tabella delle rotte 17 per la rete e assegnarla direttamente al nodo 3.

a) Fare clic sulla tabella delle rotte 17.
b) Nel campo **Fascio**, selezionare la voce **Rete**.
c) In **Regola di composizione**, selezionare la voce **Nodo 3 diretto**.
d) In **Abil. min.**, selezionare la voce **15**.
e) In **Avviso**, selezionare la voce **Nessuno**.
f) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
g) In **ID nodo GW**, selezionare la voce **3**.
h) Fare clic su **Applica**, quindi su **OK**.

10) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 4.
    a) Nel campo **Nome della regola**, immettere **Nodo 4**.
    b) In **Formato della regola di selezione** immettere **D89722E3A**.
    c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
    d) In **Tipo**, selezionare la voce **Prefisso interurbano**.
    e) Fare clic su **Applica**, quindi su **OK**.
11) Nella struttura dei menu fare clic su **Tabella delle rotte**, per configurare la tabella delle rotte 18 per la rete e assegnarla direttamente al nodo 4.
    a) Fare clic sulla tabella delle rotte 18.
    b) Nel campo **Fascio**, selezionare la voce **Rete**.
    c) In **Regola di composizione**, selezionare la voce **Nodo 4**.
    d) In **Abil. min.**, selezionare la voce **15**.
    e) In **Avviso**, selezionare la voce **Nessuno**.
    f) Fare clic su **Applica**, quindi su **OK**.

21.6.4.15 Come configurare il fascio e i relativi parametri (nodo 3, slave)

Con i seguenti passaggi, configurare il fascio e i relativi parametri per il collegamento in rete dello slave.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Fascio**.
4) Nella finestra **Cambia gruppo di linee**, nel campo **Nome del fascio**, immettere il nome `Fascio 1` per il fascio linee esterne.
5) In **Codici del fascio** digitare `0`.
6) In **Numero del sistema - entrante** , nel campo **Prefisso internazionale** digitare `39`.
7) In **Numero del sistema- entrante**, nel campo **Prefisso interurbano** digitare `02`.
8) In **Numero del sistema** - entrante, nel campo **Numero del sistema** digitare `66719`.
9) Selezionare la casella di controllo in **Numero del sistema - entrante** nel campo **Numero località**.
10) È possibile accettare le impostazioni predefinite per i parametri del fascio (Tipo nr., in uscita, Tipo di numero di telefono).
11) Fare clic su **Applica**, quindi su **OK**.

21.6.4.16 Come configurare l'LCR per il collegamento in rete (nodi 3, slave)

Nel piano di composizione LCR, le voci predefinite nell'indice 32, 33, 34 e 35 devono essere ampliate con altre voci per consentire la composizione dei

numeri nei formati "Internazionale, Nazionale e Utenti" per le chiamate ai nodi 1 e 2. "Internazionale" e "Nazionale" sono sempre richiesti; "Utenti" è necessario per i nodi partner che si trovano nella stessa rete locale. Queste informazioni vengono utilizzate per la composizione dei numeri dalle applicazioni (ad esempio myPortal for Desktop).

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.

3) Nella struttura dei menu fare clic su **Piano di composizione**.

4) Inserire i seguenti valori:

Piano di composizion	Nome	Cifre selezionate	Tabella delle rotte
31	Suite applicazioni	-171	12
32	Predefinito	88CZ	1
33	IP rete	-Z	13
34	COInternat	0C0049-Z	14
36	Nodo 1 Inter	0C0049230266758-Z	16
37	Nodo 1 Nat	0C00230266758-Z	16
38	Nodo 1 Utente	0C66758-Z	16
39	Nodo 2 Inter	0C004989722-Z	17
40	Nodo 2 Nat	0C0089722-Z	17
41	Nodo 4 Inter	0C0049230266719-Z	18
42	Nodo 4 Nat	0C0230266719-Z	18
43	Nodo 4 Utente	0C66719-Z	18
44			-

5) Fare clic su **Applica**, quindi su **OK**.

6) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 1.

a) Nel campo **Nome della regola**, immettere **Nodo 1**.

b) In **Formato della regola di selezione** immettere **D49230266758E3A**.

c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.

d) In **Tipo**, selezionare la voce **Prefisso internazionale**.

e) Fare clic su **Applica**, quindi su **OK**.

7) Nella struttura dei menu fare clic su **Tabella delle rotte** per configurare la tabella delle rotte 16 per i servizi di rete a assegnarla direttamente al nodo 1.

a) Fare clic sulla tabella delle rotte 16.
b) Nel campo **Fascio**, selezionare la voce **Rete**.
c) In **Regola di composizione**, selezionare la voce **Nodo 1**.
d) In **Abil. min.**, selezionare la voce **15**.
e) In **Avviso**, selezionare la voce **Nessuno**.
f) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
g) In **ID nodo GW**, selezionare la voce **1**.
h) Fare clic su **Applica**, quindi su **OK**.

8) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 2.

a) Nel campo **Nome della regola**, immettere **Nodo 2**.
b) In **Formato della regola di selezione** immettere **D4989722E3A**.
c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
e) Fare clic su **Applica**, quindi su **OK**.

9) Nella struttura dei menu fare clic su **Tabella delle rotte**, per configurare la tabella delle rotte 17 per la rete e assegnarla direttamente al nodo 2.

a) Fare clic sulla tabella delle rotte 17.
b) Nel campo **Fascio**, selezionare la voce **Rete**.
c) In **Regola di composizione**, selezionare la voce **Nodo 2**.
d) In **Abil. min.**, selezionare la voce **15**.
e) In **Avviso**, selezionare la voce **Nessuno**.
f) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
g) In **ID nodo GW**, selezionare la voce **2**.
h) Fare clic su **Applica**, quindi su **OK**.

10) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 4.

a) Nel campo **Nome della regola**, immettere **Nodo 4 ML**
b) In **Formato della regola di selezione** immettere **D230266719E3A**
c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**
d) In **Tipo**, selezionare la voce **Prefisso interurbano**
e) Fare clic su **Applica**, quindi su **OK**.

11) Nella struttura dei menu fare clic su **Tabella delle rotte**, per configurare la tabella delle rotte 18 per la rete e assegnarla direttamente al nodo 4.

a) Fare clic sulla tabella delle rotte 18.
b) Nel campo **Fascio**, selezionare la voce **Rete**.
c) In **Regola di composizione**, selezionare la voce **Nodo 4**.
d) In **Abil. min.**, selezionare la voce **15**.
e) In **Avviso**, selezionare la voce **Nessuno**.
f) Fare clic su **Applica**, quindi su **OK**.

21.6.4.17 Come configurare il fascio e i relativi parametri (nodo 4, master)

Con i seguenti passaggi, configurare il fascio e i parametri del fascio per il collegamento in rete dello slave.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Linee/Rete**.
3) Nella struttura dei menu fare clic su **Fascio**.
4) Nella finestra **Cambia gruppo di linee**, nel campo **Nome del fascio**, immettere il nome `Fascio 1` per il fascio linee esterne.
5) In **Codici del fascio** digitare `0`.
6) In **Numero del sistema - entrante** , nel campo **Prefisso internazionale** digitare `39`.
7) Non inserire nulla nei campi **Prefisso interurbano** e Numero del sistema.
8) Selezionare la casella di controllo in **Numero del sistema - entrante** nel campo **Numero località**.
9) È possibile accettare le impostazioni predefinite per i parametri del fascio (Tipo nr., in uscita, Tipo di numero di telefono).
10) Fare clic su **Applica**, quindi su **OK**.

21.6.4.18 Come configurare l'LCR per il collegamento in rete (nodo 4, master)

Nel piano di composizione LCR, le voci predefinite nell'indice 32, 33, 34 e 35 devono essere ampliate con altre voci per consentire la composizione dei numeri nei formati "Internazionale, Nazionale e Utenti" per le chiamate ai nodi 1 e 2. "Internazionale" e "Nazionale" sono sempre richiesti; "Utenti" è necessario per i nodi partner che si trovano nella stessa rete locale. Queste informazioni vengono utilizzate per la composizione dei numeri dalle applicazioni (ad esempio myPortal for Desktop).

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Nella struttura dei menu fare clic su **Piano di composizione**.
4) Inserire i seguenti valori nei punti liberi (in questo caso da 36 a 43) secondo i valori predefiniti:

Piano di composizion	Nome	Cifre selezionate	Tabella delle rotte
1	Chiamata di emergenza	0C112	19

Piano di composizion	Nome	Cifre selezionate	Tabella delle rotte
2	Chiamata di emergenza	0C110	19
3	Telelavoro	0C0137Z	19
4	Televoto	0C0138Z	19
5	Servizi Premium	0C0900Z	19
6	Servizio informazioni	0C118Z	19
7	Numero di telefono speciale	0C116116	19
16	Predefinito	0CZ	19
17	Predefinito	0C1Z	19
18	Predefinito	0CNZ	19
31	Suite applicazioni	-471	12
32	Predefinito	88CZ	1
33	IP rete	-Z	13
34	COInternat	0C0049-Z	15
36	Nodo 1 Inter	0C0049230266758-Z	16
37	Nodo 1 Nat	0C0230266758-Z	16
38	Nodo 1 Utente	0C66758-Z	16
39	Nodo 2 Inter	0C004989722-Z	17
40	Nodo 2 Nat	0C089722-Z	17
41	Nodo 3 Inter	0C0049230266719-Z	18
42	Nodo 3 Nat	0C0230266719-Z	18
43	Nodo 3 Utente	0C66719-Z	18
44			-

5) Fare clic su **Applica**, quindi su **OK**.

6) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 1.

a) Nel campo **Nome della regola**, immettere **Nodo 1**.

b) In **Formato della regola di selezione** immettere **D49230266758E3A**.

c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.

d) In **Tipo**, selezionare la voce **Prefisso internazionale**.

e) Fare clic su **Applica**, quindi su **OK**.

7) Nella struttura dei menu fare clic su **Tabella delle rotte** per configurare la tabella delle rotte 16 per i servizi di rete a assegnarla direttamente al nodo 1.

a) Fare clic sulla tabella delle rotte 16.
b) Nel campo **Fascio**, selezionare la voce **Rete**.
c) In **Regola di composizione**, selezionare la voce **Nodo 1**.
d) In **Abil. min.**, selezionare la voce **15**.
e) In **Avviso**, selezionare la voce **Nessuno**.
f) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
g) In **ID nodo GW**, selezionare la voce **1**.
h) Fare clic su **Applica**, quindi su **OK**.

8) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 2.

a) Nel campo **Nome della regola**, immettere **Nodo 2**.
b) In **Formato della regola di selezione** immettere **D4989722E3A**.
c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
d) In **Tipo**, selezionare la voce **Prefisso internazionale**.
e) Fare clic su **Applica**, quindi su **OK**.

9) Nella struttura dei menu fare clic su **Tabella delle rotte**, per configurare la tabella delle rotte 17 per la rete e assegnarla direttamente al nodo 2.

a) Fare clic sulla tabella delle rotte 17.
b) Nel campo **Fascio**, selezionare la voce **Rete**.
c) In **Regola di composizione**, selezionare la voce **Nodo 2**.
d) In **Abil. min.**, selezionare la voce **15**.
e) In **Avviso**, selezionare la voce **Nessuno**.
f) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
g) In **ID nodo GW**, selezionare la voce **2**.
h) Fare clic su **Applica**, quindi su **OK**.

10) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per il nodo 3.

a) Nel campo **Nome della regola**, immettere **Nodo 3 ML**
b) In **Formato della regola di selezione** immettere **D230266719E3A**
c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**
d) In **Tipo**, selezionare la voce **Prefisso internazionale**
e) Fare clic su **Applica**, quindi su **OK**.

11) Nella struttura dei menu fare clic su **Tabella delle rotte**, per configurare la tabella delle rotte 18 per la rete e assegnarla direttamente al nodo 3.

a) Fare clic sulla tabella delle rotte 18.
b) Nel campo **Fascio**, selezionare la voce **Rete**.
c) In **Regola di composizione**, selezionare la voce **Nodo 3**.
d) In **Abil. min.**, selezionare la voce **15**.
e) In **Avviso**, selezionare la voce **Nessuno**.
f) In **Gateway dedicato**, fare clic sulla voce **Forzato**.
g) In **ID nodo GW**, selezionare la voce **3**.
h) Fare clic su **Applica**, quindi su **OK**.

12) Nella struttura dei menu fare clic sulla relativa **Regola di composizione** per le chiamate esterne. Si tratta di una regola di selezione predefinita "Gateway Call".

a) Nel campo **Nome della regola**, immettere **Gateway Call**.
b) In **Formato della regola di selezione** immettere **E1A**.
c) Come **Metodo del gestore di rete** selezionare la voce **Corporate Network**.
d) Nel campo **Tipo**, selezionare la voce **Sconosciuto**.
e) Fare clic su **Applica**, quindi su **OK**.

13) Nella struttura dei menu, fare clic su **Tabella delle rotte** per configurare la tabella delle rotte 19 per l'accesso alla linea esterna dello slave. In base alla voce MultiGateway viene determinata l'appartenenza dell'utente al nodo e l'accesso alla linea esterna viene eseguito presso questo nodo.

14) Fare clic sulla tabella delle rotte 19.

a) Nel campo **Fascio**, selezionare la voce **Rete**.
b) Nel campo **Regola di selezione**, selezionare la voce **Gateway Call**.
c) In **Abil. min.**, selezionare la voce **15**.
d) In **Avviso**, selezionare la voce **Nessuno**.
e) In **Gateway dedicato**, fare clic sulla voce **Multi-Gateway**.
f) In **ID nodo GW**, selezionare la voce **1**.
g) Fare clic su **Applica**, quindi su **OK**.

21.6.5 Collegamento in rete di OpenScape Business in un ambiente di hosting

In un ambiente con più località (ambiente di hosting), a ogni località è possibile assegnare un fascio e a ogni fascio una registrazione ITSP. È possibile gestire un massimo di 8 registrazioni ITSP. Pertanto si può effettuare una registrazione per ITSP o procedere a più registrazioni tramite un ITPS. A ogni registrazione ITSP è possibile associare un indicativo località e successivamente degli utenti. Il collegamento degli utenti alle diverse località nel sistema di comunicazione avviene tramite VPN o MPLS. Se le località si trovano in paesi diversi, occorre utilizzare un proprio OpenScape Business S per ogni località (scenario 1a). Se tutte le località si trovano in uno stesso paese, è possibile utilizzare un OpenScape Business S (scenario 1b).

Entrambi gli scenari possono essere realizzati anche con i modelli hardware OpenScape Business X (ad esempio, piccole configurazioni). Presso una località è possibile utilizzare inoltre i componenti TDM.

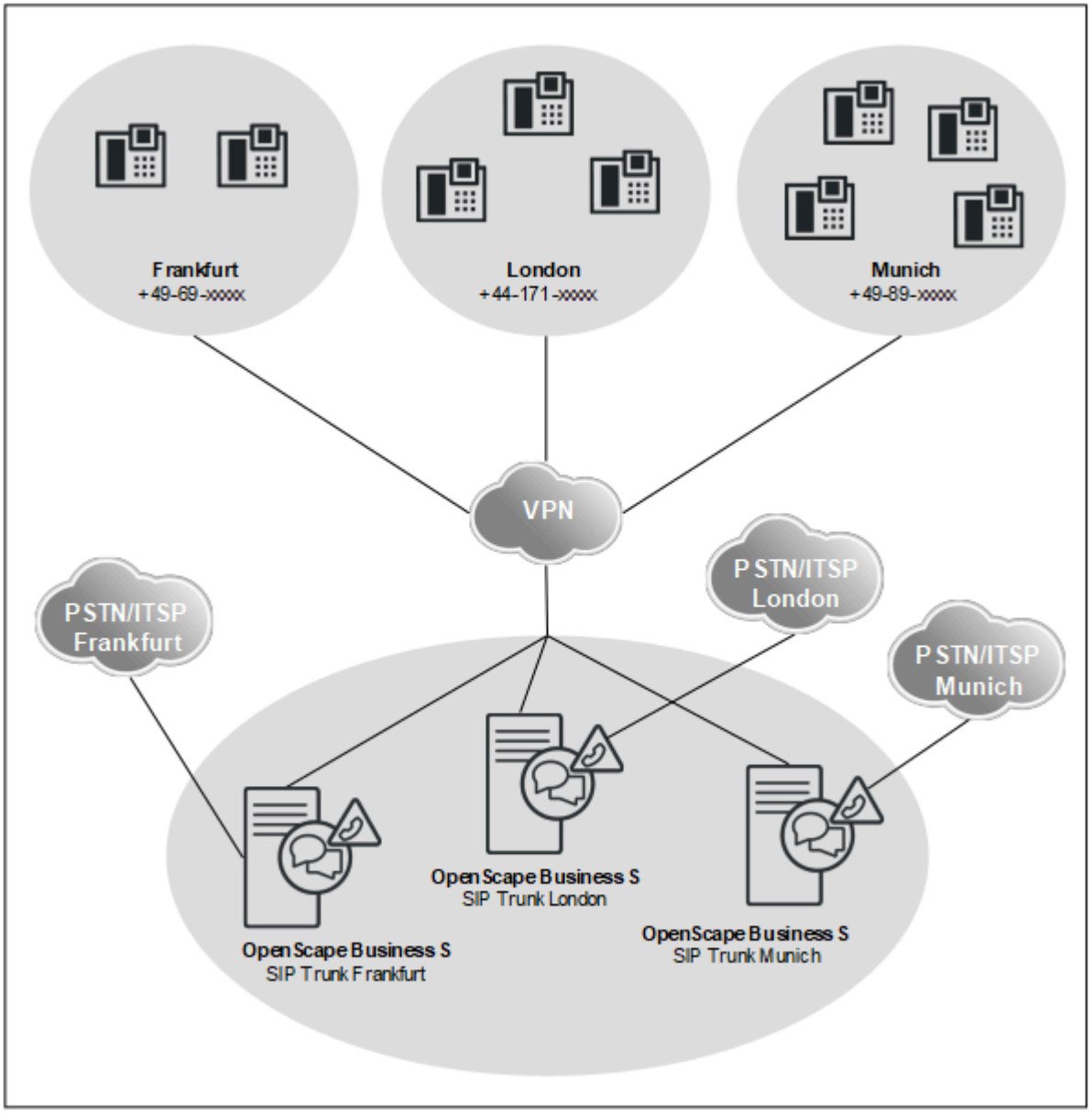
Di seguito sono descritti altri possibili scenari di hosting. È possibile realizzare le seguenti configurazioni:

- Utilizzo di OpenScape Business S e OpenScape Business X nel data Center del cliente o dell'host
- OpenScape Business S su hardware server dedicati o virtualizzati
- Per questo è richiesta un'infrastruttura VPN o MPLS, in particolare con diverse località dei clienti (nessun ruoter NAT specifico di una località per l'accesso a Internet)
- Fino a 8 ITSP per sistema e paese, MSN provider per la selezione passante
- Fino a 8 prefissi nazionali di località (area code) per sistema e paese assegnati a un massimo di 8 località del cliente (multisito)
- Scenari multisito combinabili con connessioni classiche (voce e UC)

- Multisito - supporto per > 8 località nei collegamenti in rete (collegamento in rete multisito "n" volte)
- Multisito - supporto per collegamenti in rete internazionali (collegamento in rete multisito "n" volte)
- Scenari di collegamento in rete con gateway ISDN completamente integrati
- Dal punto di vista tecnico è necessario che il numero di selezione passante per il provider ISDN, ad esempio un provider SIP, sia utilizzato ovunque.

Scenario a: hosting con OpenScape Business S per località

Dati di rete

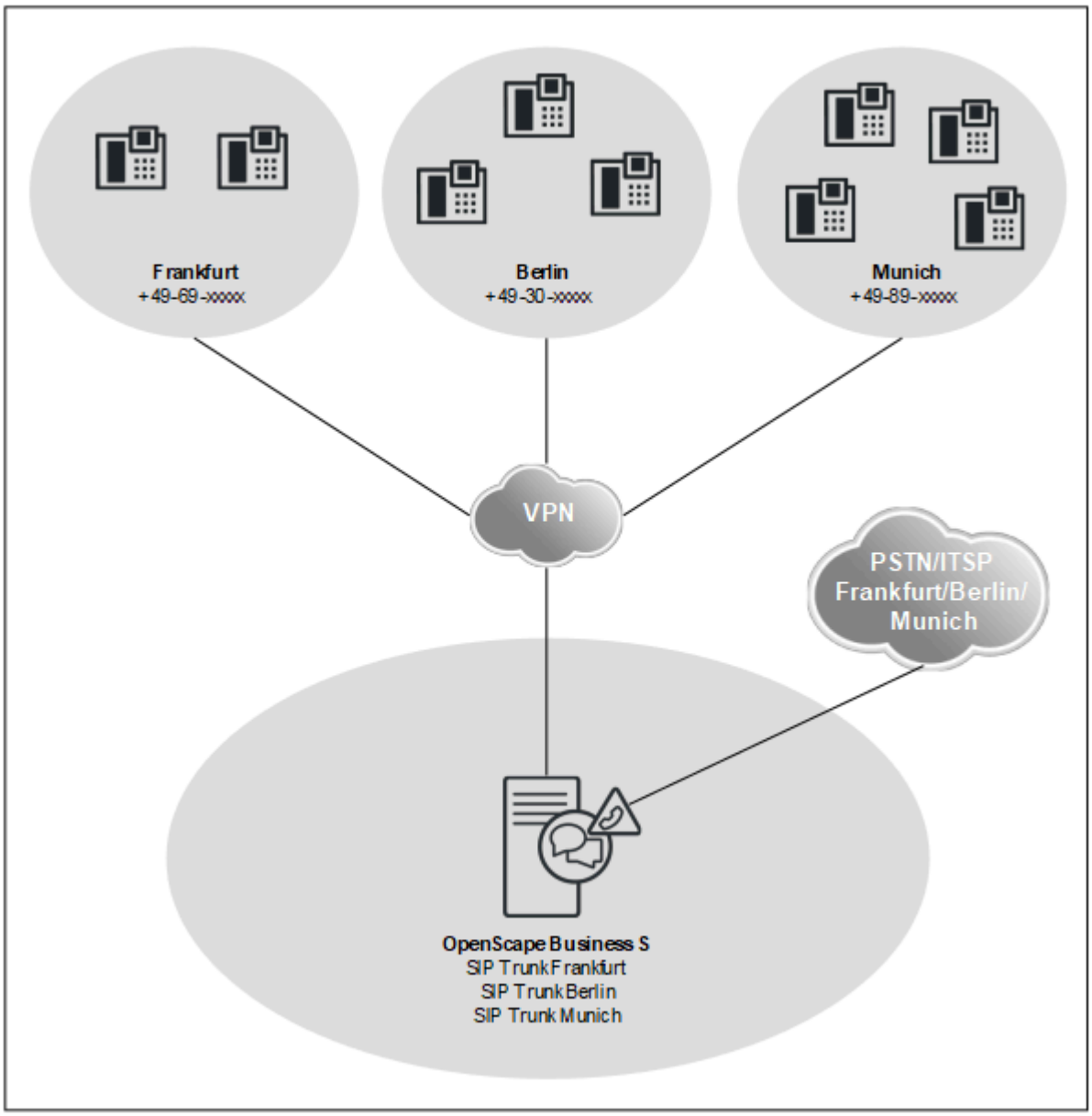


- Un cliente all'interno di una rete VPN o MPLS.
- Un OpenScape Business S per località.
- Le località possono essere distribuite all'interno di un paese o in più paesi.
- Fino a 1000 utenti e 180 linee SIP per OpenScape Business S.

- Collegamento in rete opzionale di OpenScape Business, fino a un totale di 1500 utenti. Sono possibili configurazioni di maggiori dimensioni nell'ambito di condivisioni specifiche di un progetto.

Scenario b: hosting con OpenScape Business S per più località

Dati di rete



- Un cliente all'interno di una rete VPN o MPLS.
- Un OpenScape Business S per tutte le località.
- Località solo all'interno di un paese.
- Fino a 8 località con diversi prefissi nazionali.
- Fino a 8 provider SIP per OpenScape Business S.
- Un provider SIP per località.
- Fino a 1000 utenti e 180 linee SIP.
- Collegamento in rete opzionale di OpenScape Business con più OpenScape Business S all'interno di una VPN (OS Biz S 1 nel paese 1, OS Biz S

2 nel paese 1500 ecc.), fino a un totale di 1500 utenti. Sono possibili configurazioni di maggiori dimensioni nell'ambito di condivisioni specifiche di un progetto.

- Per un esempio di configurazione, vedere il sito Unify Experts Wiki su Internet, in *Guida alla configurazione dell'ITSP*.

21.6.6 Connessione in rete di OpenScape Business X e OpenScape 4000

La connessione in rete di OpenScape Business X e OpenScape 4000 può avvenire in due configurazioni. La prima prevede l'indirizzamento diretto tra i nodi OpenScape Business (scenario 4a) mentre la seconda il routing di tutte le connessioni attraverso OpenScape 4000 (scenario 4b).

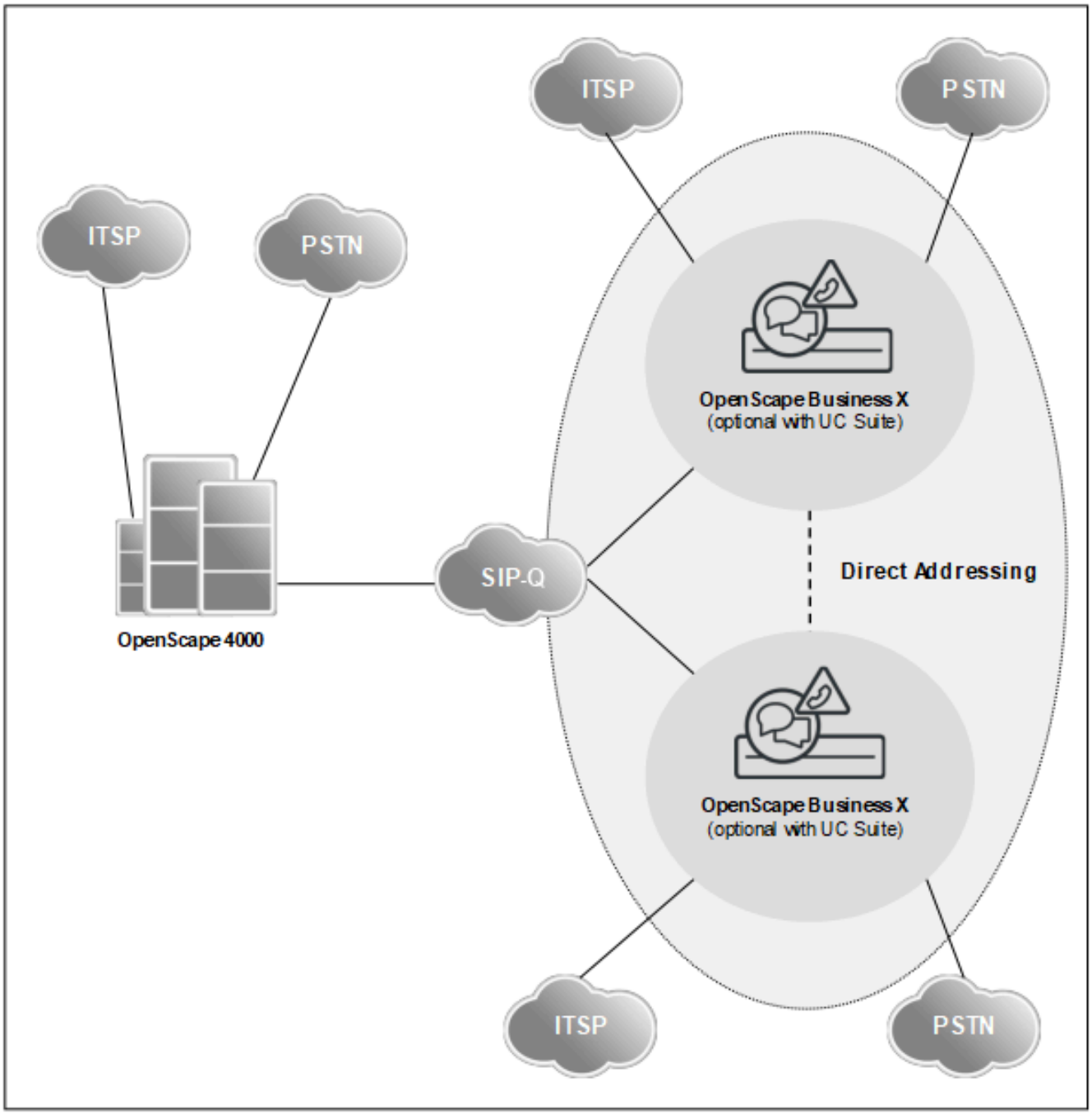
Nota: Un esempio di configurazione per la messa in rete di OpenScape Voice è disponibile in Unify Experts Wiki alla pagina `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`

Scenario a: Sistema di reti con OpenScape 4000 e indirizzamento diretto tra i nodi OpenScape Business X

Dati di rete

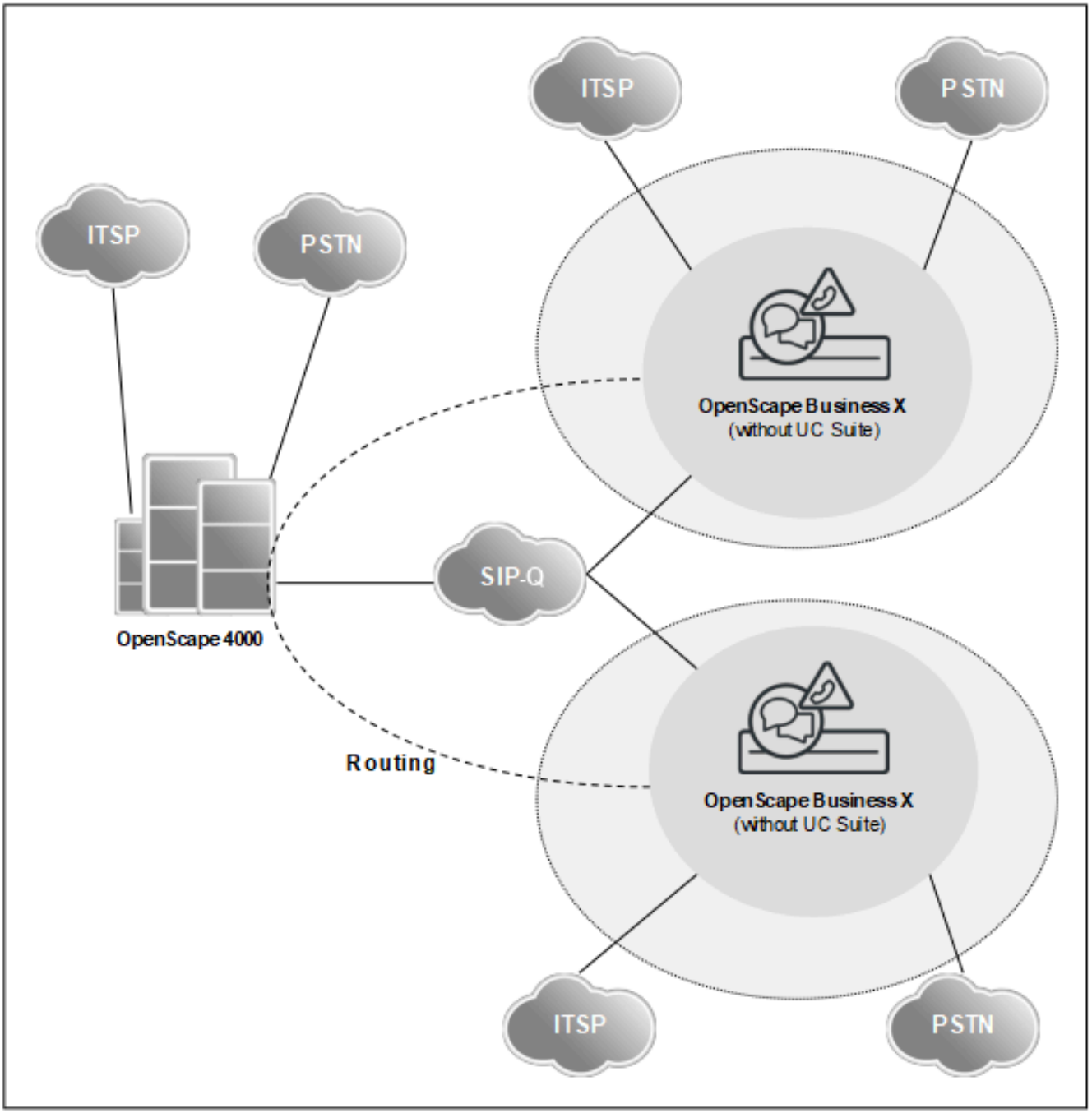
Scenario b: Sistema di reti con OpenScape 4000 e routing di tutte le connessioni attraverso OpenScape 4000

Dati di rete



- Numerazione chiusa in una connessione in rete di OpenScape Business
- Funzionalità vocali e UC a livello di rete, nell'ambito della connessione di rete di OpenScape Business

- Configurazione tramite procedura guidata Rete per la connessione in rete di OpenScape Business
- Configurazione del segmento di rete OpenScape 4000 in Modalità esperti
- Il concetto Small Remote Site (SRS) non è supportato
- Le funzionalità UC realizzate tramite l'UC Booster Server o la UC Booster Card sono opzionali.
- OpenScape Business S può essere integrato con le modalità gateway singolo o multiplo.



- Numerazione aperta
- Funzionalità voce a livello di rete

- Ogni conversazione in un altro nodo viene istradata tramite OpenScape 4000
- Soluzione UC non presente con OpenScape Business a causa dell'uso della numerazione aperta nel sistema di reti
- Il concetto Small Remote Site (SRS) non è supportato
- Per ogni nodo, la configurazione deve essere eseguita in Modalità esperti

Servizi di rete

Espansione	Numerazione chiusa in una connessione in rete di OpenScape Business (scenario 4a)	Numerazione aperta (scenario 4b)
Numero massimo di nodi	100 (32 rilasciati, a seconda del sistema OpenScape 4000)	
Numero massimo di utenti per sistema	Dipende dal modello di OpenScape Business X	
Numero massimo di utenti nella rete	1500 per il segmento di rete di OpenScape Business	Dipende da OpenScape 4000
Connessione di rete servizi voce	SIP-Q	

Connessione in rete UC	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
	Funzionalità a livello di rete all'interno di OpenScape Business	Non supportato
UC Booster Card	UC Smart: 51 - 150 utenti (0-50 utenti senza UC Booster Card) UC Suite: 0 - 150 utenti	Non supportato
UC Booster Server	UC Smart: da 150 utenti UC Suite: da 150 Utenti	Non supportato
OpenScape Business S	Supportato	Non supportato

Amministrazione	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
	WBM con procedure guidate per nodi OpenScape Business, OpenScape 4000 viene gestito tramite la Modalità esperti di OpenScape Business	Amministrazione di rete, Modalità esperti
WBM	WBM con procedure guidate	WBM con Modalità esperti
Manager E	Non consigliato	Non consigliato
Amministrazione UC Suite	WBM con procedure guidate per nodi OpenScape Business	Non supportato
Importazione di dati in blocco tramite file CSV (numeri di telefono, numeri DID, nomi)	Separatamente per ogni nodo del sistema di reti	

Concessione della licenza	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
Struttura di concessione delle licenze	È necessaria una licenza di rete per ogni OpenScape Business	

myPortal for Desktop / myPortal for Outlook (UC Suite)	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
	A livello di rete con funzionalità UC fornite da UC Booster Server, UC Booster Card e OpenScape Business S	Non supportato
Invio messaggi immediato	A livello di rete nell'ambito della connessione di rete di OpenScape Business	Non supportato
Casella vocale	Gli utenti utilizzano il proprio sistema casella vocale locale; non è disponibile una casella vocale centrale per l'intero sistema di reti.	Non supportato
Stato presenza	A livello di rete nell'ambito della connessione di rete di OpenScape Business	Non supportato
Segnalazione di occupato	A livello di rete nell'ambito della connessione di rete di OpenScape Business	Non supportato
Rubrica interna/Preferiti	A livello di rete nell'ambito della connessione di rete di OpenScape Business	Non supportato
Rubrica esterna	Locale tramite importazione di file CSV	Non supportato
Cerca nelle rubriche interne di altri nodi	Impossibile	Non supportato
Rubrica esterna non in linea (LDAP)	Tramite LDAP	Non supportato

myAttendant	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
	Con funzionalità UC fornite da UC Booster Server, UC Booster Card e OpenScape Business S	Non supportato
Invio messaggi immediato	A livello di rete nell'ambito della connessione di rete di OpenScape Business	Non supportato
Casella vocale	Gli utenti utilizzano il proprio sistema casella vocale locale; non è disponibile una casella vocale centrale per l'intero sistema di reti.	Non supportato

myAttendant	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
Stato presenza	A livello di rete nell'ambito della connessione di rete di OpenScape Business	Non supportato
Segnalazione di occupato	A livello di rete nell'ambito della connessione di rete di OpenScape Business	Non supportato
Rubrica interna/Preferiti	A livello di rete nell'ambito della connessione di rete di OpenScape Business	Non supportato
Rubrica esterna	Locale tramite importazione di file CSV	Non supportato
Cerca nelle rubriche interne di altri nodi	Impossibile	Non supportato
Rubrica esterna non in linea (LDAP)	Tramite LDAP	Non supportato

OpenScape Business Attendant	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
	Interfaccia limitata a numeri di telefono di 8 cifre	Interfaccia limitata a numeri di telefono di 8 cifre
Stato presenza	A livello di rete	
Segnalazione di occupato	A livello di rete	
Rubrica esterna	Tramite LDAP	Tramite LDAP
Console posto operatore centrale	A livello di rete nell'ambito della connessione di rete di OpenScape Business	

Company AutoAttendant (UC Suite)	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
Company AutoAttendant: dopo che AutoAttendant ha risposto a una chiamata, il chiamante deve comporre il numero di telefono con cui desidera essere connesso.	Gli script ccv permettono di comporre un numero dalla rubrica interna all'interno del sistema di reti.	Non supportato
Posto operatore automatico personale: dopo che il posto operatore automatico ha risposto a una chiamata, il chiamante deve comporre una singola cifra per connettere la chiamata alla propria destinazione.	È supportato qualsiasi numero preconfigurato da un utente UC	Non supportato

Company AutoAttendant (UC Smart)	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
Company AutoAttendant (UC Smart)	Locale	Locale

myAgent	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
	Con funzionalità UC fornite da UC Booster Server, UC Booster Card o OpenScape Business S. Tutti gli agenti sono registrati su UN nodo. Chiamate CC in arrivo tramite reti PSTN, ITSP e SIP-Q.	Non supportato
Invio messaggi immediato	In tutta la rete	Non supportato
Casella vocale (registrazione, indicazione messaggio in attesa, interrogazione)	Gli utenti utilizzano il proprio sistema casella vocale locale; non è disponibile una casella vocale centrale per l'intero sistema di reti.	Non supportato
Stato presenza	In tutta la rete	Non supportato
Segnalazione di occupato	In tutta la rete	Non supportato
Stato agente	Locale	Non supportato
Rubrica interna	In tutta la rete	Non supportato
Rubrica esterna	Locale tramite importazione di file CSV	Non supportato
Cerca nelle rubriche interne di altri nodi	Impossibile	Non supportato
Rubrica esterna non in linea (LDAP)	Tramite LDAP	Non supportato
Contatti Outlook	Locale	Non supportato
Trasferimento di una chiamata	Locale	Non supportato
Informazioni cliente	Locale	Non supportato
Reporting	Locale	Non supportato

Applicazioni esterne	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
Applicazione OpenScape Business TAPI	Vedere Application Connectivity	
Applicazioni CSTA esterne		
Application Launcher		
OpenScape Contact Center	Vedere Contact Center multimediale.	

Telefonia	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
Provider SIP (ITSP)	Locale	Locale
Provider PSTN	Locale; i nodi di rete senza provider PSTN vengono raggiunti mediante linee SIP-Q o il rispettivo gateway.	
Survivability (ridondanza in caso di guasto nel sistema di reti o in OpenScape Business S)	È supportato tra OpenScape Business X e OpenScape Business S	Non supportato

Telefonia	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
Composizione di un numero di rete pubblica nel proprio nodo	Supportato	
Composizione di un numero di rete pubblica in un nodo di rete	A livello di rete nell'ambito della connessione di rete di OpenScape Business	

Mobilità	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
Desk sharing	All'interno di un nodo; a livello di rete, in una connessione di rete OpenScape Business (con DLS)	Non supportato
Mobility con controllo DTMF del sistema:	Locale (non supportato da OpenScape Business S)	Locale
myPortal to go (Web Edition), UC Suite	Stato presenza e rubriche a livello di rete (ogni nodo richiede pertanto un UC Booster Server, una UC Booster Card, o OpenScape Business S)	Non supportato
myPortal to go (Web Edition), UC Smart	Locale, non per UC Booster Server, UC Booster Card e OpenScape Business S	Non supportato

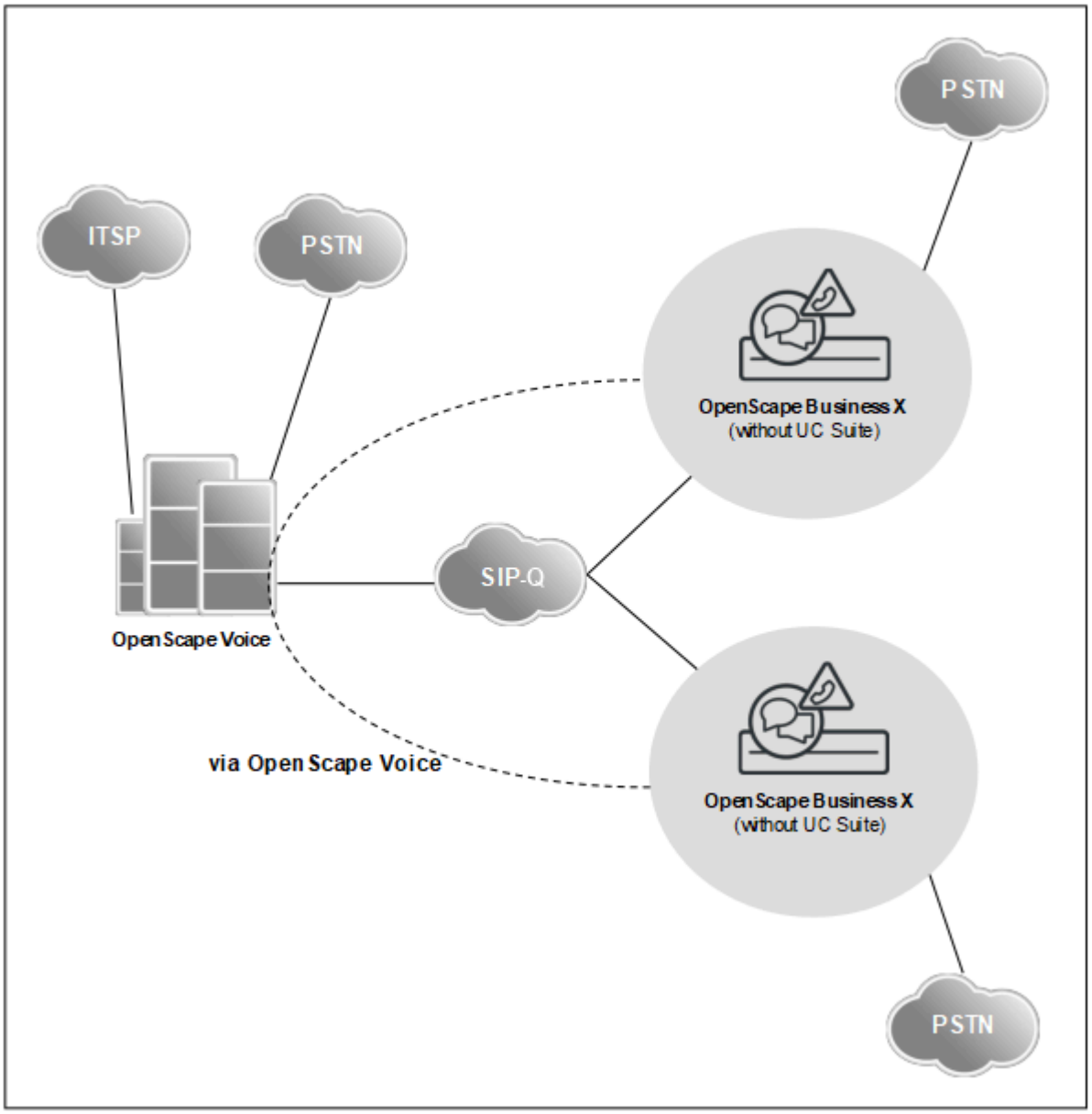
Altre funzionalità	Numerazione chiusa (scenario 4a)	Numerazione aperta (scenario 4b)
Crittografia segnalazione e payload (SPE)	Supportato in connessioni di rete OpenScape 4000/OpenScape Business. Non supportato per connessioni UC e conferenze	Supportato in connessioni di rete OpenScape 4000/ OpenScape Business. Supporto non disponibile per conferenze
Server DSS	A livello di rete nell'ambito della connessione di rete di OpenScape Business	Non supportato
Risposta per assente	Non supportato	Non supportato

21.6.7 Collegamento in rete di OpenScape Business X e OpenScape Voice

OpenScape Business X può essere collegato in rete tramite OpenScape Voice.

Nota: Un esempio di configurazione per la messa in rete di OpenScape Voice è disponibile in Unify Experts Wiki alla pagina `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`

Dati di rete



- OpenScape Business X stellt für OpenScape Voice eine netzweite Sprach- und Gateway-Funktionalität zur Verfügung
- Uno o più OpenScape Business X possono essere utilizzati come gateway per centralini digitali (ISDN, T1, CAS)
- Con i gateway di OpenScape Business X possono essere utilizzati i seguenti terminali: digitali, analogici, DECT e IP (HFA)
- In generale, le funzionalità UC sul lato OpenScape Business X non sono supportate con questa connessione in rete.
- Ogni conversazione da un nodo all'altro viene istradata tramite OpenScape Voice.
- La configurazione di ciascun nodo viene eseguita in Modalità esperti.
- Il piano di composizione di OpenScape Voice si basa su E.164, quindi non viene utilizzata alcuna numerazione aperta o chiusa.

Servizi di rete

Configurazione massima	
Numero massimo di nodi	dipende da OpenScape Voice
Numero massimo di utenti in un singolo sistema di comunicazione	a seconda del sistema OpenScape Business X
Numero massimo di utenti nella rete	dipende da OpenScape Voice

Amministrazione	
WBM	La procedura guidata Rete non può essere utilizzata. OpenScape Voice viene gestito a livello di nodo nella Modalità esperti di OpenScape Business.
Manager E	Non consigliato
Amministrazione UC	UC non è rilevante in relazione a OpenScape Voice
Importazione di dati in blocco tramite file CSV (numeri, numeri interni, nomi)	Separatamente per ogni nodo nel sistema di reti OpenScape Business

Concessione della licenza	
Struttura di concessione delle licenze	Ogni nodo singolarmente; a seconda del nodo OpenScape Business, è necessaria una licenza di rete

Limitazioni e note sulle funzionalità

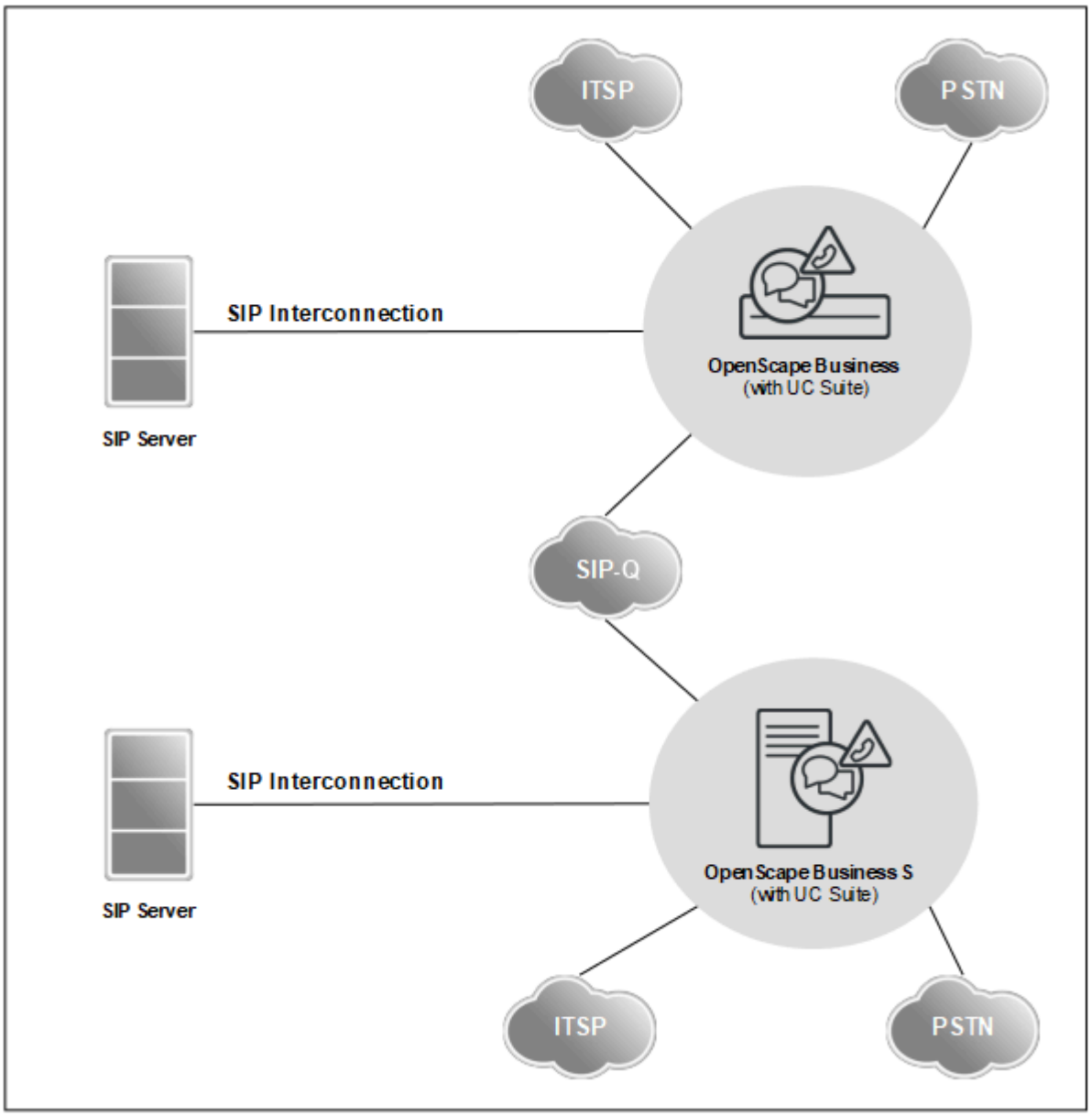
- La connessione di linee analogiche al gateway OpenScape Business è stata rilasciata **solo** per il Brasile (per il supporto per la funzione Line Reversal e liberazione a ritroso di linee urbane analogiche in Brasile).
- Reti di soli gateway OpenScape Business o con altri sistemi come OpenScape Voice non sono supportate. Le reti di gateway OpenScape Business con OpenScape Voice devono presentare una struttura a stella.
- La funzione Path Replacement (ottimizzazione delle rotte) tramite SIP-Q non viene supportata per i terminali connessi al gateway OpenScape Business.
- Per evitare una qualità voce scarsa nelle connessioni di transito linea, occorre utilizzare il codec voce G.711. Il codec G.729 è sconsigliato, poiché possono verificarsi connessioni sulle linee di transito in caso di servizi quali conferenza e deviazione di chiamata, in quanto non viene supportata la funzione Path Replacement (ottimizzazione delle rotte).
- Nessun supporto di servizi per tutto il sistema, come ad esempio Gruppi di risposta per assente, Chiamata di gruppo e Passo multiplo fra OpenScape Voice e il gateway OpenScape Business. I gruppi devono contenere solo apparecchi/utenti OpenScape Voice o OpenScape Business.
- Viene supportata la funzione crittografia (SPE) tra OpenScape Voice e i gateway OpenScape Business. La connessione tra OpenScape Voice e OpenScape Business deve essere eseguita tramite il protocollo di crittografia TLS. SRTP (SDES) non è supportato in una rete con OpenScape Voice V7R1.
- Vengono supportate soltanto reti con piano di numerazione E.164.
- Per i terminali IP collegati ai gateway di OpenScape Business (HFA) si applica quanto segue: per ogni connessione attiva OpenScape Business/ OpenScape Voice sono necessari due canali B per terminale HFA (1 canale

B per terminale TDM). Occorre verificare e prendere in considerazione la necessità di queste ulteriori risorse DSP.

21.6.8 Collegamento di porte esterne a OpenScape Business tramite interconnessione SIP

A OpenScape Business è possibile collegare dispositivi esterni tramite una interconnessione SIP, per utilizzare ad esempio applicazioni come OpenScape Alarm Server, OpenScape 4000, a OpenScape Voice o altri server SIP certificati.

Requisiti



- Possono essere collegate solo applicazioni certificate, ad esempio OScAR.
- Un server SIP esterno può essere collegato tramite il protocollo SIP o SIP-Q nativo.

- Sono disponibili al massimo due fasci SIP-Q (uno è necessario per la UC Suite, se presente) al massimo 10 fasci SIP nativi (fino a 8 fasci SIP nativi possono essere utilizzati per ITSP).

Per ulteriori informazioni, visitare il sito

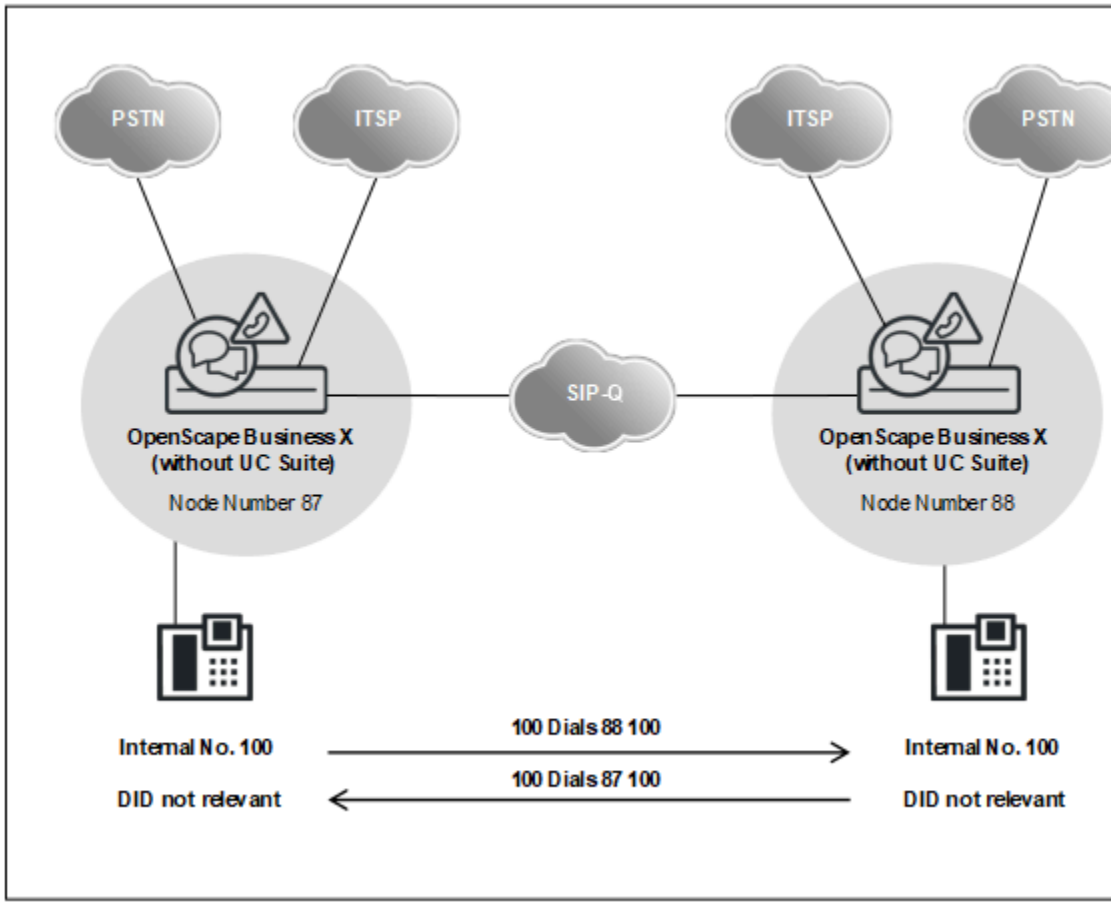
- Wiki-esperti per telefoni, sistemi di comunicazione e comunicazione unificata:

  `http://wiki.unify.com`

21.6.9 Numerazione aperta in OpenScape Business X - collegamento in rete

È possibile configurare un sistema di reti con numerazione aperta quando si collegano assieme due (o più) sistemi di comunicazione nei quali la numerazione si sovrappone (ovvero non è univoca nella rete).

Dati di rete



- Connessione voce a livello di rete tramite OpenScape Business.
- Le funzionalità UC non sono supportate.
- Ogni chiamata di un nodo viene eseguita con un numero di telefono interno.
- Ogni chiamata a un altro nodo viene eseguita con il numero del nodo (più il numero interno).

- Configurazione di ogni nodo tramite la Modalità esperti. La procedura guidata Rete è bloccata finché non viene configurato un numero di nodo per la numerazione aperta.
- Linea esterna PSTN o ITSP sono locali in ogni nodo.

Nota: In caso di estensione a livello di rete della funzionalità UC, è necessario passare da una numerazione aperta a una chiusa per adeguare i numeri interni. Pertanto, la numerazione aperta deve essere disabilitata, mentre il numero del nodo deve essere eliminato e successivamente aggiunto come prefisso (ad esempio, numero interno esteso 87100 anziché 100 e 88100 anziché 100).

Differenze:

- La selezione dei partecipanti del proprio nodo viene eseguita con il numero interno esteso.

- Il numero di interno e il numero DID possono essere diversi, se necessario, ma i numeri DID non devono essere modificati.

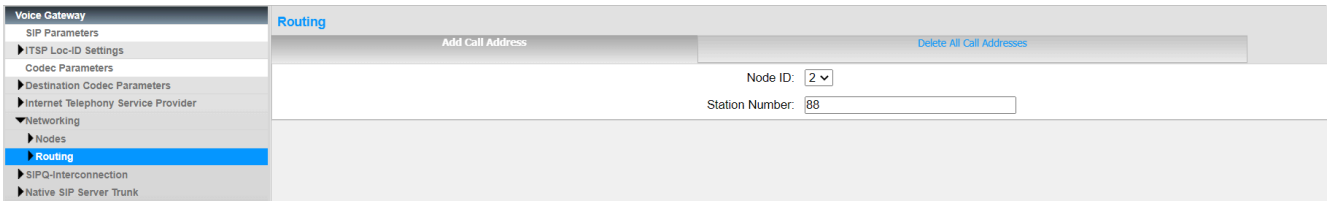
21.6.9.1 Come configurare la numerazione aperta

Configurazione della numerazione aperta

1) Consentire l'uso della **numerazione aperta** per il sistema di comunicazione tramite il flag di sistema Numerazione aperta
2) Inserire il numero del proprio nodo (nell'esempio "87")

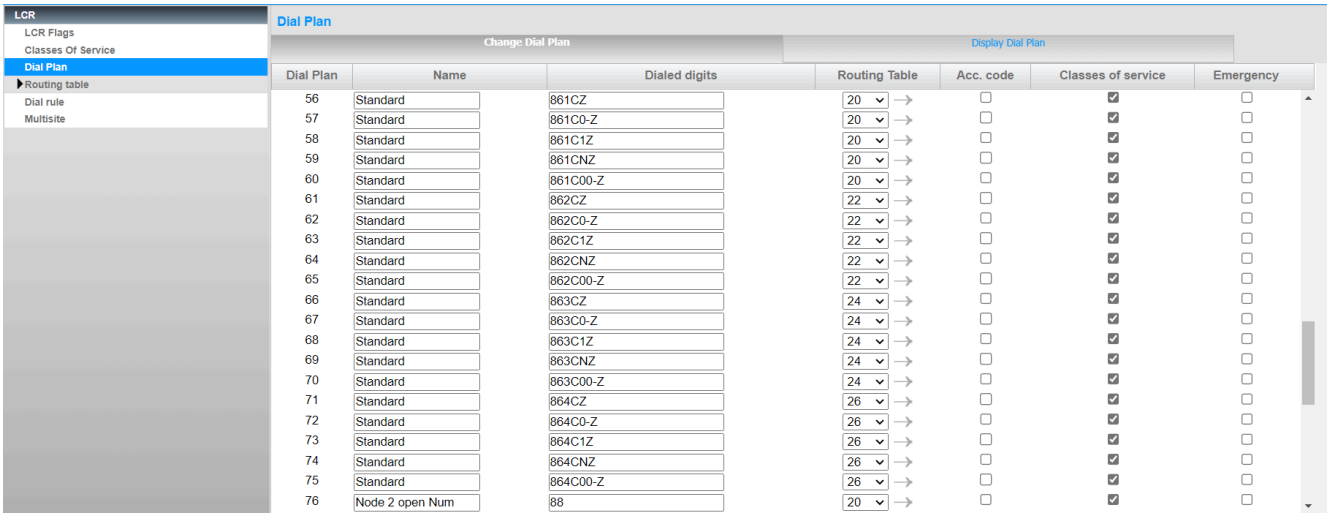
Configurazione del nodo (routing)

1) I nodi di destinazione vengono indirizzati tramite Gateway voce > Rete > Nodo > Routing (in questo esempio "88").
2) In una Numerazione aperta non è possibile usare la procedura guidata **Rete**: ciò viene impedito dal flag di sistema **Numerazione aperta**.

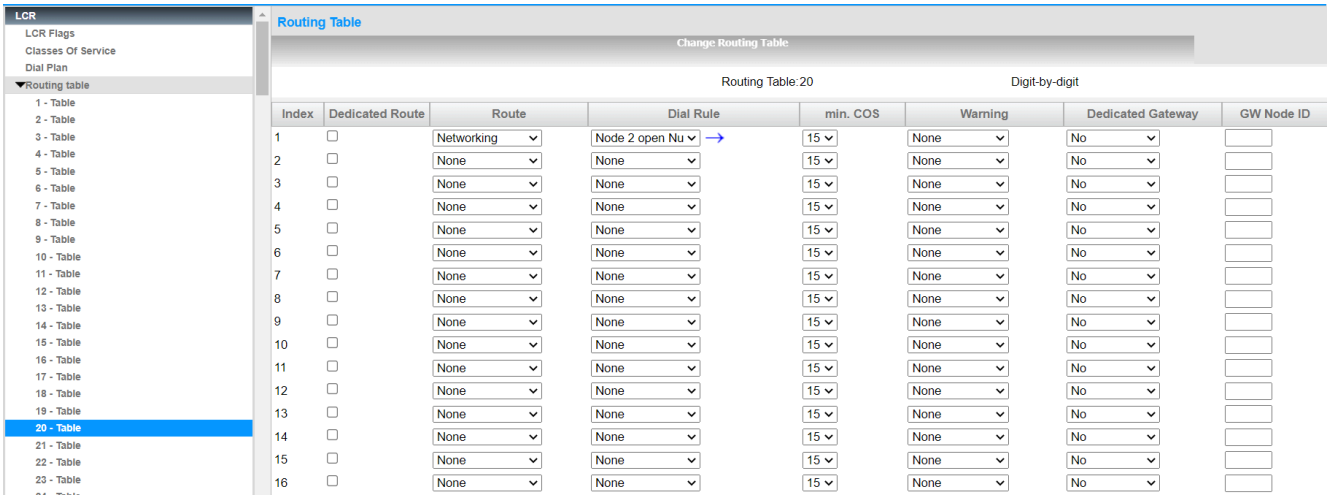


Configurazione LCR

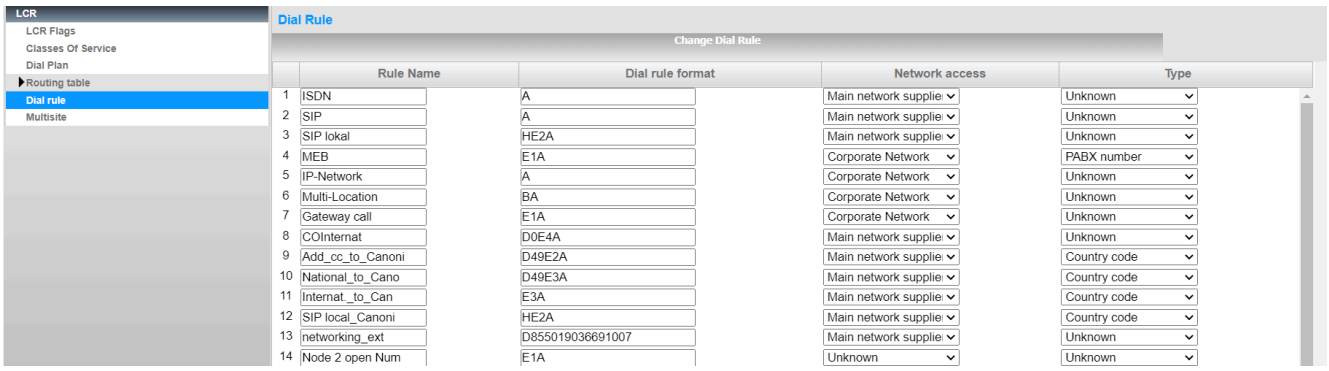
1) Definire la regola di composizione "Node 2 open Num" per il numero di nodo e la relativa tabella di routing.



2) Visualizzazione del percorso configurato



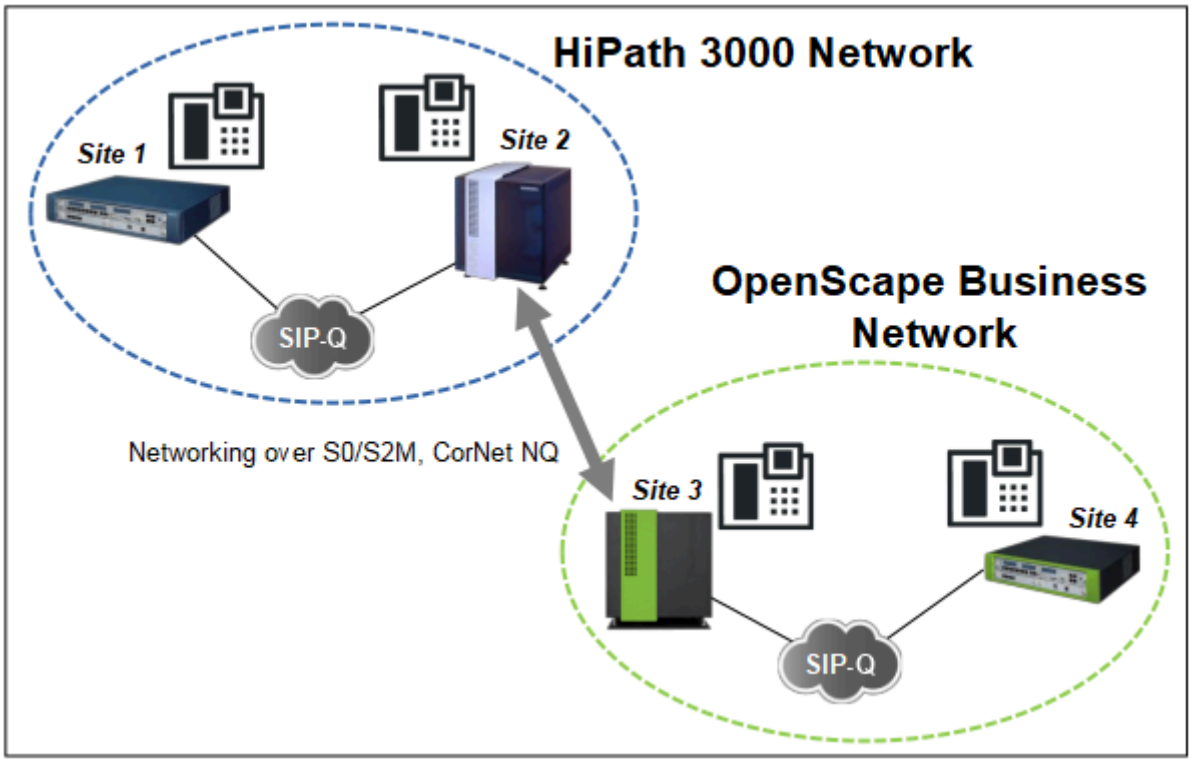
3) Inserire il nome del percorso "Rete" e la regola di composizione associata "Node 2 open Num".



21.6.10 Collegamento in rete tramite ISDN

I sistemi OpenScape Business possono essere collegati in rete tra loro e con il sistema di comunicazione HiPath 3000 e OpenScape 4000 tramite linee digitali. È possibile utilizzare per il collegamento sia linee S_0 che linee S_{2M}.

Connessione in rete con HiPath 3000



La rete HiPath 3000 esistente rimane (inizialmente) intatta. L'espansione della rete viene effettuata con OpenScape Business. I nodi HiPath 3000 possono essere gradualmente migrati nella rete OpenScape Business, se necessario.

Ogni chiamata all'interno della rete che attraversa HiPath 3000/OpenScape Business viene effettuata tramite i corrispondenti gateway TDM (S_0 o S_{2M} con protocollo CorNet NQ, eventualmente QSIG come protocollo indipendente dal costruttore).

Si applicano le seguenti condizioni:

- Attivazione delle licenze separata per HiPath 3000 / OpenScape Business
- Amministrazione separata di HiPath 3000 / OpenScape Business
- Suggerimento: numerazione chiusa nell'intera rete. La numerazione aperta può potenzialmente portare a comportamenti erratici con CLIP e con le voci del diario/liste di chiamanti.
- Suggerimento: utilizzare solo il codec G.711 per garantire una buona qualità della voce sull'intera rete.
- Il numero di canali B deve essere definito in base al volume di chiamate previsto.
- OpenScape Business richiede in ogni caso una licenza per il collegamento rete.

Collegamento di sistemi esterni tramite QSIG

Per il collegamento di sistemi esterni con il protocollo QSIG, occorre considerare quanto segue:

- Verifica della compatibilità delle varianti QSIG dei sistemi esterni coinvolti (QSIG V1 chiamato anche QSIG secondo lo standard ECMA e QSIG V2, chiamato anche QSIG secondo lo standard ISO)
- Confronto delle funzionalità dei sistemi interessati. Ciò può aiutare a determinare in che misura l'ambito previsto delle funzioni, ovvero la porzione comune di entrambi i set di caratteristiche, soddisfi le necessità del cliente.
- Quale ulteriore conferma della disponibilità delle funzioni previste, si consiglia l'esecuzione di un test di connessione sul campo. In particolare, occorre tenere in considerazione l'interazione con altri protocolli di rete e protocolli PBX.

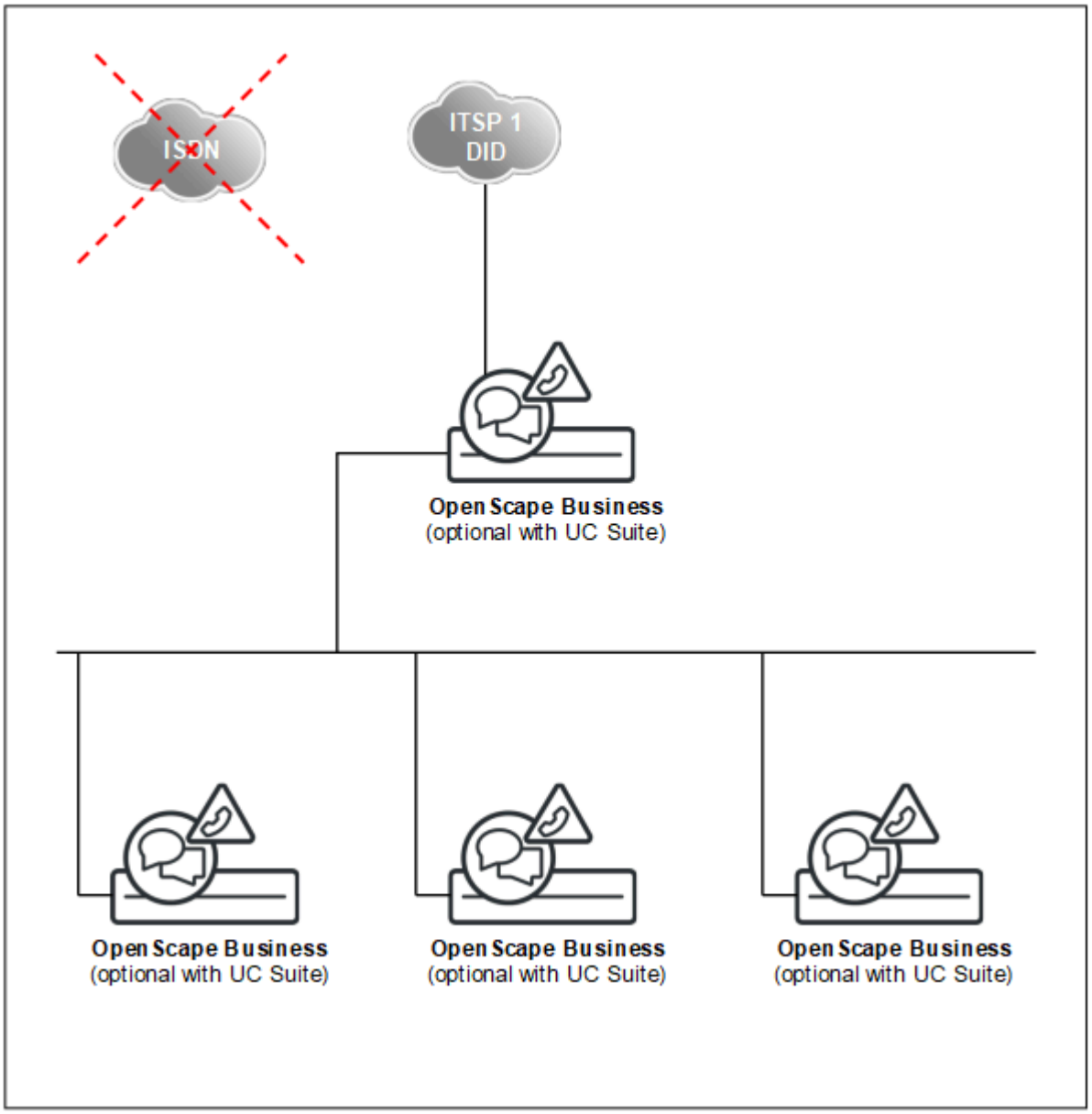
Nota:

Il fascio QSIG deve essere configurato come tipo di fascio PABX nel sistema OpenScape Business. Pertanto, le chiamate provenienti dalla rete QSIG saranno considerate come interne e seguiranno la CDL interna.

21.6.11 Sistema di reti OpenScape Business con attacco di linea urbana ITSP centralizzato

Un sistema di reti OpenScape Business puro può essere realizzato con un collegamento di linea urbana ITSP centrale con funzione di selezione passante, anziché tramite ISDN.

Collegamento in rete con collegamento di linea urbana ITSP centrale con funzione di selezione passante



Nella pianificazione della rete del cliente occorre considerare quanto segue:

- **Un** collegamento di linea urbana ITSP centrale con funzione di selezione passante per l'intera rete OpenScape Business.
- Registrazione a una sola rete locale, ciò significa the tutti i nodi della rete utilizzano uno specifico numero di linea urbana, ad esempio 0039 02 7007-xxxxx.
- I nodi collegati in rete possono in caso di emergenza, ovvero in caso di indisponibilità dell'accesso ITSP centrale, utilizzare i propri attacchi linea urbana per le connessioni in uscita. In determinate circostanze, in questo caso non è possibile una corretta identificazione del chiamante verso l'esterno. Le chiamate di emergenza in alcuni casi possono non raggiungere la destinazione corretta. La raggiungibilità delle destinazioni in uscita tramite queste linee locali è legata a limitazioni. Per i motivi indicati, è sconsigliato l'uso di collegamenti locali, tuttavia tecnicamente non sono impediti.

- Per lo stesso motivo, presso il nodo centrale non è consigliabile realizzare collegamenti ISDN aggiuntivi, ma non sono tecnicamente impediti.
- Tutte le regole per l'analisi dei numeri da comporre e per l'istradamento delle chiamate si applicano ai sistemi indipendenti e alle reti OpenScape Business. In questo caso, l'assegnazione dei numeri di telefono linea urbana dell'ITSP viene eseguita mediante configurazione della selezione passante dell'utente (non tramite la tabella della mappatura, vedere la Configurazione dell'ITSP al capitolo 9.2 e il sito Unify Experts Wiki su Internet).

21.7 Posto di rinvio centrale nel sistema di reti (non per USA)

Il sistema OpenScape Business consente di deviare ad un determinato posto di rinvio della rete tutte le chiamate in entrata non assegnate ad alcun utente o che non hanno ottenuto risposta, in modo che nessuna chiamata vada persa.

Quando il posto di rinvio centrale nel sistema di reti è configurato tramite ISDN, il funzionamento è identico a quello senza collegamento in rete.

In presenza di una linea ITSP sussistono delle limitazioni per il posto di rinvio centrale, poiché ogni nodo di regola ha un proprio ITSP:

- I criteri di rinvio ITSP valgono solo per il nodo associato.
- Funzionano Rinvio su libero, su occupato, con selezione incompleta, con selezione errata e con richiamata senza risposta.
- I tipi di rinvio "Selezione errata" e "Incompleto" non funzionano con ITSP.
- I numeri di telefono incompleti o errati vengono restituiti come segnale di occupato all'ITSP.

Quando in un sistema di reti si deve utilizzare un posto di rinvio centrale, è necessario configurare degli utenti virtuali in ciascun nodo. Tali utenti virtuali vengono deviati in modo permanente tramite il sistema di reti agli utenti myAttendant.

Esempio per linea ITSP: il numero del sistema ITSP è 0211-23456789 + numero di selezione passante ITSP; come numero centrale del sistema di comunicazione viene reso pubblico il numero di telefono 0211-23456789-0.

- L'utente 100 è myAttendant con proprio numero di selezione passante ITSP 100 e un utente virtuale 199 con numero di selezione passante ITSP "0".
- Nell'elenco di mappatura ITSP di ciascun nodo, il numero di selezione passante ITSP "0" viene assegnato al proprio utente virtuale.
- Nel campo **Chiamate in entrata/Inoltro di chiamata** gli utenti virtuali vengono assegnati all'utente 100.

  Prima destinazione: propri utenti virtuali

  Seconda destinazione: utente 100 nel nodo di destinazione

  Durata della chiamata 5 secondi

Per migliorare l'identificazione delle chiamate, è consigliabile aggiungere agli utenti virtuali di tutti i nodi nell'applicazione myAttendant (alla voce **Configurazione**/**myAttendant**/**DID**) il relativo numero di telefono (DID) e un nome (ad es. società). Ciò consente una esauriente identificazione del chiamante nella finestra **Chiamate attive** di myAttendant.

21.7.1 Come configurare il posto di rinvio centrale nel sistema di reti MultiGateway

Esempio di configurazione per un posto di rinvio centrale nel sistema di reti MultiGateway tramite gateway OpenScape Business a monte. Tutte le chiamate in entrata in un nodo che soddisfano i criteri di rinvio devono essere instradate a OpenScape Business S, dove risiede l'AutoAttendant centrale.

Prerequisiti

OpenScape Business S è il master (tutti gli utenti HFA e SIP sono connessi qui).

Molteplici OpenScape Business X sono configurati come nodo slave (con PSTN o ITSP come linea esterna). I nodi possono trovarsi nello stesso luogo oppure in località diverse (prefisso diverso).

Passo a passo

1) Configurazione un utente virtuale su OpenScape Business.
   a) Configurazione un utente virtuale denominato "Rinvio 22 System2"

2) Configurazione di un posto di rinvio centrale con criteri di rinvio su OpenScape Business.
   a) **Modalità esperti**
   b) **Impostazione di base** > **Sistema** > **Rinvio/PO/Hotline**
   c) Selezionare l'utente virtuale 22 nel campo **Posto di rinvio** in caso di servizio **giorno e notte**.
   d) Inserire i seguenti parametri per l'utente 22 in **Posto di rinvio** per **Rinvio**:

Nome	Rinvio 22 Sistema2
Selezione passante	xxxxxxx22
Tipo di terminale	virtuale

   e) Attivazione dei parametri specificati nel campo **Posto di rinvio** in caso di **Rinvio**.
   f) Configurazione dell'utente virtuale nel campo **Posto di rinvio** in caso di **Chiave elettronica**.

3) Configurazione dell'inoltro chiama su OpenScape Business.
   a) Configurazione dell'inoltro di chiamata dell'utente virtuale 22 tramite il sistema di reti a OpenScape Business S.
   b) **Modalità esperti**
   c) **Chiamate in entrata** > **Inoltro di chiamata**
   d) Selezione dell'utente virtuale 22
   e) Passare a **Modifica inoltro chiamate**
   f) dopo: **Destinazione esterna** (specificare i numeri di telefono delle code d'attesa AutoAttendant, ad es. 7410)
   g) **Direzione** = selezionare la rete (il numero di telefono delle code d'attesa AutoAttendant 7410 deve essere instradato selettivamente nell'LCR aggirando la regola predefinita -Z 33).

4) Configurazione del routing per OpenScape Business.

Il numero di telefono code d'attesa AutoAttendant 7410 deve essere instradato selettivamente nell'LCR aggirando la regola predefinita -Z 33.

Nel campo **Piano di composizione**:	Configurare il **Nome** (VSL Queue Pilot)
	Immettere il numero di telefono nel campo **Cifre selezionate** (7410)
	Selezionare la **Tabella delle rotte** (XX)
In **Tabella delle rotte** XX:	**Direzione** = selezionare la rete
	Assegnare la Regola di selezione
	In **Gateway dedicato** selezionare la voce **Forzato**
	Inserire l'ID nodo GWdi OpenScape Business S
Nel campo **Regola di selezione**:	Immettere il **Nome regola**
	Immettere il **Formato della regola di selezione** D7410 (Numero Queue Pilot)
	Metodo del gestore di rete: selezionare Corporate Network
	Tipo: Sconosciuto

5) Configurazione di una coda di attesa su OpenScape Business S.

a) Configurazione di una coda di attesa (Queue Pilot) con un CCV, ad es. **Componi interno**, **Componi per nome**, **Elabora digitazione**.

6) Configurazione di un inoltro di chiamata a OpenScape Business S.

a) Configurazione dell'inoltro di chiamata di Queue Pilot 7410 in OpenScape Business S.
b) **Modalità esperti**
c) **Chiamate in entrata** > **Inoltro di chiamata**
d) Selezione della Queue Pilot 7410
e) Passare a **Modifica inoltro chiamate**
f) prima: **Destinazione esterna** (specificare i numeri di telefono delle code d'attesa AutoAttendant, ad es. 7410)
g) dopo: selezionare la **Casella vocale**

21.8 Gestore presenze

Il gestore presence (Presence Manager) consente la segnalazione a livello di rete degli stati utente "Libero", "Occupato" e "Chiamata" con i LED dei telefoni HFA. Per questo è necessaria una numerazione chiusa e almeno un UC Booster Server sul nodo master del sistema di reti o un nodo OpenScape Business S come nodo master. È richiesta una licenza di rete per nodo.

Allo stato libero, il LED corrispondente è spento, allo stato occupato è acceso in modo continuo e durante una chiamata lampeggia. In stato di chiamata, la chiamata può essere risposta premendo il tasto corrispondente.

Gli stati dell'utente possono essere segnalati soltanto se il gestore presenze (Presence Manager) può inserire un punto Monitor CSTA su di esso.

I tasti vengono configurati dall'utente Per quanto riguarda la programmazione nel telefono stesso non vi è alcuna differenza se il numero in questione è interno o esterno.

Gestore presenze è un servizio non provvisto di interfaccia utente. Non è richiesta alcuna impostazione in quanto tutti i dati vengono automaticamente ottenuti mediante la sincronizzazione dei dati.

Gestore presenze non supporta i gruppi. Non vengono eseguite segnalazioni a LED e non è possibile rispondere per assente. I MULAP sono invece supportati da Gestore presenze

Gestore presenze non supporta attivamente alcun telefono SIP o S_0.

21.9 Stato sincronizzazione nel sistema di reti

Nel sistema di reti, lo stato della sincronizzazione nel portale Admin e lo stato di registrazione dei singoli nodi viene visualizzato mediante pulsanti colorati. La visualizzazione dello stato di sincronizzazione si applica ai nodi di rete del sistema di comunicazione ma non ad OpenScape 4000 e OpenScape Voice.

Visualizzazione dello stato di sincronizzazione

Visualizzazione	Colore	Significato per il master	Significato per lo slave
Stato sincronizzazione (visualizzazione nella pagina iniziale del portale Admin)	Rosso	-	L'indirizzo IP del nodo master è configurato ma non è stato possibile registrare il sistema slave. Ciclicamente, lo slave tenta di registrarsi presso il master.
	Giallo	-	Lo slave è registrato presso il master ma i numeri di telefono non sono coerenti a livello del sistema di reti. Ciò può verificarsi dopo un backup/ripristino o dopo la prima registrazione.
	Verde	Se il nodo è configurato come master, viene visualizzato con lo stato verde.	
Stato di registrazione dei singoli nodi (visualizzazione nella finestra di dialogo Rete > Visualizzazione dominio)	Rosso	Lo slave è configurato, tuttavia il sistema non è ancora stato registrato.	Lo slave è configurato, tuttavia il sistema non è ancora stato registrato.
	Verde	Il sistema è registrato.	Il sistema è registrato.
Alive (visualizzazione nella finestra Rete > Visualizzazione dominio)	Rosso	Vista dei nodi del sistema di reti: tutti i nodi mostrati in rosso non sono risultati raggiungibili. I motivi possono essere problemi di rete o del sistema di comunicazione.	
	Verde	Il nodo (esterno) è raggiungibile tramite la rete. Il proprio nodo è mostrato sempre in verde.	

21.9.1 Sincronizzazione manuale nel sistema di reti

Se una volta configurati, i numeri di telefono/nomi (numeri interni o di selezione passante) non vengono sincronizzati automaticamente negli altri sistemi di un sistema di reti, è possibile avviare una sincronizzazione manuale. La sincronizzazione manuale del sistema di reti funziona solo in connessioni di rete omogenei.

Master

Slave

L'operazione di sincronizzazione trasferisce solo le modifiche apportate alla configurazione.

Se l'indicazione di stato nel portale Admin è "rosso", usando il pulsante di sincronizzazione è possibile tentare di avviare manualmente la sincronizzazione dei dati sul master manuale a avvio.

Nel caso in cui dei sistemi già configurati nella rete non siano più in grado di effettuare chiamate reciproche, si deve ricercare la causa di tale anomalia. Se lo stato Alive di singoli nodi è "rosso", ciò è indice della presenza di problemi di rete o di altri motivi che non consentono di raggiungere il nodo in rete. In questi casi l'uso del pulsante di sincronizzazione non risolve il problema.

All'attivazione sul nodo master, il master richiederà ai nodi slave di aggiornare i numeri di telefono e i nomi del sistema.

All'attivazione su un nodo slave, i numeri di telefono e i nomi del sistema vengono aggiornati sul master. Contemporaneamente il nodo slave viene nuovamente registrato sul nodo master.

21.9.2 Come avviare manualmente la sincronizzazione

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

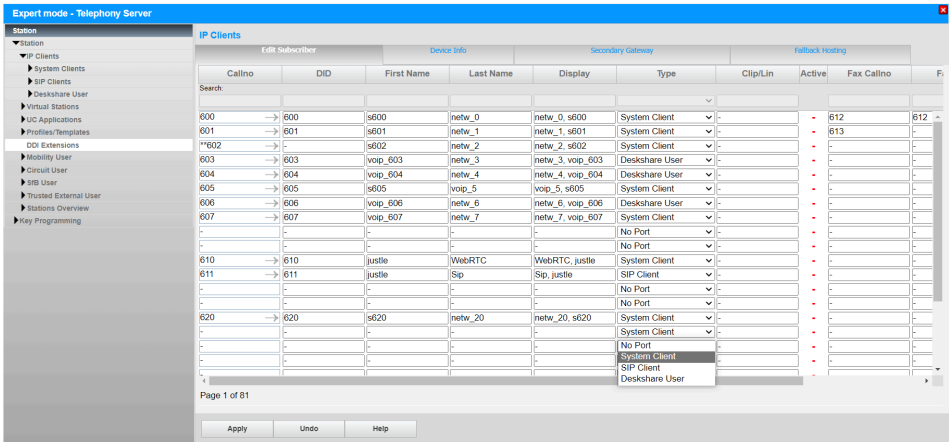
Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Riavvia / Ricarica**.
3) Premere il pulsante **Sync Network** (Sincronizza rete) per avviare manualmente la sincronizzazione.

21.10 Sopravvivenza

Sopravvivenza è una funzione all'interno di una rete di nodi OpenScape Business. Se un nodo OpenScape Business non funziona correttamente o non è raggiungibile a causa di errori di rete, i telefoni di sistema (HFA) connessi al nodo OpenScape Business possono accedere, invece, all'altro nodo OpenScape Business della rete. I numeri telefonici dei telefoni di sistema vengono conservati anche dopo il nuovo accesso. Ciò garantisce la continuità della telefonia di base; tuttavia, le funzioni di applicazioni quali

myPortal, segreteria telefonica e CTI saranno temporaneamente non disponibili.



Quando il nodo OpenScape Business che non funziona correttamente è nuovamente accessibile in modo sicuro, i telefoni di sistema passano automaticamente al nodo OpenScape Business.

Il tempo necessario per il passaggio al gateway di standby può arrivare a 30 minuti.

Se il nodo OpenScape Business non funziona correttamente, viene tentato di raggiungerlo per un periodo di tempo fisso (10 minuti, non modificabile). Solo quando questo tempo è scaduto i telefoni di sistema destinati a questo scopo vengono registrati presso il gateway di standby. Gli stati correnti dei telefoni registrati possono essere visualizzati in **Modalità esperto** > **Registri di diagnosi**.

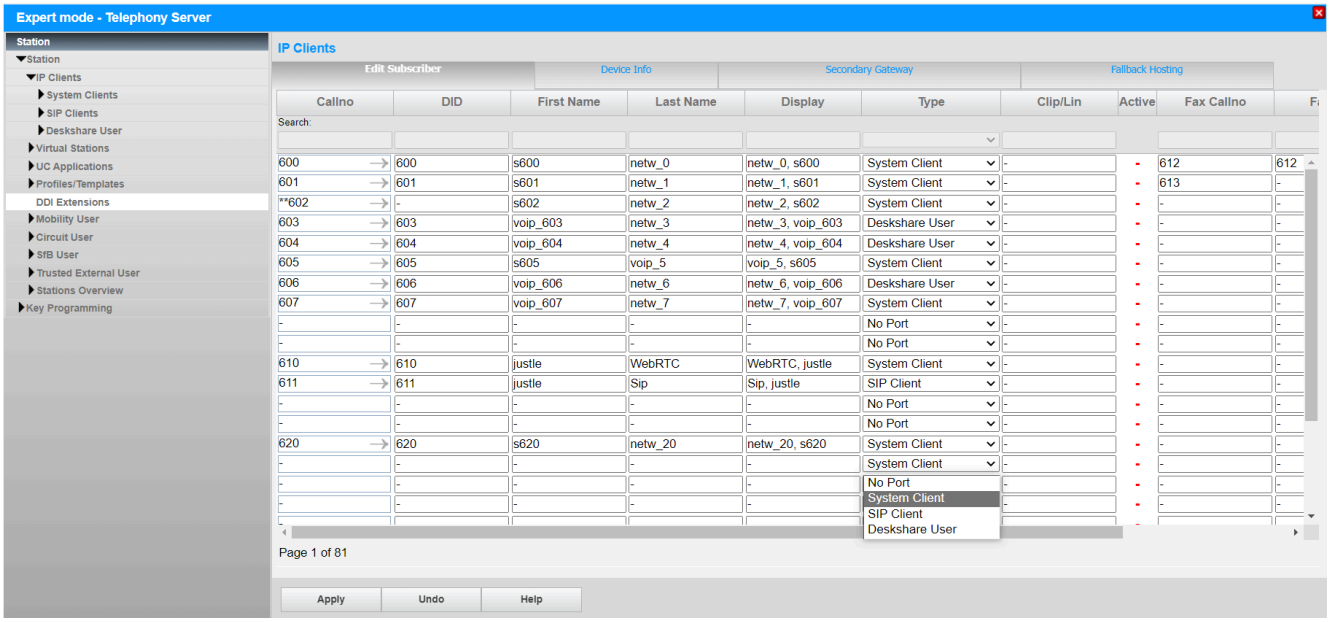
Le impostazioni di sopravvivenza sono configurate sui telefoni di sistema. Se il nodo OpenScape Business non funziona correttamente, i telefoni tenteranno inizialmente di raggiungerlo nuovamente diverse volte. È possibile configurare un timeout o la frequenza con cui il telefono tenta di accedere nuovamente tramite l'impostazione “Ridondanza del sistema” nel menu Amministrazione dei telefoni. L'impostazione predefinita per il timeout è di 30 secondi con un solo nuovo tentativo. Dopo questo periodo di tempo, i telefoni si registrano sul gateway di standby. La nuova registrazione automatica sul nodo OpenScape Business deve essere configurata anche sui telefoni del sistema.

Nota: La funzione di sopravvivenza richiede che il servizio POSTGRES funzioni correttamente. Se il firewall delle applicazioni è abilitato con una regola per il servizio POSTGRES, è necessario assicurarsi che gli indirizzi IP degli altri nodi OpenScape Business collegati in rete siano aggiunti manualmente a questa regola, altrimenti la funzione di sopravvivenza non funzionerà.

Per la sopravvivenza devono essere soddisfatti i seguenti prerequisiti:

- Sul gateway di standby deve essere disponibile un numero sufficiente di porte IP libere per i telefoni di sistema collegati al nodo OpenScape Business che devono essere “salvati” quando un nodo di rete smette di funzionare.

- Per queste porte libere sul gateway di standby, le stazioni devono essere configurate senza nome e numero di telefono.

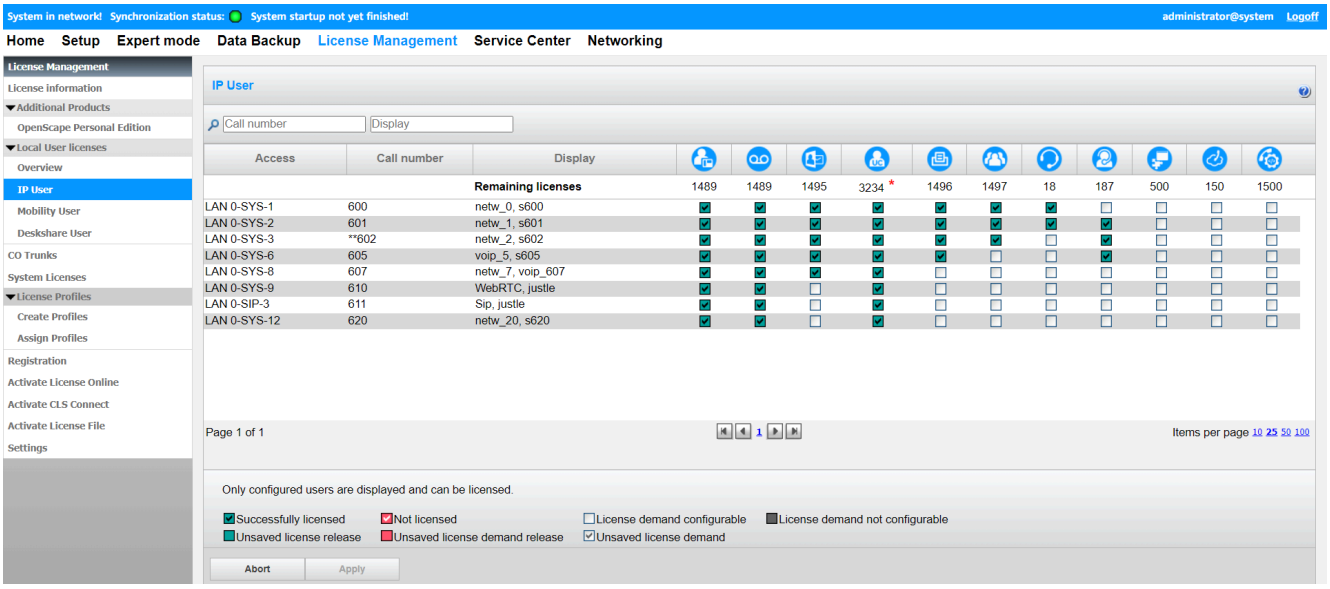


- Le stazioni devono essere configurate come telefoni di sistema (client di sistema) e disporre di una licenza utente Fallback. Se le licenze Fallback non sono disponibili nel file di licenza attivato, è possibile utilizzare le licenze utente IP. In caso di sopravvivenza, le stazioni possono utilizzare solo le funzioni di telefonia.

Nota: Durante il periodo di inattività dei client di ridondanza HFA del nodo master, i numeri di chiamata entrano in

conflitto fino a quando il nodo master non è nuovamente funzionante.

Nota: Se al sistema sono assegnate licenze utente Fallback, le licenze utente IP non possono essere utilizzate in caso di guasto.



21.10.1 Come configurare la funzione survivability

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura dei menu selezionare **Utente** > **Client IP**. In un sistema master OpenScape Business, viene visualizzata la finestra **Gateway secondario**.
3) In **ID nodo**, selezionare il sistema OpenScape Business utilizzabile dagli utenti di OpenScape Business S in caso di emergenza.
4) Selezionare la casella di controllo **Emergenza** per l'utente per emergenze.
5) Le voci per **Emergency Call no** e **Call no DID** sono disponibili e possono essere eventualmente modificate.
6) Fare clic su **Applica**, quindi su **OK**.

21.11 Eliminazione di un nodo dal sistema di reti

Se occorre eliminare un nodo dal sistema di reti, è prima necessario verificare che il nodo non sia più disponibile nella configurazione della rete. In caso contrario, il nodo cercherà autonomamente di registrarsi di nuovo nella rete e il nodo master proverà a sincronizzare i dati.

Come procedere

Per l'eliminazione dei nodi si utilizza la procedura guidata Rete, in cui vengono sempre eliminati tutti i nodi coinvolti.

- Interrompere tutti i percorsi (routing) che portano al nodo da eliminare.
- Amministrazione del sistema di reti
- Inserire "Nessuna rete" per il nodo slave interessato dalla procedura guidata Rete.
- Rimuovere il nodo slave dall'elenco di registrazione nella procedura guidata Rete del nodo master.

Se il nodo non viene eliminato correttamente, i dati di uno dei sistemi OpenScape Business vengono trasferiti all'altro, con il rischio di generare incoerenze nella rubrica interna: ad esempio, un utente potrebbe non apparire nella rubrica e quindi potrebbe non essere in grado di utilizzare ad esempio myPortal for Desktop.

22 Interfacciamenti

Gli interfacciamenti sono dispositivi esterni (ad esempio un risponditore o un apparecchio porta con apriporta), collegati alle interfacce del sistema di comunicazione.

22.1 Risponditore analogico

Un risponditore analogico può essere collegato all'interfaccia a/b per riprodurre annunci personalizzati (ad esempio per AutoAttendant centrale o in sostituzione della musica su attesa).

Nota: Prima di utilizzare annunci o musica su attesa di altre fonti, assicurarsi di non infrangere alcun copyright.

Per ogni sistema di comunicazione è possibile configurare fino a 16 fonti di annunci, ad esempio server multimediali, lettori di annunci o anche risponditori analogici.

Possono essere utilizzati i seguenti tipi di dispositivi di annuncio:

- Risponditori che all'attivazione partono sempre all'inizio del messaggio (ad esempio, annuncio di benvenuto)
- Risponditori a riproduzione continua (ad esempio, musica su attesa)

Un risponditore deve comportarsi come un utente, vale a dire deve connettersi, riprodurre l'annuncio e connettere la chiamata (passare in consultazione, comporre e disconnettere).

Varianti annuncio

Le varianti disponibili sono le seguenti:

- Annuncio di benvenuto (Annuncio prima dell'accesso)

  Per il chiamante può essere riprodotto un annuncio di saluto prima che la chiamata venga risposta.
- AutoAttendant

  Se AutoAttendant è abilitato, per un chiamante può venire riprodotta musica e/o altri annunci se il chiamante non può venire immediatamente connesso alla sua destinazione.
- Sel. passante DTMF

  Se la selezione passante DTMF è attiva, al chiamante viene comunicato mediante un annuncio che può usare DID per chiamare un altro interno. Durante l'annuncio, un ricevitore di codice è attivo e rileva e inoltra la postselezione del chiamate.

Alternative all'interfaccia a/b (moduli SLA)

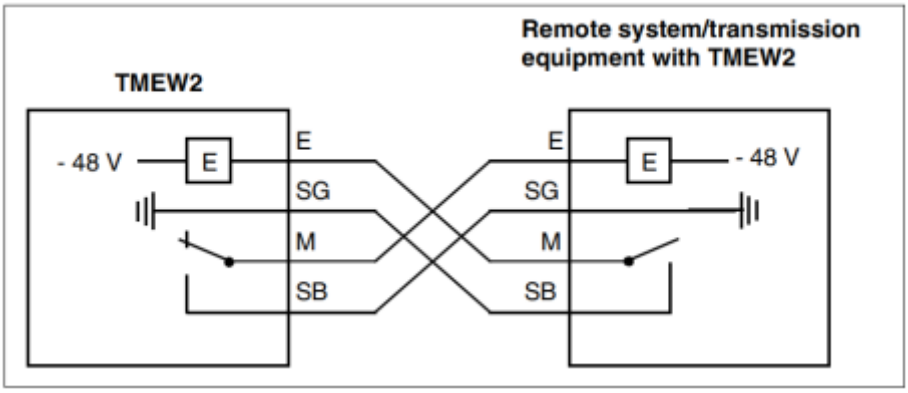
- OpenScape Business X8: modulo TMEW2
- OpenScape Business X5: modulo opzionale CTRL
- OpenScape Business X3: Modulo opzionale STRBR

Ritardo annuncio

Il tempo di ritardo annuncio indica dopo quanto tempo (configurabile da 0 a 600 s), una chiamata in attesa viene inoltrata a un risponditore.

Risponditore Genius

Per il collegamento del dispositivo risponditore Genius può essere configurato il modulo TMEW2 sul tipo di interfaccia 2. Per la descrizione del modulo TMEW2 e dell'assegnazione del connettore SIVAPAC sul backplane in fase di connessione del risponditore Genius, consultare la documentazione di manutenzione e montaggio dell'hardware al capitolo "Moduli".



Per la configurazione del risponditore Genius si utilizza Manager E selezionando **Visualizzazione sistema** > **Impostazioni** > **Interfacciamenti** > **Annuncio**.

22.1.1 Come aggiungere risponditori analogici

Prerequisiti

Il risponditore è collegato a un'interfaccia analogica.

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefoni / utenti**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Terminali analogici**. Viene visualizzato un elenco di tutti i terminali analogici.
4) Inserire il nome e il numero di telefono nella riga del risponditore.
5) Se necessario, apportare ulteriori modifiche nella riga del risponditore.
6) Fare clic su **OK & Avanti**, quindi su **Fine**.

22.1.2 Come modificare il ritardo annuncio

La configurazione viene eseguita con Manager E (vedere anche la Guida in linea di Manager E):

Passo a passo

Visualizzazione sistema, Menu **Impostazioni** > **Parametri sistema** > **Parametri di tempo**: nella tabella in corrispondenza della voce **Tempo di ritardo annuncio prima di risposta** impostare la **Base** e il **Fattore di moltiplicazione** del ritardo annuncio in base alle proprie necessità (predefinito: 100 ms x 20).

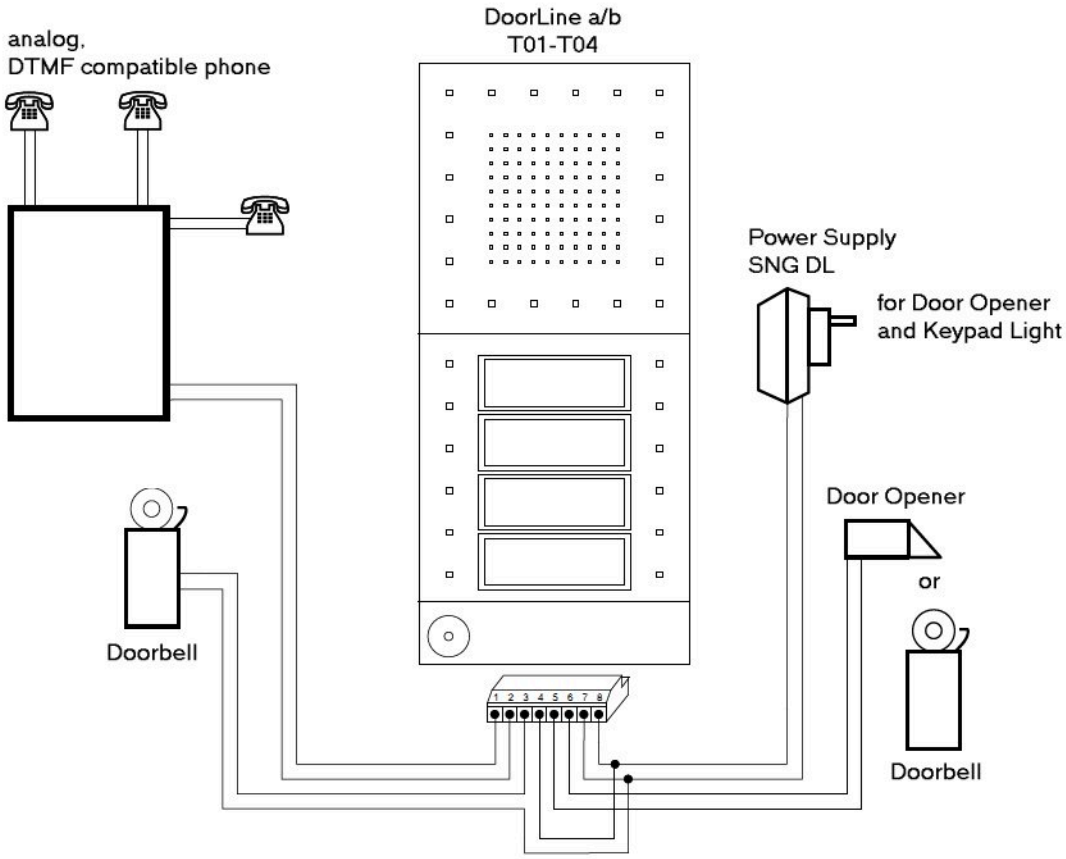
22.2 Apparecchio porta e apriporta

Gli apparecchi porta (TFE) sono oggi disponibili in un'ampia varietà di forme e di produttori diversi. Le opzioni di connessione sono essenziali per il corretto funzionamento e uso di ciascun dispositivo apriporta. Ad esempio, qui viene descritto il dispositivo Doorline a/b T01-T04 in cui l'apparecchio porta è simile alle marche Behnke, Keil, 2n EntryCom, Auerswald ecc.

22.2.1 DoorLine a/b T01-T04

L'apparecchio porta DoorLine T01-T04 a/b è collegata a un'interfaccia analogica. Con 1 - 4 tasti campanello (a seconda del modello), in grado di raggiungere più aree residenziali e commerciali indipendenti. Può essere utilizzato da qualsiasi telefono e fornisce inoltre la connessione di alimentazione elettrica per l'apparecchio apriporta.

Grazie alla tecnologia a/b a 2 conduttori, la DoorLine a/b T01-T04 può essere montata in modo rapido e semplice. Per la sincronizzazione con il sistema di comunicazione è possibile impostare il tipo di selezione e assicurarsi che i canali vocali utilizzati siano gli stessi. L'apertura della porta richiede l'immissione di un codice DoorLine (ad esempio #9). Non è più richiesto alcun modulo di connessione speciale, quale DoorLine M02, M03, M06 o M06/1.



Nota: Per la postazione apriporta non è necessaria alcuna ulteriore impostazione in OpenScape Business. Per motivi di sicurezza si consiglia di configurare l'interno come "nessun accesso alla linea" o "accesso alla linea limitato".

22.2.1.1 Come configurare la porta utente del Doorline a/b T01-T04

La configurazione viene eseguita con Manager E (vedere anche la Guida in linea di Manager E):

Passo a passo

1) **Visualizzazione sistema**, Menu **Impostazioni** > **Configurare il telefono** > **Utenti**: per la porta utente, selezionare il tipo **Standard**.
2) **Vista utenti**, scheda **Flag**: attivare il flag **Rifiuto dell'avviso di chiamata in attesa** per la porta utente.
3) **Visualizzazione sistema**, Menu **Impostazioni** > **Parametri sistema**, Scheda **Flag**: attivare il flag **DTMF automatica**.

22.2.1.2 Come configurare l'interno per Doorline a/b T01-T04

La configurazione viene eseguita con Manager E (vedere anche la Guida in linea di Manager E):

Passo a passo

1) **Vista utente**, scheda **Flag**: disattivare il flag **Rifiuto dell'avviso di chiamata in attesa** per l'interno.
2) **Vista utente**, scheda **Flag**: attivare il flag **Output della lista delle chiamate** per l'interno.

22.2.2 DoorCom Analog

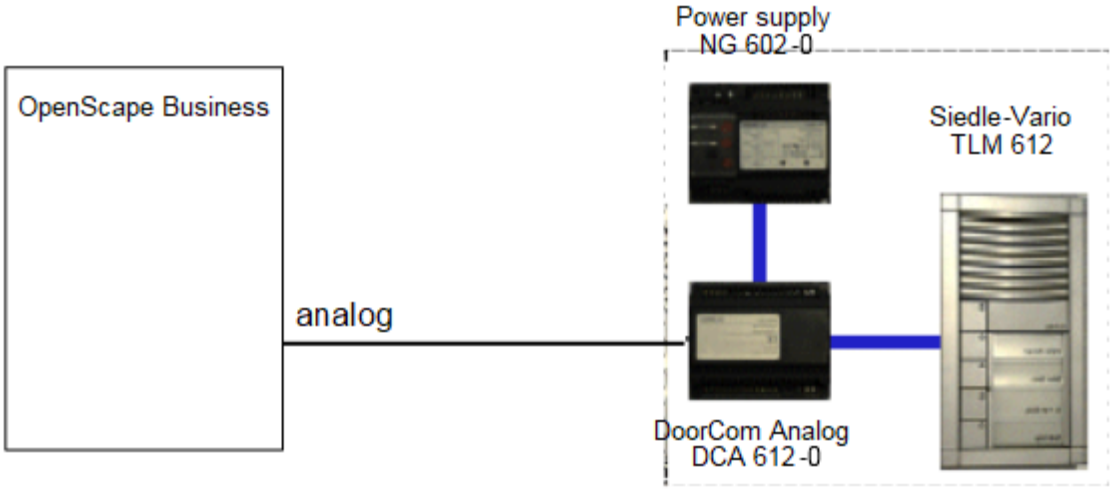
Il DoorCom® analogico è un box adattatore TFE universale per apparecchi porta e apriporta prodotti da Siedle (ad esempio, Vario TLM 612).

DoorCom® Analog è collegato a un'interfaccia analogica del sistema di comunicazione. Si comporta come un telefono analogico con selezione DTMF, rilevamento DTMF e controllo DTMF. Il controllo può essere effettuato soltanto con i segnali DTMF.

DoorCom Analog può funzionare soltanto in correlazione ai seguenti componenti:

- DoorCom Analog DCA 612-0
- Citofono Siedle-Vario TLM 612
- Interfaccia DCSF 600 di attivazione controllo remoto

  Per collegarsi con il citofono da un apparecchio interno. Senza questo modulo, il citofono non può effettuare richiamate (quando per esempio è stata rilasciata involontariamente una chiamata dal citofono).
- Alimentatore NG 602-0



Esiste la possibilità di programmare le funzioni di controllo dei dispositivi (apertura posta, selezione apparecchio porta ecc.) mediante i tasti procedura

di un telefono. La stringa DTMF memorizzata viene inviata alla postazione apparecchio porta/apriporta.

Nota: Per la postazione apriporta non è necessaria alcuna ulteriore impostazione in OpenScape Business. Per motivi di sicurezza si consiglia di configurare l'interno come "nessun accesso alla linea" o "accesso alla linea limitato".

22.2.2.1 Come configurare la porta utente di DoorCom Analog

La configurazione viene eseguita con Manager E (vedere anche la Guida in linea di Manager E):

Passo a passo

1) **Visualizzazione sistema**, Menu **Impostazioni** > **Configurare il telefono** > **Utenti**: per la porta utente, selezionare il tipo **Standard**.
2) **Vista utenti**, scheda **Flag**: attivare il flag **Rifiuto dell'avviso di chiamata in attesa** per la porta utente.
3) **Visualizzazione sistema**, Menu **Impostazioni** > **Parametri sistema**, Scheda **Flag**: attivare il flag **DTMF automatica**.

22.2.2.2 Come configurare l'interno per DoorCom Analog

La configurazione viene eseguita con Manager E (vedere anche la Guida in linea di Manager E):

Passo a passo

1) **Vista utente**, scheda **Flag**: disattivare il flag **Rifiuto dell'avviso di chiamata in attesa** per l'interno.
2) **Vista utente**, scheda **Flag**: attivare il flag **Output della lista delle chiamate** per l'interno.

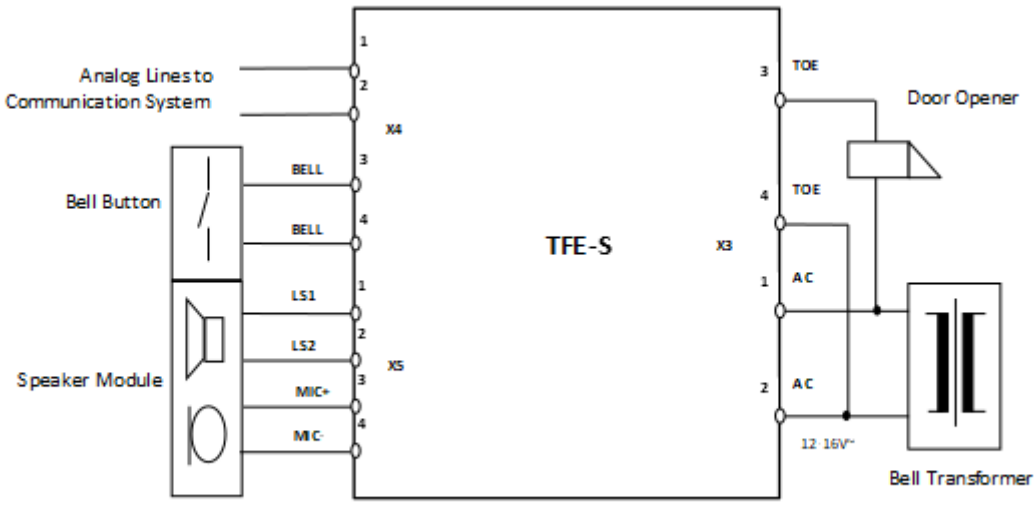
22.2.3 Citofono con amplificatore (TFE-S)

Il modulo TFE-S (S30122-K7696-T313) collega un'interfaccia analogica del sistema di comunicazione a un fascio per apparecchio porta, apriporta e tasto campanello. Il controllo viene eseguito tramite il sistema di comunicazione.

In questo modo è possibile una connessione all'apparecchio porta passivo, con caratteristiche paragonabili ai seguenti:

- Siedle (TLM511-01, 611-01)
- Rito (5760)
- Grothe (TS6216)

L'amplificazione può essere regolata manualmente. Il modulo TFE-S necessita di una propria alimentazione.



Dati tecnici

Parametri	Valore
Alimentazione	Trasformatore campanello 12V - 16 V CA, 50 Hz
Assorbimento di corrente	max. 150 mA
Interfaccia OpenScape Business	Utente analogico
Dimensioni	100 mm x 160 mm
Temperatura ambiente	0°C - +45°C

Descrizione della funzione

La pressione del tasto del campanello della porta viene segnalata come una chiamata sul telefono di un utente definito (postazione apriporta). Se l'utente accetta la chiamata, viene instaurata la connessione all'apparecchio porta. Successivamente, l'utente può attivare l'apriporta dal proprio telefono.

Se il telefono di destinazione della chiamata dalla porta non è raggiungibile, la chiamata viene rinviata. Se il posto di rinvio non è libero, ha luogo una ricerca di sistema su tutti i telefoni di sistema.

Suggerimento: Il servizio notte non viene interessato da questa segnalazione.

Suggerimento: La funzione di selezione breve non è utilizzabile con l'apparecchio porta.

Possibilità di configurazione

Sono disponibili le seguenti opzioni di configurazione:

- Apriporta:

  L'apriporta viene configurato tramite un'interfaccia a/b. All'apparecchio porta deve essere collegato un box adattatore. L'utente può quindi aprire la porta semplicemente premendo un tasto del telefono grazie al collegamento con l'apparecchio porta.
- DTMF:

  Qui viene definito se l'apriporta viene attivato con un invio in selezione multifrequenza DTMF, ovvero la postazione può aprire la porta tramite la selezione multifrequenza.
- Deviazione di chiamata (AUL):

  È possibile definire se la chiamata dall'apparecchio porta deve seguire la deviazione esterna impostata dall'utente di destinazione.

22.2.3.1 Come configurare l'apparecchio porta

La procedura guidata **Apparecchio porta** consente di definire quali utenti possono azionare l'apriporta. È possibile configurare fino a dieci apparecchi porta.

Prerequisiti

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Apparecchio porta**. Viene visualizzata la finestra **Modifica apparecchio porta**.
4) Selezionare uno o più **Apparecchi porta**.
5) Inserire la **Destinazione**.
6) Nella casella di controllo attivare le relative funzioni, come **Apriporta**, **DTMF** e **AUL**.
7) Fare clic su **OK & Avanti**, quindi su **Fine**.
8) Seguire i passaggi da 1 a 7 per configurare ciascun apparecchio porta.

22.2.4 Altoparlante

Gli altoparlanti possono essere collegati al sistema di comunicazione mediante amplificatori.

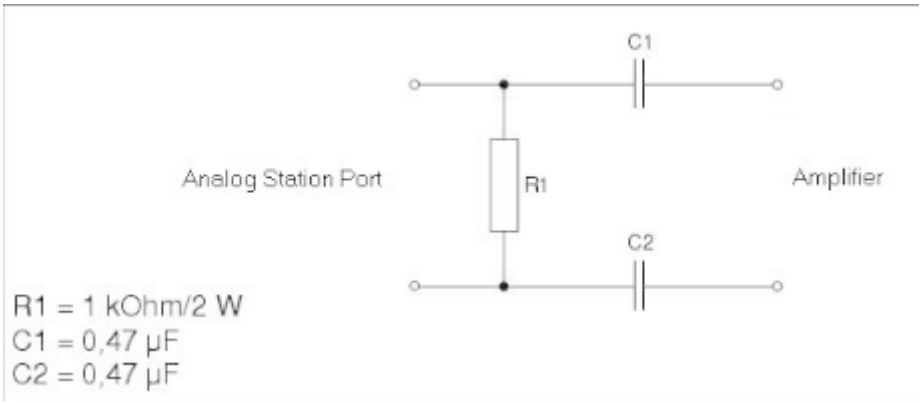
Per il collegamento di un amplificatore con altoparlante sono disponibili le seguenti opzioni:

- **Collegamento dell'amplificatore a un'interfaccia utente analogica**

  Può essere necessaria una modifica del livello di amplificazione.



  Può essere necessaria una resistenza di loop dopo la seguente connessione:



- **Collegamento dell'amplificatore al modulo TFE S**

  Tramite il modulo TFE S è possibile collegare un amplificatore/un impianto di amplificazione attivo. L'ingresso dell'amplificatore viene collegato all'uscita dell'altoparlante del modulo TFE S.

  Può essere necessario un altro contatto del modulo STRB per attivare l'amplificatore o il segnale di ingresso (soppressione del rumore).

22.2.4.1 Come configurare l'interfaccia utente analogica per un altoparlante

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Utente**.
3) Nella struttura dei menu fare clic su **Utente** > **Utente analogico**.
4) Selezionare l'utente analogico desiderato (ad esempio, 3011).
5) Nella scheda **Modifica i parametri dell'utente** modificare i dati degli utenti analogici in base alle esigenze.
6) Nell'elenco a discesa **Tipo di periferica**, selezionare la voce **Altoparlante**.
7) Fare clic su **Applica**.

22.2.4.2 Come configurare l'interfaccia utente analogica per collegare un amplificatore al modulo TFE S

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Apparecchio porta**. Viene visualizzata la finestra **Modifica apparecco porta**.
4) Selezionare un **Telefono**.
5) Selezionare la **Destinazione**.
6) Fare clic su **OK & Avanti**, quindi su **Fine**.

22.3 Relè

I relè sono uscite di comando e vengono attivati o disattivati mediante segnali di comando del sistema di comunicazione. Determinano un cambiamento di stato del dispositivo collegato e supportano funzioni di monitoraggio, allarme, controllo e regolazione. Sono principalmente utilizzati nei sistemi di gestione della sicurezza e di gestione degli edifici, in applicazioni con apparecchi apriporta.

I relè sono contenuti in moduli relè di comando opzionali. Tutti i moduli relè di comando comprendono 4 uscite di comando (relè).

Possibili moduli relè di controllo:

- REALS (OpenScape Business X8)
- STRB (OpenScape Business X3W/X5W)
- STRBR (OpenScape Business X3R/X5R)

Per una descrizione dettagliata dei moduli e delle relative assegnazioni, consultare la documentazione di manutenzione al capitolo "Moduli".

Per il controllo dei relè sono disponibili le seguenti opzioni:

- da telefono tramite codice
- da telefono di sistema tramite tasto
- a distanza, tramite la linea urbana (DISA) dagli utenti assegnati alla funzione relè
- Accesso remoto tramite l'opzione "Servizi associati"

I relè possono venire attivati o disattivati mediante le seguenti funzioni:

Nota: I codici per il controllo sono riportati nel capitolo "Modalità esperti".

- **Senza funzione**

  Il relè non è operativo o è impostato come suoneria centralizzata (in "Impostazioni" - "Chiamate in entrata" - "Elenchi destinazioni chiamata").

- **Manuale on e off**

  Il relè può essere attivato o disattivato mediante tasto o codice "attiva/disattiva interruttore selezionato". Questa funzione può essere assegnata a un utente, un gruppo o a tutti gli utenti.
- **Autom. a tempo off**

  Il relè può fungere da timer e può essere attivato o disattivato mediante tasto o codice "attiva/disattiva interruttore selezionato". Questa funzione può essere assegnata a un utente, un gruppo o a tutti gli utenti. Se come tempo di attivazione viene inserito un valore maggiore di 0, il relè viene disattivato solo una volta trascorso tale tempo.
- **Apriporta**

  Il relè può fungere da apriporta e può essere attivato o disattivato mediante tasto o codice "attiva/disattiva interruttore selezionato". Questa funzione può essere assegnata a un utente, un gruppo o a tutti gli utenti. Se come tempo di attivazione viene inserito un valore maggiore di 0, il relè viene disattivato solo una volta trascorso tale tempo. Su tutti i terminali dei telefoni associati viene visualizzato sul display il testo "Apriporta". Per esempio il fattore di moltiplicazione del tempo di commutazione: 30*100 ms = 3 sec.
- **Amplificatore altoparlante**

  Il relè viene attivato quando viene realizzata una connessione con apparecchio porta/postazione porta/ altoparlante. Si disattiva quando viene interrotta la connessione. Con questo relè può essere controllato un amplificatore per apparecchio porta in modo che venga attivato solo se necessario. Questa funzione deve essere assegnata all'apparecchio porta o alla porta altoparlante.
- **Segnalazione di occupato**

  Il relè viene attivato quando l'utente associato esce dallo stato di inattività (ricevitore sollevato o altoparlante abilitato o chiamata arrivata al terminale utente). Il relè viene disattivato quando l'utente associato torna allo stato di inattività. Il relè può essere attivato direttamente mediante il tasto o il codice "attiva/disattiva interruttore selezionato". In questo caso, lo stato dell'utente assegnato viene ignorato e il relè può essere di nuovo disattivato solo mediante tasto o codice. Questa funzione deve essere assegnata a un utente specifico. Esempio indicatore porta occupato: il direttore telefona, sulla porta si accende un indicatore che indica che il direttore non vuole essere disturbato.
- **Musica su attesa**

  Il relè viene attivato quando almeno un utente o una linea di sistema di comunicazione non è nello stato di inattività. In questo caso viene attivato un risponditore o un lettore CD. Il relè viene disattivato quando tutti gli utenti e le linee del sistemi di comunicazione sono nello stato di inattività. Questa funzione può essere assegnata solo a tutti gli utenti e deve essere usata solo una volta nel sistema di comunicazione. Come tempo di commutazione occorre indicare un valore maggiore di 0 (es. 600*100 ms = 60 sec). Il relè rimane attivo e riproduce la musica fino allo scadere del tempo di commutazione o finché non viene disattivato mediante un segnale di comando.
- **Seconda suoneria**

  Il relè viene attivato per l'utente associato, quando questo riceve una chiamata. Il relè viene disattivato quando la chiamata viene risposta o conclusa. Il relè non è sincronizzato. Questa funzione deve essere

assegnata a un utente specifico. Se come tempo di attivazione viene inserito un valore maggiore di 0, l'arresto può essere ritardato. Il tempo di attivazione è un multiplo di 3 secondi.

- **Scatto**

  Il relè viene sincronizzato sulla base del numero di utenti assegnati in funzione del numero di impulsi di addebito o messaggi di addebito. Questa funzione deve essere assegnata a un utente specifico. Il tempo di attivazione prevede impulsi di 150 ms e pause di 150 ms e non è modificabile.
- **Utente attivo**

  Il relè viene attivato quando l'utente associato è attivo (ricevitore sollevato o altoparlante abilitato). Il relè viene disattivato quando l'utente associato torna allo stato di inattività. Questa funzione deve essere assegnata a un utente specifico.

Nome relè

Ai relè può essere assegnato un nome a scelta (max 16 caratteri).

22.3.1 Come configurare un relè

Prerequisiti

Il modulo relè di controllo è inserito.

La configurazione viene eseguita con Manager E (vedere anche la Guida in linea di Manager E):

Passo a passo

1) **Visualizzazione sistema**, Menu **Impostazioni** > **Interfacciamenti** > **Relè**: in **Elenco relè** selezionare il relè da configurare.
2) **Visualizzazione sistema**, Menu **Impostazioni** > **Interfacciamenti** > **Relè**: in **Tipo relè** selezionare la funzione del relè.
3) **Visualizzazione sistema**, Menu **Impostazioni** > **Interfacciamenti** > **Relè**: nel campo **Nome relè** inserire un nome liberamente scelto per il relè (max. 16 caratteri).
4) Se la funzione deve essere assegnata a un utente, un gruppo o a tutti gli utenti, nell'area **Utenti assegnati**, nell'elenco **Numero di telefono**, selezionare il numero dell'utente o del numero di gruppo.

   Per tutti gli utenti occorre selezionare l'opzione **nessuno**.
5) Se la funzione richiede un tempo di commutazione, nell'area **Tempo di commutazione**, nel campo **Fattore** immettere il fattore che verrà moltiplicato per il valore visualizzato.

   I valori che possono essere visualizzati sono 100 ms e 3 s.

22.4 Sensori

I sensori sono ingressi di comando e riconoscono i cambiamenti di stato del dispositivo collegato. Possono attivare o disattivare le funzioni del sistema di comunicazione e quindi supportare le funzioni di monitoraggio, allarme,

controllo e regolazione. Sono principalmente utilizzati nei sistemi di gestione della sicurezza e di gestione degli edifici, in applicazioni quali monitoraggio della temperatura o rilevamento presenza.

I sensori sono contenuti in moduli relè di comando opzionali. Tutti i moduli relè di comando comprendono 4 ingressi di comando.

Possibili moduli relè di controllo:

- REALS (OpenScape Business X8)
- STRB (OpenScape Business X3W/X5W)
- STRBR (OpenScape Business X3R/X5R)

Per una descrizione dettagliata dei moduli e delle relative assegnazioni, consultare la documentazione di manutenzione al capitolo "Moduli".

I sensori possono attivare o disattivare le seguenti funzioni:

Nota: I codici per il controllo sono riportati nel capitolo "Modalità esperti".

- Segnalazione delle chiamate sui telefoni
- Messaggio a display nei telefoni di sistema
- Accensione/spegnimento di un risponditore
- Controllo di una segreteria telefonica
- Composizione automatica di un numero predefinito (numero interno, numero di gruppo o numero destinazione esterna)
- Attivazione dei seguenti servizi per un numero di telefono (con codice + numero di telefono):
  - Relè on/off
  - Non disturbare on/off
  - Deviazione di chiamata on/off
  - Chiave elettronica on/off
  - Inviare testi di risposta
  - Disattivare i testi di risposta
  - Servizio notte On/Off
  - Trasferta della chiamata On/Off
- Attivazione diretta dei seguenti servizi (solo con numero di telefono):
  - Relè on/off
  - Utilizzare la selezione breve
- Segnalazione di errore - è possibile quanto segue:
  - Output di un messaggio di errore programmabile (nome del sensore, max 10 caratteri: esempio all.temp) sul display di un telefono di sistema specifico (nessuna segnalazione acustica).
  - Visualizzazione della chiamata su un telefono di sistema specifico con messaggio di errore durante la chiamata (numero di destinazione)
  - Una voce nella cronologia degli errori (voce nella memoria degli errori = attivare)

Numero di telefono di destinazione

Per i sensori può essere programmata una porta analogica assegnata che viene chiamata dal sistema non appena viene ricevuto un segnale di instaurazione della chiamata. L'apparecchio chiamante evita il numero. Se alla

porta è connesso un risponditore, può essere trasmesso un annuncio atto ad informare l'utente chiamato sull'attivazione del sensore. Una porta analogica così programmata non può essere attivata dall'esterno. Se per il sensore è stato programmato un numero di telefono esterno, ma non per una porta analogica, la chiamata esterna viene instaurata senza che vengano trasmessi segnali in relazione all'attivazione del sensore. Sulla base del numero di telefono (CLIP), l'utente chiamato ha la possibilità di rilevare l'origine della chiamata.

Immissione dei dati di controllo

Immissione della stringa di controllo max. 24 caratteri per il sistema Phonemail (numero di casella postale). Non appena viene instaurata la chiamata, la stringa di controllo viene trasmessa alla porta dell'annuncio. Se essa non è disponibile,la stringa in questione viene trasmessa alla destinazione.

23 Application Connectivity

Application Connectivity supporta il sistema con ad esempio CSTA, TAPI e con l'Application Launcher.

23.1 CSTA

L'interfaccia CSTA permette il collegamento di applicazioni ad alte prestazioni quali CTI, Contact Center e comunicazione unificata ecc. a OpenScape Business.

Il CSTA utilizza il Transmission Control Protocol (TCP). Sussiste una connessione dedicata. La perdita di pacchetti di dati viene identificata e corretta automaticamente.

Standard

Il protocollo CSTA implementato si basa su:

- ECMA-269 Services for Computer Supported Telecommunications Applications (CSTA) Phase III
- ECMA-285ASN.1 for Computer Supported Telecommunications Applications (CSTA) Phase III
- Espansioni specifiche

Premessa

L'uso di CSTA richiede, per il sistema collegato alle applicazioni CSTA, UC Booster (Card oder Server) o OpenScape Business S. I dati di accesso per le applicazioni CSTA devono essere configurati nel sistema per attivare automaticamente l'interfaccia CSTA. Le applicazioni CSTA esterne devono utilizzare questi dati di accesso.

Caratteristiche

CSTA offre i seguenti servizi:

- Accesso via LAN Ethernet (TCP/IP)
- CSTA fase III, codifica ASN.1
- Supporto del protocollo XML CSTA per applicazioni certificate
- Ampia gamma di telefoni di sistema supportati
- Monitoraggio e controllo di tutte le risorse a livello di rete
- Multiplexing per punti di monitoraggio

Dispositivi supportati

Oltre ai telefoni supportati dal sistema, il layer CSTA supporta i seguenti dispositivi:

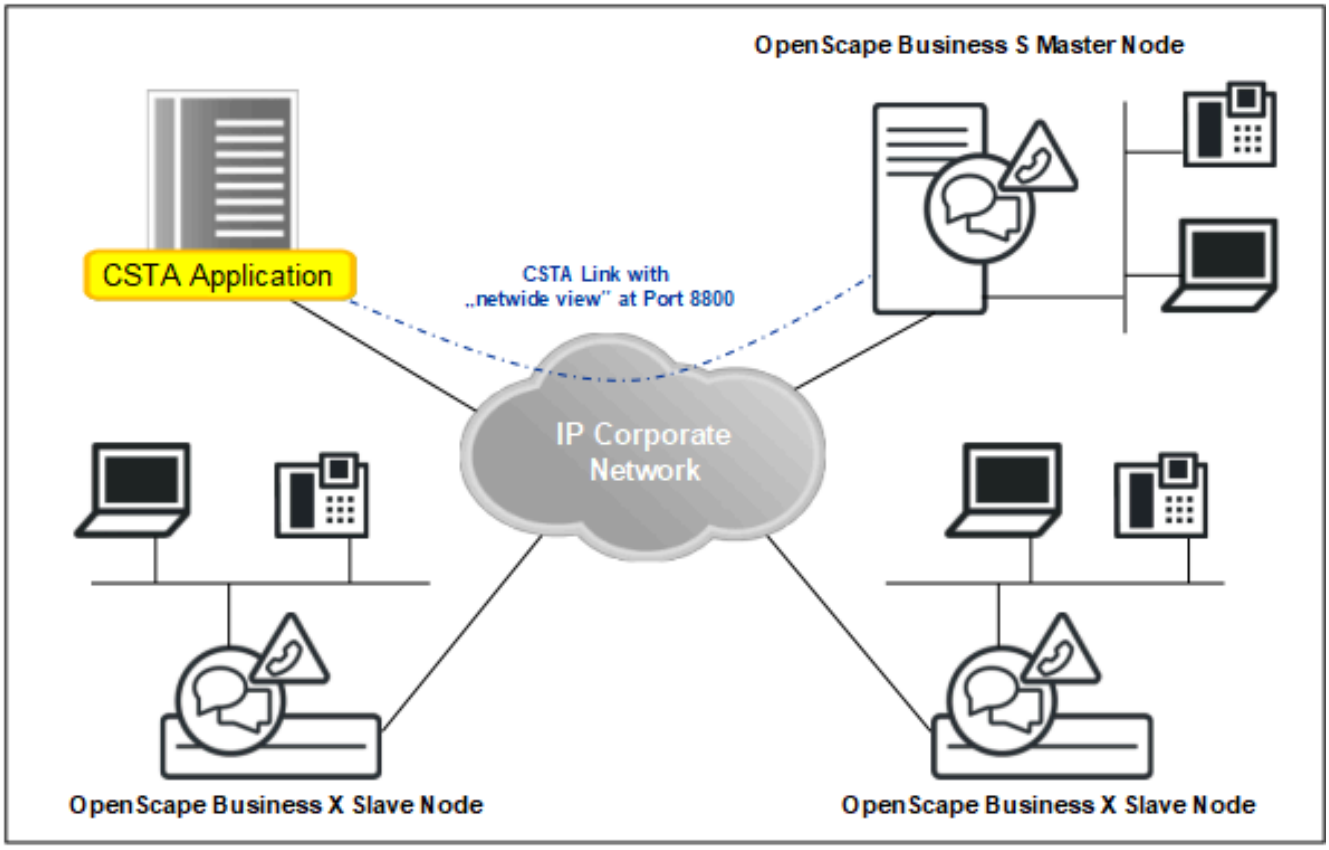
- ITSP

  Consente, ad esempio, l'uso di applicazioni del Call Center con linee esterne SIP
- ISDN
- Linea urbana analogica
- Utenti virtuali

- Gruppi UCD
- MULAP

Nota: Per maggiori dettagli sulle funzioni e sui dispositivi supportati, consultare il manuale dell'interfaccia CSTA.

Connessione per vista a livello di rete



Porte

Per impostazione predefinita, sono disponibili i seguenti numeri di porta:

Porta	Numero di porta	Uso
CSP	8800	Qualsiasi applicazione CSTA
CMD	8900	riservato per client TAPI 120, indipendentemente dal numero di client, viene utilizzato esattamente un collegamento logico CSTA

Per stabilire la connessione, le applicazioni CSTA esterne o provider di servizi TAPI 120 devono usare l'indirizzo IP del server UC o del sistema con i numeri di porta corrispondenti. Il corrispondente indirizzo IP viene visualizzato nel WBM, nell'area di selezione dell'applicazione.

Collegamenti CSTA

Per impostazione predefinita, è disponibile un collegamento CSTA della porta CSP per applicazioni CSTA esterne. Per impostazione predefinita, altri tre collegamenti CSTA sono assegnati ai seguenti servizi o applicazioni CSTA integrati:

- CMD (CSTA Message Dispatcher) per client TAPI 120 sulla porta CMD
- DSS (Direct Station Server)
- UC Suite

Se non sono richiesti questi servizi o applicazioni CSTA, i corrispondenti collegamenti CSTA possono all'occorrenza essere assegnati ad applicazioni CSTA esterne.

Nota: Un collegamento CSTA fornisce il servizio TDS solo ai dispositivi locali. I clienti devono disporre di un collegamento CSTA ad ogni nodo su cui è richiesta la fornitura di un servizio TDS.

In generale, le applicazioni CSTA possono essere collegate a un sistema OpenScape Business tramite CSP, LAS (un componente del sistema) o PCC (un componente LDH).

Nota: Se un'applicazione si connette tramite CSP, è necessario impostare anche le credenziali rispetto a CSP.

Più in particolare:

- UC Suite, OSCC, TAPI 170 e applicazioni di terze parti (esterne) collegate tramite CSP

  La connessione di applicazioni CSTA di terze parti (esterne) che richiedono informazioni sui trunk può essere effettuata solo in modalità UC Suite o interrogando i punti di monitoraggio dei trunk stessi tramite CSTA, nella propria applicazione.
- UC Smart è collegato tramite LAS

Plus prodotti

Nel sistema sono sempre attivati i seguenti flag:

- Il prefisso viene sempre trasmesso assieme al numero
- Gestione avanzata CSTA-CAUSE
- Segnalazione CSTA CSP
- Monitoraggio MULAP

Concetti correlati

Telefoni supportati alla pagina 108

23.1.1 Come modificare il numero di porta per CSTA

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Gestione della porta**.
4) Nella riga per **CSP** nel campo di input della colonna **Numero di porta** inserire il numero di porta desiderato.
5) Fare clic su **Applica**, quindi su **OK**.
6) Riavviare il sistema.

Concetti correlati

OpenScape Business TAPI 120 alla pagina 1163

23.1.2 Come attivare o disattivare il CMD per l'uso di TAPI 120

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Middleware**.
3) Nella struttura dei menu fare clic su **Middleware** > **CSTA Message Dispatcher (CMD)**.
4) Fare clic sulla scheda **Impostazioni - CSTA Message Dispatcher (CMD)**.
5) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare il CMD, nell'area **Attivazione**, selezionare la casella di controllo **Il servizio verrà avviato automaticamente**.
   - Se si desidera disattivare il CMD, nell'area **Attivazione**, deselezionare la casella di controllo **Il servizio verrà avviato automaticamente**.
6) Selezionare una delle seguenti opzioni:
   - Se si desidera utilizzare la registrazione automatica dei client, nell'area **Registrazione automatica**, selezionare la casella di controllo **Registrazione automatica client abilitata**.
   - Se non si desidera utilizzare la registrazione automatica dei client, nell'area **Registrazione automatica**, deselezionare la casella di controllo **Registrazione automatica client abilitata**.
7) Fare clic su **Applica**.

Concetti correlati

OpenScape Business TAPI 120 alla pagina 1163

23.1.3 Come attivare o disattivare il server DSS per l'uso di tasti DSS a livello di rete

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Middleware**.
3) Nella struttura dei menu fare clic su **Middleware** > **Server DSS**.
4) Fare clic sulla scheda **Impostazioni - Server DSS**.
5) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare il server DSS, nell'area **Attivazione**, selezionare la casella di controllo **Il servizio verrà avviato automaticamente**.
   - Se si desidera disattivare il server DSS, nell'area **Attivazione**, deselezionare la casella di controllo **Il servizio verrà avviato automaticamente**.
6) Fare clic su **Applica**.

23.1.4 Come attivare o disattivare il CSP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Middleware**.
3) Nella struttura dei menu fare clic su **Middleware** > **CSTA Service Provider (CSP)**.
4) Fare clic sulla scheda **Impostazioni - CSTA Service Provider (CSP)**.
5) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare il CSP, nell'area **Attivazione**, selezionare la casella di controllo **Il servizio verrà avviato automaticamente**. Per poter utilizzare un'applicazione CSTA occorre inoltre inserire un ID e una password utente CSTA.
   - Se si desidera disattivare il CSP, nell'area **Attivazione**, deselezionare la casella di controllo **Il servizio verrà avviato automaticamente**.

     Nota: Se il CSP è disattivato, non è possibile utilizzare TAPI 120 (tramite CMD), TAPI 170, server DSS e UC Suite!
6) Fare clic su **Applica**.

23.1.5 Come attivare o disattivare Media Extension Bridge

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Middleware**.
3) Nella struttura dei menu, fare clic su **Middleware** > **Media Extension Bridge (MEB)**.
4) Fare clic sulla scheda **Impostazioni - Media Extension Bridge (MEB)**.
5) Selezionare una delle seguenti opzioni:
   - Se si utilizza il Media Extension Bridge, nell'area **Attivazione**, selezionare la casella di controllo **Il servizio verrà avviato automaticamente**.
   - Se si desidera rilasciare questo collegamento CSTA, nell'area **Attivazione**, deselezionare la casella di controllo **Il servizio verrà avviato automaticamente**.
6) Fare clic su **Applica**.

23.2 OpenScape Business TAPI 120/170

Simili a CallBridge Collection, OpenScape Business TAPI 120 e OpenScape Business TAPI 170 sono due provider di servizi TAPI (TSP) ottimizzati per l'architettura di sistema e la topologia di rete di OpenScape Business che mettono a disposizione di applicazioni basate su TAPI l'interfaccia Microsoft TAPI per la connessione al sistema di comunicazione OpenScape Business.

Il collegamento a OpenScape Business avviene esclusivamente tramite LAN. I componenti add-on hardware e software, quali ad esempio CSTA Message Dispatcher (CMD) o CSTA Service Provider (CSP), non sono più necessari per l'uso di OpenScape Business. La licenza è basata sull'utente e non distingue tra utenti OpenScape Business TAPI 120 o TAPI 170. L'utilizzo della licenza inizia con i primi utenti TAPI.

La scelta dei provider di servizi TAPI più adatto dipende essenzialmente dal numero di PC client da collegare alle applicazioni TAPI e dall'infrastruttura IT disponibile, oltre che dai telefoni utilizzati.

- **CallBridge Collection**

  è utilizzato come provider di servizi TAPI First Party classico per i telefoni di sistema che dispongono di una porta LAN o USB. È adatto a sistemi che dispongono solo di pochi PC. Per l'uso di CallBridge Collection non è necessaria una LAN. CallBridge Collection viene installato su ogni PC su cui viene eseguita un'applicazione TAPI. Non sono supportati telefoni analogici, cordless e di sistema senza interfaccia USB/IP.

  Gli interfacciamenti TAPI tramite CallBridge Collection non sono forniti di licenza.
- **OpenScape Business TAPI 120**

  viene preferibilmente usato come provider di servizi TAPI First Party in reti Microsoft con o senza un controller di dominio quando occorre utilizzare

anche telefoni analogici, cordless o di sistema senza interfaccia USB/IP assieme all'applicazione TAPI. Il provider di servizi TAPI 120 viene installato su ogni PC client su cui viene eseguita un'applicazione TAPI.

Gli interfacciamenti TAPI tramite OpenScape Business TAPI 120 sono soggetti a licenza nell'ambito di OpenScape Business. Per la connessione a OpenScape Business, a seconda del tipo di utilizzo/collegamento, è necessario un collegamento CSTA o un collegamento all'interfaccia WebService, indipendentemente dal numero di client TAPI 120 utilizzati. Il servizi disponibili sul lato TAPI dipendono dal tipo di utilizzo/collegamento.

- **OpenScape Business TAPI 170**

  è un provider di servizi TAPI Third Party classico. Viene installato su un server della LAN e utilizzato centralmente nel sistema OpenScape Business. In alternativa a TAPI 120, è possibile utilizzare TAPI 170 se è disponibile un controller di dominio sulla rete Microsoft. Quando si utilizza la cosiddetta funzione TAPI remota, non è richiesta l'installazione del provider di servizi TAPI su PC client. Ciò assicura un notevole risparmio di tempo nei sistemi con più PC client. Nelle seguenti topologie, tuttavia, l'uso di OpenScape Business TAPI 170 è comunque richiesto.

  – Collegamento di utenti TAPI ai sistemi OpenScape Business in rete se tali utenti si trovano su nodi diversi.
  – Collegamento di applicazioni TAPI utilizzate su un Terminal Server.
  – Collegamento di applicazioni TAPI basate su server.

  Gli interfacciamenti TAPI tramite OpenScape Business TAPI 170 sono soggetti a licenza nell'ambito di OpenScape Business. Per la connessione a OpenScape Business è necessario un collegamento CSTA, indipendentemente dal numero di utenti TAPI 170 utilizzati.

23.2.1 OpenScape Business TAPI 120

OpenScape Business TAPI 120 è un provider di servizi di telefonia First Party che supporta funzionalità Microsoft TAPI V2.1. OpenScape Business TAPI 120 consente ad applicazioni CTI basate su Windows di monitorare e controllare un telefono di sistema connesso a OpenScape Business.

In alternativa, OpenScape Business TAPI 120 può essere connesso a OpenScape Business tramite l'interfaccia CSTA (modalità CSTA) o WSI (Web Services Interface) (modalità UC Smart). Non è consentito il funzionamento misto nell'interfacciamento con un sistema. Se nel sistema OpenScape Business è inserita una UC Booster Card o è collegato un UC Booster Server, TAPI 120 può essere utilizzato solo in modalità CSTA. I requisiti di sistema, ovvero il numero massimo di utenti TAPI e le funzionalità TAPI disponibili, dipendono dal modo di utilizzo.

Connessioni a OpenScape Business TAPI 120

Il software OpenScape Business TAPI 120 è installato su un PC client con Microsoft Windows. La connessione al sistema OpenScape Business viene eseguita tramite LAN. Non è richiesta una connessione fisica tra il PC Windows e il telefono.

- **Modalità CSTA TAPI 120**

  Tutti i PC client TAPI 120 sono collegati allo stesso collegamento CSTA di OpenScape Business. OpenScape Business effettua il multiplexing interno di tutte le connessioni TAPI 120.

  In modalità CSTA, TAPI 120 supporta OpenScape Business X3, X5, X8 e OpenScape Business S.

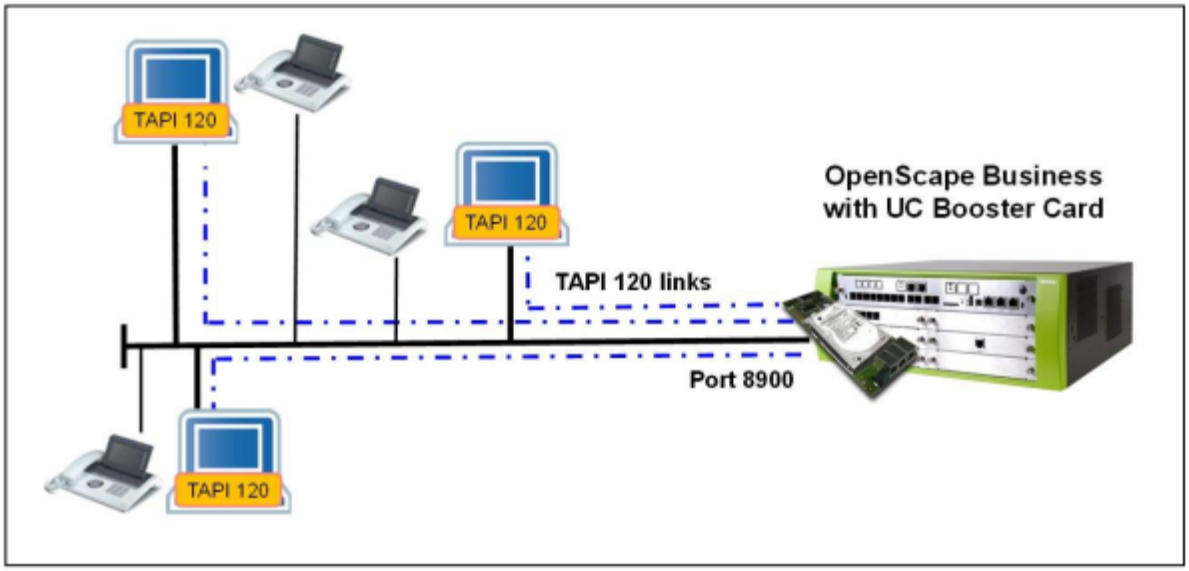


Figura 11: TAPI 120 in modalità CSTA con OpenScape Business X5R e UC Booster Card

- **TAPI 120 modalità UC Smart**

  Tutti i PC client TAPI 120 client sono collegati alla scheda madre di OpenScape Business tramite LAN e interfaccia Web Server. OpenScape Business effettua il multiplexing interno di tutte le connessioni TAPI 120.

  In modalità CSTA, TAPI 120 supporta OpenScape Business X1/X3/X5/X8.

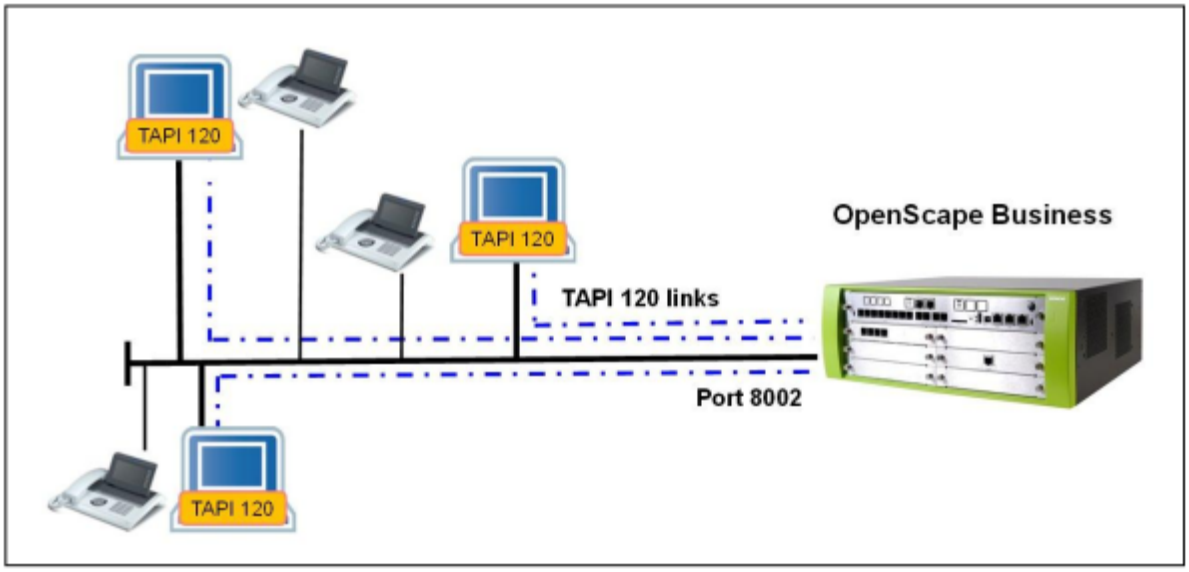


Figura 12: TAPI 120 in modalità UC Smart con OpenScape Business X5R

Caratteristiche

Vengono supportati i seguenti servizi:

Caratteristica	TAPI 120 CSTA	TAPI 120 UC Smart
Provider di servizi TAPI First Party con collegamento centralizzato tramite LAN	X	X
Compatibile con lo standard Microsoft TAPI 2.1	X	X
Collegamento a sistemi OpenScape Business singoli	X	X
Supporto per OpenScape Business CTI Firewall	X	-
Funzioni supportate tramite TAPI		
Segnalazione di chiamate in entrata e in uscita con identificazione del numero di telefono e dell'origine della chiamata	X	X
Informazioni aggiuntive nella segnalazione della chiamata con chiamate inoltrate	X	X
Risposta a chiamate interne/esterne	X	X
Connessioni controllate con interlocutori interni ed esterni	X	X
Composizione manuale/post-selezione DTMF	X	X
Attivazione di chiamate esistenti	X	X
Esecuzione di una consultazione con interlocutori interni ed esterni	X	X
Richiamata alternata	X	X
Trasferta accompagnata	X	X
Trasferta accompagnata con successiva selezione della destinazione della consultazione (trasferta One-step)	X	X
Trasferta non accompagnata (Blind transfer)	X	-
Impostazione e cancellazione del trasferimento di chiamata	X	X
Impostazione e cancellazione del blocco chiamate	X	X
Avvio di una conferenza	X	-
Estendi conferenza	X	-
Inoltro della chiamata in arrivo	X	-
Risposta per assente diretta (Call pickup)	X	-
Segnalazione chiamata a gruppo e risposta chiamata a gruppo (Group pickup)	X	-
Parcheggio di chiamate in corso	X	-
Ripresa di chiamate parcheggiate	X	-
messa in attesa manuale di chiamate in corso	X	-

Caratteristica	TAPI 120 CSTA	TAPI 120 UC Smart
Ripresa manuale di chiamate in attesa	X	-
Impostazione richiamata	X	-
Supporto di funzioni controllate da codice	X	-
Scambio di dati basato sulla chiamata tra applicazioni TAPI	X	-
Controllo dei tasti nei telefoni di sistema (HFA)	X	-
Controllo guadagno del microfono nei telefoni di sistema (HFA)	X	-
Controllo/selezione dell'uso del portatile/altoparlante/ cuffie nei telefoni di sistema (HFA)	X	-
Controllo del volume della tastiera del portatile/ altoparlante/cuffie nei telefoni di sistema (HFA)	X	-
Accesso ai display optiPoint/OpenStage e ai LED (con limitazione a 50 schermi attivi per sistema)	X	-

Valori massimi

Il numero massimo di PC client TAPI 120 collegabili a OpenScape Business dipende dal modello (vedere Livelli di espansione disponibili presso il reparto commerciale).

Sistemi operativi approvati

I sistemi operativi attualmente approvati per il server Microsoft Windows, il Terminal Server e il PC client remoto sono elencati nelle informazioni di vendita correnti.

Con TAPI 120 essere utilizzati solo i sistemi operativi Microsoft Windows.

Per l'installazione di Terminal Server, viene utilizzato OpenScape Business TAPI 170 al posto di OpenScape Business TAPI 120.

Concessione della licenza

La licenza per l'uso di OpenScape Business TAPI 120 è basata sugli utenti. Le licenze TAPI sono gestite all'interno del sistema OpenScape Business e possono essere utilizzate per entrambe le modalità di TAPI 120. Quando si utilizza la funzione MULAP è necessaria una licenza TAPI per ogni utente all'interno del MULAP.

Nota: Per TAPI 120 in modalità UC Smart non sono necessarie licenze Utente UC.

Implementazione del software

Il software OpenScape Business TAPI 120 è fornito su supporto dati. Non è parte del software OpenScape Business System.

Requisiti hardware

Il PC deve soddisfare come minimo i requisiti indicati da Microsoft per il sistema operativo utilizzato, oltre a quelli dell'applicazione TAPI. Inoltre, è necessaria un'interfaccia Ethernet LAN.

- con TAPI 120 CSTA

  Indipendentemente dal numero di client TAPI 120 connessi, è necessario un collegamento CSTA di OpenScape Business. Per questo motivo è richiesta una soluzione OpenScape Business UC Booster (Card o Server).
- con TAPI 120 UC Smart

  È necessaria l'interfaccia Web Services. Nel sistema non deve essere presente alcuna soluzione OpenScape Business UC Booster (Card o Server).

Terminali supportati

I terminali supportati e le relative caratteristiche dipendono dalle funzionalità CSTA o WSI del sistema OpenScape Business utilizzato. Queste informazioni sono contenute nei dati di vendita di OpenScape Business.

Indirizzo IP/Porta IP occupati per impostazione predefinita da TAPI 120

Nella modalità TAPI 120 CSTA, il collegamento CSTA a OpenScape Business occupa la porta IP 8900.

Nella modalità TAPI 120 UC Smart, il collegamento WSI a OpenScape Business occupa la porta IP 8802 in caso di connessione crittografata (HTTPS) o 8801 in caso di connessione non crittografata (HTTP).

Nella configurazione TAPI 120, l'indirizzo IP del sistema OpenScape Business deve essere inserito in funzione della modalità. Questo indirizzo IP viene visualizzato nel WBM, nell'area **Selezione applicazione**.

Attività correlate

Come modificare il numero di porta per CSTA alla pagina 1159
Come attivare o disattivare il CMD per l'uso di TAPI 120 alla pagina 1160

23.2.2 OpenScape Business TAPI 170

OpenScape Business TAPI 170 è un provider di servizi di telefonia Third Party che supporta funzionalità Microsoft TAPI V2.1. TAPI 170 consente alle applicazioni CTI basate su Microsoft Windows di monitorare e controllare più telefoni connessi contemporaneamente a OpenScape Business.

Servizi

OpenScape Business TAPI 170 offre i seguenti servizi:

- Provider di servizi TAPI Third Party con collegamento centralizzato
- Compatibile con lo standard Microsoft TAPI 2.1
- Le funzioni di telefonia sono disponibili su ogni PC client collegato tramite l'architettura client/server TAPI 2.1
- Non è richiesto altro software client TSP

- Funzioni di telefonia supportate:
  - Selezione in entrata e in uscita da PC
  - Trasmissione del numero di telefono in arrivo, se segnalato
  - Consultazione e trasferimento
  - Richiamata alternata
  - Conferenza
  - Deviazione di chiamata
  - Inoltra chiamata
  - Risposta a una chiamata tramite l'applicazione
  - Disconnessione di una chiamata tramite l'applicazione
  - Trasferta rapida/monitorata
  - Trasmissione dei codici funzione
  - Monitoraggio del telefono (stati, interruzioni di corrente ecc.)
  - Disponibilità di interfaccia ACD
  - Monitoraggio/accesso alla tastiera su telefoni di sistema (HFA)
  - Controllo del display/LED tramite telefoni di sistema (HFA)
  - Collegamento a sistemi OpenScape Business singoli e sistemi di rete
  - Supporto utenti/numeri di telefono MULAP

Interfacciamenti di OpenScape Business TAPI 170

Il software OpenScape Business TAPI 170 è installato su un server Microsoft Windows sulla rete. Il collegamento a OpenScape Business avviene esclusivamente tramite connessione CSTA. Non è richiesta una connessione fisica tra il PC Windows e il telefono. OpenScape Business TAPI 170 può essere configurato in diversi modi ai sistemi singoli o in reti OpenScape Business. Il server e i client TAPI devono essere gestiti dallo stesso controller di dominio di rete.

- **Connessioni di applicazioni TAPI basate su server a OpenScape Business tramite TAPI 170**

  L'applicazione server e il software TAPI 170 sono installati sul cosiddetto server di telefonia sulla rete. L'applicazione server mette a disposizione dei propri client in rete funzioni di telefonia per gli utenti configurati in OpenScape business TAPI 170. Il software TAPI 170 è collegato tramite LAN all'interfaccia CSTA di OpenScape Business. Per questa connessione

è necessario un collegamento CSTA da OpenScape Business oltre a una licenza TAPI per ogni utente TAPI configurato.

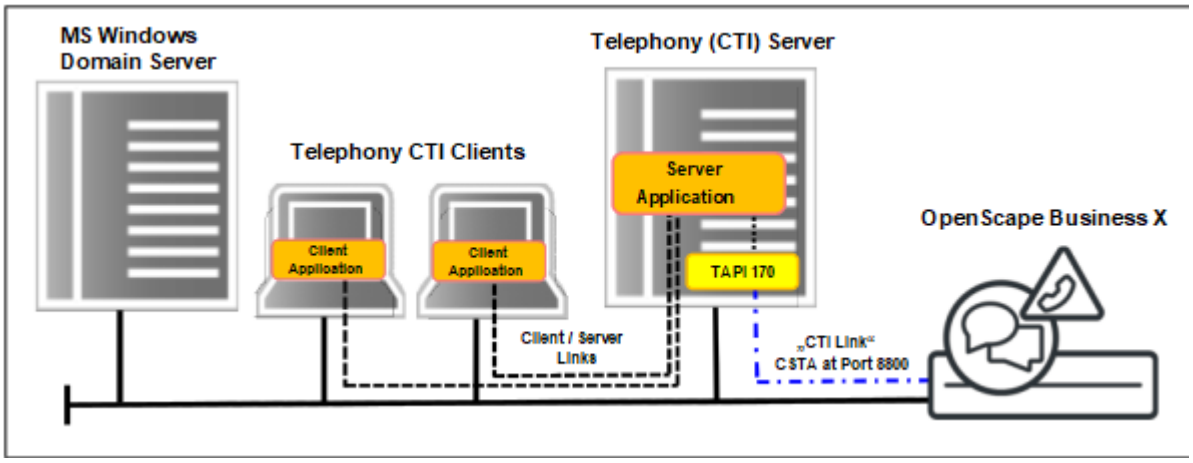


Figura 13: Applicazione TAPI basata su server collegata tramite TAPI 170 a OpenScape Business

- **Connessioni di applicazioni TAPI basate su client a OpenScape Business tramite TAPI 170 con funzione "TAPI remoto"**

  In questo scenario, il software OpenScape Business TAPI 170 è installato su un server sulla rete. Sui PC client con le applicazioni TAPI è abilitata la cosiddetta funzione "TAPI remota", tramite la quale l'applicazione TAPI sul client comunica con il software TAPI 170 sul server. Pertanto a tal fine sul client non deve essere installato alcun software TAPI 170. Il software TAPI 170 è collegato tramite LAN all'interfaccia CSTA di OpenScape Business. Per questa connessione è necessario un collegamento CSTA di OpenScape Business oltre a una licenza per ogni utente TAPI configurato.

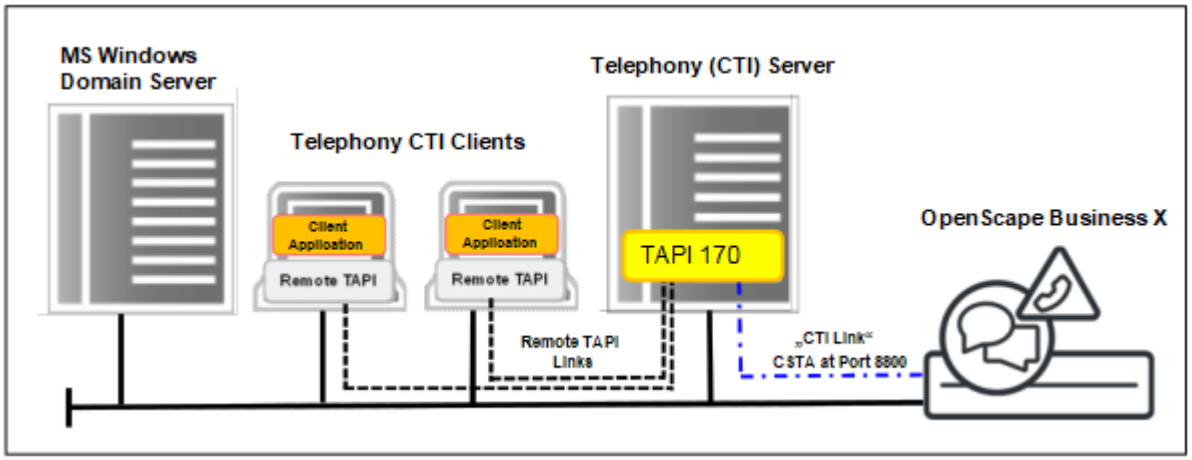


Figura 14: L'applicazione TAPI basata su client collegata tramite "TAPI remoto" a OpenScape Business

- **Connessioni di applicazioni TAPI basate su Terminal Server a OpenScape Business tramite TAPI 170**

  In questo scenario, le applicazioni TAPI basate sul client sono installate su uno o più Terminal Server. In questo caso, il software TAPI 170 è installato sul Terminal Server. Nel caso esistano più cluster Terminal Server, il software TAPI 170 deve essere installato su ogni Terminal Server del cluster. Ogni software TAPI 170 installato è collegato tramite LAN a OpenScape

Business. Per ogni software TAPI 170 installato su un Terminal Server è necessario un collegamento CSTA di OpenScape Business. È inoltre necessaria una licenza TAPI per ogni utente TAPI configurato.

È previsto un numero massimo di server OpenScape Business TAPI 170 che è possibile connettere a OpenScape Business.

Nota: È possibile utilizzare tanti Terminal Server nel cluster quanti sono i collegamenti CSTA liberi in OpenScape Business, disponibili per la connessione al software TAPI 170. Il valore massimo delle connessioni possibili diminuisce se i collegamenti CSTA di OpenScape Business sono occupati da altre applicazioni CSTA.

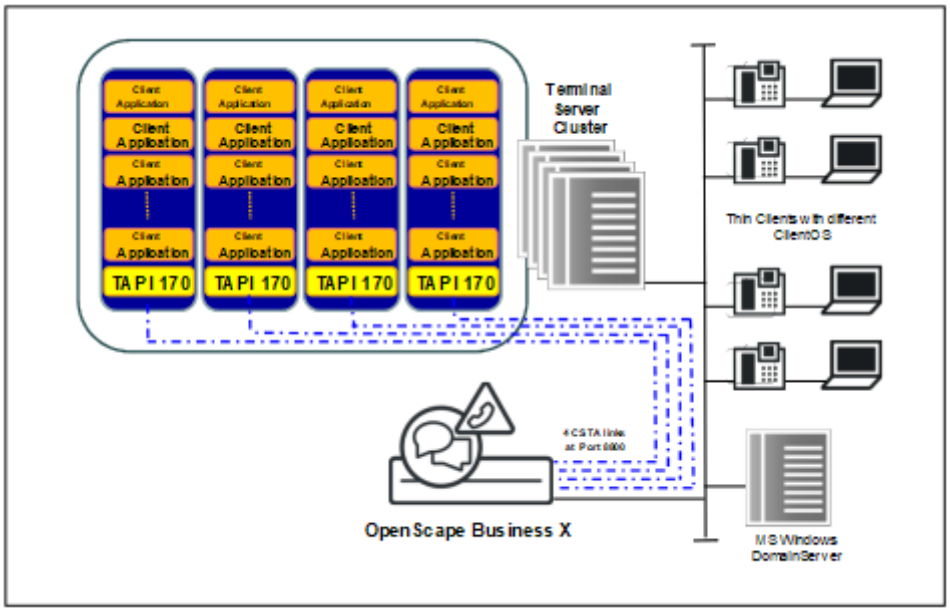


Figura 15: Applicazione TAPI basata su client su Terminal Server per OpenScape Business

- **Collegamento di TAPI 170 ai sistemi OpenScape Business in rete**

  Nei sistemi OpenScape Business in rete, il software TAPI 170 è installato su un server collegato tramite LAN all'interfaccia CSTA del nodo master. Questa connessione è indipendente dal tipo di funzionamento precedentemente descritto del provider di servizi TAPI 170 (TAPI remoto o interfaccia basata su server). Per la realizzazione è necessario un collegamento CSTA del nodo master di OpenScape Business oltre a una licenza per ogni utente TAPI in rete.

  Nota: Tramite il nodo master, il software TAPI 170 ha accesso a tutti gli utenti sulla rete. In caso di collegamento di TAPI 170 a un nodo slave anziché al nodo master, il software TAPI 170 potrà accedere solo agli utenti del nodo slave. Se

si utilizzano più TAPI 170 in un cluster Terminal Server, è necessario un collegamento CSTA al nodo master.

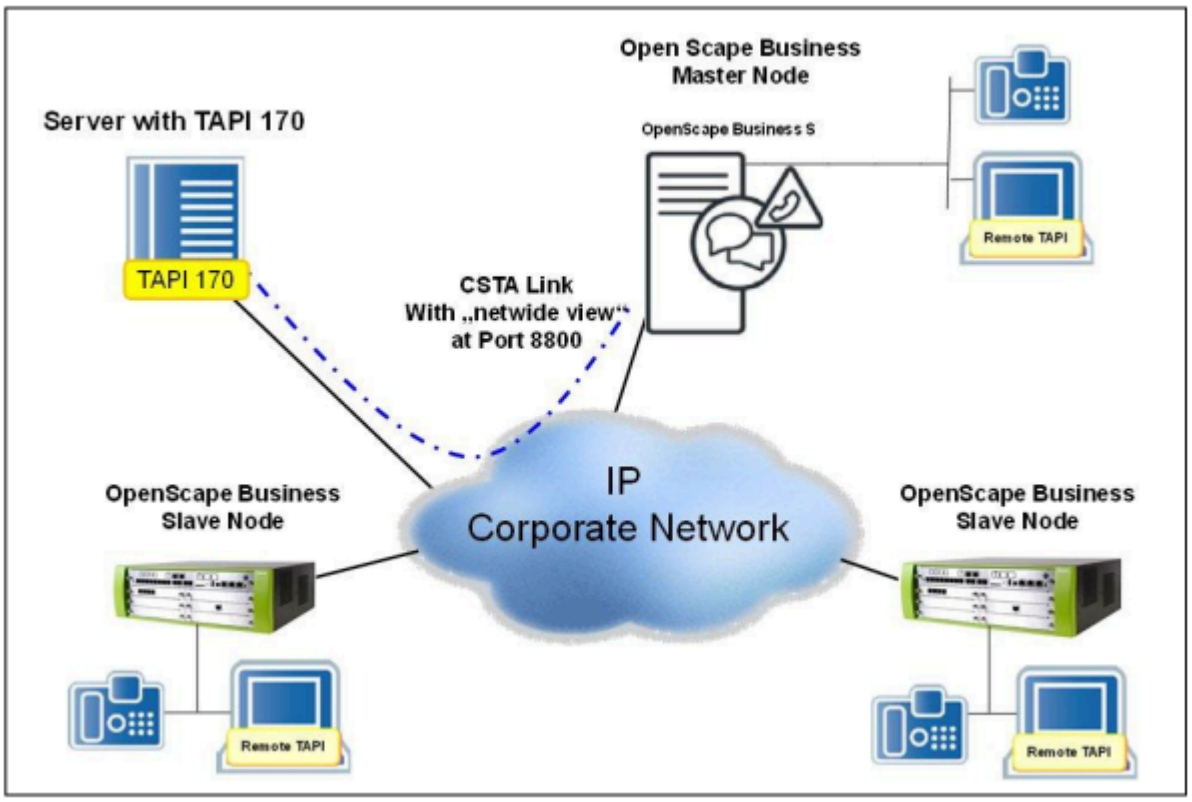


Figura 16: Collegamento di TAPI 170 ai sistemi OpenScape Business in rete

Limiti prestazionali

Il numero massimo di PC client TAPI 170 collegabili a OpenScape Business dipende dal modello. Per ulteriori informazioni, consultare il capitolo 1.3.9.4

Sistemi operativi approvati

I sistemi operativi attualmente approvati per il server Microsoft Windows, il Terminal Server e il PC client remoto sono elencati nelle informazioni di vendita correnti.

Con TAPI 170 possono essere utilizzati solo i sistemi operativi Microsoft Windows.

Il modello di licenza Microsoft richiede, oltre alla licenza per il sistema operativo del server, anche il corrispondente Microsoft Device o User CAL nel numero richiesto per l'espansione pianificata. Questi CAL non sono compresi nella fornitura di OpenScape Business TAPI 170, e devono essere acquistati separatamente. In determinate condizioni previste da Microsoft, per OpenScape Business TAPI 170 è possibile utilizzare anche un "Windows Server for embedded systems" con la cosiddetta "licenza Telco integrata".

Concessione della licenza

La licenza per l'uso di OpenScape Business TAPI 170 è basata sugli utenti. Le licenze vengono gestite all'interno dei sistemi OpenScape Business. Quando

si utilizza la funzione MULAP è necessaria una licenza TAPI per ogni utente all'interno del MULAP.

Implementazione del software

Il software OpenScape Business TAPI 170 è fornito su supporto dati. Non è parte del software OpenScape Business System.

Requisiti hardware

Per il collegamento di OpenScape Business TAPI 170, indipendentemente dal numero di client TAPI 170 collegati è necessario un collegamento CSTA di OpenScape Office. Questo si applica anche ai sistemi OpenScape Business in rete.

Il PC deve soddisfare come minimo i requisiti indicati da Microsoft per il sistema operativo utilizzato, a condizione che non siano utilizzate altre applicazioni software oltre a TAPI 170. Inoltre, è necessaria un'interfaccia Ethernet LAN.

Terminali supportati

I terminali supportati e le relative caratteristiche dipendono dalle funzionalità CSTA o WSI del sistema OpenScape Business utilizzato. Queste informazioni sono contenute nei dati di vendita di OpenScape Business.

23.3 Interfaccia Web Services

L'interfaccia integrata di Web Services permette il monitoraggio e il controllo delle risorse di telefonia in un sistema con utenti UC.

Servizi

L'interfaccia Web Services offre le seguenti funzionalità:

- Accesso via LAN Ethernet (TCP/IP)
- Supporto per HTTP e HTTPS
- Supporto per sistemi singoli
- orientato all'utente, funzioni chiaramente strutturate per:
  - Controllo delle chiamate
  - Controllo delle periferiche
  - Monitoraggio dei dispositivi
  - Rubrica
  - Diario degli utenti
  - Stato presenza dell'utente

Nota: In base al tipo di client WSI (Web Services Interface), i servizi associati al flag utente devono essere attivati per consentire l'esecuzione di alcuni dei comandi WSI.

Web Server - Sessioni Web

Il numero di sessioni del server Web disponibili è comune per tutte le applicazioni corrispondenti, quali myPortal to go (Web Edition), Application Launcher, optiClient Attendant (server) e optiClient BLF.

Punti di monitoraggio interni

I punti di monitoraggio interni sono indipendenti dai punti di monitoraggio dell'interfaccia CSTA. Se più applicazioni monitorano lo stesso utente UC tramite l'interfaccia Web Services, il server Web utilizza a tal fine solo un singolo punto di monitoraggio interno.

Porte

Sono disponibili i seguenti numeri di porta:

Porta	Protocollo
8801	HTTP (non crittografato)
8802	HTTPS (crittografato)

23.4 Open Directory Service

Open Directory Service (ODS) è un servizio di directory aperto, integrato e basato su LDAP. Agisce da servizio di meta-directory, aggregando i risultati provenienti da diverse fonti di directory interne ed esterne tramite un'unica interfaccia. Open Directory Service è accessibile da diversi tipi di client, applicazioni e dispositivi di comunicazione all'interno di un'azienda.

Open Directory Service svolge due funzioni:

1) Fornisce accesso a dati di contatto aggiuntivi provenienti da fonti esterne tramite l'accesso dai SQL o ODBC ai database nella rete del cliente che contengono dati di directory
2) Espone directory interne ed esterne a client, dispositivi di comunicazione e applicazioni.

Open Directory Service è disabilitato per impostazione predefinita. Durante la sua attivazione, assicurarsi anche che i firewall per il protocollo LDAP siano aperti sulla porta TCP/389.

Open Directory Service su diverse varianti di OpenScape Business

Open Directory Service è offerto con diverse funzionalità a seconda della piattaforma OpenScape Business:

- Schede madri di OpenScape Business S, OpenScape Business X V3 Advanced, server Booster o scheda Booster:

  Viene offerta la piena funzionalità, in modo da poter utilizzare sia fonti di dati interne che esterne
- Schede madri di OpenScape Business X V3 Basic:

  La funzionalità è limitata alle fonti di dati interne predefinite.
- Scheda madri di OpenScape Business X V2:

  Per utilizzare Open Directory Service è necessaria una scheda Booster o un server Booster.

Per connettersi all'Open Directory Service tramite il protocollo LDAP, utilizzare l'indirizzo IP indicato nel portale di amministrazione:

- Sul lato destro della pagina iniziale di OpenScape Business Assistant, sotto **Applicazioni**.

- Nella pagina **Selezione applicazione** della procedura guidata **Installazione iniziale**, sotto la voce **Configurazione** > **Installazione di base**.

Origini dati interne

In Open Directory Service sono disponibili per impostazione predefinita le seguenti origini dati interne:

- Rubrica esterna
- Directory interna
- Numeri di selezione diretta centralizzati

Per queste origini dati interne, i nomi dei campi sono mappati in modo permanente allo schema dei dati di Open Directory Service.

Queste origini dati interne non possono essere eliminate o modificate.
Per esporre le origini dati interne tramite ODS, è necessaria una licenza "OpenScape Business OpenDirectory Base".

Origini dati esterne

Gli amministratori possono integrare le informazioni di contatto dai seguenti tipi di database come origini dati per l'accesso in sola lettura tramite SQL o ODBC.

- Origini dati con driver integrati (Microsoft SQL Server, PostgreSQL, Sybase SQL).
- Le origini dati senza driver integrati richiedono l'installazione e la configurazione di ODBC Bridge Server sul client ODS (scaricabile tramite WBM all'indirizzo **Centro assistenza** > **Software**).

Nota: Per una connettività corretta, è necessario definire un valore (il valore può essere diverso dal nome dell'origine dati, ma il campo non può essere vuoto) nel campo **Descrizione**. Nel caso di origini dati bridge ODBC per Access, Firebird, Excel e Oracle, aggiungere il nome dell'origine dati, rispettivamente "access", "firebird", "excel" e "oracle", come valore del campo **Descrizione**.

Nota: Per l'integrazione del database ODS con Microsoft Excel, è supportato solo il formato di file *.xsl* (ma non *.xlsx*). Nelle versioni recenti di MS Office, evitare di modificare/salvare i file Excel per non compromettere la codifica del file. Inoltre, è necessario un driver ODBC Bridge specifico per Microsoft Excel.

Per accedere a origini dati esterne da ODS, è necessaria una licenza "OpenScape Business OpenDirectory Connector" per ogni origine dati collegata.

Numero massimo di tipi diversi di database: 3

Numero massimo di fonti di dati esterne: 4

Assicurarsi che Open Directory Service sia autorizzato ad accedere all'origine dati esterna. Contattare in anticipo l'amministratore responsabile del database per assicurarsi che sia così. Per consentire l'accesso da parte del sistema, potrebbe essere necessario aggiungere un utente separato nell'origine dati esterna.

Le origini dati esterne possono essere utilizzate sia nel contesto delle ricerche nelle directory che nella risoluzione dei numeri di chiamata in nomi.

È possibile configurare l'accesso diretto a una tabella di database da un'origine dati esterna o da una query SQL personalizzata per l'origine dati.

Qualsiasi colonna che serve da ID deve contenere valori univoci e non nulli/non vuoti. Utilizzare la proprietà UNIQUE o PRIMARY KEY per assicurarsi che sia così.

Nei casi in cui siano integrati database esterni, si applicano le seguenti restrizioni:

- I caratteri speciali ´[]'" non sono supportati dall'ODS nei nomi delle tabelle e delle colonne.
- I tipi di colonna "nchar" e "nvarchar" non sono supportati dall'ODS.
- I caratteri di spazio vuoto intermedi (almeno nelle ultime 4-5 cifre) non sono supportati dall'ODS per i dati telefonici.

Query SQL personalizzate per origini dati esterne

Le query SQL personalizzate supportano anche tabelle correlate, ad esempio:

```
SELECT * FROM users LEFT OUTER JOIN phonenumbers ON
users.id = phonenumbers.uid;
```

La struttura dei dati deve essere di tipo 1:1 o n:1, ovvero ogni record può avere una sola riga.

L'accesso tramite query SQL personalizzate può talvolta risultare molto più lento rispetto all'accesso diretto a una tabella di database.

Le query SQL personalizzate che presentano potenziali rischi per la sicurezza non vengono eseguite, ad esempio:

- Modifica dei dati
- Arresto del server SQL
- Esecuzione di programmi tramite il server SQL
- Modifica dei diritti utente

Pertanto, le query SQL personalizzate con i seguenti comandi SQL non vengono eseguite:

- PUNTO DI CONTROLLO
- CHIUSI
- CLUSTER
- IMPEGNA
- COPIA
- CREA
- DEALLOCA
- DICHIARA
- ELIMINA
- SCARTA
- ESEGUI
- RILASCIA
- FINE
- ESEGUI
- SPIEGA
- RECUPERA

- CONCEDI
- INSERISCI
- CARICA
- BLOCCA
- SPOSTA
- PREPARA
- RIASSEGNA PROPRIETARIO
- REINDICIZZA
- RILASCIA PUNTO DI SALVATAGGIO
- RIPRISTINA
- REVOCA
- PUNTO DI SALVATAGGIO
- ETICHETTA DI SICUREZZA
- SELEZIONA IN
- IMOPOSTA
- MOSTRA
- AVVIA TRANSAZIONE
- TRONCA
- ANNULLA ASCOLTO
- AGGIORNA
- VUOTO
- VALORI

Mappatura dei campi per le origini dati

Per queste origini dati, è possibile personalizzare la mappatura dei nomi dei campi allo schema dati di Open Directory Service. È possibile assegnare ciascun campo nello schema dati di Open Directory Service a non più di un campo della fonte dati esterna. Tuttavia, è possibile assegnare un campo dell'origine dati esterna a più campi nello schema dati di Open Directory Service.

Mappature dell'output dei dati LDAP

Una mappatura dell'output dei dati LDAP determina quali campi dello schema dati di Open Directory Service devono essere emessi tramite LDAP, ad esempio per specifici client LDAP o per diversi gruppi di abbonati che non desiderano visualizzare tutti i dettagli, ma solo un sottoinsieme definito.

La mappatura dell'output dei dati LDAP **web** è disponibile per impostazione predefinita e non può essere eliminata o modificata. Tutti i campi dello schema dati in Open Directory Service sono assegnati in modo permanente all'output LDAP in esso contenuto. È inoltre possibile configurare altre mappature di output dei dati LDAP.

I client LDAP possono accedere a una mappatura specifica dell'output dei dati LDAP tramite il parametro dc nell'accesso LDAP, ad esempio: `dc=web`.

Normalizzazione dei numeri di telefono nel formato canonico

Per ogni origine dati, è possibile configurare la normalizzazione dei numeri di telefono nel formato canonico. Durante questo processo vengono rimossi spazi vuoti, parentesi, trattini e virgole. Ciò è necessario per identificare correttamente il nome del chiamante e per la composizione dei numeri dal desktop. Si sconsiglia di saltare la normalizzazione, a meno che i numeri di telefono utilizzati nell'origine dati non siano già presenti in formato canonico. È possibile

inserire automaticamente dal sistema i valori relativi alla normalizzazione, come il codice di area, ecc. Se la fonte dati esterna si trova in un sito diverso dal sistema, potrebbe essere necessario modificare questi valori.

Stato delle origini dati

Il display di stato sotto la voce **OpenDirectory** > **Origini dati** ha il seguente significato:

Colore	Stato
verde	attivo
rosso	ODBC e LDAP non funzionano, configurazione errata o origine dati non disponibile
giallo	LDAP non funziona: riavviare Open Directory Service
grigio	Configurazione incompleta

Provisioning delle directory

I seguenti tipi di client, dispositivi di comunicazione e applicazioni possono utilizzare le directory fornite da Open Directory Service:

- Client UC
- Application Launcher
- Directory di sistema
- OpenStage con supporto LDAP locale
- Telefoni IP DECT (tramite LDAP)
- Telefoni SIP (tramite LDAP)
- Applicazioni, ad esempio suite CRM come Microsoft Dynamics CRM (tramite LDAP, ODBC o esportazione CSV OpenLDAP)

Open Directory Service è in grado di identificare nei risultati della ricerca la fonte dei dati da cui proviene un risultato.

Concetti correlati

Requisiti per l'uso di Application Launcher alla pagina 1188

23.4.1 Come attivare o disattivare Open Directory Service

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Open Directory Service**.
3) Nella struttura dei menu fare clic su **Open Directory** > **Impostazioni di base**.

4) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare Open Directory Service, selezionare la casella di controllo **Attivo**.
   - Se si desidera disattivare Open Directory Service, deselezionare la casella di controllo **Attivo**.
5) Fare clic su **Salva**.
6) Fare clic su **OK**.
7) Fare clic su **OK**.

23.4.2 Come riavviare Open Directory Service

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Open Directory Service è attivato.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Open Directory Service**.
3) Nella struttura dei menu fare clic su **Open Directory** > **Manutenzione**.
4) Fare clic su **Riavvia**.
5) Fare clic su **OK**.

23.4.3 Come configurare la password per l'accesso a Open Directory Service

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Procedere come descritto di seguito per definire la password con cui i client, i dispositivi di comunicazione e le applicazioni possono accedere a Open Directory Service.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Open Directory Service**.
3) Nella struttura dei menu fare clic su **Open Directory** > **Impostazione di base**.
4) Inserire la **Password LDAP** desiderata.
5) Fare clic su **Salva**.
6) Fare clic su **OK**.

23.4.4 Come configurare ODBC-ODBC Bridge Server

Prerequisiti

L'ODBC Bridge Server è stato scaricato dal WBM in **Centro assistenza** > **Software** e installato su un PC con Windows (32 bit o 64 bit) con origini dati in grado di accedere a database sia relazionali che non relazionali. L'ODBC Bridge Server è necessario per consentire ai driver ODBC di accedere all'origine dati.

Nota:

A causa dei recenti aggiornamenti di Windows 10/Windows Server da parte di Microsoft, l'interfaccia ODBC del sistema operativo è stata modificata e quindi solo i driver a 32 bit sono supportati da ODBC-ODBC Bridge. Per il momento si consiglia vivamente di utilizzare driver ODBC a 32 bit per connettersi alle origini dati ODBC.

Si tratta di una limitazione temporanea.

L'origine dati deve essere configurata come DSN sul client ODS tramite amministrazione dell'origine dati ODBC.

Il nome utente e la password dell'origine dati sono noti.

La configurazione dell'ODBC Bridge Server è descritta per l'interfaccia utente inglese. Naturalmente, la configurazione può essere eseguita anche in altre lingue dell'interfaccia (scheda **Gestione server** > **Lingua**).

Passo a passo

1) Fare clic destro con il mouse sull'icona di ODBC Bridge Server nella barra delle applicazioni, quindi selezionare la voce di menu **Impostazioni**.

2) Definire le impostazioni generali del server:

a) Fare clic sulla scheda **Impostazioni server**.

b) In **Impostazioni di connessione**, nell'elenco a discesa **Interfaccia di rete**, selezionare l'indirizzo IP al quale ODBC Bridge Server sarà raggiungibile per il client ODBC (OpenScape Business).

L'indirizzo IP deve essere inserito nella configurazione ODS del WBM di OpenScape Business.

c) In **Porta**, indicare la porta attraverso la quale si dovranno ricevere le interrogazioni del client ODBC (OpenScape Business).

Tale porta deve essere inserita nella configurazione ODS del WBM di OpenScape Business.

d) Se il servizio viene arrestato, è possibile attivare **Stato servizio** impostandolo su **On** in **Controllo servizio** ,oppure selezionando **Avvia servizio** nella barra delle applicazioni.

e) Se il servizio viene connesso, è possibile disattivare **Stato servizio** impostandolo su **Off**, oppure selezionando **Arresta servizio** nella barra delle applicazioni.

f) In **Impostazioni di rete** è possibile attivare la crittografia impostandola su **On**.

g) In **Impostazioni di rete**, inserire il numero massimo di connessioni simultanee ai client ODBC (minimo: 1, massimo: 20) nel campo **Connessioni massime**.

h) Fare clic su **Salva impostazioni**.

Nota: Dopo aver salvato le impostazioni, è necessario riavviare il servizio.

---

3) Creare un utente per l'accesso del client ODBC all'origine dati:

a) Fare clic sulla scheda **Gestione ruoli**.

b) Fare clic su **Aggiungi utente**.

c) Assegnare un nome utente al client ODBC nel campo **Nome utente**.

d) Inserire la password per il client ODBC nei campi **Password** e **Immetti nuovamente password**.

Gli stessi dettagli di utente devono essere inseriti nella configurazione ODS del WBM di OpenScape Business.

e) Selezionare il DSN al quale il client ODBC deve accedere, spuntando la relativa casella nella colonna **Accesso**.

f) Inserire **Nome utente DB** e **Password**, se richiesti.

g) Fare clic su **Salva impostazioni**.

4) Fare clic sulla scheda **Monitoraggio** per monitorare le connessioni. Vengono visualizzati i seguenti dettagli:

- I nomi dei driver ODBC installati e le relative versioni.
- Il nome e l'indirizzo IP del client ODS, l'ora dell'ultima connessione attiva e il tempo totale delle connessioni attive.
- Le origini dati ODBC disponibili (attraverso il collegamento **Apri amministratore origine dati Windows**).

5) Fare clic sulla scheda **Registri** per consentire la creazione dei file di registro e impostare i livelli di traccia che dovranno essere registrati:
   a) Attivare la registrazione impostandola su **On**.
   b) Selezionare **Livello di registro**: **Tutto** per tutti i registri, **Normale** per i registri di servizio o solo **Avvisi ed errori**.
   c) Selezionare il tipo di registro dall'elenco a discesa. È possibile scegliere di visualizzare la cartella dei registri o la console dei registri.
6) Fare clic sulla scheda **Aspetto** per cambiare l'aspetto:
   a) Selezionare un tema (chiaro o scuro).
   b) Selezionare uno stile.
   c) Impostare la lingua desiderata.
   d) Indicare se il servizio deve essere eseguito automaticamente all'avvio.
   e) Indicare se il servizio può essere ridotto a icona nella barra delle applicazioni.
7) Fare clic sulla scheda **Info** per visualizzare i dettagli del servizio e gli aggiornamenti disponibili.

   Nota: Se è disponibile una nuova versione, fare clic su **Installa** per eseguire l'aggiornamento.

8) Selezionare **Esci** nella barra delle applicazioni per chiudere la configurazione del servizio.

23.4.5 Come aggiungere un'origine dati esterna per Open Directory Service

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

I dati di accesso del database esterno sono disponibili.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Open Directory Service**.
3) Nella struttura dei menu, fare clic su **Origini dati**.
4) Fare clic su **Aggiungi**.
5) Fare clic sulla scheda **Database**.
6) Inserire il **Nome** dell'origine dati.
7) Inserire una **Descrizione** dell'origine dati.

8) Se si desidera aggiungere un database SQL:

a) Selezionare il tipo **PostgreSQL**, **Microsoft SQL Server, Sybase SQL** o **ODBC Bridge** dal menu a discesa **Driver ODBC**.

b) Nel campo **Indirizzo server del database**, inserire l'indirizzo IPv4 del database.

c) Indicare la **Porta server del database**.

d) In **Nome del database**, inserire il relativo nome rispettando le maiuscole/minuscole.

e) In **Nome utente database**, inserire il relativo nome rispettando le maiuscole/minuscole.

f) In **Password database**, inserire la relativa password rispettando le maiuscole/minuscole.

g) Se è stato selezionato il tipo **Microsoft SQL Server, Sybase SQL** nell'elenco a discesa **Driver ODBC**, inserire anche la **Versione del protocollo TDS**.

9) Se si desidera aggiungere un database non SQL:

a) Nell'elenco a discesa **Driver ODBC** selezionare il tipo **ODBC Bridge**.

b) Nel campo **Indirizzo ODBC Bridge Server**, inserire l'indirizzo IPv4 del database.

c) Inserire la **Porta ODBC Bridge Server**.

d) Inserire il **DSN remoto di ODBC Bridge**

e) In **Credenziali ODBC Bridge Server**, inserire il relativo valore rispettando le maiuscole/minuscole.

f) In **Password ODBC Bridge**, inserire il relativo valore rispettando le maiuscole/minuscole.

10) Fare clic su **Verifica accesso database** per testare l'accesso al database.

11) Fare clic su **Salva**.

12) Fare clic sulla scheda **Accesso ai dati**.

13) Se si desidera utilizzare una tabella del database:

a) Fare clic su **Selezione semplice - Accesso a una tabella**.

b) Fare clic su **Interroga tabella del database** e nell'elenco **Tabelle del database** selezionare la tabella desiderata.

Nota: Questa funzionalità non è supportata per alcune origini dati (ad es. Oracle). In tal caso, inserire manualmente il nome della tabella.

---

c) Fare clic su **Anteprima tabella database**, quindi nell'anteprima scorrere i record con l'aiuto dei corrispondenti pulsanti.

14) Se si desidera utilizzare una query SQL definita dall'utente:

a) Fare clic su **Query SQL definita dall'utente**.

b) Inserirla in **Query SQL**.

Nota: Quando si definisce una nuova origine dati con un'istruzione SQL, è necessario formulare la query in modo da garantire che gli ID dei record siano costanti. È necessario utilizzare gli attributi ID inclusi nelle rispettive tabelle, invece di calcolare gli ID durante l'esecuzione della query. Evitare istruzioni come "SELECT ROW_NUMBER() OVER As ID" che creano ID durante l'esecuzione della query e che forniscono

ID diversi a seconda dell'ordinamento e della quantità di record. In caso di unione di tabelle con intervalli di ID sovrapposti con UNION ALL, ridurre il rischio di ID duplicati incrementando gli ID delle tabelle esistenti con un numero diverso per ciascuna tabella da unire (ad esempio "SELECT (table2.ID+1000) AS ID").

c) Fare clic su **Anteprima del risultato della query**, quindi nell'anteprima scorrere i record con l'aiuto dei corrispondenti pulsanti.

15) Fare clic sulla scheda **Mappature campi**.

Nota: Sono disponibili per la mappatura dei campi tutte le colonne della tabella selezionata e quelle restituite dalle interrogazioni SQL definite dall'utente.

16) Fare clic su **Mappature campi**.

17) Nell'elenco a discesa a sinistra, selezionare il campo dell'origine dati esterna e nell'elenco a discesa a destra, nella stessa riga, il campo che si desidera associare nello schema dati di Open Directory Service. A scopo di verifica, viene visualizzata sulla destra un'anteprima dei record in questione, che è possibile scorrere utilizzando i pulsanti corrispondenti.

Nota: Il campo **Numero di identificazione** deve essere assegnato a un campo univoco della fonte dati esterna.

18) Se si desidera rimuovere una riga dalle mappature campi, fare clic a sinistra sull'icona del cestino.

19) Fare clic sulla scheda **Conversione numero**.

a) Selezionare la casella di controllo **Attivo**.

b) Fare clic su **Leggi impostazioni di sistema**.

c) Se il database esterno si trova in una località diversa rispetto al sistema Inserire **Prefisso internazionale**, **Prefisso interurbanoPrefisso per linea esterna**, **Prefisso nazionale**, **Lunghezza numero interno max.**

d) Selezionare una delle seguenti opzioni:

- Se si desidera rimuovere, nell'origine dati esterna, un prefisso per linea esterna eventualmente presente, selezionare la casella di controllo **Rimuovere prefisso linea esterna**.

- Se non si desidera eliminare il prefisso per linea esterna, deselezionare la casella di controllo **Rimuovere prefisso linea esterna**.

20) Fare clic su **Salva**.

21) Fare clic su **OK**.

Passaggi successivi

Riavviare Open Directory Service per rendere effettive le modifiche.

Visualizzare un'anteprima dei risultati della ricerca LDAP.

23.4.6 Come visualizzare un'anteprima dei risultati della ricerca LDAP per Open Directory Service

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Procedere come descritto di seguito per controllare se una ricerca LDAP in Open Directory Service restituisce record nella forma desiderata e con il formato dei numeri di telefono corretto.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Open Directory Service**.
3) Nella struttura dei menu, in **Open Directory** > **Utenti OpenScape Business** > **Origini dati**, fare clic sull'origine dati desiderata.
4) Fare clic sulla scheda **Test LDAP**.
5) Fare clic su **Esegui test**. In **Risultati della ricerca LDAP** viene visualizzata un'anteprima dei risultati della ricerca.

Nota: Il limite di risposta predefinito di OpenLDAP è di 500 voci. Anche il motore di backend ODS (Open Directory Service) impone un limite di 500 voci per ogni origine di dati.

La funzionalità di test LDAP di Open Directory Service (ODS) esegue una query di ricerca che raggiunge il limite di 500 voci. Lo scopo dell'opzione di test LDAP non è il recupero dei risultati ma convalidare che la connettività LDAP sia corretta.

Pertanto, se esistono più di 500 record, le aggiunte e le modifiche ai dati LDAP possono non essere riflesse sulla WBM dopo l'esecuzione di un test LDAP.

23.4.7 Come eliminare un'origine dati esterna da Open Directory Service

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **Open Directory Service**.
3) Nella struttura dei menu fare clic su **Open Directory** > **Origini dati**.
4) Nell'area di lavoro, fare clic sull'origine dati in questione.
5) Fare clic su **Cancella**.
6) Fare clic su **OK**.

Passaggi successivi

Riavviare Open Directory Service per rendere effettive le modifiche.

23.5 Servizio di integrazione Active Directory

Active directory è un servizio di directory Microsoft per le reti di domini. Con il servizio di integrazione Active Directory offerto, OpenScape Business è in grado di leggere il database Active Directory e sincronizzare gli utenti con il proprio database utenti per semplificarne l'amministrazione e ridurne gli sforzi di configurazione.

Premessa

Per consentire la sincronizzazione del servizio di integrazione Active Directory, devono essere soddisfatti i seguenti requisiti:

- Un server Microsoft Active Directory è distribuito dal cliente
- Active Directory è usato come singolo punto di configurazione per i dati di dipendenti e in particolare per i dati utente. I seguenti campi devono essere mappati fra Active Directory e OpenScape Business:
  - nome
  - cognome
  - nome visualizzato
- Solo questo Active Directory è usato per aggiungere, modificare o eliminare dati di dipendenti.
- È previsto che tutte le modifiche effettuate su Active Directory si ripercuotano automaticamente sul sistema di comunicazione.

Sincronizzazione

L'ID univoco degli utenti OpenScape Business usato per la sincronizzazione è il numero DID. Questo numero è sincronizzato con il campo Numero di telefono di AD (Active Directory).

Ogni modifica effettuata nell'Active Directory dell'azienda viene immediatamente sincronizzata con OpenScape Business. Questo significa che ogni nuovo utente aggiunto ad AD viene aggiunto anche a OpenScape Business e che gli viene assegnata una licenza utente IP.

Qualsiasi modifica effettuata in AD a utenti già sincronizzati viene applicata immediatamente agli utenti OpenScape Business.

Se un utente sincronizzato viene eliminato da AD, il nome, l'sn e il nome visualizzato dell'utente vengono eliminati anche da OpenScape Business e la licenza utente IP è nuovamente disponibile. Tuttavia, il numero DID e il numero di telefono interno non vengono eliminati da OpenScape Business e restano disponibili per essere assegnati a un altro utente.

Nota: L'accesso ad Active Directory è in lettura sola. Questo significa che la sincronizzazione dei dati utente viene effettuata solo da Active Directory a OpenScape Business. Le modifiche alle informazioni utente in OpenScape Business non vengono sincronizzate con Active Directory e vengono sovrascritte dai dati di Active Directory alla sincronizzazione seguente.

Mappature campi

È possibile modificare l'assegnazione dei nomi dei campi in base allo schema dati di Active Directory Service. In questo modo, si può controllare il modo in cui i campi di OpenScape Business vengono aggiornati con i dati di Active Directory.

La mappatura predefinita dei campi è data nella tabella seguente:

Campo OpenScape Business	Campo Active Directory
nome	nome
cognome	sn
nome visualizzato	displayName
DID	telephoneNumber

Normalizzazione dei numeri DID

I dati di ubicazione del gateway nel sistema OpenScape Business sono usati per convertire il numero DID di un utente in un formato di numero canonico.

È necessario che anche il formato del numero di telefono in Active Directory sia nel formato canonico, in modo da consentire la sincronizzazione automatica.

23.5.1 Come configurare il servizio Active Directory

Prerequisiti

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su > **Procedure guidate**Telefonia centrale.
3) Fare clic su **Modifica.** per avviare la procedura guidata **Servizio di integrazione Active Directory**.
4) Fare clic sulla casella di controllo **Attiva** per attivare il servizio di integrazione Active Directory .
5) Impostare l'**Indirizzo IP** del server Active Directory, il **Nome utente** e la **Password** per un utente valido.

   Il **Nome utente** richiesto qui non è un nome utente OpenScape Business, ma un nome utente Active Directory che deve essere fornito secondo il formato della specifica delle directory X.500. In questo formato, gli utenti sono definiti con i seguenti nodi:

CN	Nome generale
OU	Unità organizzativa

DC	Componente dominio

Il nome utente è descritto partendo dalle informazioni più specifiche (a sinistra) a quelle più generali (a destra). Ciascuna informazione è fornita sotto forma di coppie separate da un segno di uguale (=).

Un esempio di nome utente potrebbe essere `CN=Mario.Rossi,OU=Amministratori,DC=LaSocietà`.

6) Fare clic su **Recupera DN** per recuperare i DN disponibili e selezionarne uno come ContestoNome di base.

   Se vi sono problemi con le credenziali utente, verrà visualizzato il messaggio `Errore di autenticazione! Verificare le credenziali`.

7) Se necessario, modificare i campi **Contenitore** e **Filtro**.

   Il valore predefinito per il contenitore è `cn=Utenti` e per il filtro è `(&(categoriaOggetto=persona)(classeOggetto=utente))`

8) Fare clic su **Recupera dati**.

   Saranno visualizzate le prime 1000 voci di AD, ordinare per cognome(sn).

9) Per visualizzare i dettagli, fare clic su un utente.

10) Fare clic su **OK & Avanti** per passare alla finestra **Mappature campi** .

11) Effettuare le modifiche necessarie nei valori di mappatura dei campi.

    I valori nella colonna di sinistra fanno parte dello schema di database di OpenScape Business e i valori nella colonna di destra corrispondono agli attributi di Active Directory.

    Il campo **Numero di telefono** sarà usato per trovare il numero DID di OpenScape Business.

12) Fare clic su **Fine** per avviare la procedura guidata di integrazione Active Directory.

23.6 Application Launcher

L'Utilità di avvio dell'applicazione è un'applicazione Windows basata su Java che consente di controllare sulla base delle chiamate le altre applicazioni del PC client di utenti UC Suite e myAgent. In un sistema CRM, l'Utilità di avvio dell'applicazione può ad esempio essere utilizzata per l'apertura automatica del modulo contatti per ogni chiamante.

L'Application Launcher offre i seguenti servizi:

- Consultare le informazioni relative alle chiamate al numero di telefono (ad esempio Numero di telefono, Nome interlocutore, ID cliente) nell'Open Directory Service o nelle rubriche del sistema
- Richiamo di applicazioni Windows o Web all'arrivo o all'esecuzione di chiamate
- Trasferimento di informazioni relative a una chiamata alle applicazioni Windows o Web
- funzionamento automatico in background all'arrivo delle chiamate
- finestra popup configurabile opzionale per le chiamate in arrivo con informazioni relative alla chiamata e i pulsanti per le azioni utente
- Lista chiamate con funzione chiamata
- Funzioni di anteprima per test durante la configurazione

- facile importazione della configurazione dal primo client configurato a tutti gli altri mediante i profili di configurazione disponibili nel sistema

23.6.1 Requisiti per l'uso di Application Launcher

Per poter utilizzare Application Launcher, il PC client del singolo utente della UC Suite deve disporre di hardware e software adeguato.

I diritti di amministratore del PC client sono necessari per l'installazione, ma non per gli aggiornamenti automatici.

Sistema operativo

Application Launcher può essere utilizzato in combinazione con i seguenti sistemi operativi:

- Microsoft Windows 10 / 8.1 / 8 / 7 (32 bit o 64 bit)
- Microsoft Windows Vista (32 bit)

Suggerimento: Il sistema operativo utilizzato richiede sempre lo stato attuale di tutti gli aggiornamenti disponibili (service pack e patch).

Aggiornamento Windows

I PC richiedono sempre lo stato attuale di tutti gli aggiornamenti disponibili, inclusi i Service Pack.

Software aggiuntivo

Oracle Java 8 o versioni successive oppure, in alternativa, OpenJDK 8 (vedere **Centro assistenza** > **Software**)

Web Service per telefoni cellulari

I Web Service per i telefoni cellulari sono stati abilitati per la connessione al sistema. Le porte configurate nel sistema devono essere aperte nei firewall della LAN e nei PC client.

Open Directory Service (opzionale)

Se Application Launcher deve utilizzare i dati di Open Directory Service, tale servizio deve essere configurato nel sistema. La porta configurata a tale scopo nel sistema deve essere aperta nei firewall della LAN e nei PC client.

Concetti correlati

Konfiguration von myPortal to go und Mobility Entry alla pagina 954
Open Directory Service alla pagina 1173

23.6.2 Profilo con i dati di configurazione dell'Application Launcher

Un profilo con i dati di configurazione dell'Application Launcher consente di configurare in modo rapido e facile tale programma in tutti i PC client.

Il profilo contiene tutti i dati di configurazione eccetto quelli relativi alla connessione del sistema e ai dati degli utenti. Una volta completamente configurata l'Application Launcher per un utente iniziale, l'amministratore può rendere tale profilo, unitamente ai dati di configurazione dell'Application Launcher, disponibili nel sistema di comunicazione. Successivamente tutti gli utenti possono eseguire la configurazione dell'Application Launcher mediante l'importazione di questo profilo.

23.6.2.1 Come predisporre il profilo con i dati di configurazione dell'Application Launcher

Prerequisiti

L'Application Launcher è già interamente configurata per un utente.

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Application Launcher**.
3) Fare clic su **Sfoglia** e selezionare il file seguente: `C:\Documents and Settings\<Nome utente Windows>\Application Data\Tray_Tool\profile.xml`.
4) Fare clic su **Apri**.
5) Fare clic su **Carica**.

Passaggi successivi

Tutti gli utenti possono importare questo profilo nell'Application Launcher e quindi eseguire la configurazione.

23.7 Panoramica di myPortal for Teams

Il plug-in myPortal for Teams viene utilizzato per integrare l'applicazione Microsoft Teams con OpenScape Business.

myPortal for Teams richiede la nuova scheda madre OpenScape Business V3 o il sistema OpenScape Business S ed è supportato con la versione software V3R1 FR2 e versioni successive.

Con myPortal for Teams è possibile:

- Filtrare e gestire la cronologia chiamate.
- Visualizzare e cercare i contatti.
- Organizzare i contatti nei gruppi Preferiti.
- Inviare e-mail ai contatti.
- Selezionare un dispositivo controllato (disponibile per utenti MULAP).
- Avviare una chiamata.
- Rispondere, rifiutare o deviare una chiamata.
- Mettere in attesa una chiamata.
- Trasferire una chiamata.
- Effettuare una consultazione.

- Effettuare richiamate alternate.
- Effettuare un trasferimento monitorato.

Nota: La ricerca dei contatti nelle rubriche esterne, come LDAP, non è disponibile.

Nota: La funzionalità VoIP non è supportata per myPortal for Teams.

23.7.1 How to configure myPortal for Teams

Prerequisiti

- Official and trusted Microsoft certificate to be imported in OpenScape Business WBM
- Microsoft application ID which needs to be generated before configuring myPortal for Teams

Passo a passo

1) Andare su **Configurazione > Servizi cloud**.
2) Fare clic su Modifica accanto a **Plug-in client Microsoft Teams**.
3) The domain name and port number in the **URL** field are already filled in.

   The domain name is the domain of your OpenScape Business system.

   The default value for the port number is 8805. You can change the domain ID and port number if you want.
4) Inserire **ID applicazione**.

   The Application ID is generated by the administrator of the Microsoft Azure portal.
5) Fare clic su **OK & scarica**.

   Il plug-in viene scaricato come file zip. The downloaded file is a customized plugin based on your system configuration.

Nota:

Microsoft Teams tab prevents loading web content from a server that uses self-signed certificates. This is a security aspect and the use of self-signed certificates is essentially an unsafe practice as this interface is exposed to the internet.

Therefore, a Microsoft Trusted certificate must be installed in the system. For more information, refer to chapter Come importare un certificato server (PKCS#12) alla pagina 1035.

23.7.2 Come caricare myPortal for Teams nell'archivio di Teams

Prerequisiti

È necessario disporre dei diritti di amministratore per l'applicazione Microsoft Teams.

Passo a passo

1) Fare clic su **App** nella barra di navigazione sinistra dell'applicazione Microsoft Teams.
2) Fare clic su **Carica un'app personalizzata** e selezionare **Carica per la mia organizzazione**.

   Selezionare il file scaricato da WBM e caricarlo.

Passaggi successivi

Una volta caricato il plug-in myPortal for Teams, gli utenti possono aggiungerlo nella propria applicazione Microsoft Teams.

23.8 Unify Phone

Gli utenti OpenScape Business possono effettuare chiamate telefoniche utilizzando il client Unify Phone. Questa funzionalità è disponibile sia dal client Unify Phone che dal dispositivo. Per fare questo, è necessario configurare la connettività di Unify Phone con OpenScape Business e aggiungere gli utenti Unify Phone.

La funzionalità Unify Phone disponibile include:

- Effettuazione/risposta alle chiamate
- Annullamento/rifiuto di chiamate
- Messa in attesa/ripresa della linea
- Deviazione chiamata
- Supporto DTMF
- Scambio di chiamata (alternativo)
- Inoltro di chiamata
- Numero alternativo
- Routing delle chiamate
- Accesso alla directory e al diario
- Controllo delle chiamate da parte di terzi tramite i seguenti client UC integrati: myPortal @work, myPortal for Desktop, myPortal for Outlook, myAttendant, my Agent e myPortal for Teams.

Oltre alle funzioni sopra menzionate, non sono state rilasciate altre funzioni, in particolare i codici funzione.

Nota: Il controllo delle chiamate da parte di terzi (controllo CTI) è attualmente possibile solo per il client Unify Phone Desktop. Il controllo si verifica sempre tramite il client Unify Phone Desktop (Web/PWA) e non è previsto per il client Unify Phone mobile. È possibile spostare una chiamata al client Unify Phone mobile dopo averla accettata. Inoltre, il controllo delle chiamate da parte di terzi non deve essere utilizzato in combinazione con una funzione "numero alternativo" di Unify Phone attiva.

23.8.1 Come configurare la connettività Unify Phone

Prerequisiti

Per eseguire più chiamate simultaneamente sono stati inseriti i valori **Upstream fino a (Kbps)** in **Configurazione** > **Procedure guidate** > **Installazione base** > **Installazione base** > **Upstream della connessione a Internet**. Ad esempio, immettere "256" per 2 chiamate simultanee.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Servizi cloud**.
3) Fare clic su **Modifica** accanto a **Connettività Unify Phone** per configurare le impostazioni di connettività di base.
4) Selezionare la casella di controllo **Abilita Unify Phone** per attivare la connettività Unify Phone.
5) In **Credenziali dominio Unify Phone**, inserire i seguenti dati:
   a) Selezionare il **Dominio** dall'elenco a discesa disponibile.

      Sono disponibili le seguenti possibilità:

      - phoneapp.unify.com
      - Personalizza

      Nota: Se viene selezionato Personalizza, compilare il campo **Dominio personalizzato**.

   b) Immettere la chiave API generata per il proprio tenant nel campo **Chiave API Unify Phone**.
6) In **Chiamate Unify Phone simultanee**, selezionare il numero di chiamate Unify Phone simultanee dall'elenco a discesa disponibile. Tale numero dipende dal valore a monte, configurato in precedenza.

   Nota: Se la qualità della chiamata si deteriora, occorre ridurre il numero di chiamate simultanee.

7) Fare clic su **OK & Avanti**.
8) Nella finestra **Numero di posizione Unify Phone** selezionare lo schema di numerazione che si desidera utilizzare. Questa selezione influisce sul formato dei numeri SIP e WSI.

   - Per utilizzare i numeri internazionali, abilitare la casella di controllo **Usa numerazione internazionale**.

     Se si sceglie Numeri internazionali, la procedura guidata richiede di configurare i numeri di posizione mancanti della route Unify Phone, che verranno utilizzati per formare il numero internazionale. Inoltre, i parametri della route Unify Phone per il tipo di numero vengono aggiornati in base alla selezione.
   - Numeri interni
9) Fare clic su **OK & Avanti**.
10) Fare clic su **Esegui funzione** nel pop-up per creare un trunk SIP per Unify Phone.

11) Fare clic su **OK & Avanti**, quindi su **Fine**.

Nota: Si consiglia di salvare i dati di configurazione selezionando **Backup dei dati** > **Backup - Immediato** dal menu principale.

Passaggi successivi

Se si desidera disabilitare la connettività Unify Phone, è necessario prima eliminare tutti gli utenti Unify Phone, come descritto in Come rimuovere o eliminare nuovi utenti Unify Phone alla pagina 1196.

Nota: Ad esempio, è fondamentale eliminare gli utenti Unify Phone attivi prima di migrazioni di sistema, per evitare discrepanze critiche tra il database di OpenScape Business e il database del cloud.

23.8.2 Come configurare l'istanza di un utente Unify Phone

Prerequisiti

La **Connettività Unify Phone** è configurata.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Servizi cloud**.
3) Fare clic su **Modifica** accanto a **Istanza utente Unify Phone**.
4) Fare clic su **OK e avanti**, quindi su **Fine**.

23.8.3 Come gestire gli utenti Unify Phone

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Servizi cloud**.
3) Fare clic su **Modifica** accanto a **Istanza utente Unify Phone**.

   Appare un elenco con gli utenti Unify Phone configurati per il sistema specifico.

Nota: Se sono già presenti utenti Unify Phone registrati, verrà richiesto di eseguire la procedura guidata Connettività Unify Phone senza modificare la configurazione.

23.8.3.1 Come creare nuovi utenti Unify Phone

Prerequisiti

La **Connettività Unify Phone** è configurata.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Servizi cloud**.
3) Fare clic su **Modifica** accanto a **Istanza utente Unify Phone**.
   Vengono visualizzati gli utenti Unify Phone disponibili.
4) Fare clic su **Crea** accanto a **Crea un nuovo utente per Unify Phone**.
5) Nella pagina **Creazione utente Unify Phone**, procedere come segue:
   a) Il campo **Codice di accesso trunk + Numero di chiamata dell'utente Unify Phone** è di sola lettura e viene generato automaticamente in base allo schema di numerazione selezionato (internazionale o nazionale).
   b) Inserire il **Numero di chiamata dell'utente Unify Phone**.
   c) Inserire il **DID dell'utente Unify Phone**.
   d) Inserire il **Nome**.
   e) Inserire il **Cognome**.
   f) Inserire l'**Indirizzo e-mail** dell'utente Unify Phone.
6) Fare clic su **OK & Avanti**.
7) Fare clic su **Fine**.
   Dopo aver completato correttamente questo processo, viene inviata all'indirizzo e-mail digitato un'e-mail che consente all'utente Unify Phone di completare la configurazione.
8) Ripetere i passaggi 4-6 per aggiungere altri utenti Unify Phone.

23.8.3.2 Come aggiungere utenti Unify Phone esistenti

Prerequisiti

La **Connettività Unify Phone** è configurata.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Servizi cloud**.
3) Fare clic su **Modifica** accanto a **Istanza utente Unify Phone**.
   Vengono visualizzati gli utenti Unify Phone disponibili.
4) Fare clic su **Aggiungi** accanto a **Aggiungere un utente esistente a Unify Phone**.

5) Nella pagina **Assegnazione utente Unify Phone**, gli utenti disponibili sono visualizzati come icone. Per aggiungere un utente esistente, procedere come segue:
   a) Il campo **Codice di accesso trunk + Numero di chiamata dell'utente Unify Phone** è di sola lettura e viene generato automaticamente in base allo schema di numerazione selezionato (internazionale o nazionale).
   b) Inserire il **Numero di chiamata dell'utente Unify Phone**.
   c) Inserire il **DID dell'utente Unify Phone**.
   d) È possibile cercare un utente per **Nome** o **E-mail**.
   e) Selezionare un utente Unify Phone utilizzando le icone disponibili.

      Ci sono tre tipi di icone per gli utenti Unify Phone:

      - Icone verdi: Utenti disponibili e attivi.
      - Icone verdi disattivate: Utenti non disponibili e non attivi.
      - Icona verde disattivata in cornice rossa: Utenti non disponibili e non attivi, già configurati con un numero in Unify Phone.

      I campi **Nome** e **Cognome** degli utenti Unify Phone vengono compilati automaticamente.
6) Fare clic su **OK & Avanti**.
7) Ripetere i passaggi 4-6 per aggiungere altri utenti Unify Phone.

Passaggi successivi

Assegnare le licenze agli utenti Unify Phone come descritto in Come concedere licenze agli utenti (indipendente) alla pagina 312 o Come concedere licenze agli utenti (sistema di reti) alla pagina 323.

Quando si integra un utente Unify Phone in un team (MULAP), tenere presente quanto segue:

- Solo un telefono fisso IP o TDM può essere incluso nel team con l'utente Unify Phone. La funzione di instradamento di Unify Phone viene utilizzata per determinare quale dispositivo finale deve essere utilizzato per segnalare una chiamata in arrivo.
- Il deskphone del team con Unify Phone può comunque essere controllato da applicazioni esterne tramite TAPI, WSI o CSTA. Ciò vale quando Unify Phone viene controllato tramite applicazioni di terze parti.
- Gli abbonati cordless non sono approvati in relazione a Unify Phone.

23.8.3.3 Come modificare i dettagli dell'utente Unify Phone

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Servizi cloud**.
3) Fare clic su **Modifica** accanto all'utente Unify Phone corrispondente.

4) È possibile modificare i seguenti dettagli:
   a) **Codice di accesso alla linea esterna + numero di telefono dell'utente Unify Phone** è di sola lettura e viene generato automaticamente in base allo schema di numerazione selezionato (internazionale o interno).
   b) Il **Numero di telefono dell'utente Unify Phone**.
   c) Il **DID utente Unify Phone**.
   d) Il **Nome** dell'utente Unify Phone.
   e) Il **Cognome** dell'utente Unify Phone.

   Nota: Il campo Utente Unify Phone selezionato che contiene l'indirizzo e-mail dell'utente non è modificabile.

5) Fare clic su **OK & Avanti**.

23.8.3.4 Come rimuovere o eliminare nuovi utenti Unify Phone

Esistono sono scenari in cui l'eliminazione degli utenti di Unify Phone dal sistema OpenScape Business è assolutamente necessaria. Ad esempio:

- Quando si migra da un sistema di laboratorio di prova a un sistema reale.
- Quando si sostituisce una scheda madre da V2 H/W a V3 H/W o a causa di errori H/W.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Servizi cloud**.
3) Fare clic su **Modifica** accanto a **Istanza utente Unify Phone**.
4) Fare clic su **Modifica** accanto all'utente Unify Phone corrispondente.
5) Fare clic su **Rimuovi** oppure su **Elimina**.
6) Ripetere i passaggi 1-5 per aggiungere altri utenti Unify Phone.

   Tenere presente che l'eliminazione degli utenti amministratori è diversa dall'eliminazione degli utenti Unify Phone non amministratori:

   Quando gli utenti Unify Phone, con o senza ruolo di amministratore, vengono rimossi dal sistema, non vengono rimossi dal tenant Unify Phone a cui appartengono. Questi utenti esistono ancora, ma non hanno più un numero di telefono ad essi assegnato.

   Quando gli utenti di Unify Phone senza ruolo di amministratore vengono eliminati dal sistema, vengono rimossi anche dal tenant a cui appartengono.

   Quando gli utenti di Unify Phone con ruolo di amministratore vengono eliminati dal sistema, non vengono rimossi dal tenant a cui appartengono. Questi utenti esistono ancora, ma non hanno più un numero di telefono ad essi assegnato.

   Nota: Se si configura un nuovo sistema tramite clonazione o ripristino dei dati (migrazione), e sul sistema originale era configurato un accesso al connettore Unify Phone, è necessario assicurarsi di evitare discrepanze tra lo stato del

cloud UP e quello del database OSBiz. Per questo motivo, è essenziale rimuovere tutti gli utenti UP, se necessario, e disabilitare il connettore Unify Phone prima di clonare o eseguire il backup del sistema originale.

23.8.3.5 Come preparare Numero alternativo e Routing delle chiamate per l'interoperabilità Unify Phone

Perché OpenScape Business supporti le funzionalità Numero alternativo e Routing delle chiamate di Unify Phone, occorre configurare le seguenti impostazioni in Modalità esperti.

Passo a passo

1) In **Modalità esperti**, fare clic su **Server telefonia** > **Chiamate in entrata** > **Inoltri**.
2) Fare clic sulla scheda **Elenchi destinazioni chiamata - Definizione**.
3) Alla voce **Modifica inoltro**, procedere alle seguenti configurazioni:
   a) Come **1ª dest.** selezionare `* Utente selezionato`.
   b) Come **2ª dest.** selezionare `** Definito dall'utente`.
   c) Come **3ª dest.** selezionare `Numero casella vocale` (facoltativo).

23.9 Servizio Let's Encrypt

Let's Encrypt è un'autorità di certificazione automatica che offre certificati TLS/SSL gratuiti attraverso il protocollo Automatic Certificate Management Environment (ACME). Il servizio verifica la proprietà del dominio utilizzando token e richieste univoci, come la richiesta HTTPS. Dopo la verifica, i server Let's Encrypt forniscono certificati firmati per la comunicazione sicura tra server e utenti.

Per i sistemi con scheda madre V2 che utilizzano OCAB o Booster Server, il certificato Let's Encrypt è sincronizzato all'interno del server Booster. Per facilitare l'attivazione, un meccanismo è integrato nell'applicazione Java. Il processo di attivazione dei sistemi con scheda madre V2 potrebbe richiedere del tempo in più, poiché il certificato deve essere trasferito e attivato all'interno di Booster (scheda o server). Si deve prevedere un leggero ritardo nel tempo di attivazione dovuto a questo processo di sincronizzazione. Quando la funzione è disattivata, il certificato server predefinito è abilitato per il server OCAB o Booster.

23.9.1 Come configurare il servizio Let's Encrypt

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Servizi cloud**.
3) Fare clic su **Modifica** accanto a **Servizio Let's Encrypt**.

4) In **configurazione del nome di dominio**, inserire i seguenti dati:
   - Immettere il nome di dominio nel campo **Nome di dominio primario**.
   - In alternativa, digitare un secondo dominio nel campo **Nome di dominio secondario (facoltativo)**.
5) In **Configurazione dell'aggiornamento automatico del certificato**, nel campo **Ora aggiornamento automatico** inserire l'ora in cui deve avvenire l'aggiornamento automatico.

   Nota: Dopo un aggiornamento automatico, il sistema viene riavviato.

6) Fare clic su **Attiva** per attivare o su **Disattiva** per disattivare il servizio.
7) In **Stato del servizio Let's Encrypt** sono riportate informazioni dettagliate sul servizio e sul suo stato:
   - Il campo **Stato del servizio** indica se il servizio è attualmente `Attivo` o `Inattivo`.
   - **Data di attivazione del certificato** indica la data di attivazione del certificato.
   - **Data del rinnovo** mostra la data di scadenza del rinnovo automatico del certificato.
   - **Stato del rinnovo** mostra lo stato del processo di rinnovo automatico.

   Nota: Il protocollo Let's Encrypt utilizza la porta HTTP TCP/80 per la richiesta HTTP durante la creazione iniziale del certificato o l'aggiornamento del certificato.

   Nella home page di WBM viene visualizzato un messaggio che informa gli amministratori del sistema quando il certificato scade (X giorni) e quando il tentativo di aggiornamento del certificato non è andato a buon fine.

23.10 CloudLink Service

CloudLink consente la comunicazione tra i sistemi OpenScape Business in loco e le applicazioni Mitel basate sul cloud.

Connettività SIP

La funzione Connettività SIP viene utilizzata per connettere OpenScape Business a servizi cloud come Workflow Studio.

Per abilitare questa funzione, consultare il capitolo Come configurare il connettore SIP.

Suggerimento: Prima di farlo, assicurarsi che la connessione Internet sia configurata a monte (vedere la sezione Come configurare l'accesso a Internet tramite un router Internet esterno).

Supporto contenitori in OpenScape Business

In OpenScape Business è disponibile un runtime dei contenitori per supportare il contenitore CAS (Cloudlink Gateway). A causa di limitazioni relative alle

prestazioni/capacità, è disponibile solo nelle seguenti versioni di OpenScape Bisness:

- Schede madri V3 con disco NVMe collegato (sistemi integrati)
- Sistemi OpenScape Business S (varianti di server)

Sui sistemi integrati, il runtime del contenitore è preinstallato come parte dell'immagine software OpenScape Business per V3 HW. Non viene avviato automaticamente all'avvio del sistema per risparmiare risorse di sistema. Viene attivato solo dopo che l'amministratore ha abilitato il supporto dei contenitori nell'interfaccia utente web di Cloudlink.

Nelle varianti server, il runtime dei contenitori (pacchetto docker) deve essere installato dall'amministratore durante l'installazione del sistema operativo SLES15.

Per configurare il servizio di supporto container, consultare il capitolo Come configurare l'interfaccia web CloudLink Daemon.

23.10.1 Come configurare il servizio CloudLink

Passo a passo

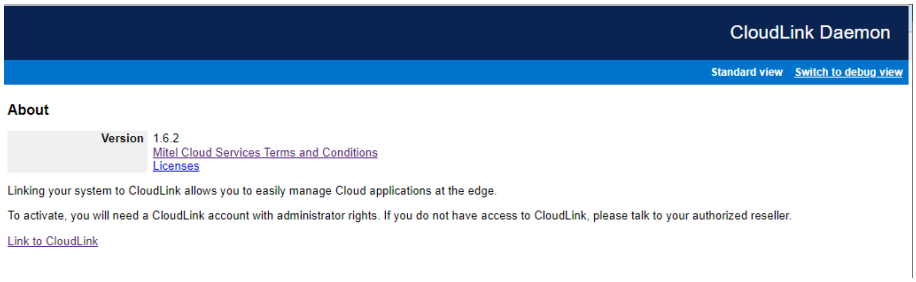
1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Servizi cloud**.
3) Fare clic su **Modifica** accanto a **CloudLink Service**.
4) Fare clic sulla casella di controllo accanto a **Abilita CloudLink Service**.
5) Se necessario, fare clic sulla casella di controllo accanto a **Usa proxy**.
6) Digitare l'indirizzo IP e la porta del proxy rispettivamente nei campi **Proxy HTTP** e **Porta proxy HTTP**.
7) Digitare le proprie credenziali nei campi **Nome utente** e **Password**.
8) Se necessario, fare clic sulla casella di controllo accanto a **Abilita connettore SIP**.
9) Fare clic su **Applica** per salvare le impostazioni.
10) Fare clic sul pulsante **CloudLink** per aprire la finestra dell'interfaccia web di CloudLink Daemon.

23.10.2 Come aprire l'interfaccia web CloudLink Daemon

L'interfaccia web CloudLink Daemon consente la configurazione e l'integrazione di sistemi cloud e on-premise, migliorando le funzionalità delle applicazioni di comunicazione OpenScape Business.

Passo a passo

1) Fare clic su **Link a CloudLink**.



   Si verrà trasferiti al portale CloudLink.
2) Inserire il **nome utente** e la **password** per accedere al portale CloudLink.
3) Avviare una connessione.

23.10.3 Come configurare l'interfaccia web CloudLink Daemon

È possibile eseguire le seguenti azioni utilizzando la vista Standard o la vista Debug. Per passare da una vista all'altra, fare clic su **Passa alla vista debug** o **Passa alla vista standard**.

Passo a passo

1) Fare clic su **Termini e condizioni dei servizi cloud Mitel** per visualizzare i termini e le condizioni.
2) Fare clic su **Licenze** per visualizzare le licenze correlate.
3) Fare clic su **Portale CloudLink**.

   Si verrà trasferiti al portale CloudLink.
4) Fare clic su **Disconnettiti da CloudLink** per disconnettersi dal servizio.
5) Modificare il giorno e l'ora in cui devono avvenire gli aggiornamenti automatici e fare clic su **Ripianifica**.
6) Fare clic su **Pausa** per mettere in pausa il prossimo aggiornamento.
7) Fare clic su **Avvia tutti i tunnel** e **Arresta tutti i tunnel** per avviare o arrestare tunnel configurati.
8) Fare clic su **Avvia** o **Arresta** per avviare o interrompere l'accesso remoto tramite il portale CloudLink Gateway.
9) Per le schede madri V3 OCCe con NVMe e i sistemi OpenScape Business S, è possibile configurare la funzione di supporto dei contenitori procedendo come segue:
   a) Fare clic su **Attiva supporto contenitori**.
   b) Nella finestra di conferma a comparsa, fare clic su **Sì**.
   c) Se necessario, fare clic su **Riavvia** o **Disattiva supporto contenitori** per riavviare o arrestare il servizio rispettivamente.

23.10.4 Come abilitare/configurare il connettore SIP per connettersi a Workflow Studio

Prerequisiti

Assicurarsi che la connessione Internet sia configurata a monte (vedere la sezione Come configurare l'accesso a Internet tramite un router Internet esterno).

È necessario disporre di un account CloudLink e stabilire una connessione con CloudLink (Vedere Come configurare l'interfaccia web CloudLink Daemon).

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Servizi cloud**.
3) Fare clic su **Modifica** accanto a **CloudLink Service**.
4) Fare clic sulla casella di controllo accanto a **Abilita CloudLink Service**.
5) Se necessario, fare clic sulla casella di controllo accanto a **Usa proxy**.
6) Digitare l'indirizzo IP e la porta del proxy rispettivamente nei campi **Proxy HTTP** e **Porta proxy HTTP**.
7) Digitare le proprie credenziali nei campi **Nome utente** e **Password**.
8) Se necessario, fare clic sulla casella di controllo accanto a **Abilita connettore SIP**.
   a) Selezionare un valore dall'elenco a discesa per il campo **Numero di chiamate CloudLink simultanee**.
9) Fare clic su **OK & Avanti**.
   I trunk vengono aggiunti (non sono necessarie licenze per i trunk).
   CloudLink è configurato e la connessione è stata stabilita.
10) Nella finestra pop-up è possibile visualizzare lo stato della connettività.
    Fare clic su **Fine**.

23.11 Numeri pilota CloudLink

Chiamando qualsiasi numero pilota CloudLink configurato, la chiamata viene instradata a Wokflow Studio per l'ulteriore elaborazione.

I numeri pilota per i servizi Cloudlink per ogni sistema OpenScape Business sarà limitato a 60 per sistema OpenScape Business.

Le linee trunk per il sistema OpenScape Business sono limitate dalla capacità complessiva di 250.

Inoltre, le linee trunk sono limitate dalla larghezza di banda upstream definita nella procedura guidata di installazione di base (128 Kbps per linea).

L'interconnessione trunk Cloudlink occuperà 1 dei 10 percorsi ITSP/Native-SIP dedicati in un sistema OpenScape Business.

23.11.1 Come configurare i numeri pilota CloudLink

Prerequisiti

Viene configurata la procedura guidata di CloudLink.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Servizi cloud**.
3) Fare clic su **Modifica** accanto a **Numeri pilota CloudLink**.
4) Fare clic su **Aggiungi**.
5) Sotto la colonna **Numeri pilota CloudLink** inserire i numeri richiesti.
6) Per ciascun numero, inserire un nome sotto la colonna **Nome visualizzato**.
7) Fare clic su **OK & Avanti**.
8) Se necessario, fare clic su **Elimina** o **elimina tutto** per eliminare una singola voce o tutte le voci, seguito da **OK** per confermare l'eliminazione.
9) Fare clic su **OK & Avanti**, quindi su **Fine**.

24 Accounting

Accounting comprende la registrazione dei dati di connessione, i codici dei progetti, il download e la visualizzazione dei dati delle connessioni e di controllo dei costi, oltre ad Accounting Tools.

24.1 Dati di connessione

I dati di connessione comprendono il rilevamento dei dati delle connessioni e dei codici di addebito.

24.1.1 Registrazione dei dati di connessione

Il sistema può registrare i dati di connessione delle sue linee utilizzate.

Per ogni connessione terminata o per ogni connessione in entrata viene registrato un record dei dati sulla connessione. Per ogni nuovo segmento temporale di una connessione (ad es. in seguito a trasmissione o inoltro ad un altro utente) viene registrato un record dati separato. Le connessioni interne non vengono registrate.

L'amministratore può attivare le opzioni seguenti per la rilevazione dei dati di connessione:

- Registrazione On o Off
- Durata della connessione
- Importo in denaro o unità tariffarie:

  La conversione delle unità tariffarie (scatti) in importi in denaro viene eseguita mediante il fattore tariffario configurabile (imposto in denaro per unità tariffaria).
- Formato decimale

  Divide l'importo in denaro per cento per visualizzare ad esempio 6 centesimi come 0,06
- Soppressione delle ultime quattro cifre del numero di destinazione
- Registrazione delle connessioni in entrata
- Chiamata in uscita senza connessione:

  Il chiamante riceve ad esempio una conferma della mancata risposta alla chiamata da parte dell'utente di destinazione (contrassegnata con la durata della connessione "00:00:00"). L'opzione è valida per i collegamenti ISDN e per tutti gli utenti.
- Protocollo di connessione

  Protocollo a inizio chiamata
- Registrazione dei numeri MSN
- Output del numero LCR in uscita o del numero di telefono composto in entrata
  - in uscita:

    il numero di telefono effettivamente inviato dal LCR alla PSTN
  - in entrata:

    Il numero interno originariamente selezionato

Se sono presenti costi di connessione già prima di realizzare la connessione (come ad esempio in Austria), vengono inclusi indipendentemente dall'attivazione della registrazione delle chiamate in uscita senza connessione attiva.

Il sistema tiene in considerazione le connessioni tramite linea QSIG solo se per queste è stato configurato un codice di linea.

Non avviene alcuna registrazione in caso di:

- in caso di interruzione anzitempo della selezione
- Connessioni non consentite (LCR, Liste nr.vietati).

Concetti correlati

Codici di addebito alla pagina 1208

24.1.1.1 Come attivare o disattivare la registrazione dei dati di connessione

Mediante la procedura guidata **Registrazione dettagli chiamata** è possibile attivare la registrazione dei dati di connessione.

Prerequisiti

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Registrazione dettagli chiamata**.
4) Selezionare una delle seguenti opzioni:
   - Per attivare la registrazione dei dati di connessione, selezionare la casella di controllo **Attiva registrazione di addebito chiamate**.
   - Per disattivare la registrazione dei dati di connessione, deselezionare la casella di controllo **Attiva registrazione di addebito chiamate**.
5) Fare clic su **OK & Avanti**, quindi su **Fine**.

24.1.1.2 Come attivare o disattivare la registrazione della durata connessione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Addebiti - Formato di output**.

4) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Messa a protocollo durata di chiam. on**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Messa a protocollo durata di chiam. on**.
5) Fare clic su **Applica**, quindi su **OK**.

24.1.1.3 Come configurare la registrazione degli importi in denaro o delle unità tariffarie (scatti)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Addebiti - Formato di output**.
4) Selezionare una delle seguenti opzioni:
   - Se si desidera che il sistema registri gli importi in denaro, selezionare la casella di controllo **Mostra importi e non scatti**.
   - Se si desidera che il sistema registri le unità tariffarie (scatti), deselezionare la casella di controllo **Mostra importi e non scatti**.
5) Fare clic su **Applica**, quindi su **OK**.

24.1.1.4 Come configurare il fattore tariffario, la valuta e la precisione del computer

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Fattori di addebito**.
4) Per ogni fascio in questione immettere nei campi **Moltiplicatore** e **Moltipl.ISDN** i valori corrispondenti.
5) Immettere il valore corrispondente nel campo **Valuta**, nella parte inferiore del modulo.

6) Per ogni fascio in questione con il protocollo QSIG, selezionare una delle seguenti opzioni, in linea con il sistema di comunicazione collegato:
   - Se occorre inviare e ricevere importi in denaro, selezionare la casella di controllo **Importo in denaro**.
   - Se è necessario ricevere e inviare unità tariffarie (scatti), deselezionare la casella di controllo **Importo in denaro**.
7) In ogni riga con un fascio con il protocollo QSIG, che riceve e invia unità tariffarie (scatti), nel campo **Valuta** inserire uno spazio.
8) Nell'elenco a discesa **Precisione del computer**, selezionare la voce **Nessun decimale**, **1 decimale**, **2 decimali**, **3 decimali** o **Sugli impulsi d'addebito**.
9) Fare clic su **Applica**, quindi su **OK**.

24.1.1.5 Come attivare o disattivare la registrazione delle ultime quattro cifre

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Addebiti - Formato di output**.
4) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Sopprimi ultime 4 cifre**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Sopprimi ultime 4 cifre**.
5) Fare clic su **Applica**, quindi su **OK**.

24.1.1.6 Come attivare o disattivare la funzione di messa a protocollo delle chiamate in uscita senza collegamento

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Addebiti - Formato di output**.

4) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **In uscita senza collegamento**.
   - Per disattivare la funzione, deselezionare la casella di controllo **In uscita senza collegamento**.
5) Fare clic su **Applica**, quindi su **OK**.

24.1.1.7 Come attivare o disattivare la registrazione delle connessioni in entrata

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Addebiti - Formato di output**.
4) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Protocollo delle chiamate in entrata**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Protocollo delle chiamate in entrata**.
5) Fare clic su **Applica**, quindi su **OK**.

24.1.1.8 Come attivare o disattivare il protocollo di connessione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Addebiti - Formato di output**.
4) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Protocollo di chiamata on**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Protocollo di chiamata on**.
5) Fare clic su **Applica**, quindi su **OK**.

24.1.1.9 Come attivare o disattivare la registrazione del MSN

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Addebiti - Formato di output**.
4) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Output del MSN on**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Output del MSN on**.
5) Fare clic su **Applica**, quindi su **OK**.

24.1.1.10 Come attivare o disattivare la funzione Formato decimale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Addebiti - Formato di output**.
4) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Formato decimale**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Formato decimale**.
5) Fare clic su **Applica**, quindi su **OK**.

24.1.2 Codici di addebito

I codici di addebito consentono l'assegnazione basata su progetti di dati e costi di connessione. Il sistema registra nei record di connessione corrispondenti i codici di addebito inseriti nel telefono dall'utente.

Il codice di addebito viene utilizzato assieme alla funzione di registrazione dei dati di connessione ed è a disposizione di ogni utente.

L'utente può immettere il codice di addebito nel telefono prima dell'inizio o dopo il termine della selezione. La composizione di un numero da un client non è possibile se è attivo il codice addebito.

Se durante una conferenza con utenti esterni viene inserito un codice di addebito, questo viene assegnato a tutte le connessioni/linee interessate.

L'amministratore può decidere se salvare o meno il codice di addebito per la ripetizione della selezione.

In una voce della rubrica personale è possibile salvare il codice del servizio Codice addebito + il codice addebito + il numero di telefono.

Procedura di immissione del codice addebito

L'amministratore definisce la procedura di immissione del codice addebito nel piano di composizione LCR:

- Forzato

  Il codice di addebito deve essere immesso prima dell'inizio della chiamata (prima o dopo l'impegno di un fascio).
- Facoltativo

  Il codice di addebito può essere immesso facoltativamente prima dell'inizio della chiamata. Nei telefoni IP client l'immissione è possibile anche durante una chiamata, anche in entrata.

Procedura di controllo del codice di addebito

Il sistema è in grado di verificare la validità di un codice di addebito inserito nei seguenti modi:

- Controllo delle liste

  Sono validi solo i codici di addebito predefiniti. Dopo aver immesso un codice di addebito valido, l'utente può continuare immediatamente la selezione. Il sistema rifiuta un codice di addebito non valido. Il display visualizza il messaggio "Voce errata" e il sistema emette un tono di mancato riconoscimento.
- Esame del numero di cifre

  Sono validi tutti i codici di addebito teoricamente possibili con il numero di cifre impostato. Dopo aver immesso un codice di addebito valido, l'utente può continuare immediatamente la selezione.
- Nessun controllo

  La validità del codice di addebito non viene controllata. I codici di addebito con meno di 11 cifre devono essere separati dalle altre cifre selezionate digitando "#". Con terminali ISDN questa variante richiede sempre il codice di addebito a 11 cifre, altrimenti la selezione non ha luogo.

Quando, durante una connessione, un utente determina che il codice di addebito assegnato ad una chiamata non è corretto, ne può immettere un altro, che andrà a sostituire quello corrente. La funzione di registrazione dei dati di connessione determina la creazione di un record dopo ogni segmento. Pertanto, i segmenti precedentemente conclusi vengono contrassegnati con il codice d'addebito precedente.

Concetti correlati

Registrazione dei dati di connessione alla pagina 1203

24.1.2.1 Come configurare un codice addebito

Mediante la procedura guidata **Registrazione dettagli chiamata** è possibile configurare il codice di addebito.

Prerequisiti

Si è connessi al WBM.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonia centrale**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Registrazione dettagli chiamata**.
4) In **Codici di addebito** immettere i codici di addebito nelle modalità descritte dalla procedura guidata.
5) Fare clic su **OK & Avanti**, quindi su **Fine**.

24.1.2.2 Come configurare la procedura di controllo del codice di addebito

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Addebiti chiamata - Codici di addebito**.
4) Nella riga dell'elenco codici addebito in questione, nell'elenco a discesa **Controllo**, selezionare la voce desiderata: **Nessun controllo**, **Controllo liste** o **Esame del numero di cifre**.
   a) Eventualmente, nell'elenco a discesa **Numero delle cifre da controllare**, selezionare il valore desiderato.
5) Fare clic su **Applica**, quindi su **OK**.

24.1.2.3 Come attivare o disattivare la funzione Ripetizione ultimo numero con PKZ

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Sistema** > **Flag di sistema**.

4) Selezionare una delle seguenti opzioni:

- Per attivare la funzione, selezionare la casella di controllo **Rip.ultimo nr. con PKZ**.
- Per disattivare la funzione, deselezionare la casella di controllo **Rip.ultimo nr. con PKZ**.

5) Fare clic su **Applica**, quindi su **OK**.

24.2 Visualizzazione e trasmissione dei dati di connessione

Sono disponibili diverse opzioni di visualizzazione dei dati di connessione nel display dei telefoni di sistema e di trasmissione degli stessi sotto forma di file.

24.2.1 Trasmissione degli addebiti (non per USA)

Il sistema può visualizzare sul display del telefono gli addebiti per i collegamenti esterni correnti comunicati dal gestore di rete.

Il gestore di rete deve supportare la visualizzazione degli addebiti mediante il servizio Advice Of Charge (AOC-D o AOC-S). Il sistema somma gli importi delle corrispondenti unità tariffarie.

L'addebito può essere visualizzato nei seguenti momenti:

- all'inizio e durante la chiamata (AOC-S)
- durante la chiamata (AOC-D)

Il parametro Precisione del computer consente all'amministratore di evitare imprecisioni nella registrazione dei dati relativi alla chiamata. La precisione del computer determina

- il numero di decimali utilizzato nella valutazione della durata della chiamata (importo in denaro minimo)
- l'importo massimo delle somme di denaro cumulative.

La precisione di calcolo impostata deve essere pari ad almeno quella dell'ISDN. Se il numero massimo di decimali, cioè tre, non è sufficiente, ha luogo un arrotondamento automatico. La precisione del computer può assumere i seguenti valori:

Precisione di calcolo	Importo in denaro minimo	Importo in denaro più elevato
Nessun decimale	1	approssimativamente. 4,3 miliardi
1 decimale	0,1	circa 430 milioni
2 decimali (ad esempio per l'Euro)	0,01	circa 43 milioni
3 decimali (ad esempio per la Sterlina inglese)	0,001	circa 4,3 milioni

24.2.1.1 Come configurare la trasmissione degli importi in denaro

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Fattori di addebito**.
4) Per ogni fascio desiderato, selezionare la voce **Avviso di addebito**, **durante la connessione**, **Al termine della connessione**, **durante/al termine della connessione** o **Nessun addebito**.
5) Nel menu a tendina **Precisione del computer**, nella parte inferiore del modulo, selezionare il numero di decimali che devono essere presi in considerazione.
6) Fare clic su **Applica**, quindi su **OK**.

24.2.2 Visualizzazione dei costi di connessione sul telefono

Il sistema può visualizzare sul display del telefono le informazioni sugli addebiti per l'attuale chiamata esterna sotto forma di importo in denaro.

Il sistema somma gli importi delle corrispondenti unità tariffarie. L'importo viene calcolato sulla base delle unità tariffarie (scatti) e del fattore tariffario configurati. Il provider di servizi deve supportare la funzionalità di addebito Advice of Charge (AOC).

Le informazioni sui costi di connessione possono essere trasmesse nei seguenti momenti:

- all'inizio e durante la chiamata (AOC-S)
- durante la chiamata (AOC-D)
- alla fine della chiamata (AOC-E)

Alla fine della connessione, il display visualizza l'addebito definitivo della connessione per circa 5 secondi, a condizione che l'utente non esegua un'altra operazione.

Con la richiamata alternata, vengono sempre visualizzati i costi di connessione per la connessione corrente.

Nel caso il trasferimento assistito abbia esito negativo, viene visualizzato e calcolato l’importo complessivo.

A un utente a cui sia stata trasferita una connessione, il sistema mostrerà e addebiterà solo i costi di connessione maturati a partire da quel momento.

24.2.3 Visualizzazione della durata della connessione sul telefono

Il sistema consente di visualizzare sul display del telefono la durata delle connessioni esterne in entrata e in uscita.

Formato HH:MM:SS.

Se la visualizzazione del tempo di connessione è disattivata, il display del telefono visualizza le informazioni sui costi di connessione della PSTN. Nel caso in cui non sia disponibile nessuna informazione sui costi di connessione, il display visualizza il numero di telefono dell'interlocutore, se noto.

24.2.3.1 Come attivare o disattivare la visualizzazione della durata connessione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Sistema** > **Display**.
4) Selezionare una delle seguenti opzioni:
   - Per attivare la funzione, selezionare la casella di controllo **Visualizzare la durata della chiamata**.
   - Per disattivare la funzione, deselezionare la casella di controllo **Visualizzare la durata della chiamata**.
5) Fare clic su **Applica**, quindi su **OK**.

24.2.4 Trasmissione dei dati di connessione

Il sistema è in grado di trasmettere i dati di connessione in un file tramite HTTPS.

È possibile analizzare il file trasferito con un programma adatto.

L'output continuo dei dati di connessione è possibile solo tramite CSTA.

Per i dati di connessione, l'amministratore può scegliere tra i seguenti formati (ASCII 8 bit):

- Formato compresso
- Formato non compresso

Formato compresso, predefinito

Ogni record dati di connessione in formato compresso contiene i seguenti campi separati dal carattere "|" e termina con CRLF:

Posizione del campo	Lunghez	Descrizione
1	8	Data conclusione della connessione
2	8	Ora conclusione della correzione
3	3	Numero linea occupato

Posizione del campo	Lunghez	Descrizione
4	16	Numero utente interno
5	8	Tempo avviso per connessione in entrata
6	8	Durata della connessione
7	max. 25	Numero di telefono esterno composto o ricevuto
8	11	Unità tariffaria/importo
9	2	Altre informazioni (ad esempio, in entrata, in uscita, connessioni trasferite, conferenza, DISA, addebiti per instaurazione connessione)
10	Max. 11	Codice add.
11	Max. 11	Solo con connessioni punto - multipunto: utente MSN
12	6	Access Code LCR (codice di accesso alla linea esterna)
13	2	Rotta LCR utilizzata, regola di composizione
14	25	Numero di telefono composto o ricevuto (opzionale)

Esempi per record di connessione:

- Connessione in uscita:

```
13.02.13|14:18:02|201|33388|00:02|00:00:07|0123456789||
1||||||
```

- Connessione in entrata:

```
13.02.13|14:28:02|202|33388|00:05|00:00:12|0123456789||
1|||||
```

Formato compresso, specifico USA

Ogni record dati di connessione in formato compresso contiene i seguenti campi separati dal carattere "|" e termina con CRLF:

Posizione del campo	Lunghez	Descrizione
1	8	Data conclusione della connessione
2	8	Ora conclusione della correzione
3	3	Numero linea occupato
4	16	Numero utente interno
5	8	Tempo avviso per connessione in entrata
6	8	Durata della connessione
7	max. 25	Numero di telefono esterno composto o ricevuto
8	11	Unità tariffaria/importo
9	2	Altre informazioni (ad esempio, in entrata, in uscita, connessioni trasferite, conferenza, DISA, addebiti per instaurazione connessione)

Posizione del campo	Lunghez	Descrizione
10	Max. 11	Codice add.
11	Max. 11	Solo con connessioni punto - multipunto: utente MSN
12	6	Access Code LCR (codice di accesso alla linea esterna)
13	2	Rotta LCR utilizzata, regola di composizione
14	2	PRI Nodal Service
15	1	PRI WATS band
16	3	PRI CIC
17	25	Numero di telefono composto o ricevuto (opzionale)

Nota: Nelle chiavi di registro *HKEY_LOCAL_MACHINE \SOFTWARE* relative a *Strumento di contabilità*, il valore di **DateFormat DWORD** deve essere impostato su 1 per il formato della data del Nord America (MM.GG.AA). Il valore predefinito è 0 e corrisponde al formato della data europeo/dell'America Latina (GG.MM.AA).

Nota: Le registrazioni dati di Accounting Manager in formato compresso sono separate dal delimitatore |. Questa opzione è configurabile solo tramite Manager E.

Formato non compresso

Il formato non compresso è adatto per la stampa. Inoltre, viene eseguito un avanzamento di pagina e viene generata una riga intestazione. Un record dati sulla chiamata in formato di output compresso contiene i seguenti campi separati dal carattere "|":

Posizione del campo	Posizione dei caratteri, lunghezza	Descrizione
1	1-8 (8)	Data conclusione della connessione: GG.MM.AA (GG = giorno: intervallo di valori 01 ... 31, MM = mese: intervallo di valori 01 ... 12, AA = anno: intervallo di valori 00 ... 99)
2	9-16 (8)	Ora al termine del segmento della connessione o una chiamata in arrivo non risposta: hh.mm.ss (hh = ore: intervallo di valori 00 ... 23, mm = minuti: intervallo di valori 00 ... 59, ss = secondi: intervallo di valori 00 ... 59)
3	17-19 (3)	Linea: numero della linea Valori consentiti: 1 ... 250

Posizione del campo	Posizione dei caratteri, lunghezza	Descrizione
4	20-35 (16)	Utenti: Numero utente interno Per le chiamate non risposte viene visualizzato sempre l'ultimo utente chiamato (ad esempio, gruppo di ricerca, deviazione di chiamata, inoltro di chiamata). In una chiamata di gruppo questo è l'ultimo utente registrato. Nelle chiamate risposte, viene indicato l'utente che ha risposto alla chiamata. Non viene visualizzato un prefisso RNR programmato (solo per connessione in rete). Se la numerazione interna viene convertita nel formato a 7 cifre, viene visualizzato il numero di telefono convertito. Il numero di telefono dell'utente interno può essere preceduto da un numero di telefono del nodo a 7 cifre. Se la somma del numero di telefono del nodo e del numero di telefono dell'utente è superiore a 7, vengono visualizzate solo le ultime 7 cifre del numero.
5	36-40 (5)	Durata chiamata per una connessione in entrata: mm:ss (mm = minuti: valori consentiti 00 ... 59, ss = secondi: valori consentiti 00 ... 59) Vengono visualizzati i dati all'arrivo delle chiamate, a condizione che nel sistema sia configurata l'uscita "Durata chiamata". In caso di overflow del contatore (durata > 59:59) viene visualizzato "59:59". Questo si può verificare ad esempio quando si modifica la data o l'ora mentre il sistema è in funzione. All'arrivo di una chiamata a un utente occupato, la durata della chiamata assume il valore "00:00".
6	41-48 (8)	Durata della connessione o segmento di connessione: hh:mm:ss (hh = ore: intervallo di valori 00 ... 23, mm = minuti: intervallo di valori 00 ... 59, ss = secondi: intervallo di valori 00 ... 59) Se in seguito a una chiamata non si è avuta nessuna connessione, vengono inseriti spazi vuoti. In caso di overflow del contatore (durata > 23:59:59) viene visualizzato "23:59:59".
7	49-73 (25)	Il numero di telefono composto, o se disponibile, il numero di telefono esterno ricevuto: nnnnnnnnnnnnnnnnnnnnnnnnn (n = cifre composte o ricevute: intervallo di valori consentiti 0 ... 9, *, #, ?) La visualizzazione viene generata con chiamate in ingresso e uscita, ove presenti. Con le chiamate in uscita, viene visualizzato il numero di telefono composto e, ove disponibile, il numero di telefono trasmesso. Con la funzione di protezione dei dati attivata, le ultime 4 cifre del numero vengono sostituite da "????". Se non è disponibile alcuna informazione relativa al numero, vengono visualizzati spazi vuoti.

Posizione del campo	Posizione dei caratteri, lunghezza	Descrizione
8	74-84 (11)	Unità tariffarie per un segmento di connessione: ccccccccccc (c = cifra: valori consentiti 0 ... 9) È possibile scegliere fra unità tariffarie (scatti) e importi in denaro. La conversione delle unità tariffarie (scatti) in importi in denaro avviene sulla base del fattore tariffario, che viene determinato sotto forma di importo in denaro (incluso un supplemento eventualmente necessario) per unità tariffaria. Per l'impostazione del fattore tariffario, si applica quanto segue: • con precisione di calcolo: fattore tariffario = 100% + supplemento eventualmente necessario • senza precisione di calcolo: fattore tariffario = importo/unità + supplemento eventualmente necessario A seconda della precisione di calcolo, i costi di connessione vengono registrati con o senza supplemento. Viene sempre prodotto un output quando una sezione della connessione genera un addebito (ad esempio, anche nelle chiamate trasferite).

Posizione del campo	Posizione dei caratteri, lunghezza	Descrizione
9	85-86 (2)	Elemento informativo: informazioni supplementari Valori consentiti 0 ... 9 Significato: • 1 = connessione in entrata (chiamata vocale / audio 3.1 kHz) • 2 = connessione in uscita (chiamata vocale / audio 3.1 kHz) • 3 = connessione in entrata (servizio generale) • 4 = connessione in uscita (servizio generale) • 5 = connessione in entrata inoltrata • 6 = connessione in uscita inoltrata • 7 = conferenza int/est/est con connessione in entrata / transito mediante trasferimento verso l'esterno • 8 = conferenza con connessione in uscita / transito mediante trasferimento verso l'sterno • 9 = connessione in uscita tramite deviazione di chiamata verso destinazione esterna • 0 = info connessione (elenco chiamate), viene visualizzata immediatamente all'arrivo di una chiamata (la visualizzazione può essere soppressa). Ad esempio è possibile eseguire una ricerca nel database da un PC. Nel caso vengano chiamati più utenti, viene visualizzata una riga per ogni utente (senza durata della chiamata, durata della connessione, informazioni sull'addebito). • +10 = offset identificativo per chiamate in lista nera • +20 = offset identificativo per i costi di instaurazione della connessione (senza durata della connessione) • +30 = offset identificativo per il set di dati seguente in – Durata della connessione > 24 h. – sessioni di connessione continue con lo stesso numero utente/ linea (ad esempio dopo il trasferimento di una connessione, dopo l'annullamento di una conferenza). • +40 = offset per un set dati con identificativo di transito (tramite un interno del sottosistema). Può essere riscontrato in combinazione con offset +30. • +50 = offset identificativo per connessioni DISA • +70 = combinazione dell'offset +30 e +40
10	87-97 (11)	Codice addebito inserito dall'utente per questa connessione: aaaaaaaaaaa (a = cifra del codice di addebito: valori consentiti 0 ... 9) Le cifre mancanti vengono sostituite da spazi.
11	98-108 (11)	Utente MSN: mmmmmmmmmmm (m = cifra del numero MSN: valori consentiti 0 ... 9) La visualizzazione avviene se l'utente ha configurato il tasto MSN. Con le connessioni in uscita di un utente MULAP viene visualizzato il numero di telefono del MULAP occupato. Le cifre mancanti vengono sostituite da spazi.

Posizione del campo	Posizione dei caratteri, lunghezza	Descrizione
12	109-113 (5)	Codice impegno utilizzato, codice di accesso: bbbbb (b = cifra del codice di impegno: valori consentiti 0 ... 9)
13	114-115 (2)	Rotta LCR utilizzata: rr (r = cifra della rotta scelta: valori consentiti 0 ... 9)

Sequenza comunicazione

Può essere richiesta la trasmissione dei dati di connessione (richiesta di download), alla quale il sistema reagisce di conseguenza (risposta per download).

Successivamente è possibile chiedere la cancellazione dei dati della connessione (Delete Request), alla quale il sistema reagisce di conseguenza (Download Response).

Richiesta di download - Definizione

Elemento	Indice
Intestazione HTTP	Metodo richiesta = GET
URL	https://<Indirizzo IP del sistema>/management/portlet
Parametri	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=get
	nome utente=<nome utente>
	password=<password>

Nota: Quando si accede ai dati di addebito con l'interfaccia di riferimento, vengono applicate restrizioni alle richieste HTTP GET. I seguenti caratteri speciali non possono essere utilizzati nella password, quando si tenta di ottenere dati tramite la richiesta URL:

:/?#[]@ !$&'()*+,;=

Esempio:

```
https://192.148.108.151/management/portlet/?portlet=
hipath-
accountingdownload::HiPathAccountingDownloadPortlet&
entity=accounting&action=get&username=xbert@system&
password=not4u;-)
```

Risposta di download - Definizione

Elemento	Indice
Intestazione HTTP	ContentType = "text/plain"
Parametri	nomefile allegato = "<charging file>"
	data=<content of the charging file>

Codice di risposta	Significato
SC_OK(200)	Riuscito
SC_BAD_REQUEST(400)	Parametro mancante nella richiesta
SC_UNAUTHORIZED(401)	Errore durante l'accesso o nome utente o password errati
SC_INTERNAL_SERVER_ERROR(500)	Errore interno

Cancellazione richiesta - Definizione

Elemento	Indice
Intestazione HTTP	Metodo richiesta = POST
URL	https://<Indirizzo IP del sistema>/management/portlet
Parametri	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=delete
	nome utente=<nome utente>
	password=<password>

Esempio:

```
https://192.148.108.151/management/portlet/?portlet=
hipath-
accountingdownload::HiPathAccountingDownloadPortlet&
entity=accounting&action=get&username=xbert@system&
password=not4u;-)
```

Cancellazione risposta - Definizione

Codice di risposta	Significato
SC_OK(200)	Riuscito
SC_BAD_REQUEST(400)	Parametro mancante nella richiesta
SC_UNAUTHORIZED(401)	Errore durante l'accesso o nome utente o password errati
SC_INTERNAL_SERVER_ERROR(500)	Errore interno

Concetti correlati

Accounting Tools alla pagina 1223

24.2.4.1 Come selezionare il formato

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Addebiti - Formato di output**.
4) Selezionare una delle seguenti opzioni:
   - Se si desidera utilizzare il formato compresso, selezionare la casella di controllo **Formato di output compresso**.
   - Se si desidera utilizzare il formato non compresso, deselezionare la casella di controllo **Formato di output compresso**.
5) Fare clic su **Applica**, quindi su **OK**.

24.2.4.2 Come attivare o disattivare la trasmissione dei dati delle connessioni tramite HTTPS

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Addebiti** > **Addebiti - Formato di output**.
4) Nell'elenco a discesa **Output**, selezionare una delle seguenti opzioni:
   - Se si desidera attivare la funzione, selezionare la voce **HTTPS**.
   - Se si desidera disattivare la funzione, selezionare la voce **Nessuno**.
5) Fare clic su **Applica**, quindi su **OK**.

24.3 Controllo dei costi

Per il controllo dei costi sono disponibili i servizi Informazioni su rotte a tariffe costose e Protezione da frodi legate all'utilizzo delle linee esterne.

24.3.1 Notifica dell'utilizzo delle rotte a tariffe più elevate

Nel caso in cui la destinazione della chiamata selezionata non sia momentaneamente raggiungibile attraverso una rotta a tariffa conveniente, il telefono è in grado di notificare all'utente l'utilizzo di una rotta a tariffa più elevata.

L'utente potrà così decidere se effettuare o meno la connessione in questo momento nonostante la rotta a tariffa elevata. La notifica può avvenire in diversi modi:

- Testo sul display
- Tono
- Testo sul display e tono

Il sistema notifica all'utente l'utilizzo di una rotta a tariffa più elevata se nella tabella dei collegamenti è impostata una tale notifica e non utilizza il fascio dell'indice 1 della tabella dei collegamenti.

La notifica sul display viene visualizzata solo se per la regola di composizione corrispondente non è stato configurato nessun nome. In caso sia stato configurato un nome, questo viene visualizzato.

24.3.1.1 Come configurare un avviso rotta a tariffa elevata

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Telefonia** > **LCR**.
3) Nella struttura dei menu fare clic su **Routing** > **LCR** > **Tabella delle rotte** e sulla tabella delle rotte corrispondente.
4) Per ogni percorso di connessione a tariffa più alta, (colonna **Fascio**) selezionare nell'elenco a discesa **Avviso** la voce desiderata: **Tono**, **Display** o **Display + Tono**.
5) Fare clic su **Applica**, quindi su **OK**.

24.3.2 Protezione da frodi tariffarie

Il sistema è in grado di monitorare le connessioni per individuare una possibile frode tariffaria (Toll Fraud Monitoring). Questo controllo viene effettuato sulle connessioni che entrano attraverso una linea urbana per poi uscire nuovamente attraverso una linea urbana.

Il primo utente segnala il superamento della durata impostata per la chiamata e consente, se necessario, di interrompere la chiamata. L'amministratore può determinare se e quando deve essere segnalata una connessione di questo tipo.

24.3.2.1 Come attivare o disattivare la protezione dall'abuso dell'utilizzo delle linee urbane

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Sistema** > **Temporizzazioni**.
4) Selezionare una delle seguenti opzioni:
   - Se si desidera attivare la protezione da frodi sull'utilizzo delle linee urbane, selezionare **Tempo di controllo del traffico di transito** nel menu a tendina **Base** la voce desiderata e inserire nel campo **Fattore** un valore diverso da 255. **Base** * **Fattore** è il tempo di connessione trascorso il quale viene segnalata una connessione potenzialmente fraudolenta.
   - Per disattivare la protezione da frodi sull'utilizzo delle linee urbane, inserire in **Tempo di controllo del traffico di transito** nel campo **Fattore** il valore 255.
5) Fare clic su **Applica**, quindi su **OK**.

24.4 Accounting Tools

Accounting Tools contiene Accounting Manager e Teledata Office.

Concetti correlati

Centro assistenza – Documenti alla pagina 128
Trasmissione dei dati di connessione alla pagina 1213

24.4.1 Accounting Manager

Accounting Manager è un'applicazione Windows per il recupero dei dati relativi alle connessioni tramite HTTPS e comprendente anche funzionalità di analisi mediante tabelle e grafici.

Accounting Manager è fornito con una propria documentazione. Accounting Manager richiama i dati relativi alle connessioni dei singoli nodi. È possibile utilizzare Accounting Manager anche per testare l'interfaccia utilizzata per i dati di connessione. È possibile scaricare Accounting Manager dal**Centro assistenza** del WBM. Accounting Manager richiede il possesso dei diritti di amministratore locale e l'attivazione di TLS 1.2 in Microsoft Internet Explorer.

24.4.2 TeleData Office

TeleData Office è un'applicazione Windows per l'analisi dei dati di connessione.

25 Manutenzione

Il sistema fornisce diverse funzionalità di manutenzione. Tra queste vi sono: modifica delle impostazioni di telefonia, backup e ripristino dei dati di configurazione, aggiornamento e upgrade del software, funzioni Ricarica / Riavvia. Oltre a ciò, comprende funzioni quali il rilevamento dello stato, il monitoraggio e la manutenzione. Il sistema supporta funzionalità di accesso remoto e offre diverse possibilità di assistenza remota.

Manutenzione dell'UC Booster Server

Se oltre al sistema di comunicazione, viene usato un UC Booster Server, quest'ultimo offre diverse opzioni di manutenzione. Per la manutenzione dell'UC Booster Server, l'amministratore non deve inserire l'indirizzo IP del sistema di comunicazione quando richiama il WBM, ma l'indirizzo IP del server Linux.

25.1 Configurazione telefonia

Il sistema di comunicazione offre diverse possibilità di configurazione per la telefonia, ad esempio, data e ora, SNTP, display personalizzato e musica su attesa.

25.1.1 Data e Ora

Il sistema di comunicazione è dotato di un orologio di sistema con data e ora myPortal for Desktop e i display di tutti i terminali visualizzano questo orario.

Per impostare o sincronizzare l'ora di sistema, esistono le seguenti possibilità:

- mediante un server dell'ora SNTP
- mediante una linea ISDN tramite una chiamata in uscita
- mediante impostazione manuale

Una volta attivato un server SNTP non è più possibile eseguire alcuna impostazione personalizzata dell'orologio di sistema.

Nel caso in cui un server SNTP non dovesse essere raggiungibile e i telefoni di sistema HFA utilizzino un'origine ora diversa da quella del sistema, l'ora visualizzata nei telefoni può essere diversa da quella del sistema.

L'orario di sistema impostato manualmente dopo l'inizializzazione del sistema viene sempre sovrascritto dalle informazioni sull'orario ISDN ottenute durante la prima chiamata ISDN in uscita, a condizione che il gestore della rete trasmetta tale informazione. Se la differenza tra l'orario di sistema impostato manualmente e le informazioni sull'orario ISDN di un sistema in funzione si colloca tra i 2 e i 70 minuti, il sistema applica le informazioni di orario ISDN. In caso contrario viene mantenuto l'orario di sistema impostato manualmente.

L'amministratore può scegliere per la rappresentazione della data sul display del telefono tra i seguenti formati. Il formato dipende inoltre dal tipo di telefono:

Formato della data	OpenStage	optiPoint 410, optiPoint 420
Europa	Ma 20.11.07	20 NOV 07

Formato della data	OpenStage	optiPoint 410, optiPoint 420
USA	Ma 11/20/07	Ma NOV 20.07
International1	Ma 20.11.07	MA 20 NOV 07
International2	Ma 20.11.07	MA 20.11.07

Se l'amministratore del sistema imposta inavvertitamente una data precedente al 2007, il sistema non consentirà più l'accesso al WBM. Dopo un riavvio sarà di nuovo possibile reimpostare la data 01.01.2007.

25.1.1.1 Come configurare manualmente data e ora

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Procedere come descritto di seguito se il sistema non ottiene la data e l'ora tramite linee digitali o SNTP.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Server telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu, fare clic su **Impostazioni di base** > **Data e ora** > **Data e ora**.
4) Indicare la **Data e Ora**.
5) Fare clic su **Applica**.
6) Fare clic su **Disconnetti**.
7) Disconnettersi dal WBM e accedere di nuovo.

25.1.1.2 Come impostare il fuso orario

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Server telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu, fare clic su **Impostazioni di base** > **Data e ora** > **Impostazioni delle zone orarie**.
4) Nell'elenco a discesa selezionare la **Zona oraria**.
5) Fare clic su **Applica**.
6) Disconnettersi dal WBM e accedere di nuovo.

25.1.1.3 Come configurare il formato data

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Server telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Sistema** > **Display**.
4) Nell'elenco a discesa selezionare il **Formato data**.
5) Fare clic su **Applica**.

25.1.2 SNTP

Tramite SNTP è possibile sincronizzare la data e l'ora del proprio sistema mediante server di riferimento ora NTP.

L'SNTP (Simple Network Time Protocol) è una versione semplificata dell'NTP (Network Time Protocol), uno standard per la sincronizzazione di data e ora mediante reti di comunicazione basate su pacchetti. Per sincronizzare la data e l'ora è necessario che il sistema disponga di un collegamento ad un server NTP. Questo collegamento può avvenire nella rete locale o in Internet. Internet offre una vasta gamma di server NTP a cui è possibile accedere liberamente e consente di scegliere un server situato nella propria zona oraria. Attenersi alle condizioni di utilizzo del server scelto e, se necessario, richiedere l'autorizzazione.

25.1.2.1 Fare riferimento alla data e all'ora di un server SNTP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nell'area di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu, fare clic su **Impostazioni di base** > **Data e ora** > **Impostazioni di SNTP**.
4) Inserire l'**Indirizzo IP/Nome DNS del server di riferimento orario esterno**, ad esempio, `0.de.pool.ntp.org`.
5) Nell'elenco a discesa **Stato amministrativo del server SNTP**, fare clic sulla voce **Attivato**.
6) Nel menu a discesa**Tempo di polling del server dell'ora esterno**, selezionare l'intervallo di tempo desiderato per ottenere la data e l'ora dal server SNTP.
7) Fare clic su **Applica**.
8) Disconnettersi dal WBM e accedere di nuovo.

25.1.3 Loghi del telefono

I telefoni di sistema con display possono mostrare il logo specifico del cliente sullo sfondo dell'interfaccia di telefonia.

L'amministratore può importare, assegnare, o eliminare i loghi dai telefoni di sistema con display. I diversi tipi di telefoni di sistema possono utilizzare loghi diversi.

Concetti correlati

Aggiornamento dei telefoni del sistema alla pagina 1255

25.1.3.1 Come caricare un logo del telefono nel sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Il file immagine con il logo del telefono soddisfa i seguenti requisiti:

Telefono	Formato	Colore
OpenStage 40	112 x 32, BMP	monocromatico
OpenStage 60 OpenStage 80	240 x 71, JPEG	monocromatico o a colori
OpenScape Desk Phone CP 400 OpenScape Desk Phone CP 400T/405T	112 x 32, BMP	monocromatico
OpenScape Desk Phone CP 600/700/700X OpenScape Desk Phone CP 710	220 x 70, PNG	24 bit con alfa (trasparenza)
OpenScape Desk Phone CP 600E	220 x 70, PNG	24 bit con alfa (trasparenza) o 256 scala di grigi con alfa

Si ha accesso ai file immagine con il logo del telefono nel file system del PC di amministrazione.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Manutenzione** > **Immagine del software**.
3) Nella struttura dei menu, fare clic su **Loghi immagine telefono** > **Carica**.
4) Fare clic su **Sfoglia** per selezionare un file immagine corrispondente.
5) Fare clic su **Carica**.

25.1.3.2 Come distribuire un logo per telefono ai telefoni di sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Immagine del software**.
3) Nella struttura dei menu, fare clic su **Loghi immagine telefono** > **Distribuire**.
4) Nella riga delle immagini dei loghi del telefono da distribuire, selezionare la casella di controllo **Distribuire**.
5) Nell'elenco a discesa **Distribuisci ai workpoint con il tipo periferica selezionato**, selezionare il tipo di telefono di sistema desiderato.
6) Fare clic su **Applica**.

25.1.3.3 Come eliminare il logo dei telefoni

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Si ha accesso ai file immagine con il logo del telefono nel file system del PC di amministrazione.

Per rimuovere un logo dal sistema di comunicazione, procedere come segue:

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Immagine del software**.
3) Nella struttura dei menu, fare clic su **Loghi immagine telefono** > **Carica**.
4) Nella riga dei loghi del telefono da eliminare, selezionare la casella di controllo **Cancella**.
5) Se si desidera eliminare altri loghi telefono, ripetere il passo precedente.
6) Fare clic su **Cancella**. Tutti i loghi del telefono selezionati vengono cancellati dal sistema di comunicazione.

25.1.4 Display personalizzato

Il display personalizzato consente ad esempio la visualizzazione del nome società nel display del telefono di sistema allo stato inattivo.

Può essere modificata soltanto la parte destra (max. 18 caratteri) della seconda riga del display, predefinita con la visualizzazione "OpenScape". Il testo viene disposto sotto la data, se la lunghezza del medesimo lo consente.

```
16:30       VE 29 FEB 08          123456  Hotel Posta >
```

25.1.4.1 Come modificare il display personalizzato (nome del sistema)

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Gateway**.
4) Nel campo **Nome del sistema** immettere il nome che si desidera visualizzare.

   Nota: Utilizzare esclusivamente i caratteri A-Z, a-z e 0-9.

5) Fare clic su **Applica**, quindi su **OK**.

25.1.5 Testo in più lingue

La lingua dei messaggi a display può essere impostata per tutto il sistema o per apparecchi singoli.

Lingue disponibili: cinese, danese, tedesco, inglese, estone, finlandese, francese, greco, italiano, catalano, lettone, lituano, olandese, norvegese, polacco, portoghese, russo, svedese, serbocroato, slovacco, sloveno, spagnolo, tedesco (Telecom), ceco, turco, ungherese, inglese (USA), serbo, bulgaro, rumeno e macedone.

L'impostazione della lingua viene eseguita all'avvio del sistema quando si inserisce il codice di inizializzazione del paese.

Concetti correlati

Configurazione degli utenti alla pagina 443

Attività correlate

Come configurare utenti IP e SIP alla pagina 196

25.1.6 Menu Flexible

I Menu Flexible consentono la personalizzazione delle opzioni del menu nel display dei telefoni del sistema.

Accedendo come amministratore, è possibile mostrare o nascondere le singole opzioni dei menu.

25.1.6.1 Come modificare Menu Flexible

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu fare clic su **Impostazioni di base** > **Sistema** > **Menu Flexible**.
4) Modificare la **Lista di mascheramento** come segue:
   - Per nascondere un'opzione del menu, selezionare la relativa casella di controllo.
   - Per mostrare un'opzione del menu, deselezionare la relativa casella di controllo.
5) Fare clic su **Applica**, quindi su **OK**.

25.1.7 Musica su attesa

Durante le procedure svolte al posto operatore, il sistema di comunicazione è in grado di riprodurre musica su attesa (Music On Hold, MOH) per gli utenti in attesa. I motivi musicali, se la funzione è configurata, vengono trasmessi ai chiamanti che si trovano in stato di attesa di consultazione, parcheggio o trasferta. Ciò si applica anche per i chiamanti nella coda di attesa della distribuzione chiamate.

Il sistema può riprodurre musica su attesa dalle seguenti fonti:

- Musica su attesa (MOH)
- EXMR

  Vedere Installazione di OpenScape Business X1/X1W, Documentazione di manutenzione o Installazione OpenScape Business X3/X5/X8, Documentazione di manutenzione.
- Modulo plugin MUSIC

  Vedere Installazione di OpenScape Business X1/X1W, Documentazione di manutenzione o Installazione OpenScape Business X3/X5/X8, Documentazione di manutenzione.
- Modulo MPPI-USB EXM (solo per OpenScape Business X3/X5)

  Vedere Installazione di OpenScape Business X3/X5/X8, Documentazione di manutenzione.

File audio

L'amministratore può trasferire i file audio per la musica su attesa interna dal PC al sistema di comunicazione al fine di utilizzarli come musica su attesa interna alternativa.

Nota: Prima di utilizzare annunci o musica su attesa di altre fonti, assicurarsi di non infrangere alcun copyright.

Importante: Se l'utente in attesa è un client Workpoint IP o una linea esterna IP, si utilizza il MoH interno. Il MoH esterno non è inteso per l'uso con IP.

I file audio devono essere disponibili come file `wave` con le seguenti proprietà:

- 16 bit PCM
- Mono o Stereo
- Frequenze campione consentite: 8/22.05/24/32/40/44.1 o 48 kHz.
- Lunghezza massima del nome del file audio: 30 caratteri

Consigliato: **16 bit PCM - Mono - 8 kHz, lunghezza circa 2 min**

Musica su attesa (MOH)

Per i servizi notte e giorno, possono essere configurate musiche su attesa diverse.

Nota: Per UC Suite non c'è differenza fra file musica su attesa giorno e notte. Viene usato il **file musica su attesa giorno**.

L'amministratore può configurare le seguenti funzioni:

- Musica su attesa con tono di chiamata (segnale di libero):

  Durante la consultazione, all'utente in attesa viene trasmessa innanzitutto la musica su attesa. Dopo il trasferimento dell'utente in attesa alla destinazione, viene riprodotto lo squillo anziché la musica su attesa.
- Musica su attesa senza tono di chiamata (segnale di libero):

  all'utente in attesa viene trasmesso un motivo musicale fino a che l'utente chiamato non risponde.
- Nessuna musica su attesa:

  l'utente in attesa non sente niente (silenzio). Se una chiamata esterna viene trasferita mediante la funzione Trasferta rapida, al chiamante viene trasmesso il segnale di libero.

25.1.7.1 Come importare musica su attesa

Con la procedura guidata **Musica su attesa/annunci** è possibile importare file audio come musica di attesa interna nel sistema di comunicazione.

Prerequisiti

Si è connessi al WBM.

I file audio da riprodurre sono disponibili come file WAVE nel formato richiesto.

Nota: Prima dell'uso assicurarsi di non violare alcun copyright.

Nota: Per UC Suite non vi è alcuna distinzione tra i file giorno e notte. Viene utilizzato il **File musica su attesa giorno**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.

2) Nella struttura di navigazione fare clic su > **Procedure guidate**Telefonia centrale.

3) Fare clic su **Modifica** per avviare la procedura guidata **Musica su attesa/ annunci**.
4) In **File musica su attesa giorno** per il servizio giorno o **File musica su attesa notte** per il servizio notte, fare clic su **Sfoglia**.
5) Selezionare un file audio, quindi fare clic su **Apri**. Il percorso per il file audio viene visualizzato in **File musica su attesa giorno** e/o **File musica su attesa notte**.
6) Fare clic su **Carica**.
7) Confermare il messaggio con **OK** e fare clic su **OK & Avanti**.
8) Fare clic su **Fine**.

25.1.7.2 Come configurare la funzione della musica su attesa interna

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Il nome del file della musica su attesa può avere una lunghezza massima di 30 caratteri.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Interfacciamento**.
3) Nella struttura dei menu fare clic su **Interfacce** > **Annunci / Musica su attesa**.
4) Nell'area **Musica su attesa**, nell'elenco a discesa **Tipo musica di attesa** selezionare la voce **Nessuna musica su attesa**, **MOH senza tono di chiamata** o **MOH con tono di chiamata**.
5) Fare clic su **Applica**, quindi su **OK**.

25.1.7.3 Come modificare la musica su attesa interna per ogni gruppo con restrizioni di traffico

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia > Interfacciamenti**.
3) Nella struttura dei menu fare clic su **Interfacciamenti > Annunci / Musica su attesa interna**.
4) Fare clic sulla Scheda **Modifica musica su attesa**.
5) Nella riga del corrispondente del gruppo con restrizioni di traffico, nell'elenco a discesa File audio, selezionare la musica su attesa desiderata.
6) Se a un gruppo con restrizioni di traffico non è associata musica su attesa, per tale gruppo verrà riprodotta la musica su attesa degli utenti interni
7) Nella riga corrispondente del gruppo con restrizioni di traffico, inserire una Descrizione.
8) Fare clic su **Applica**.

9) Fare clic su **OK**.

Nota: Questa funzionalità è applicabile solo ai sistemi OpenScape Buisness S e non è supportata da OpenScape Business X.

25.1.8 Annunci

Il sistema di comunicazione consente di riprodurre annunci di attesa per i chiamanti prima di rispondere a una chiamata e anche quando si utilizza la distribuzione delle chiamate e la selezione diretta DTMF. In alcune situazioni è possibile sostituire la melodia MOH con un annuncio, ad esempio se un utente viene messo in attesa o se è occupato o instradato.

Il sistema può importare annunci dalle seguenti fonti:

- Annunci interni
- Lettore di annunci (solo con funzionalità UC Booster)

  il lettore di annunci è un programma software interno disponibile insieme alla funzionalità UC Booster (UC Booster Card o UC Booster Server). Quando si chiama un abbonato, il lettore di annunci riproduce prima l'annuncio desiderato e poi stabilisce la connessione con l'abbonato.
- Dispositivo per annunci analogico

  Vedere la sezione Apparecchiature ausiliarie - Dispositivo per annunci analogico nella *Documentazione per l'amministratore di OpenScape Business*.
- Modulo MPPI USB EXM (solo per OpenScape Business X3/X5)

  Per ulteriori informazioni, vedere la sezione *Installazione di OpenScape Business X3/X5/X8, Documentazione di servizio*.

L'amministratore può configurare gli annunci per la riproduzione singola (avvio/arresto) o continua.

Un dispositivo di annuncio esterno deve comportarsi come una stazione, ossia annunciarsi, riprodurre l'annuncio e commutare la chiamata (entrare in attesa di consultazione, comporre e riagganciare).

File audio

L'amministratore può trasferire i file audio con gli annunci dal PC al sistema di comunicazione.

Nota: Prima di utilizzare annunci o musica da altre fonti, assicurarsi di non violare alcun copyright.

I file audio devono essere disponibili come file `Wave` con le seguenti proprietà:

- PCM a 16 bit
- Mono o stereo
- Frequenze di campionamento possibili: 8 / 22,05 / 24 / 32 / 40 / 44,1 o 48 kHz
- Lunghezza massima del nome del file audio: 30 caratteri

Raccomandato: **PCM a 16 bit - Mono - 8 kHz, durata circa 2 minuti**

25.1.8.1 Come configurare gli annunci (UC Suite & UC Booster)

La procedura guidata **Musica su attesa/Annunci** può essere utilizzata anche per configurare gli annunci.

Prerequisiti

- In **Modalità Esperto > Middleware > Lettore di annunci**, selezionare la casella di controllo **Il servizio verrà avviato automaticamente** per abilitare il lettore di annunci.
- Il numero di chiamata di un lettore di annunci deve essere impostato in **Modalità Esperto in > Impostazioni di base > Casella vocale / Lettore di annunci**.
- Verificare che il numero sia configurato correttamente in **Modalità Esperto > LCR > Piano di composizione**, nel campo **Lettore annunci**.
- La **Tabella di instradamento** è impostata su **12**, **UC Suite** è impostato per il **Percorso** e **MEB** è impostato per **Regola di composizione**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.

2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonai centrale**.

3) Fare clic su **Modifica** per avviare la procedura guidata **Musica su attesa/ Annunci**.

4) Saltare la selezione di **Carica file per musica su attesa tramite file HTTP**, facendo clic su **OK & Avanti**.

> **Nota:** Prima di utilizzare annunci o musica, assicurarsi di non violare alcun copyright.

5) Per trasferire un file audio al sistema di comunicazione, procedere come segue:

a) Fare clic su **Scegli file**.
b) Selezionare un file audio.
c) Fare clic su **Apri**.
d) Fare clic su **Carica**.
e) Confermare il messaggio con **OK**.
f) Se si desidera caricare altri file audio sul sistema, ripetere questi passaggi.

6) Fare clic su **OK & Avanti**.

> **Suggerimento:** Sono descritti anche i parametri di configurazione degli **annunci**, che possono essere configurati tramite **Modalità esperto > Apparecchiature ausiliarie > Annunci**.

7) Selezionare il tipo di annuncio da riprodurre nella colonna **Tipo**.

8) Selezionare la porta a cui è collegato il dispositivo nella colonna **Accesso**. Le destinazioni esterne possono essere utilizzate per indirizzare i dispositivi di annuncio in un altro nodo del sistema.
9) Selezionare un file di annuncio dall'elenco a discesa nella colonna **File wave** (solo per il tipo **Lettore di annunci** e in modalità UC Suite).
10) Selezionare il tipo di riproduzione dall'elenco a discesa nella colonna **Modalità**.
11) Fare clic su **OK & Avanti**, quindi su **Fine**.

25.1.8.2 Come configurare gli annunci (UC Smart)

La procedura guidata **Musica su attesa/Annunci** può essere utilizzata anche per configurare gli annunci.

Prerequisiti

Alle porte analogiche impostate come porte di annuncio deve essere assegnato il valore **Segreteria telefonica** in **Tipo di interno**.

Le porte EVM impostate come porte di annuncio dovrebbero essere:

- avere il valore **Standard** in **Tipo di interno** assegnato.
- rimosse dal gruppo di ricerca della casella vocale.
- avere una casella vocale assegnata per il numero di chiamata della porta in modalità Esperto **Modalità Esperto > Apparecchiature ausiliarie > Smart VM**.

Passo a passo

1) Nella barra di navigazione fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Telefonai centrale**.
3) Fare clic su **Modifica** per avviare la procedura guidata **Musica su attesa/ Annunci**.
4) Saltare la selezione di **Carica file per musica su attesa tramite file HTTP**, facendo clic su **OK & Avanti**.

Suggerimento: I parametri di configurazione per gli **Annunci** sono descritti e possono essere configurati tramite Modalità Esperto > Apparecchiature ausiliarie > Annunci.

---

5) Selezionare il tipo di annuncio da riprodurre nella colonna **Tipo**.
6) Selezionare la porta a cui è collegato il dispositivo nella colonna **Accesso**. Le destinazioni esterne possono essere utilizzate per indirizzare i dispositivi di annuncio in un altro nodo del sistema.
7) Selezionare un file di annuncio dall'elenco a discesa nella colonna **File wave** (solo per il tipo **Lettore di annunci** e in modalità UC Suite).
8) Selezionare il tipo di riproduzione dall'elenco a discesa nella colonna **Modalità**.
9) Fare clic su **OK & Avanti**, quindi su **Fine**.

25.1.9 Segnalazione da utente a utente

Il sistema di comunicazione consente di trasmettere in modo trasparente i messaggi tra i vari terminali (User to User Signalling, UUS). Il sistema supporta anche la variante UUS1 per lo scambio di informazioni nei messaggi di controllo in sede di creazione e conclusione della connessione.

In caso di connessione a più terminali è necessario garantire che il messaggio alla chiamata in entrata venga trasmesso al massimo da un terminale.

25.1.10 Protezione da segnalazione su canale fonia

Il sistema di comunicazione offre un sistema di protezione contro la contraffazione dei dati mediante l'emissione di toni indesiderati nel canale di fonia che può essere configurata dall'amministratore. L'inclusione in una conversazione con tale protezione non è possibile. Tutti gli utenti configurati come fax dispongono automaticamente di questa protezione da segnalazione.

Le richiamate vengono differite fino a che gli interni non risultano liberi.

Un apparecchio in attesa è sempre protetto da segnalazione

25.1.11 Temporizzazioni

Il sistema di comunicazione offre all'amministratore la possibilità di impostare diverse temporizzazioni, come ad es. la durata della richiamata automatica o il tempo di ripetizione automatica dell'ultimo numero selezionato.

Le temporizzazioni sono preimpostate nel sistema di comunicazione e di norma non devono essere modificate.

25.1.12 Controllo dei servizi Centrex

Per il controllo dei servizi Centrex, è necessario trasmettere i caratteri di composizione * e # su ISDN e all'ITSP.

Accendendo come amministratore, è possibile attivare o disattivare questo servizio.

Il codice deve essere immesso durante la selezione del numero (ad esempio dopo l'immissione del codice di linea). L'immissione di valori inizia sempre con * o #, seguiti da una cifra o una combinazione di cifre, quindi termina con #.

25.1.12.1 Come attivare o disattivare il comando dei servizi Centrex

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione, fare clic su **Telefonia** > **Impostazioni di base**.
3) Nella struttura dei menu selezionare **Sistema** > **Flag di sistema**.
4) Selezionare una delle seguenti opzioni:
   - Per attivare il controllo dei servizi Centrex, selezionare la casella di controllo **Selezione di * e # sulle interfacce di linea**.
   - Per disattivare il controllo dei servizi Centrex, deselezionare la casella di controllo **Selezione di * e # sulle interfacce di linea**.
5) Fare clic su **Applica**, quindi su **OK**.

25.2 Capitolo 24.2 Backup e ripristino

I dati di configurazione del sistema di comunicazione possono essere salvati e ripristinati.

I dati di configurazione vengono memorizzati in un set di backup. Ogni salvataggio crea un proprio set di backup. Il backup può essere eseguito immediatamente in modo manuale o automaticamente a determinati orari.

Nota: Si consiglia vivamente di eseguire con regolarità il backup dei dati di configurazione sotto forma di set di backup.

In caso di aggiornamento a una nuova Minor Release è necessario creare un nuovo set di backup.

Ogni backup è crittografato utilizzando una chiave specifica del sistema.

Un set di backup crittografato può essere utilizzato solo per il ripristino del sistema che ha crittografato il backup.

I set di backup possono essere salvati anche su supporti di backup diversi (ad esempio, un supporto USB, un'unità di rete o il disco rigido della UC Booster Card).

A seconda della configurazione del sistema, dell'uso del sistema di comunicazione e del tipo di supporto di backup, il backup o il ripristino può richiedere un tempo maggiore; in particolare con la UC Suite, in alcuni casi possono essere necessarie fino a tre ore. Questa procedura non deve essere interrotta manualmente o mediante riavvio del sistema.

L'interruzione del ripristino dati può portare a una configurazione del sistema non coerente, che non può garantire il funzionamento corretto del sistema. Un ripristino interrotto deve necessariamente essere ripetuto fino a quando non viene completato correttamente. In caso contrario, è necessario riconfigurare completamente il sistema. Se si effettuano diversi tentativi di ripristino con esito negativo, contattare il servizio di assistenza e assicurarsi che, nel frattempo, il backup utilizzato non venga sovrascritto da nuovi backup. A tal fine, il backup automatico deve essere temporaneamente disattivato.

Set di backup a scopo di diagnostica

Per lo svolgimento di funzioni di diagnostica possono essere creati set di backup più piccoli, contenenti dati utili per la ricerca degli errori da parte del personale di assistenza. Diversamente dai normali set di backup, il volume di

dati generato è notevolmente inferiore e quindi più facile da inviare ad esempio tramite e-mail. I set di backup di diagnostica contengono fra l'altro i dati di configurazione del sistema di comunicazione e della soluzione UC installata. Non contengono invece i messaggi vocali, i messaggi fax e gli annunci.

Directory di backup "Hard disk" (solo con UC Booster Card)

Se la UC Booster Card è inserita, i dati di configurazione del sistema di comunicazione possono venire memorizzati in una partizione specifica del disco rigido della UC Booster Card, nella directory di backup. Questa directory di backup è già disponibile quale archivio predefinito "Disco rigido".

Backup dei dati di configurazione dell'UC Booster Server

Se oltre al sistema di comunicazione, viene usato un UC Booster Server, quando si esegue un backup dei dati di configurazione del sistema, occorre eseguire il backup anche dei dati di configurazione dell'UC Booster Server. Il backup dell'UC Booster Server è identico a quello del sistema di comunicazione, con un'unica differenza: dopo aver richiamato il WBM, l'amministratore non deve inserire l'indirizzo IP del sistema di comunicazione, ma l'indirizzo IP del server Linux.

25.2.1 Set di backup

I dati di configurazione del sistema di comunicazione vengono memorizzati in un set di backup.

Oltre al set di backup è necessario salvare anche un file di testo associato al set di backup. Contiene informazioni sulla data e l'ora del backup e sulla versione software di cui è stato eseguito il backup. Il file di testo è necessario per il ripristino del set di backup.

Se il numero dei set di backup salvati è superiore al valore impostato, i set di backup più vecchi vengono cancellati.

Dati dei set di backup

Per un set di backup vengono visualizzate le seguenti informazioni:

- **Nome archivio**: Nome del set di backup
- **Dimensioni**: dimensioni del set di backup, espresso in byte.
- **Data**: data nella quale è stato creato il set di backup.
- **Commento**: commento che può essere aggiunto nel momento della creazione del set di backup (facoltativo).

I set di backup visualizzati in grigio non possono essere ripristinati.

25.2.1.1 Come visuallizare i set di backup

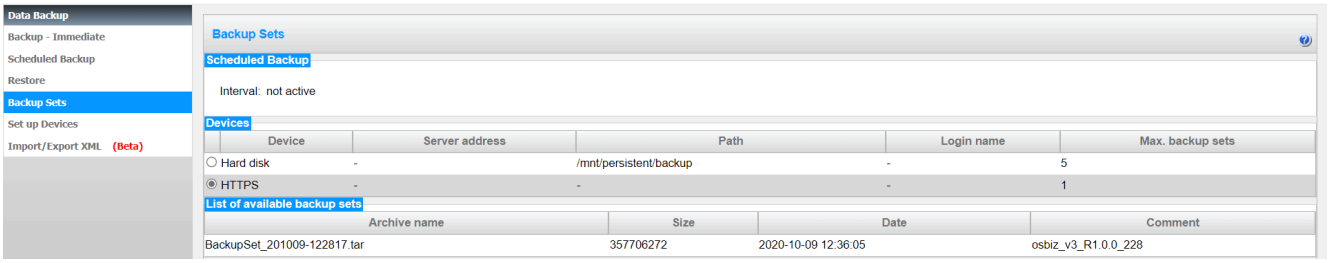
Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Backup dati**.

2) Nella struttura di navigazione fare clic su **Set di backup**.
3) Nell'area **Periferiche**, selezionare il supporto di backup di cui si vuole visualizzare il set di backup. Contiene un elenco di tutti i set di backup disponibili su questo supporto.



25.2.1.2 Come cancellare un backup

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Backup dei dati**.
2) Nella struttura di navigazione fare clic su **Set di backup**.
3) Nell'area **Periferiche**, selezionare il supporto di backup di cui si vuole visualizzare il set di backup. Contiene un elenco di tutti i set di backup disponibili su questo supporto.
4) Selezionare la casella di controllo del set di backup da cancellare, quindi premere **Cancella**. Il set di backup verrà cancellato.

25.2.2 Supporti di backup

I supporti di backup sono utilizzati per il salvataggio dei set di backup.

Per il backup possono essere utilizzati i seguenti supporti di backup:

- Supporto USB inserito
- Unità di rete
- PC client tramite HTTPS (possibile solo con backup immediato)
- Disco rigido della UC Booster Card
- Server FTP/FTPS

Per ogni supporto di backup è possibile determinare il numero massimo di set di backup da salvare nella directory specificata.

Supporto USB

Qualora per il backup venga usato un supporto USB (ad esempio un disco rigido o una chiave USB), questo deve essere inserito nella porta USB del server del sistema di comunicazione per poter essere disponibile per il backup. Inoltre, tale supporto USB deve essere formattato in FAT-32. A causa della limitazione del file system, le dimensioni massime del set di backup non devono superare i 4 GB. Altrimenti sarà necessario scegliere un supporto di backup alternativo. Un supporto USB formattato NTFS consente solo la lettura. Qualora

siano disponibili più partizioni, il salvataggio può essere eseguito solo sulla prima.

Non è supportato l'avvio da supporto USB.

Con OpenScape Business S e OpenScape UC Booster Server, il dispositivo USB viene inserito nella porta USB del server Linux.

Server FTP/FTPS e unità di rete

I server FTP/FTPS e le unità di rete possono essere aggiunti come nuovi supporti, modificati o eliminati. I server FTP/FTPS e le unità di rete possono essere indicati anche più volte se sugli stessi vengono utilizzate più directory. Come protocollo di trasferimento file crittografato (FTPS), viene supportato TLS 1.2.

Per il backup dei dati di configurazione su un server FTP/FTPS, l'utente deve disporre dei diritti di scrittura per la directory root. Per il backup su un'unità di rete, occorre disporre dei diritti di scrittura per la directory desiderata.

Una velocità di trasmissione al server FTPS troppo bassa può comportare errori nell'esecuzione del backup dei dati. In questo caso, il backup dei dati deve essere riavviato.

Con FTPS sono supportati i certificati fino a 2048 bit. Questi certificati sono necessari per l'autenticazione presso il server FTPS.

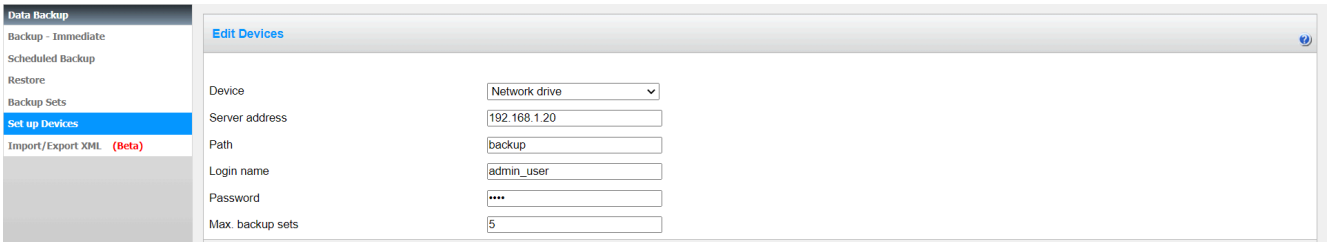
25.2.2.1 Come aggiungere i supporti di backup

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Backup dati**.
2) Nella struttura di navigazione fare clic su **Configurazione apparecchi**.
3) Fare clic su **Aggiungi**.



4) Nell'elenco a discesa nella colonna **Apparecchio**, selezionare il supporto di backup desiderato.
   - Se si desidera eseguire il backup su un server FTP/FTPS, selezionare **(S)FTP**.
   - Se il backup deve essere eseguito su un'unità di rete, selezionare **Unità di rete**.

Nota: La versione Samba supportata è SMB2.

5) Nel campo **Indirizzo server**, indicare il nome dell'host o l'indirizzo IP del supporto.
6) Nel campo **Rubrica** indicare il percorso da utilizzare per la memorizzazione del set di backup.
7) Se il backup deve essere eseguito su server FTP/FTPS, inserire il **Nome utente** e la **Password** per l'accesso a tale server FTP/FTPS.

Nota: I caratteri accettati per il campo Password sono:
`0-9 A-Z a-z ~ ! @ # $ % ^ _ - + = ? / , . :`

Il numero massimo consentito di caratteri per la password è 64.

---

8) Se il salvataggio deve essere eseguito su un'unità di rete, inserire il **Nome utente** e la **Password** per accedere all'unità di rete.

Nota: Per impostazione predefinita, viene utilizzato un dominio vuoto per l'autenticazione. Nel caso in cui si desideri fornire il dominio, utilizzare una barra (/) come separatore nel campo **Nome utente**. Ad esempio: `dominio/utente`.

---

9) Nel campo **Numero massimo di set di backup**, immettere il massimo numero di set di backup che può essere salvato nella rubrica.
10) Fare clic su **OK & Avanti**. Il supporto di backup creato viene visualizzato nell'elenco di supporti di backup disponibili.
11) Nella struttura di navigazione fare clic su **Set di backup**.
12) Nell'area **Periferiche**, attivare il supporto di backup appena aggiunto. Se nell'elenco dei set di backup disponibili non è presente alcuna barra rossa con un messaggio di errore, il supporto di backup è configurato correttamente.
13) Se viene visualizzato un messaggio di errore, verificare nuovamente le voci (vedere Come modificare i supporti di backup alla pagina 1242

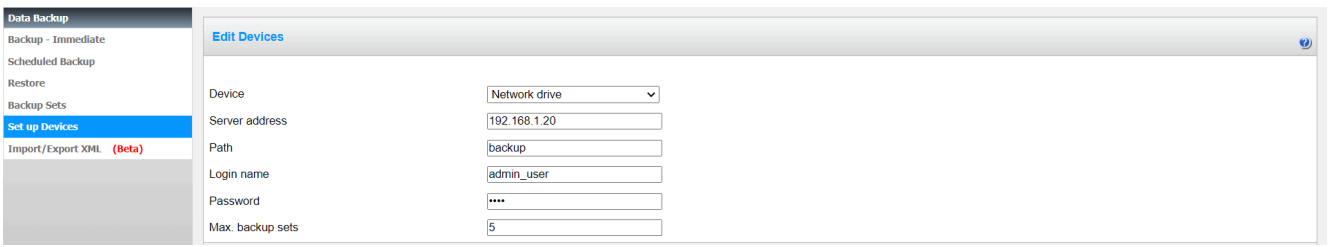
25.2.2.2 Come modificare i supporti di backup

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Backup dati**.
2) Nella struttura di navigazione fare clic su **Configurazione apparecchi**.
3) Attivare il supporto di backup da modificare, quindi premere **Modifica**.



4) Modificare i valori desiderati.
5) Fare clic su **OK & Avanti**.

25.2.2.3 Come cancellare i supporti di backup

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Backup dati**.
2) Nella struttura di navigazione fare clic su **Configurazione apparecchi**.
3) Selezionare il supporto di backup da eliminare, quindi premere **Elimina**.

   È inoltre possibile selezionare più supporti di backup da eliminare.
4) Confermare la richiesta con **OK**. Il supporto di backup viene eliminato dall'elenco di supporti di backup disponibili.

25.2.3 Salvataggio immediato

I dati di configurazione possono essere salvati immediatamente in modalità manuale.

Il backup può essere eseguito su diversi supporti di backup. Per impostazione predefinita, il supporto di backup è configurato come **HTTPS**. In questo modo è possibile memorizzare il set di backup in tutti i percorsi accessibili al client PC con cui ci si è connessi a WBM. La posizione di memoria scelta deve essere accessibile anche in caso di ripristino del set di backup. Se è collegato al sistema di comunicazione un dispositivo USB, questo viene visualizzato come supporto di backup aggiuntivo **Periferica USB**. Se la UC Booster Card e il relativo disco rigido sono inseriti, viene visualizzato un ulteriore supporto di backup **Disco rigido locale**.

Il nome del set di backup viene assegnato automaticamente al momento del salvataggio. Comprende, tra l'altro, la data in cui viene eseguito il backup. Inoltre questi dati sono contenuti anche in un file di testo che deve essere anch'esso salvato. Per poter riconoscere facilmente il set di backup in caso di ripristino, è possibile inserire un commento.

Concetti correlati

Salvataggio pianificato alla pagina 1245

Attività correlate

Come modificare la propria password amministratore alla pagina 121

25.2.3.1 Come eseguire il salvataggio immediato dei set di backup

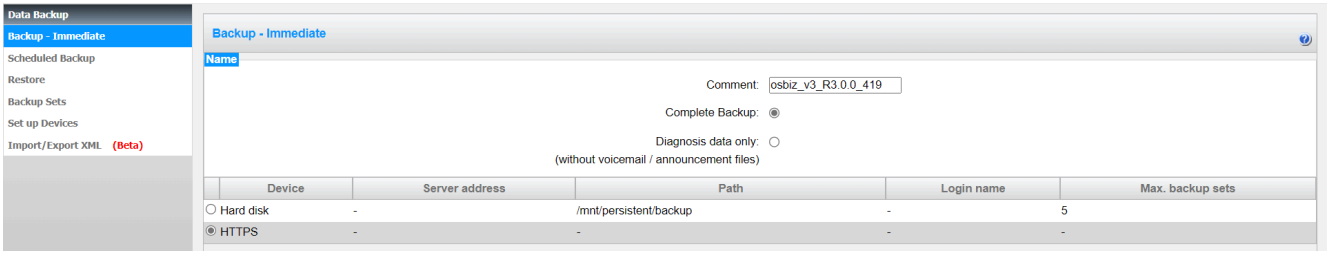
Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Solo quando si utilizza UC Suite: UC Suite è stato avviato correttamente.

Passo a passo

1) Nella barra di navigazione fare clic su **Backup dati**.
2) Nella struttura di navigazione fare clic su **Backup - immediato**.



3) Nel campo **Commento**, immettere un commento per il set di backup per facilitare l'identificazione in caso di ripristino dei dati. Non utilizzare dieresi e caratteri speciali.
4) Se si desidera creare un set di backup comprensivo di messaggi vocali e annunci, selezionare l'opzione **Backup completo**.
5) Se si desidera creare un set di backup senza messaggi vocali e annunci, selezionare l'opzione **Solo dati diagnostici**.
6) Nell'area **Dispositivi**, selezionare l'unità di destinazione sulla quale si vuole salvare il set di backup.
7) Fare clic su **OK & Avanti**. Viene visualizzata una finestra a parte in cui è mostrato l'avanzamento del backup.

Nota: Se il pulsante **OK & Avanti** viene visualizzato in grigio, significa che non tutte le applicazioni (ad esempio, la UC Suite) di cui occorre salvare i dati sono state avviate correttamente.

Se non si dispone dell'abilitazione per la directory archivio selezionata, viene visualizzato un messaggio di errore. Selezionare un'altra unità di destinazione o modificare il percorso dell'archivio.

Se l'unità di destinazione non dispone di uno spazio di memoria sufficiente per il set di backup, il sistema visualizza un messaggio d'errore. Selezionare un'altra unità di destinazione o eliminare il set di backup e riavviare il backup.

---

8) Il backup ha esito positivo se viene visualizzato il messaggio **Backup completato! 100%**.
9) Se per il supporto di backup è stata attivata l'opzione **HTTPS**, è necessario salvare il set di backup e il corrispondente file di testo in una posizione a scelta. Per gli altri supporti di backup, questo avviene automaticamente. La finestra del browser deve restare aperta fino al termine dell'operazione di salvataggio del set di backup e del file di testo.

Nota: Se per il backup si utilizza un supporto USB, attendere fino a quando il LED di tale supporto non smette di lampeggiare. A questo punto il backup sul supporto USB è completo. Rimuovere il supporto USB.

---

10) Fare clic su **Fine**.

25.2.4 Salvataggio pianificato

Un backup pianificato può prevedere il salvataggio dei dati di configurazione. È possibile impostare l'orario, l'intervallo e l'ubicazione del backup automatico.

Il backup pianificato può avere una frequenza giornaliera o settimanale e venire avviato automaticamente all'ora pianificata. Questo "Ordine di backup" può essere configurato per un supporto interno o esterno. Non è possibile configurare più ordini di backup.

Concetti correlati

Salvataggio immediato alla pagina 1243

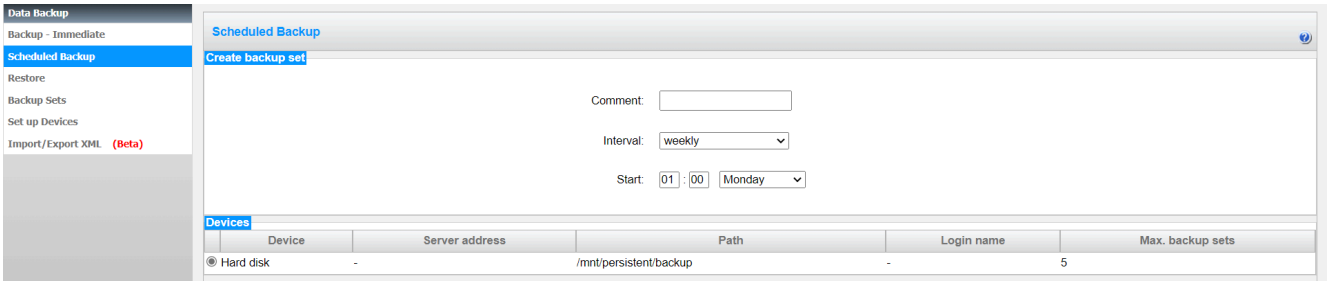
25.2.4.1 Come eseguire il salvataggio temporizzato di set di backup

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Backup dati**.
2) Nella struttura di navigazione fare clic su **Backup pianificato**.



3) Nell'area **Crea set di backup**, nel campo **Commento**, immettere un commento per il set di backup al fine di facilitare l'identificazione in caso di ripristino dei dati. Non utilizzare dieresi e caratteri speciali.
4) Definire la frequenza del backup:
   - Backup giornaliero: nell'elenco a discesa **Si ripete**, selezionare la voce **Giornaliero** e indicare in **Backup il** il momento del giorno in cui verrà avviato il backup.
   - Backup settimanale: nell'elenco a discesa **Si ripete** selezionare la voce **Settimanale** e nel campo **Backup il** indicare il giorno e l'ora della settimana in cui deve essere avviato il backup.
5) Nell'area **Dispositivi**, selezionare l'unità di destinazione sulla quale si vuole salvare il set di backup.
6) Fare clic su **OK & Avanti**. Il backup verrà avviato automaticamente con frequenza giornaliera o settimanale, al momento indicato.

25.2.5 Ripristino

Il ripristino dei dati di configurazione viene eseguito manualmente sulla base dei set di backup.

Per il ripristino possono essere utilizzati tutti i supporti di backup compatibili.

25.2.5.1 Come ripristinare i set di backup

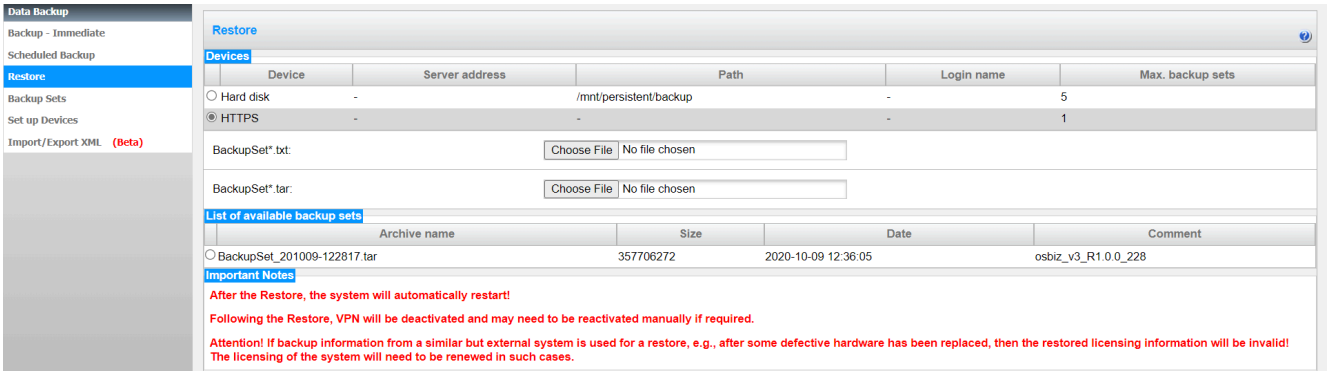
Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Solo quando si utilizza UC Suite: UC Suite è stato avviato correttamente.

Passo a passo

1) Nella barra di navigazione fare clic su **Backup dati**.
2) Nella struttura di navigazione fare clic su **Ripristina**.



3) Nell'area **Dispositivi**, selezionare il supporto che contiene il set di backup da ripristinare.
4) Se per il supporto di backup è stata attivata l'opzione **HTTPS**, selezionare il percorso di memorizzazione del set di backup, quindi selezionare il set di backup stesso. Successivamente, navigare fino alla posizione di memorizzazione del file di testo e selezionarlo.
5) Se si è attivato un altro supporto di backup come **HTTPS**, nell'area **Elenco dei set di backup disponibili**, selezionare il set di backup che contiene i dati di configurazione da ripristinare.
6) Attendere fino a quando il file non viene caricato nel sistema, quindi fare clic su **OK & Avanti**. Si avvia il ripristino dei dati di configurazione. Viene visualizzato l'avanzamento del ripristino.
7) Dopo il messaggio **Ripristino completato con successo!** il sistema si riavvia automaticamente. Il ripristino ha esito positivo se il sistema è di nuovo operativo.

25.3 Aggiornamenti

Gli aggiornamenti consentono di portare il software dei componenti del sistema alla versione più recente della release corrente.

Per poter installare gli aggiornamenti, è necessario un piano di assistenza software di 3 anni.

La versione del software installata e la data di scadenza dell'assistenza software sono visualizzate nella pagina iniziale del WBM. Viene inoltre segnalata la disponibilità di eventuali aggiornamenti.

Nota: In caso di aggiornamento a una nuova Minor Release è necessario creare un nuovo set di backup.

L'aggiornamento del software viene eseguito con il WBM. In un modello hardware, vi è inoltre la possibilità di aggiornare il software direttamente da un supporto USB senza accesso al WBM. In un sistema di comunicazione con UC Booster Server, il modello hardware e l'UC Booster Server vengono aggiornati separatamente.

Con il WBM, il software può essere aggiornato tramite un server Web Internet, un server Web locale o direttamente tramite un file immagine.

I seguenti componenti del sistema vengono aggiornati:

- Software del sistema di comunicazione
- Software dei client UC
- Software dei telefoni di sistema (possibile anche l'aggiornamento indipendente)
- Documentazione

Quando viene aggiornato il software del sistema di comunicazione, si esegue anche l'aggiornamento del software del client UC. Quando si rende disponibile un aggiornamento, gli utenti dei client UC vengono avvisati tramite la funzione aggiornamento automatico con un messaggio.

L'aggiornamento del software dei telefoni IP di sistema viene eseguito automaticamente assieme all'aggiornamento del sistema di comunicazione, ma può essere effettuato anche manualmente. Per i telefoni di sistema UP0, l'aggiornamento viene eseguito manualmente tramite Manager E.

L'aggiornamento del software può essere avviato immediatamente oppure è possibile definire in modo separato la data e l'ora per la trasmissione e l'attivazione del software. L'aggiornamento deve essere effettuato al di fuori dell'orario d'ufficio del cliente poiché in tale occasione il sistema di comunicazione e/o i telefoni di sistema vengono riavviati e le chiamate in corso e l'uso dei client UC vengono temporaneamente interrotti.

Se il software è stato trasferito al sistema di comunicazione, questo verrà attivato al momento selezionato. Successivamente viene scaricata automaticamente sul telefono IP del sistema l'immagine del telefono più aggiornata. Dopo un riavvio del sistema di comunicazione e dei telefoni di sistema IP, il software appena caricato sarà attivo.

Nota: L'aggiornamento del software non deve essere eseguito contemporaneamente in tutti i sistemi e nelle versioni software diverse.

File immagine

Per l'aggiornamento dei componenti del sistema sono necessari dei file immagine che contengono il software dei componenti del sistema. I file immagine possono essere scaricati dal server software (server Web Internet) e salvati in modo indipendente in un server Web locale, nella rete interna o su un supporto USB. È disponibile un file immagine per il sistema di comunicazione senza UC Booster Card e un file immagine per il sistema con UC Booster Card. Entrambi i file immagine contengono anche il software per i telefoni di sistema. Inoltre, per ogni tipo di telefono di sistema è disponibile un proprio

file immagine, nel caso in cui i telefoni di sistema debbano essere aggiornati singolarmente.

Sono disponibili i seguenti tipi di file immagine:

- **tgz**: per il software del sistema di comunicazione. Nel file tgz è presente un file tar. Il file tar deve essere decompresso, ad esempio utilizzando WinZip o 7-Zip, dal file tgz. Viene reso disponibile per il download un file tgz perché in questo modo durante il download dal server del software viene eseguita la verifica se il file è danneggiato o meno.
- **tar**: per il software del sistema di comunicazione. Contiene i file compressi per i singoli componenti del sistema.
- **app**: per il software del telefono di sistema.

Server Web locale

Per impostazione predefinita, con l'aggiornamento software tramite server Web, viene eseguito l'accesso al software server (server Web Internet).

Per l'aggiornamento è anche possibile utilizzare un server Web locale. A tal fine, il file immagine deve essere salvato sul server Web locale e il percorso per tale server deve essere configurato nel WBM.

Speed Upgrade

Non è possibile effettuare uno speed upgrade con HiPath 3000.

Importante: L'estrazione della scheda SDHC durante l'uso determina la perdita dei dati!

Rete - Licenze

Durante l'aggiornamento o la migrazione di sistemi in una rete, in cui il nodo master viene utilizzato per le licenze dei nodi slave, iniziare con i nodi slave prima del nodo master.

25.3.1 Uso di un server Web locale

È possibile aggiornare il software tramite un server Web locale.

I file immagine correnti devono essere salvati sul server Web locale. Inoltre occorre inserire i dati di accesso del server Web locale nel WBM. Questa modifica può essere eseguita solo da un amministratore con il profilo **Expert**. Se i dati di accesso per il server Web locale sono stati inseriti, verranno impostati come predefiniti e per tutti i successivi aggiornamenti del sistema di comunicazione verrà ora usato il server Web locale al posto del server Internet.

25.3.1.1 Come configurare l'accesso al server Web locale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È disponibile una connessione al server Web locale.

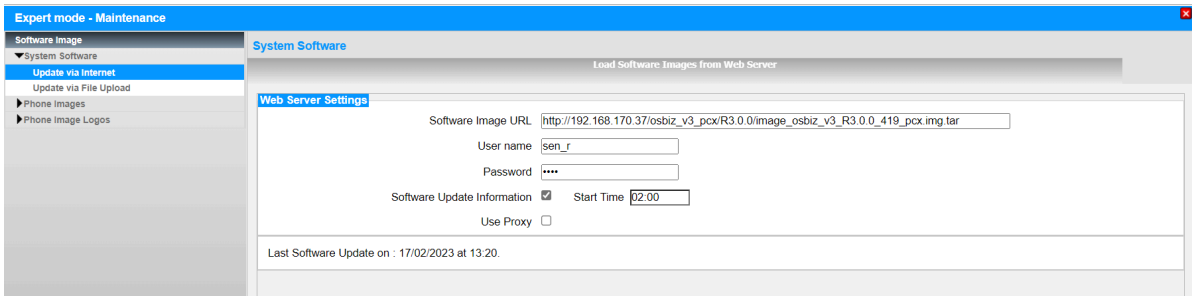
È necessario l'indirizzo WEB (URL) e i dati di accesso del server Web locale, nonché il nome del file immagine.

Il file immagine è memorizzato come file tar sul server Web locale e si conosce il percorso di memorizzazione. Se necessario, il file tar deve venire decompresso dal file tgz salvato.

Se si utilizza un server proxy per l'aggiornamento sono necessari questi dati (eventualmente anche nome utente e password).

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Immagine del software**.
3) Nella struttura dei menu, fare clic su **Software di sistema**.
4) Fare clic su **Aggiorna via Internet**.



5) Configurare l'accesso al server Web locale:
   a) In **URL dell'immagine del software**, inserire l'indirizzo del server Web locale, comprensivo di nome del file immagine.

      Nota: Il pulsante **Preimpostazione** consente di ripristinare i valori predefiniti.

   b) Nel campo **Nome utente** e nel campo **Password** immettere nome utente e password per l'accesso al server Web locale.
   c) Selezionare la casella di controllo **Informazioni aggiornamento del software** e indicare nel campo **Ora inizio** il momento in cui si dovrà verificare nel server indicato la disponibilità di aggiornamenti software.
   d) Se per la trasmissione si utilizza un server proxy, selezionare la casella di controllo **Utilizza proxy** e immettere i dati per il server proxy.
6) Fare clic su **Applica**. I dati di accesso inseriti per il server Web locale vengono impostati come predefiniti.

   Se sul server Web locale è già disponibile un nuovo file immagine, viene avviato l'aggiornamento del software e viene visualizzato il contratto di licenza (vedere Come aggiornare il sistema tramite un server Web). È anche possibile impedire all'occorrenza l'avvio dell'aggiornamento software.

25.3.2 Aggiornamento del sistema di comunicazione

L'aggiornamento del sistema di comunicazione comprende, oltre all'aggiornamento del software del sistema di comunicazione stesso, anche le immagini software dei telefoni di sistema salvate nel sistema di comunicazione. Pertanto, l'aggiornamento completo di tutti i componenti è rapido e semplice da eseguire.

Prima di ogni aggiornamento del software, occorre salvare i dati di configurazione del sistema di comunicazione (Backup e ripristino).

Aggiornamento tramite server Web

Per impostazione predefinita, con l'aggiornamento software tramite server Web, viene eseguito l'accesso al software server (server Web Internet).

Se viene utilizzato un server Web locale, il file immagine deve essere salvato sul server Web locale.

Per un sistema di comunicazione senza UC Booster Card è indifferente se un file immagine per un sistema viene utilizzato con o senza UC Booster Card. Vengono installati solo i componenti necessari.

Una volta stabilita automaticamente una connessione al server Web, viene verificata la disponibilità di aggiornamenti software. In sistemi senza UC Booster, i singoli pacchetti di aggiornamento software possono essere deselezionati, per ridurre il tempo di download. Vengono scaricati solo i pacchetti che sono stati modificati rispetto alla versione software installata. È possibile selezionare il momento id inizio del download del software e il momento di inizio dell'attivazione del software. Se si raggiunge il momento previsto per l'attivazione del software prima che l'aggiornamento del software sia completato, l'attivazione non viene eseguita automaticamente. Occorre definire manualmente un nuovo momento per l'attivazione.

Aggiornamento mediante supporto USB

Il file immagine è salvato su un supporto USB. Il supporto USB viene inserito nell'interfaccia USB del server del sistema di comunicazione. Questo tipo di aggiornamento può essere eseguito solo da un amministratore con il profilo **Expert** e non è possibile con OpenScape Business S e OpenScape Business UC Booster Server.

Aggiornamento mediante Carica file

Il file immagine si trova in una rubrica nella rete interna o nel PC Admin.

Aggiornamento mediante supporto USB senza accesso WBM

Il sistema di comunicazione può essere aggiornato direttamente senza richiedere accesso al WBM, utilizzando un supporto USB. A tal fine, inserire il supporto USB nella porta USB del server del sistema e porre il file immagine nel livello di directory superiore di tale supporto. Se viene eseguito un reset con il dispositivo USB collegato, l'aggiornamento del software viene automaticamente avviato. Questo tipo di aggiornamento non è possibile con OpenScape Business S. In un sistema con OpenScape Business UC Booster Server, è inoltre necessario aggiornare il server.

Aggiornamento di UC Booster Server

Se oltre al sistema di comunicazione, viene usato un UC Booster Server, quando si esegue un aggiornamento del software di sistema, occorre aggiornare anche il software di comunicazione dell'UC Booster Server. Il software del sistema di comunicazione e dell'UC Booster Server deve essere sempre aggiornato all'ultima versione. L'aggiornamento software dell'UC Booster Server è identico a quello del sistema di comunicazione, con un'unica differenza: dopo aver richiamato il WBM, l'amministratore non deve inserire l'indirizzo IP del sistema di comunicazione, ma l'indirizzo IP del server Linux.

25.3.2.1 Come aggiornare il sistema tramite un server Web

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

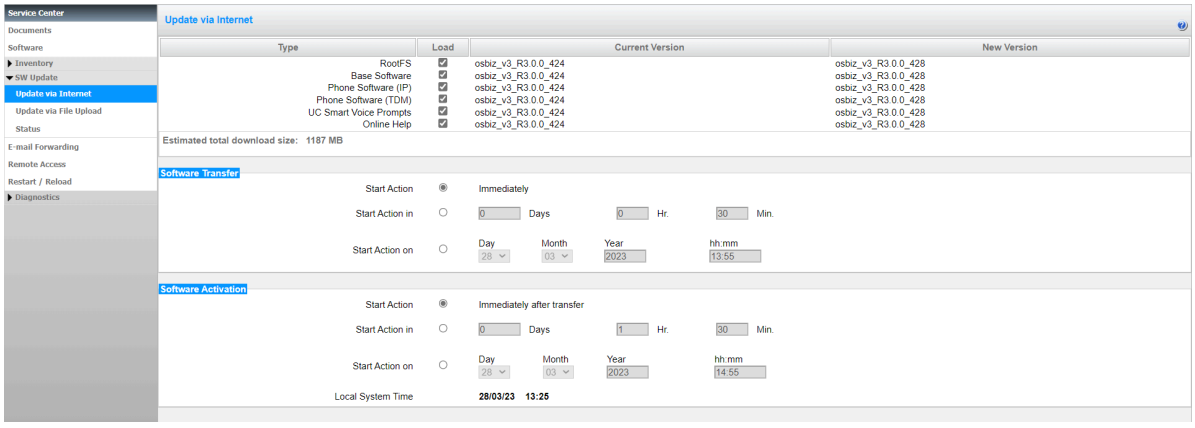
Nella pagina iniziale del WBM viene indicata la disponibilità di una nuova versione del software.

È possibile accedere al server Web. Per impostazione predefinita, viene realizzata la connessione a un server Web su Internet. Al suo posto può essere configurato un server Web locale. (Vedere Uso di un server Web locale).

Se l'aggiornamento viene eseguito tramite un server Web locale, occorre salvare il file immagine più aggiornato su tale server.

Passo a passo

1) Nella barra di navigazione fare clic su **Inizio** e quindi sul collegamento **I dettagli sul contenuto sono reperibili qui: Collegamento**. Si apre un file PDF con informazioni importanti sulla nuova versione software. Leggere le informazioni e rispettare le istruzioni per l'aggiornamento del sistema. Chiudere successivamente la finestra.
2) Nella barra di navigazione fare clic su **Centro assistenza**.
3) Nella struttura di navigazione, fare clic su **Aggiornamento SW** > **Aggiornamento via Internet**. Viene visualizzata la versione software attualmente installata.
4) Fare clic su **OK & Avanti**.
5) Leggere il contratto di licenza (EULA) e attivare il pulsante di opzione **Accetto il contratto di licenza**.
6) Fare clic su **OK & Avanti**.



7) All'occorrenza, nella colonna **Carica** deselezionare i pacchetti che non devono essere aggiornati. Ciò è utile per connessioni Internet lente o aggiornamenti software via ISDN.
8) Selezionare la data e l'ora per il trasferimento e l'attivazione del software:
   - **Inizio dell'azione - Immediato/Subito dopo la trasmissione**: Il software viene immediatamente scaricato e attivato subito dopo il trasferimento. L'aggiornamento software viene caricato in background nel sistema di comunicazione. Dopo due riavvii il software viene aggiornato.

- **Inizio dell'azione tra**: Il software viene scaricato e attivato una volta trascorso un periodo di tempo predefinito. Inserire il periodo in giorni, ore e minuti.
- **Inizio dell'azione il**: Il software viene scaricato e attivato in un momento preciso. Indicare la data e l'ora del momento prescelto.

Nota: Se si raggiunge il momento previsto per l'attivazione del software prima che l'aggiornamento del software sia completato, l'attivazione non viene eseguita automaticamente. Occorre definire manualmente un nuovo momento per l'attivazione.

---

9) Fare clic su **OK & Avanti**. L'aggiornamento del software verrà scaricato nel sistema e attivato alla data e all'ora indicate dall'utente. Per l'attivazione del software vengono eseguiti automaticamente due riavvii consecutivi.

Nota: La finestra del browser può essere chiusa in qualsiasi momento.

---

10) Lo stato dell'aggiornamento può essere richiesto tramite il WBM selezionando **Centro assistenzaAggiornamento del softwareStato**.

25.3.2.2 Come aggiornare il sistema tramite un supporto USB

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Il supporto USB deve essere formattato con FAT-32.

Il file immagine corrente è memorizzato come file tar su supporto USB. È inoltre possibile salvare più file immagine in cartelle diverse.

Se il dispositivo USB comprende più partizioni, il file immagine deve essere memorizzato nella prima partizione.

Passo a passo

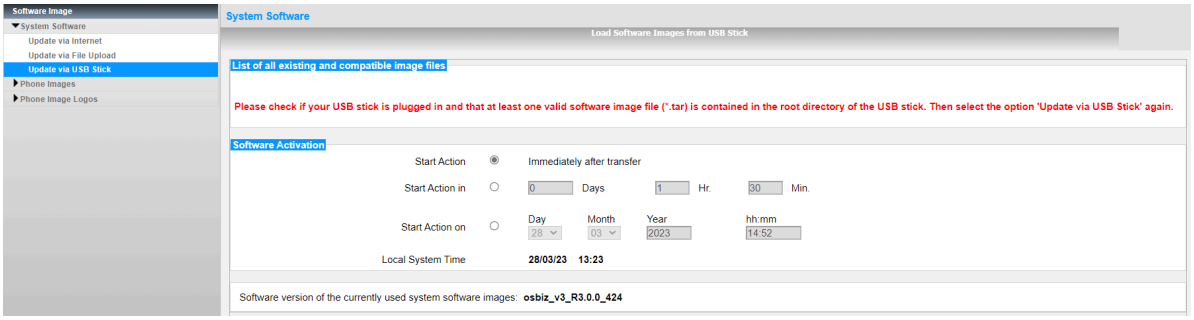
1) Inserire il supporto USB nella porta server USB della scheda madre.

2) Nella barra di navigazione fare clic su **Modalità esperti**.

3) Nella struttura di navigazione fare clic su **Manutenzione** > **Immagine del software**.

4) Nella struttura dei menu, fare clic su **Software di sistema**.

5) Fare clic su **Aggiorna via chiave USB**. Vengono visualizzati tutti i file immagine validi memorizzati su supporto USB con il relativo numero di versione e nome file.



6) Se sono memorizzati più file immagine, selezionare il file di immagine desiderato, in caso contrario, il file di immagine viene automaticamente evidenziato.

7) Selezionare il momento di attivazione del software:

- **Inizio dell'azione - Subito dopo la trasmissione**: il software viene attivato immediatamente dopo la trasmissione al sistema di comunicazione.
- **Inizio dell'azione tra**: il software viene scaricato nel sistema di comunicazione immediatamente. Il software verrà attivato una volta trascorso un tempo definito. Inserire il periodo in giorni, ore e minuti.
- **Inizio dell'azione il:** il software viene scaricato nel sistema di comunicazione immediatamente. Il software verrà attivato in un momento definito. Indicare la data e l'ora del momento prescelto.

8) Fare clic su **Carica**. Il file immagine viene scaricato nel sistema di comunicazione e ne viene verificata l'integrità. Per entrambi i processi, l'operazione può richiedere diversi minuti. Durante questo periodo, il supporto USB deve restare inserito.

9) Estrarre il supporto USB quando richiesto dal WBM, quindi fare clic su **Fine**. Al momento indicato per l'attivazione del software vengono eseguiti automaticamente due riavvii consecutivi.

10) Lo stato dell'aggiornamento può essere richiesto tramite il WBM selezionando **Centro assistenza** > **Aggiornamento del software** > **Stato**.

25.3.2.3 Come aggiornare il sistema tramite il caricamento di un file

Prerequisiti

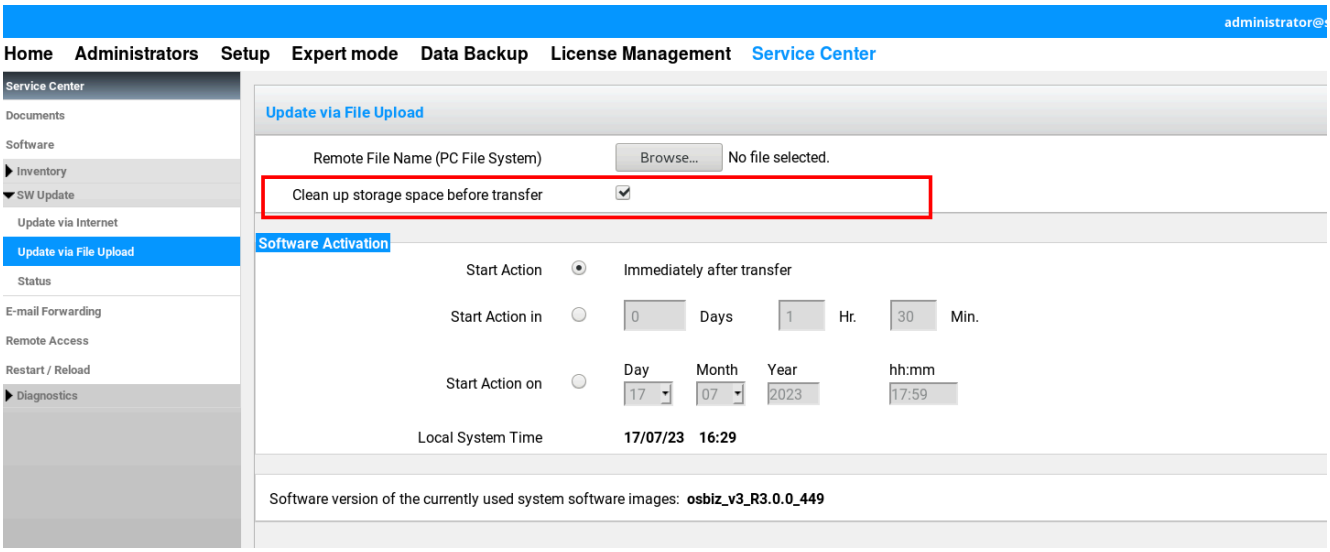
Il file immagine è memorizzato come file tar sulla rete interna o direttamente nel PC Admin e si conosce il percorso di memorizzazione. Se viene salvato un file .tgz, il file tar deve venire decompresso dal file .tgz.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.

2) Nella struttura di navigazione fare clic su **Aggiornamento SW** > **Aggiornamento tramite Carica file**. Viene visualizzata la versione software correntemente installata.

3) Fare clic su **OK & Avanti**.



4) Con il pulsante **Sfoglia**, selezionare il percorso per il salvataggio del file immagine (`*.tar`).

5) Il flag **Pulisci lo spazio di archiviazione prima del trasferimento** è attivato per impostazione predefinita. Vengono attivate le seguenti azioni per liberare memoria di archiviazione in preparazione del caricamento del file software.

   - Tutti i registri e le tracce vengono eliminati.
   - Tutte le immagini del software del telefono vengono eliminate.
   - Eventuali dump TCP vengono eliminati.

6) Selezionare il momento di attivazione del software:

   - **Inizio dell'azione - Subito dopo la trasmissione**: Il software viene scaricato nel sistema di comunicazione immediatamente, in background. Dopo due riavvii il software viene aggiornato.
   - **Inizio dell'azione tra**: Il software viene scaricato nel sistema di comunicazione immediatamente, in background. Il software verrà attivato una volta trascorso un tempo definito. Inserire il periodo in giorni, ore e minuti.
   - **Inizio dell'azione il:** Il software viene scaricato nel sistema di comunicazione immediatamente, in background. Il software verrà attivato in un momento definito. Indicare la data e l'ora del momento prescelto.

7) Fare clic su **OK & Avanti**.

8) Il file immagine viene scaricato nel sistema di comunicazione e ne viene verificata l'integrità. Per entrambi i processi, l'operazione può richiedere diversi minuti.

Nota: Se si chiude la finestra del browser durante il download del software, il processo viene interrotto. Durante i controlli di coerenza, è possibile continuare a lavorare con il WBM o chiuderlo.

---

9) Se il software deve attivato immediatamente, al termine della verifica della coerenza completata con esito positivo, vengono eseguiti due riavvii consecutivi.

10) Se il software non viene attivato immediatamente, al termine del download, fare clic su **Fine**. Per l'attivazione del software vengono eseguiti automaticamente due riavvii consecutivi.

11) Lo stato dell'aggiornamento può essere richiesto tramite il WBM selezionando **Centro assistenza** > **Aggiornamento del software** > **Stato**.

25.3.2.4 Come aggiornare il sistema tramite un supporto USB senza accesso al WBM

Prerequisiti

Il supporto USB deve essere formattato con FAT-32.

Il file immagine corrente è memorizzato come file tar nel livello di directory superiore del supporto USB. Qui è possibile memorizzare solo un file immagine.

Se il dispositivo USB comprende più partizioni, il file immagine deve essere memorizzato nella prima partizione.

La versione del software del file immagine deve essere più recente della versione del software del sistema. Attenzione: è anche possibile "eseguire l'aggiornamento" a versioni precedenti del software.

Il sistema di comunicazione viene avviato.

Passo a passo

1) Inserire il supporto USB nella porta server USB della scheda madre.

2) Tenere premuto il pulsante di reset per 1-4 secondi. Il sistema si spegne e si riavvia.

Durante l'inizializzazione, il software viene testato. Se il dispositivo USB contiene un file immagine adatto, tale file viene caricato sul sistema di comunicazione. Il LED rosso lampeggia con la frequenza di 1 Hz (0,5 sec acceso/0,5 sec spento). Al termine del processo di copia, il software viene automaticamente decompresso e i dati del cliente vengono automaticamente trasferiti. Durante questo processo, il LED rosso lampeggia con una frequenza di 5 Hz (100 ms acceso/100 ms spento).

3) Rimuovere il dispositivo USB quando il LED rosso lampeggia a intervalli di 5 Hz.

4) Infine, il sistema esegue due riavvii automatici consecutivi. Se il LED verde lampeggia con una frequenza di 1 Hz (0,5 s On/0,5 s Off), il sistema è di nuovo operativo.

25.3.3 Aggiornamento dei telefoni del sistema

Il software dei telefoni di sistema viene aggiornato tramite un file immagine. Per ogni tipo di telefono di sistema è disponibile un file immagine separato che contiene il software per quel tipo di telefono. I file immagine sono inclusi nel software del sistema di comunicazione e vengono caricati automaticamente durante l'aggiornamento nel sistema di comunicazione.

Per impostazione predefinita, i telefoni IP di sistema ricevono automaticamente il software aggiornato. Se col WBM viene riconfigurato un telefono di sistema IP (da **Client del sistema** a **Client SIP** o viceversa), sul telefono di sistema IP viene automaticamente caricato il software corrispondente memorizzato nel

sistema di comunicazione, tramite il DLI. Per i telefoni di sistema IP già in uso con il sistema o con un altro sistema, è necessario resettare le impostazioni in uso (Factory Reset) prima di poter procedere all'aggiornamento automatico del software.

L'amministratore può trasferire un software del telefono diverso da quello predefinito manualmente tramite il WBM a tutti i telefoni di sistema di un tipo specifico. L'aggiornamento del software per i telefoni di sistema con interfaccia UP0 viene effettuato con Manager E.

Se, nel WBM, un software per telefoni (file immagine) viene identificato come predefinito, al primo accesso di un telefono IP di sistema dello stesso tipo, questa immagine viene automaticamente trasferita al telefono.

In caso di aggiornamento manuale, verificare che il software dei telefoni di sistema sia compatibile con la versione software del sistema di comunicazione (vedere la release note).

Concetti correlati

Loghi del telefono alla pagina 1228

25.3.3.1 Come caricare il software dei telefoni nel sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

I file immagini sono memorizzati sulla rete locale e si conoscono i percorsi di memorizzazione. Ogni tipo di telefono di sistema richiede un proprio file immagine.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Immagine del software**.
3) Nella struttura dei menu, fare clic su **Telefon Image**.
4) Fare clic su **Carica**. Viene visualizzato un elenco dei file immagine attualmente disponibili nel sistema di comunicazione.
5) In **Nome del file remoto (sistema di file del PC)** selezionare con **Ricerca** il percorso del file immagine (`*.app`).
6) Fare clic su **Carica**. Il file immagine viene caricato e verificato per la presenza di errori.

   Nota: In caso di errori, viene emesso un messaggio d'errore. Verificare le immissioni e ripetere i passaggi da 5 a 6.

   ---

7) Se la verifica riesce, confermare con **OK**. Il file immagine viene inserito nella lista dei file immagine attualmente disponibili sul sistema di comunicazione.
8) Se si desidera caricare altri file immagine per ulteriori tipi di telefono di sistema, ripetere i passaggi da 5 a 7.

25.3.3.2 Come distribuire il software per telefoni ai telefoni di sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Immagine del software**.
3) Nella struttura dei menu, fare clic su **Telefon Image**.
4) Se si desidera distribuire un'immagine telefono a tutti i telefoni di sistema di un tipo specifico, procedere come segue:
   a) Fare clic su **Distribuire**. Viene visualizzato un elenco dei file immagine attualmente disponibili nel sistema di comunicazione.
   b) Selezionare la casella di controllo **Distribuire** per una o più immagini telefono desiderate.
5) Se si desidera distribuire un'immagine telefono a un telefono di sistema specifico, procedere come segue:
   a) Fare clic su **Distribuire per terminale**. Viene visualizzata un elenco dei telefoni del sistema.
   b) Dal menu a discesa **Software disponibile per la distribuzione**, selezionare i telefoni di sistema desiderati ai quali si desidera distribuire l'immagine.
6) Fare clic su **Applica**.

25.3.3.3 Come eliminare il software per telefoni

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Immagine del software**.
3) Nella struttura dei menu, fare clic su **Telefon Image**.
4) Fare clic su **Carica**. Viene visualizzato un elenco dei file immagine attualmente disponibili nel sistema di comunicazione.
5) Nella riga delle immagini del telefono da eliminare, selezionare la casella di controllo **Cancella**.
6) Se si desidera eliminare altre immagini telefono, ripetere il passo precedente.
7) Fare clic su **Cancella**. Tutte le immagini del telefono selezionate vengono cancellate dal sistema di comunicazione.

25.3.3.4 Come attivare o disattivare la distribuzione automatica del software dei telefoni

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Immagine del software**.
3) Nella struttura dei menu, fare clic su **Telefon Image**.
4) Fare clic su **Distribuire**. Viene visualizzato un elenco dei file immagine attualmente disponibili nel sistema di comunicazione.
5) Se il software del telefono deve essere trasferito automaticamente ai telefoni di sistema, nella riga del file immagine desiderato, selezionare la casella di controllo **Predefinito** (impostazione predefinita).
6) Se il software del telefono non deve essere trasferito automaticamente ai telefoni di sistema, nella riga del file immagine desiderato, deselezionare la casella di controllo **Predefinito**.
7) Fare clic su **Applica**.

25.3.3.5 Come configurare il reflashing automatico

Il reflashing automatico è un modo facile per eseguire il flashing del software HFA solo alla prima installazione del software preconfigurato o quando si ripristinano le impostazioni di fabbrica di OpenScape Desk Phone IP 35G Eco e OpenScape Desk Phone CP 100/110/200/205/210/400/600/600E/700/700X/710 utilizzando il server DLI del sistema.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Nota: Il reflashing automatico è valido solo per i dispositivi preconfigurati (in fabbrica). In caso contrario, le impostazioni di fabbrica devono essere ripristinate sul dispositivo ("reset delle impostazioni predefinite") prima di procedere al reflashing automatico.

Passo a passo

1) Configurare il dispositivo con un numero e come client di sistema:
   a) Nella barra di navigazione fare clic su **Modalità esperti**.
   b) Nella struttura di navigazione fare clic su **Server telefonia > Utente > Client IP**.
   c) Inserire il numero di interno nel campo **N° tel.**.
   d) Inserire il numero pubblico nel campo **DID**.
   e) Inserire un nome per il dispositivo.
   f) Selezionare **Client di sistema** dal menu a discesa **Tipo**.
   g) Fare clic su **Applica**.

2) Configurare il server DHCP a cui inviare l'indirizzo IP del DLI tramite l'opzione DHCP:
   a) Nella barra di navigazione fare clic su **Modalità esperti**.
   b) Nella struttura di navigazione fare clic su **Server telefonia > Interfaccia di rete > DHCP > Server DHCP > Modifica parametri globali**.
   c) Selezionare l'opzione **Usa DLI interno** nella sezione **Server DNS**.
3) Collegare il dispositivo e, una volta avviato il telefono, specificare il numero del terminale.
4) Il telefono è inoltre registrato presso il database DLI. Per verificare la registrazione del dispositivo:
   a) Nella barra di navigazione fare clic su **Modalità esperti**.
   b) Nella struttura di navigazione fare clic su **Manutenzione > Immagine del software**.
   c) Nella struttura dei menu, fare clic su **Immagini telefono**.
   d) Fare clic su **Distribuire per terminale**.
5) Il reflashing automatico si avvia e carica il software HFA salvato nel sistema di comunicazione al dispositivo.

Nota: Non scollegare il dispositivo durante questo processo.

Il dispositivo è ora configurato.

Nota: Se il dispositivo è impostato su SIP (in **Server telefonia > Utente > Client IP**), si aggiornerà al software SIP più recente solo se è disponibile l'aggiornamento nella corrispondente versione software.

Quando un client SIP viene modificato in client di sistema, per caricare il software HFA è necessario riavviare manualmente il telefono.

Nota: Se il processo di reflashing ha esito negativo, è necessario ripristinare sul dispositivo le impostazioni di fabbrica (reset delle impostazioni predefinite).

25.3.4 Stato del software

Lo stato del software fornisce informazioni sulla versione software e sul relativo aggiornamento.

È possibile visualizzare i seguenti stati:

- Versione corrente del software
- È disponibile una versione più recente per l'aggiornamento
- Momento in cui viene eseguito l'aggiornamento del software
- Il nuovo software viene caricato nel sistema
- Caricamento non riuscito o errore durante il caricamento

25.3.4.1 Come interrogare lo stato del software

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

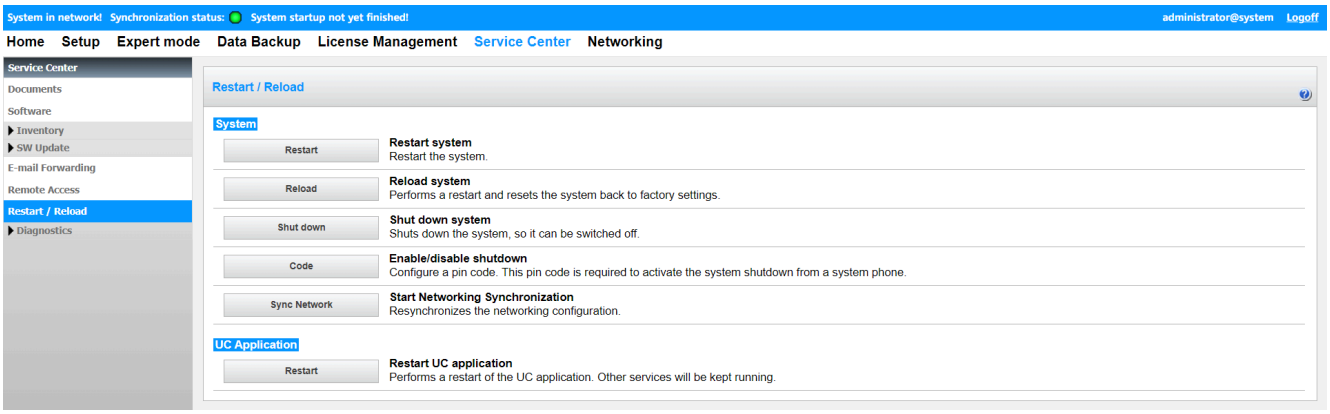
1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Aggiornamento del software** > **Stato**. Viene visualizzata la versione corrente del software. Queste informazioni sono visualizzate anche nella pagina iniziale del WBM.

   Qui viene inoltre indicato se è già in corso un aggiornamento in background del software o

   se è disponibile un nuovo aggiornamento sul server Web Queste informazioni sono visualizzate anche nella pagina iniziale del WBM.

25.4 Riavvia, Ricarica, Arresta

Tramite la relativa funzione, è possibile riavviare o ricaricare il sistema di comunicazione OpenScape Business, avviare la UC Booster Card o arrestare in modo controllato OpenScape Business X. Oltre a ciò è possibile attivare il riavvio dell'applicazione UC (UC Smart o UC Suite). Per consentire un arresto controllato di OpenScape Business X tramite un telefono di sistema, è possibile impostare un PIN.



Riavvio e ricarica dell'UC Booster Server

Se oltre al sistema di comunicazione, viene usato un UC Booster Server, il software di comunicazione dell'UC Booster Server può anche essere riavviato o ricaricato. Le operazioni di riavvio/ricarica dell'UC Booster Server sono identiche a quelle del sistema di comunicazione, con un'unica differenza: dopo aver richiamato il WBM, l'amministratore non deve inserire l'indirizzo IP del sistema di comunicazione, ma l'indirizzo IP del server Linux.

Nota: Vedere anche Come rimuovere o eliminare nuovi utenti Unify Phone alla pagina 1196.

25.4.1 Riavvio di OpenScape Business

Con la funzione **Riavvia sistema** è possibile eseguire un riavvio controllato di OpenScape Business.

Occorre tenere in considerazione le seguenti differenze:

- OpenScape Business S e OpenScape Business X

  Viene eseguito un riavvio controllato del sistema di comunicazione. Dopo l'inizializzazione il sistema di comunicazione è di nuovo operativo.

  Il tempo richiesto per l'inizializzazione dipende dalla struttura del sistema e dallo scenario di collegamento in rete utilizzato da OpenScape Business.

  Se OpenScape Business X3/X5/X8 è dotato di una UC Booster Card (scheda applicazioni OCAB), viene eseguito un riavvio controllato dell'applicazione UC (UC Smart o UC Suite).
- OpenScape Business UC Booster Server (Application Server)

  Viene eseguito un riavvio controllato della sezione OpenScape Business e dell'applicazione UC (UC Suite). Dopo l'inizializzazione l'applicazione UC è di nuovo operativa.

In caso di riavvio, le connessioni a tutte le applicazioni attive, ad esempio myPortal for Desktop e myAttendant, vengono interrotte. Dopo l'inizializzazione, tutte le connessioni vengono automaticamente ripristinate.

25.4.1.1 Come eseguire il riavvio di OpenScape Business

Con la funzione **Riavvia sistema** è possibile riavviare il sistema OpenScape Business.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Suggerimento: In caso di riavvio, le connessioni a tutte le applicazioni attive, ad esempio myPortal for Desktop e myAttendant, vengono interrotte. Dopo l'inizializzazione, tutte le connessioni vengono automaticamente ripristinate.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Riavvia / Ricarica**.
3) Fare clic su **Riavvia sistema**, quindi su **OK**. OpenScape Business esegue un riavvio.

   OpenScape Business S e OpenScape Business X: dopo l'inizializzazione il sistema di comunicazione è di nuovo operativo.

   OpenScape Business UC Booster Server: dopo l'inizializzazione l'applicazione UC (UC Suite) è di nuovo operativa.

25.4.2 Ricarica di OpenScape Business

Con la funzione **Ricarica sistema** è possibile avviare la ricarica di OpenScape Business.

Occorre tenere in considerazione le seguenti differenze:

- OpenScape Business S e OpenScape Business X

  Viene ricaricato il sistema di comunicazione. Dopo l'inizializzazione, il sistema di comunicazione si trova nello stato base.

  – Andranno perse tutte le impostazioni internazionali e del cliente (sigla internazionale del sistema = Germania).
  – Il sistema di comunicazione ha l'indirizzo IP predefinito 192.168.1.2 e l'intervallo di indirizzi IP interni 192.168.3.xxx.
  – La concessione delle licenze rimane invariata.

  Il tempo richiesto per l'avvio dipende dallo struttura del sistema.
- OpenScape Business UC Booster Server

  Viene ricaricata la sezione relativa a OpenScape Business. Dopo l'inizializzazione, tale sezione si trova nello stato base.

  – Tutte le impostazioni della sezione OpenScape Business specifiche del cliente (ad esempio, l'indice utenti) sono state eliminate.
  – La concessione delle licenze rimane invariata.

  Il sistema operativo non viene reimpostato.

25.4.2.1 Come attivare la ricarica di OpenScape Business

Con la funzione **Ricarica sistema** è possibile ricaricare il sistema OpenScape Business.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

OpenScape Business S e OpenScape Business X: i dati di configurazione del sistema di comunicazione vengono memorizzati in un set di backup.

Nota:

Ricaricando il sistema di comunicazione, questo viene riportato allo stato base (impostazioni predefinite). Andranno perse tutte le impostazioni internazionali e del cliente (sigla internazionale del sistema = Germania). Il sistema di comunicazione riceve l'indirizzo IP predefinito 192.168.1.2.

OpenScape Business UC Booster Server: i dati di configurazione della sezione relativa a OpenScape Business vengono memorizzati in un set di backup.

Nota:

Ricaricando il sistema, la sezione OpenScape Business viene riportata allo stato base (impostazioni predefinite). Tutte le

impostazioni della sezione OpenScape Business specifiche del cliente (ad esempio, l'indice utenti) vengono eliminate.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Riavvia / Ricarica**.
3) Fare clic su **Ricarica sistema**, quindi su **OK**. OpenScape Business viene ricaricato.

Suggerimento: OpenScape Business S e OpenScape Business X: dopo l'inizializzazione, il sistema di comunicazione si trova nello stato base. Dopo la configurazione delle impostazioni di base, con la procedura **Prima installazione** è possibile caricare nuovamente le informazioni specifiche del paese e del cliente. Per informazioni sulla procedura, vedere Ripristino.

OpenScape Business UC Booster Server: dopo l'inizializzazione, la sezione relativa a OpenScape Business si trova nello stato base. Possono essere ricaricati i dati sicuri specifici di un cliente. Per informazioni sulla procedura, vedere Ripristino.

25.4.3 Arresto di OpenScape Business X

Con la funzione **Arresta sistema** è possibile arrestare in modo controllato i sistemi di comunicazione OpenScape Business X.

25.4.3.1 Come arrestare OpenScape Business X

Con la funzione **Arresta sistema** è possibile arrestare in modo controllato i sistemi di comunicazione OpenScape Business X.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Riavvia / Ricarica**.
3) Fare clic su **Arresta sistema**, quindi su **OK**. Il sistema di comunicazione verrà arrestato in modo controllato.

Suggerimento: OpenScape Business X1/X3/X5: la successiva inizializzazione del sistema di comunicazione è

possibile solo dopo aver scollegato e ricollegato il sistema alla presa di rete.

OpenScape Business X8: la successiva inizializzazione del sistema di comunicazione è possibile solo dopo aver scollegato e ricollegato tutte le fonti di alimentazione LUNA2.

25.4.4 PIN per l'arresto controllato di OpenScape Business X

L'attivazione dello spegnimento tramite telefono di sistema è protetto da PIN.

All'attivazione tramite un telefono di sistema è sempre necessario inserire il PIN impostato nel sistema di comunicazione. La configurazione di questo PIN viene eseguita da un amministratore con il profilo **Advanced**.

25.4.4.1 Come configurare un PIN per l'arresto controllato di OpenScape Business X

Il PIN si applica per l'attivazione di un arresto tramite un telefono di sistema.

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Riavvia/Ricarica**.
3) Fare clic su **Abilita/disabilita arresto**.
4) Nel campo **PIN** immettere il PIN a sei cifre desiderato.
5) Fare clic su **Salva**, quindi su **OK**.

Passaggi successivi

L'attivazione di un arresto tramite un telefono di sistema richiede l'inserimento del codice corrispondente (codice predefinito = *997) e quindi di un PIN a sei cifre.

- Per telefoni IP: è possibile effettuare l’arresto controllato dai primi due dispositivi configurati.
- Per telefoni UP0: è possibile effettuare l’arresto controllato da ognuno di questi telefoni. In questo caso, i client IP non hanno i diritti per effettuare l’arresto.

25.4.5 Riavvio della UC Booster Card (scheda applicazioni OCAB)

Con la funzione **Riavvia scheda applicazioni**, l'amministratore può riavviare in modo controllato la scheda applicazioni OCAB, comprensiva dell'applicazione UC (UC Smart o UC Suite).

In caso di riavvio, le connessioni a tutte le applicazioni attive, ad esempio myPortal for Desktop e myAttendant, vengono interrotte. Dopo l'inizializzazione, tutte le connessioni vengono automaticamente ripristinate.

Inoltre, vengono riavviati anche l'interfaccia CSTA, Presence Manager, Announcement Player, Media Extension Bridge e Open Directory Service.

25.4.5.1 Come attivare il riavvio della UC Booster Card (scheda applicazioni OCAB)

Con la funzione **Riavvia scheda applicazioni**, è possibile riavviare in modo controllato la scheda applicazioni OCAB, comprensiva dell'applicazione UC (UC Smart o UC Suite).

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Suggerimento: In caso di riavvio, le connessioni a tutte le applicazioni attive, ad esempio myPortal for Desktop e myAttendant, vengono interrotte. Dopo l'inizializzazione, tutte le connessioni vengono automaticamente ripristinate.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Riavvia / Ricarica**.
3) Fare clic su **Riavvia la scheda applicazioni**, quindi su **OK**. La UC Booster Card (scheda applicazioni OCAB) esegue il riavvio.

25.4.6 Ricarica della UC Booster Card (scheda applicazioni OCAB)

Tramite la funzione **Ricarica UC Booster Card** è possibile ricaricare la scheda applicazioni OCAB comprensiva dell'applicazione di comunicazione unificata (UC Smart o UC Suite).

La ricarica della UC Booster Card consente di riportare la scheda alle impostazioni di fabbrica e successivamente di rimuoverla dal sistema. Ciò può essere necessario ad esempio se la scheda non deve più essere usata nel sistema poiché si è passati a utilizzare un UC Booster Server o se la scheda deve essere integrata in un altro/nuovo sistema OpenScape Business.

Tutti i dati specifici del cliente e di diagnostica presenti sulla UC Booster Card verranno cancellati e il sistema verrà spento. Successivamente il sistema verrà scollegato dalla rete elettrica e la UC Booster Card rimossa.

Dopo aver rimosso la UC Booster Card e riavviato il sistema, è necessario creare un nuovo set di backup, poiché i dati di configurazione sono stati modificati e il set di backup precedente non è più compatibile. Se in precedenza il disco rigido della UC Booster Card era utilizzato come supporto di backup, è ora necessario selezionare un altro supporto di backup, ad esempio un'unità di rete, un dispositivo USB o un server FTP/FTPS (vedere anche il capitolo Backup e ripristina).

25.4.6.1 Come attivare la ricarica della UC Booster Card (scheda applicazioni OCAB)

Con la funzione **Ricarica UC Booster Card**, è possibile ricaricare la scheda applicazioni OCAB, comprensiva dell'applicazione UC (UC Smart o UC Suite).

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Riavvia / Ricarica**.
3) Fare clic su **Ricarica scheda UC Booster**, quindi su **OK**. Si viene disconnessi dal WBM. La scheda viene quindi riportata alle impostazioni di fabbrica e il sistema viene arrestato.
4) Non appena il LED RUN verde sulla scheda madre e i LED del controller della UC Booster Card sono completamente spenti, scollegare il sistema dalla rete elettrica e rimuovere la UC Booster Card (vedere Backup e ripristina).

25.4.7 Riavvio dell'applicazione UC

Con la funzione **Riavvia applicazione UC**, l'amministratore può riavviare in modo controllato l'applicazione UC (UC Smart o UC Suite).

In caso di riavvio dell'applicazione UC, le connessioni a tutte le applicazioni attive, ad esempio myPortal for Desktop e myAttendant, vengono interrotte. Dopo l'inizializzazione, tutte le connessioni vengono automaticamente ripristinate.

25.4.7.1 Come eseguire il riavvio dell'applicazione UC

Con la funzione **Riavvia applicazione UC**, è possibile riavviare l'applicazione UC (UC Smart o UC Suite).

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Suggerimento: In caso di riavvio, le connessioni a tutte le applicazioni attive, ad esempio myPortal for Desktop e myAttendant, vengono interrotte. Dopo l'inizializzazione, tutte le connessioni vengono automaticamente ripristinate.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Riavvia/Ricarica**.
3) Fare clic su **Riavvia applicazione UC**, quindi su **OK**. L'applicazione UC esegue il riavvio.

25.5 Gestione inventario

Per Gestione inventario si intende il rilevamento dello stato corrente dei sistemi di comunicazione OpenScape Business X e OpenScape Business S e la configurazione dell'hardware dei sistemo di comunicazione OpenScape Business X.

25.5.1 Stato del sistema

Lo stato corrente dei sistema di comunicazione OpenScape Business X e OpenScape Business S può essere comunicato da un amministratore con WBM. Si possono richiamare informazioni sullo stato dell'utente, della connessione, dell'ITSP, della VPN e dell'elenco degli indirizzi IP configurati.

Stato utente

Lo stato utente consente di richiedere le seguenti informazioni sull'utente configurato:

- Numero di telefono dell'utente
- Servizio
- Tipo di dispositivo
- Indirizzo IP (inoltre, con i telefoni di sistema viene visualizzato un collegamento che consente di aprire il WBM del telefono.)
- Indirizzo MAC
- Versione software corrente
- Versione HW
- Stato (attivato/disattivato)

Stato connessione

Lo stato connessione consente di richiedere informazioni sulle connessioni esistente ai partner PSTN (Public Switched Telephone Network, ad esempio reti di telecomunicazione pubbliche o private) del sistema di comunicazione OpenScape Business X.

Stato ITSP

Lo stato ITSP consente di richiedere informazioni sullo stato corrente di ITSP (Internet Telephony Service Provider) preconfigurati o aggiunti. Viene inoltre visualizzato quali utenti sono configurati per ciascun ITSP.

Lo stato di ogni ITSP attivo viene segnalato dal colore della casella corrispondente (verde = OK, arancione = presenti errori di configurazione per almeno un utente).

Stato VPN

Lo stato VPN consente di richiedere informazioni sul tunnel VPN configurato del sistema di comunicazione OpenScape Business X.

Panoramica indirizzi IP

Vengono visualizzati gli indirizzi IP configurati nel sistema di comunicazione OpenScape Business X.

Oltre a ciò, viene indicato tramite quale procedura guidata e quali menu è possibile configurare gli indirizzi IP in modalità Esperti.

Viene inoltre visualizzata una panoramica della scheda Booster e delle interfacce Ethernet della scheda madre.

25.5.1.1 Come richiedere lo stato utente

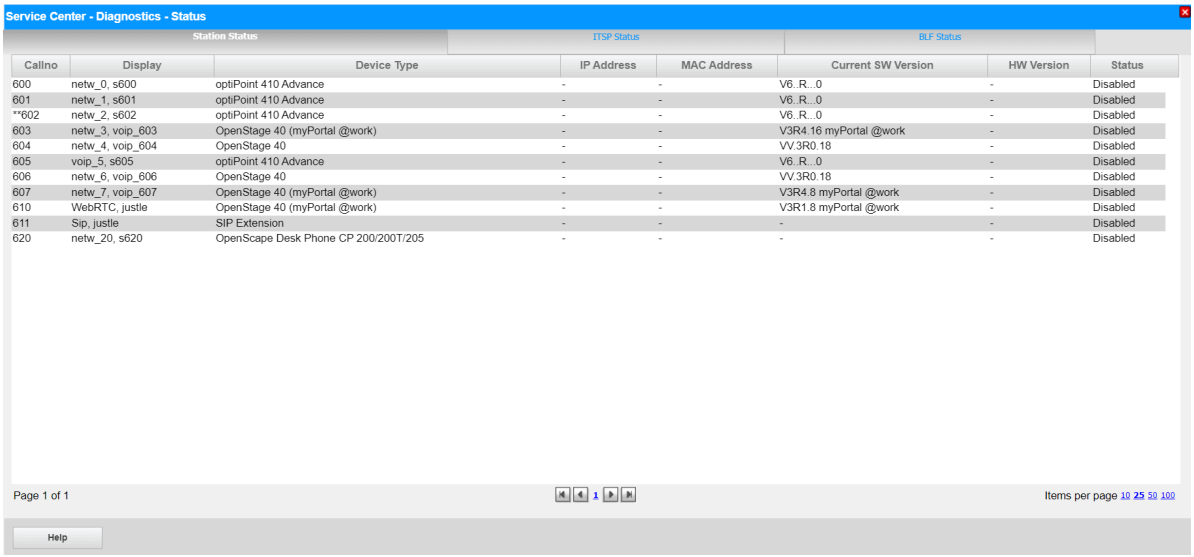
La procedura guidata **Stato** consente di segnalare lo stato corrente di tutti gli utenti configurati.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Stato**.
3) Fare clic sulla scheda **Stato utente**. Viene visualizzato lo stato di tutti gli utenti configurati.



4) Fare clic su **Fine**.

25.5.1.2 Come richiedere lo stato della connessione

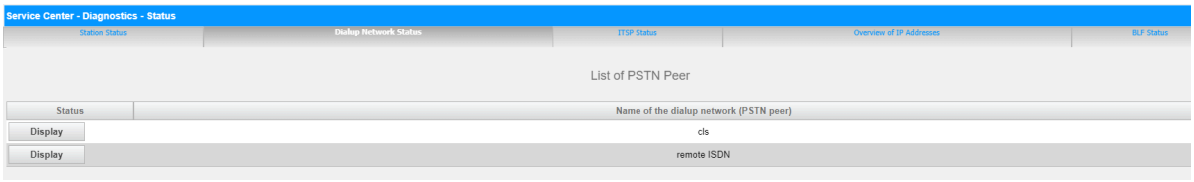
La procedura guidata **Stato** consente di rilevare lo stato corrente del partner PSTN di un sistema di comunicazione OpenScape Business X.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Stato**.
3) Fare clic sulla scheda **Stato connessione remota**. Viene visualizzato l'elenco di tutti i componenti del profilo di traccia (Partner PSTN).
4) Nella riga della connessione desiderata (Partner PSTN), fare clic su **Visualizza**. Viene visualizzato lo stato corrente di questa connessione (partner PSTN).



5) Se si desidera visualizzare le informazioni di stato di un'altra connessione (partner PSTN), procedere come descritto al passaggio 3.
6) Fare clic su **OK**, quindi su **Fine**.

25.5.1.3 Come richiedere lo stato ITSP

La procedura guidata **Stato** consente di segnalare lo stato corrente del provider di servizi di telefonia Internet (ITSP).

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Stato**.
3) Fare clic sulla scheda **Stato ITSP**. Viene visualizzato lo stato corrente dell'ITSP preconfigurato ed, eventualmente, di quelli aggiunti in un secondo tempo.
4) Per ottenere maggiori informazioni sulla connessione SIP, fare clic su **Diagnostica**.
5) Fare clic su **Fine**.

25.5.1.4 Come visualizzare gli indirizzi IP

Con la procedura guidata **Stato** è possibile richiamare un elenco degli indirizzi IP configurati in un sistema di comunicazione OpenScape Business X. Oltre a ciò, viene indicato tramite quale procedura guidata e quali menu è possibile configurare gli indirizzi IP in modalità Esperti.

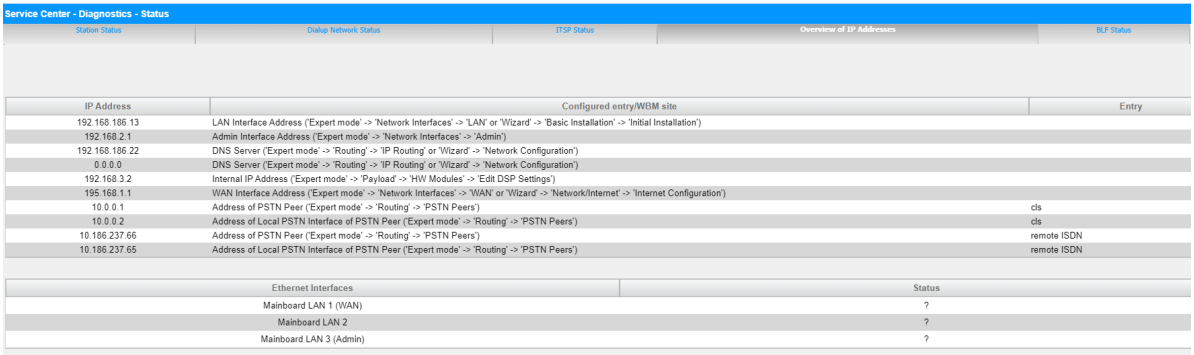
Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.

2) Nella struttura di navigazione fare clic su **Diagnostica** > **Stato**.
3) Fare clic sulla scheda **Panoramica indirizzi IP**. Viene visualizzato un elenco degli indirizzi IP configurati nel sistema di comunicazione.



4) Fare clic su **Fine**.

25.5.2 Inventario

L'inventario consente all'amministratore di recuperare informazioni sull'hardware e sul software di OpenScape Business X e sul software di OpenScape Business S.

OpenScape Business X

Vengono recuperati di seguenti dettagli:

- Sistema di comunicazione

  Tra le altre cose, vengono visualizzate le seguenti informazioni:

  – Rappresentazione grafica del sistema di comunicazione e delle schede
  – Numero di serie della scheda madre, indirizzo MAC, indirizzo IP, nome host e versione del software
  – Tipo di CPU e RAM (in GB) del sistema
  – Dettagli sulla quantità di memoria, compreso lo spazio disponibile e utilizzato sulla scheda SDHC
  – Stato di tutte le applicazioni
- Schede

  Le informazioni visualizzate includono: slot, tipo, numero di serie e stato di tutte le schede installate.
- Scheda UC Booster (scheda di applicazione OCAB), se disponibile

  Tra le altre cose, vengono visualizzate le seguenti informazioni:

  – Indirizzo MAC, indirizzo IP, nome host e versione del software
  – Dettagli sulla quantità di memoria, compreso lo spazio disponibile e utilizzato sul disco rigido.
  – Stato di tutte le applicazioni
  – Panoramica di tutte le interfacce delle schede Booster

  Il link **Scheda UC Booster accessibile** nella home page di WBM indirizza l'utente al **Centro assistenza > Inventario >Scheda Booster** per una vista

dettagliata. Il link sarà presente anche se c'è un problema con la scheda Booster e il testo mostra **Scheda UC Booster non accessibile**.

A seconda dell'errore, nella pagina iniziale di WBM vengono visualizzati i seguenti messaggi di errore:

1) Link del circuito inter-integrato con scheda Booster non possibile
2) Connettività Internet tramite protocollo v6 alla scheda Booster non possibile
3) Connettività Internet tramite protocollo v4 alla scheda Booster non possibile
4) Connettività Secure Socket Shell alla scheda Booster non possibile
5) Connettività in rete del file system alla scheda Booster non possibile
6) Una o più interfacce Ethernet sono in modalità Half Duplex, si consiglia vivamente di utilizzare la modalità Full Duplex

OpenScape Business S

Vengono recuperati di seguenti dettagli:

- Software

  Tra le altre cose, vengono visualizzate le seguenti informazioni: Indirizzo MAC, indirizzo IP, nome host e versione del software.
- Informazioni sul disco rigido

  Dettagli sulla quantità di memoria, compresa quella disponibile e quella utilizzata.
- Applicazioni

  Vengono visualizzate tutte le applicazioni e i rispettivi stati.

25.5.2.1 Come controllare l'inventario di OpenScape Business X

La procedura guidata **Inventario** consente di verificare lo stato di aggiornamento dell'hardware e del software dei sistemi di comunicazione OpenScape Business X.

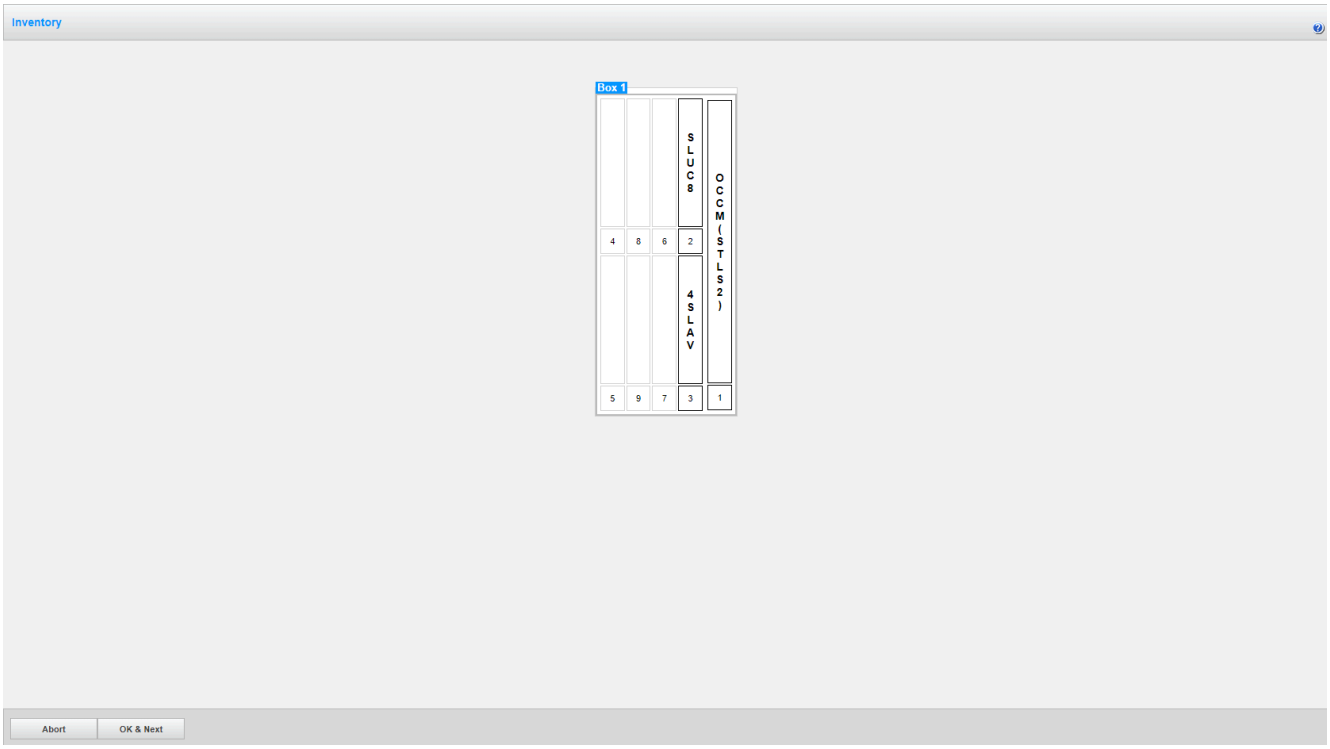
Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

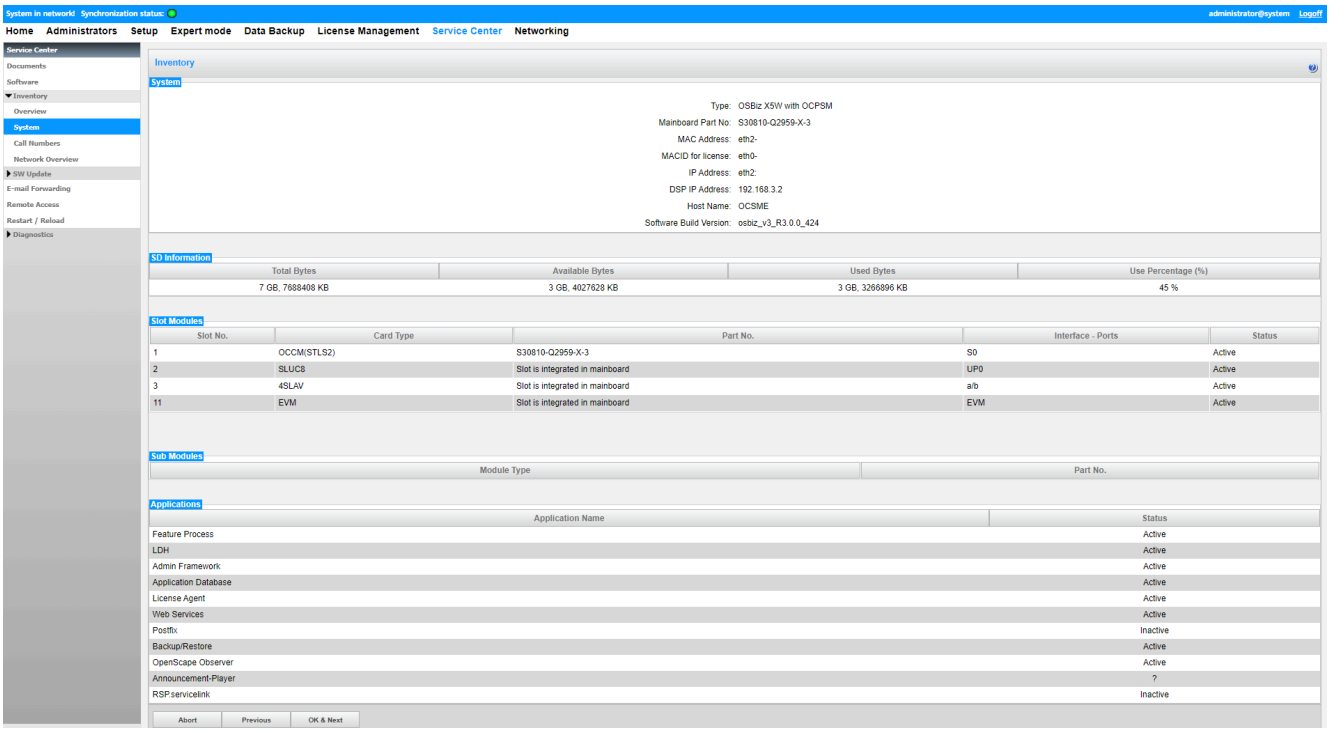
Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.

2) Nella struttura di navigazione, fare clic su **Inventario** > **Panoramica**. Viene visualizzata una rappresentazione grafica del sistema di comunicazione e dei moduli.



3) Fare clic su **OK & Avanti**. Vengono visualizzate le informazioni sul sistema di comunicazione, sullo spazio di memoria occupato e libero della scheda SDHC, sui moduli e sugli stati delle applicazioni.



4) Fare clic su **OK & Avanti**. L'informazione successivamente visualizzata dipende dalla presenza o meno di una UC Booster Card (scheda applicazioni OCAB) nel sistema di comunicazione:
   a) Se il sistema di comunicazione non è dotato di una UC Booster Card: Vengono visualizzate informazioni sull'assegnazione dei numeri di telefono ai moduli.
   b) Se il sistema di comunicazione è dotato di una UC Booster Card: Vengono visualizzate informazioni sulla scheda OCAB, sullo spazio di archiviazione disponibile e utilizzato sul disco rigido e sullo stato dell'applicazione e sullo stato delle interfacce della Booster Card.

      Fare clic su **OK & Avanti**. Vengono visualizzate informazioni sull'assegnazione dei numeri di telefono ai moduli.
5) Fare clic su **Fine**.

25.5.2.2 Come controllare l'inventario di OpenScape Business S

La procedura guidata **Inventario** consente di verificare lo stato di aggiornamento del software OpenScape Business S.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Inventario**. Vengono visualizzate informazioni sul software del sistema di comunicazione, sullo spazio su disco disponibile e sullo stato delle applicazioni.

25.6 Azioni automatiche

Questa funzione consente di definire le azioni da eseguire una tantum o regolarmente. Tali azioni possono quindi essere eseguite, al momento appropriato e in modo automatico, dal sistema di comunicazione.

25.6.1 Azione automatica Garbage Collection

Con l'azione automatica Azione automatica Garbage Collection, è possibile eseguire periodicamente una pulizia della memoria del sistema di comunicazione. Al termine della pulizia della memoria, il sistema di comunicazione si riavvia.

Nella visualizzazione dell'albero dei menu, il colore dei punti elenco consente di distinguere lo stato dell'azione (verde = azione attivata, rosso = azione non attivata).

Selezionando **Avvia/arresta azione** è possibile avviare un'azione disattivata (punto elenco rosso)e, viceversa, disattivare un'azione attiva (punto elenco verde).

Per impostazione predefinita, l'azione automatica Garbage Collection non è attivata.

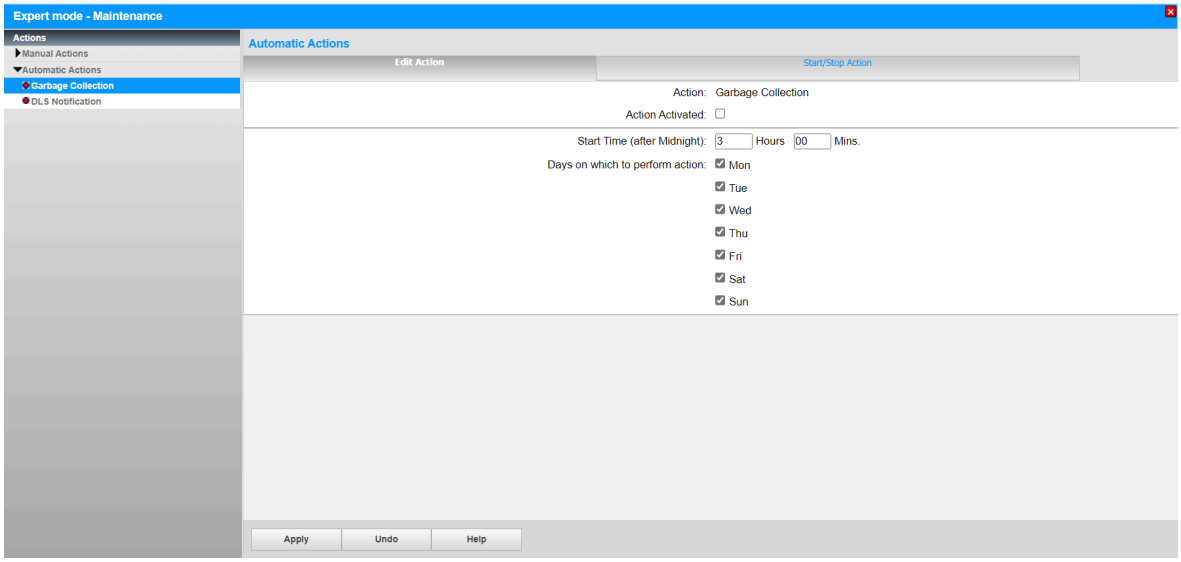
25.6.1.1 Come modificare l'azione automatica Garbage Collection

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Azioni**.
3) Nella struttura dei menu, selezionare **Azioni** > **Azioni automatiche** > **Garbage Collection**.
4) Fare clic sulla scheda **Modifica azione**.



5) Selezionare l'impostazione desiderata:
   - Se è necessario eseguire l'azione Garbage Collection, selezionare la casella di controllo **Azione attivata**.
   - Se non deve essere eseguita l'azione Garbage Collection, deselezionare la casella di controllo **Azione attivata**.
6) Modificare come necessario **Avvio dopo la mezzanotte**.

   Nel campo **Ore** inserire l'ora e nel campo **Min.** i minuti trascorsi i quali deve essere avviata l'azione.

   Esempio: nel campo **Ore** è stato inserito `3` e nel campo **Min.** `30`. Ciò significa che l'azione Garbage Collection viene eseguita la mattina alle 3:30.
7) Modificare i giorni della settimana come necessario con **Esegui azione i seguenti giorni della settimana**.

   Selezionare la casella di controllo dei giorni della settimana in cui l'azione deve essere eseguita. Deselezionare la casella di controllo dei giorni della settimana in cui l'azione non deve essere eseguita.
8) Fare clic su **Applica**, quindi su **OK**.

25.6.1.2 Come avviare (attivare) l'azione automatica Garbage Collection

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Azioni**.
3) Nella struttura dei menu, fare clic su **Azioni** > **Azioni automatiche**. Nella struttura dei menu viene visualizzato il nome di tutte le azioni automatiche. Le azioni non attive sono contrassegnate da un punto elenco rosso. Le azioni attive sono contrassegnate da un punto elenco verde.
4) Nella struttura dei menu fare clic su **Garbage Collection**.
5) Fare clic sulla scheda **Avvia/arresta azione**.
6) Fare clic su **Avvia**, quindi su **OK**.

25.6.1.3 Come arrestare (disattivare) l'azione automatica Garbage Collection

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Azioni**.
3) Nella struttura dei menu, fare clic su **Azioni** > **Azioni automatiche**. Nella struttura dei menu viene visualizzato il nome di tutte le azioni automatiche. Le azioni non attive sono contrassegnate da un punto elenco rosso. Le azioni attive sono contrassegnate da un punto elenco verde.
4) Nella struttura dei menu fare clic su **Garbage Collection**.
5) Fare clic sulla scheda **Avvia/arresta azione**.
6) Fare clic su **Arresta**, quindi su **OK**.

25.6.2 Azione automatica Notifica DLS

Con l'azione automatica Notifica DLS, è possibile avviare la registrazione automatica su un server DLS esterno dopo l'inizializzazione del sistema di comunicazione.

Nella visualizzazione dell'albero dei menu, il colore dei punti elenco consente di distinguere lo stato dell'azione (verde = azione attivata, rosso = azione non attivata).

Selezionando **Avvia/arresta azione** è possibile avviare un'azione disattivata (punto elenco rosso)e, viceversa, disattivare un'azione attiva (punto elenco verde).

Per impostazione predefinita, l'azione automatica Notifica DLS non è attivata.

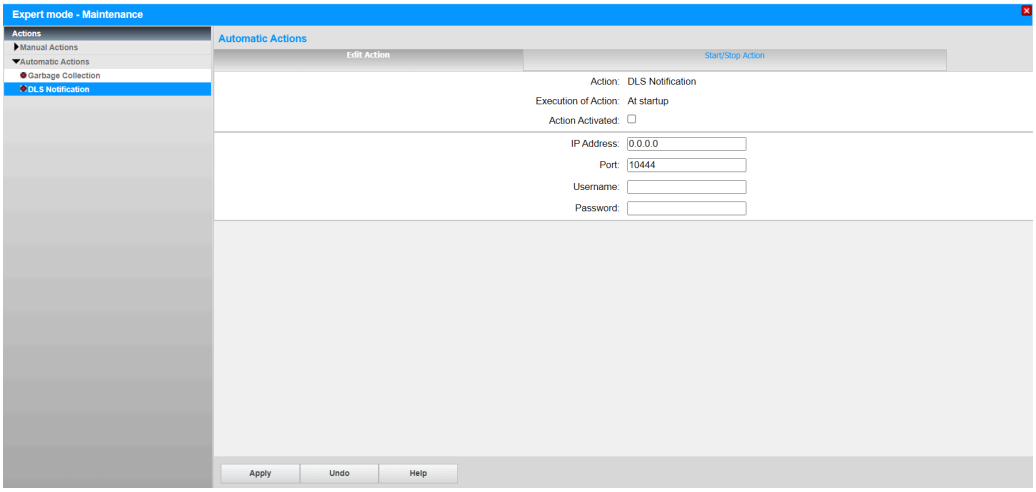
25.6.2.1 Come modificare l'azione automatica notifica DLS

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Azioni**.
3) Nella struttura dei menu selezionare **Azioni** > **Azioni automatiche** > **Avviso DLS**.
4) Fare clic sulla scheda **Modifica azione**.



5) Selezionare l'impostazione desiderata:
   - Se è necessario eseguire l'azione DLS Notification, selezionare la casella di controllo **Azione attivata**.
   - Se non deve essere eseguita l'azione DLS Notification, deselezionare la casella di controllo **Azione attivata**.
6) Modificare se necessario il campo **Indirizzo IP** immettendo l'indirizzo IP del server DLS esterno.
7) Modificare se necessario il campo **Porta** immettendo la porta del server DLS esterno.
8) Modificare se necessario il campo **Nome utente** immettendo il nome utente per la registrazione sul server DLS esterno.
9) Modificare se necessario il campo **Password** immettendo la password per la registrazione sul server DLS esterno.
10) Fare clic su **Applica**, quindi su **OK**.

25.6.2.2 Come avviare (attivare) la notifica DLS automatica delle azioni

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Manutenzione** > **Azioni**.
3) Nella struttura dei menu, fare clic su **Azioni** > **Azioni automatiche**. Nella struttura dei menu viene visualizzato il nome di tutte le azioni automatiche. Le azioni non attive sono contrassegnate da un punto elenco rosso. Le azioni attive sono contrassegnate da un punto elenco verde.
4) Nella struttura dei menu fare clic su **DLS Notification**.
5) Fare clic sulla scheda **Avvia/arresta azione**.
6) Fare clic su **Avvia**, quindi su **OK**.

25.6.2.3 Come arrestare (disattivare) la notifica DLS automatica delle azioni

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Azioni**.
3) Nella struttura dei menu, fare clic su **Azioni** > **Azioni automatiche**. Nella struttura dei menu viene visualizzato il nome di tutte le azioni automatiche. Le azioni non attive sono contrassegnate da un punto elenco rosso. Le azioni attive sono contrassegnate da un punto elenco verde.
4) Nella struttura dei menu fare clic su **DLS Notification**.
5) Fare clic sulla scheda **Avvia/arresta azione**.
6) Fare clic su **Arresta**, quindi su **OK**.

25.6.3 Meccanismo di avviso per la scadenza delle schede SDHC

L'azione automatica Meccanismo di avviso per la scadenza SDHC è un metodo per ottenere informazioni sullo stato di salute delle schede SDHC mediante un controllo del file system all'avvio. Si avvia una procedura guidata WBM che dirige il tecnico nel processo di impostazione di un orario in cui il sistema dovrà eseguire un riavvio ed effettuare il controllo.

Nota: Se non vengono identificati errori del file system dal controllo, **Stato di salute scheda** verrà impostato su verde o su giallo anche se gli errori sono stati segnalati in precedenza.

Tutte le informazioni vengono registrate nella Traccia clienti. L'azione automatica Meccanismo di avviso per la scadenza SDHC è disattivata per impostazione predefinita

---

Nota: Questa opzione determina un riavvio del sistema, visualizzando il riquadro di avviso"`Nota: per riavviare il sistema, premere OK.`"

La schermata iniziale WBM riconosce due stati:

- Se le informazioni del sistema sono disponibili, nella schermata iniziale viene visualizzato un testo che indica lo stato generale della scheda: "**Stato di salute scheda**" (verde, giallo, rosso o grigio).

  La durata generale della scheda viene calcolata in base alle specifiche del produttore e ai cicli di scrittura medi del sistema. Sono disponibili valori diversi per la durata della scheda. Questa informazione è presente insieme ad altre nella pagina di controllo della salute SDHC in WBM.

  All'interno del sistema sono memorizzate una durata stimata di 4 anni per le schede standard e una durata di 10 anni per quelle High endurance.

  Nota: I valori stimati per la durata costituiscono esclusivamente la base per il meccanismo di avviso dello stato di salute della scheda integrato. Tali valori non implicano automaticamente che una scheda sia difettosa una volta terminato il periodo indicato per la durata.

  Lo stato di salute verde indica che la scheda non ha ancora raggiunto la durata stimata e che il file system non presenta problemi.

  Lo stato di salute giallo indica che la scheda ha raggiunto la durata stimata.

  Lo stato di salute rosso indica che sono stati rilevati oltre 50 errori del file system.

  Lo stato di salute grigio indica che la scheda non è supportata o che non è possibile recuperare le informazioni relative alla scheda. La scheda SDHC deve essere sostituita con un tipo supportato.

  Il meccanismo di avviso per lo stato di salute giallo si basa sulla data di produzione e sulla durata stimata della scheda. Poiché le schede possono essere conservate in magazzino per lungo tempo prima di essere utilizzate in OpenScape Business, anche la data di creazione del file system viene considerata all'interno dell'algoritmo di calcolo.

  Di seguito viene visualizzata una tabella di calcolo per lo stato di salute della scheda con una durata stimata di 4 anni.

Fattore	**Anni e peso**									
Data di produzione	< 4 anni	< 5 anni		< 6 anni		< 7 anni		< 8 anni		< 8 anni
File system creato	< 4 anni	< 4 anni	4 - 5 anni	< 4 anni	4 - 6 anni	< 3 anni	3 - 7 anni	< 2 anni	2 - 8 anni	-
Stato di salute	Verde	Verde	Giallo	Verde	Giallo	Verde	Giallo	Verde	Giallo	Giallo

- Se le informazioni non sono disponibili viene visualizzato: "**Stato di salute scheda** sconosciuto".

  Nota: Nel caso in cui il file system sia danneggiato, è necessario scaricare l'immagine appropriata del SW di sistema da SWS e copiarla sulla scheda SDHC utilizzando lo strumento Card Manager. Dopo avere avviato il sistema con la nuova scheda SDHC, è possibile ripristinare la configurazione utilizzando l'ultimo backup.

Inoltre il testo "**Stato di salute scheda**" fornisce un collegamento alla "Pagina azioni"

25.6.3.1 Come impostare una notifica in caso di errori nella scheda SDHC

Se la funzione di controllo del file integrata segnala un numero di errori superiore alla soglia (50 errori) o se il sistema non riesce più a leggere/scrivere dalla/sulla scheda SDHC durante il normale funzionamento, il sistema invia una notifica con un'e-mail o un evento SNMP.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Eventi**.
3) Nella struttura dei menu fare clic su **Eventi** > **Tabella delle reazioni**. Nella struttura dei menu vengono visualizzati i nomi della tabella delle reazioni.
4) Selezionare **FP_EVT_HW_067** nella struttura dei menu.
5) Selezionare una delle seguenti opzioni disponibili:
   a) Invia Trap SNMP.
   b) Invia e-mail.
6) Fare clic su **Applica**, quindi su **OK**.

Nota:

È necessario configurare l'indirizzo e-mail in **Modalità esperti > Manutenzione > Eventi > E-mail**.

25.6.3.2 Come avviare l'azione automatica Meccanismo di avviso per la scadenza SDHC

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Salvare il sistema con la funzione di backup su un supporto esterno.
2) Nella barra di navigazione fare clic su **Modalità esperti**.
3) Nella struttura di navigazione, fare clic su **Manutenzione** > **Azioni**.
4) Nella struttura dei menu, fare clic su **Azioni** > **Azioni automatiche**. Nella struttura dei menu viene visualizzato il nome di tutte le azioni automatiche.
5) Fare clic su **Controllo di salute SDHC** nella struttura dei menu.

   Vengono visualizzate la data e l'ora di **Ora del sistema locale** e **Ultimo controllo salute**. Viene inoltre visualizzato il contenuto del **file di registro**.

6) Selezionare una delle seguenti opzioni disponibili:
   a) Avvia immediatamente controllo di salute
   b) Avvia controllo di salute a una data specifica
7) Fare clic su **Applica**, quindi su **OK**.

25.6.3.3 Come clonare e cambiare una scheda SDHC

In generale, le schede SDHC hanno una durata limitata. Tale durata dipende principalmente dal numero di cicli di scrittura della scheda SDHC. OpenScape Business supporta un meccanismo di rilevamento integrato "Stato di salute SDHC" per la durata della scheda, nonché una funzione integrata "Backup dati SDHC", descritta di seguito, per la sostituzione della scheda SDHC esaurita e la creazione di una nuova scheda pienamente funzionale.

Nota: La funzione "Backup dati SDHC" è in grado di copiare il contenuto della scheda SDHC correntemente inserita nel sistema senza arrestarlo. Vedere anche Come rimuovere o eliminare nuovi utenti Unify Phone alla pagina 1196.

Una copia di backup dei dati rilevanti può essere salvata in diverse posizioni e diversi supporti di memorizzazione, come:

- Chiave USB connessa al sistema.
- Lettore di schede SDHC USB connesso al sistema.
- Unità Network File System (NFS).
- Unità Network File System (NFS) via USB.

Nota: Le opzioni chiave USB o lettore di schede SDHC USB non sono disponibili per OpenScape Business X1. In questo caso, il backup dei dati SDHC deve essere archiviato su un'unità NFS.

Qualora venga utilizzato un lettore di schede USB, esiste l'eventualità che non sia possibile accedere alla scheda SDHC o formattarla. In tal caso, è necessario utilizzare un altro lettore di schede USB o un'altra chiave USB.

Nel caso in cui si utilizzi un lettore di schede USB direttamente connesso al sistema e con la nuova scheda SDHC inserita, la funzione Backup dati SDHC integrata crea una scheda SDHC completamente funzionale. In tutti gli altri casi, crea un cosiddetto "file .tar" che contiene tutti i dati di sistema e di configurazione.

Nota: Il file .tar non può essere utilizzato dalla funzione di ripristino del sistema.

La dimensione della copia di backup dei dati SDHC (file .tar) dipende dai dati specifici del sistema e può aumentare fino a più GB se sono memorizzati file multimediali (messaggi vocali, record chiamate ecc.).

Per clonare e cambiare una scheda SDHC in un sistema in funzione, occorre attenersi alla seguente procedura:

1) Creare un file di backup dei dati SDHC con un supporto adatto (vedere Come creare un file di backup dei dati SDHC).
2) Creare una nuova scheda SDHC operativa comprensiva di tutti i dati del sistema (vedere Come utilizzare Card Manager per scrivere il software di comunicazione sulla scheda SDHC alla pagina 1341).
3) Spegnere il sistema, cambiare la scheda SDHC e riaccenderlo (vedere Come utilizzare Card Manager per scrivere il software di comunicazione sulla scheda SDHC alla pagina 1341).

25.6.3.4 Come creare un file di backup dei dati SDHC

Prerequisiti

Una chiave USB con almeno la stessa capacità della scheda SDHC del sistema o un lettore di schede USB con una nuova scheda SDHC inserita con almeno le stesse dimensioni della scheda del sistema o un'unità NFS (Network File System) alla quale si può accedere dal sistema.

Passo a passo

1) Nella barra di navigazione, fare clic su **Backup dati**.
2) Nella struttura di navigazione, fare clic su **Backup dati SDHC** > **Backup dati**.
3) Selezionare una delle seguenti opzioni disponibili in base al percorso e al supporto di memoria disponibili:
   a) NFS

      È necessario configurare un indirizzo server valido, il percorso pertinente e le credenziali di accesso valide.

      Fare clic su **Salva e verifica**.

      Nota: È disponibile un backup pianificato. È possibile pianificare una sola azione alla volta e l'utente sarà in grado di modificarla o annullarla.

   b) Lettore di schede

      Questa opzione crea una copia funzionale completa della scheda SDHC senza traccia e file di registro.

      Un lettore di schede SDHC USB con una scheda SDHC inserita deve essere collegato al sistema prima dell'avvio del processo di copia.

      Dopo l'avvio del processo, la scheda SDHC inserita viene formattata e tutti i file rilevanti vengono trasferiti sulla scheda SDHC inserita.

      Nota: Non rimuovere il lettore di schede SDHC USB o la scheda SDHC inserita prima che il processo sia terminato.

      Nota: La nuova scheda SDHC è completamente funzionale per l'uso immediato nel sistema OpenScape

Business. La nuova scheda contiene tutti i file e i dati tranne i file di registro e traccia.

Nota: È disponibile un backup pianificato. È possibile pianificare una sola azione alla volta e l'utente sarà in grado di modificarla o annullarla.

c) NFS via USB.

È necessario configurare un indirizzo server valido, il percorso pertinente e le credenziali di accesso valide.

Fare clic su **Salva e verifica**.

Nota: È disponibile un backup pianificato. È possibile pianificare una sola azione alla volta e l'utente sarà in grado di modificarla o annullarla.

d) USB.

Un dispositivo USB vuoto formattato FAT32 deve essere collegato al sistema.

Nota: Non rimuovere la chiave USB prima che il processo sia terminato.

Nota: Il file di dati di backup SDHC copiato (file .tar) può essere utilizzato nello strumento Card Manager per creare una scheda SDHC funzionale completa per il sistema.

Nota: È disponibile un backup pianificato. È possibile pianificare una sola azione alla volta e l'utente sarà in grado di modificarla o annullarla.

4) Fare clic su **OK & Avanti**. Viene visualizzata una finestra a parte in cui è mostrato l'avanzamento del backup.

Nota: Viene visualizzato un messaggio di errore se la condivisione NFS o l'USB non è compatibile, oppure se il supporto di memorizzazione non può essere formattato.

5) Il messaggio **Attività di backup conclusa correttamente** viene visualizzato dopo che il file di backup è stato copiato correttamente.

6) Fare clic su **Fine**.

Nota: L'ulteriore procedura differisce a seconda della posizione di memorizzazione e del supporto scelti.

In caso di utilizzo del lettore di schede SDHC con scheda SDHC, è possibile utilizzare immediatamente la nuova scheda SDHC.

In tutti gli altri casi, per generare una nuova scheda SDHC, il file di backup della scheda SDHC generato deve essere utilizzato in combinazione con lo strumento Card Manager.

Passaggi successivi

Seguire i passaggi per creare una nuova scheda SDHC operativa e modificarla nel sistema in funzione (vedere Come utilizzare Card Manager per scrivere il software di comunicazione sulla scheda SDHC).

25.6.3.5 Come sostituire una scheda SDHC

Prerequisiti

Si è connessi a WBM con il profilo **Advanced**.

Solo quando si utilizza UC Suite: UC Suite è stato avviato correttamente.

Il downgrade alla versione software precedente non è supportato. Se è installata una scheda con il software V2, è possibile ripristinare solo le release secondarie precedenti di V2.

È necessario utilizzare la versione corrente del software per evitare effetti collaterali.

Nota: Se la scheda SDHC è guasta e il sistema è inattivo, occorre utilizzare un backup precedente e ignorare le prime 10 fasi della procedura riportata di seguito. Vedere anche Come rimuovere o eliminare nuovi utenti Unify Phone alla pagina 1196.

Passo a passo

1) Nella barra di navigazione fare clic su **Backup e ripristina**.
2) Nella struttura di navigazione fare clic su **Backup - immediato.**
3) Nel campo **Commento**, immettere un commento per il set di backup per facilitare l'identificazione in caso di ripristino dei dati. Non utilizzare dieresi e caratteri speciali.
4) Se si desidera creare un set di backup comprensivo di messaggi vocali e annunci, selezionare l'opzione **Backup completo**.
5) Nell'area **Dispositivi**, selezionare l'unità di destinazione sulla quale si vuole salvare il set di backup.
6) Fare clic su **OK & Avanti**. L'avanzamento del processo di backup viene visualizzato in una finestra separata.

Nota: Se il pulsante **OK & Avanti** viene visualizzato in grigio, significa che non tutte le applicazioni (ad esempio,

la UC Suite) di cui occorre salvare i dati sono state avviate correttamente.

Se non si dispone dell'abilitazione per la directory archivio selezionata, viene visualizzato un messaggio di errore. Selezionare un'altra unità di destinazione o cambiare il percorso dell'archivio.

Se l'unità di destinazione non dispone di uno spazio di memoria sufficiente per il set di backup, il sistema visualizza un messaggio d'errore. Selezionare un'altra unità di destinazione o eliminare il set di backup e riavviare il backup.

Nota: Se per il backup si utilizza un supporto USB, attendere fino a quando il LED di tale supporto non smette di lampeggiare. A questo punto il backup sul supporto USB è completo. Rimuovere il supporto USB.

Nota: Oltre al set di backup è necessario salvare anche un file di testo associato al set di backup. Contiene informazioni sulla data e l'ora del backup e sulla versione software di cui è stato eseguito il backup.

---

7) Il backup ha esito positivo se viene visualizzato il messaggio **Backup completato! Viene visualizzato 100%**.

8) Se per il supporto di backup è stata attivata l'opzione **HTTPS**, è necessario salvare il set di backup e il corrispondente file di testo in una posizione a scelta. Per gli altri supporti di backup, questo avviene automaticamente. La finestra del browser deve restare aperta fino al termine dell'operazione di salvataggio del set di backup e del file di testo.

9) Fare clic su **Fine**.

10) Spegnere il sistema.

11) Rimuovere la scheda SDHC esistente.

12) Installare la nuova scheda SDHC.

13) Accendere il sistema.

Quando si installa una nuova scheda SDHC, la versione del software inclusa nella scheda con la configurazione predefinita viene installata automaticamente nel sistema. Dopo l'avvio, il sistema presenta l'indirizzo IP predefinito.

14) Nella barra di navigazione fare clic su **Backup e ripristina**.

15) Nella struttura di navigazione fare clic su **Ripristina**.

16) Nell'area **Dispositivi**, selezionare il supporto che contiene il set di backup da ripristinare.

17) Se per il supporto di backup è stata attivata l'opzione **HTTPS**, selezionare il percorso di memorizzazione del set di backup, quindi selezionare il set di backup stesso. Successivamente, navigare fino alla posizione di memorizzazione del file di testo e selezionarlo.

18) Se si è attivato un altro supporto di backup come **HTTPS**, nell'area Elenco dei set di backup disponibili, selezionare il set di backup che contiene i dati di configurazione da ripristinare.

19) Attendere fino a quando il file non viene caricato nel sistema, quindi fare clic su **OK & Avanti**. Si avvia il ripristino dei dati di configurazione. Viene visualizzato l'avanzamento del ripristino.

20) Dopo il messaggio **Ripristino completato con successo!** il sistema si riavvia automaticamente. Il ripristino ha esito positivo se il sistema è di nuovo operativo.

Nota: Dopo il ripristino, è necessario eliminare il dispositivo dal server RSP e riconfigurarlo.

25.7 Risparmio energia

La funzione Risparmio energia porta il sistema in condizioni di risparmio energetico sulla base del carico del sistema stesso. In questo modo, il fabbisogno energetico del sistema si riduce con un vantaggio per il rispetto dell'ambiente. Il periodo nel quale il sistema può passare alla condizione di risparmio energetico si può impostare (ad es. di notte).

La funzione Risparmio energia può essere attivata solo se l'interfaccia LAN del sistema si trova in Modo collegamento Ethernet **Auto**. In condizioni di risparmio energetico, l'interfaccia LAN del sistema passa automaticamente alla modalità Full duplex. Anche le interfacce LAN dell'infrastruttura collegata devono trovarsi in modalità Autosense.

Stato

- Stato attivo (Active Mode)

  Nello stato attivo le funzioni del sistema di comunicazione vengono utilizzate ed è presente un trasferimento di dati significativo fra il sistema e l'infrastruttura collegata.
- Stato di riposo (Idle Mode)

  Nello stato di riposo, solo poche funzioni del sistema di comunicazione vengono utilizzate e il trasferimento di dati fra il sistema e l'infrastruttura collegata non è significativo. Se viene avviata una funzione, il sistema passa dallo stato di riposo a quello attivo.
- Stato di risparmio energetico (Low Power Mode)

  Lo stato di risparmio energetico, a differenza di quello di riposo, presenta un fabbisogno di energia ridotto. Il sistema si trova in modalità Full duplex a 100 Mbit/s.

Esiste inoltre la possibilità di utilizzare il sistema in Modo collegamento Ethernet 100 Mbit/s Full duplex o 100 Mbit/s Half duplex)

25.7.1 Come attivare o disattivare la funzione Risparmio energia

Prerequisiti

L'interfaccia LAN della scheda madre, tramite la quale il sistema è connesso all'infrastruttura LAN, si trova in Modo collegamento Ethernet **Auto**.

Solo se è collegata una UC Booster Card: l'interfaccia LAN della UC Booster Card, tramite la quale la UC Booster Card è collegata all'infrastruttura LAN, si trova in Modo collegamento Ethernet **Auto**.

Le interfacce LAN dell'infrastruttura collegata (ad es. telefoni IP) si trovano in modalità Autosense.

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione fare clic su **Procedure guidate** > **Installazione di base**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Risparmio energia**.
4) Per attivare la funzione Risparmio energia:
   a) Selezionare la casella di controllo **Attivazione/disattivazione Risparmio energia**.
   b) In **Inizio di LowPowerMode** e **Fine di LowPowerMode**, immettere il periodo durante il quale il sistema di comunicazione deve passare alla modalità di risparmio energetico.
5) Se si desidera disattivare la funzione Risparmio energia, deselezionare la casella di controllo **Attivazione/disattivazione Risparmio energia**.
6) Fare clic su **OK & Avanti**. Le impostazioni vengono applicate.
7) Fare clic su **Fine**.

25.7.2 Modifica della modalità di collegamento Ethernet dell'interfaccia LAN

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Telefonia** > **Interfacce di rete**.
3) Selezionare Modalità collegamento Ethernet per l'interfaccia LAN nella scheda madre:
   a) Nella struttura dei menu, fare clic su **Scheda madre** > **LAN 2**. Il sistema è collegato all'infrastruttura LAN tramite l'interfaccia LAN 2.
   b) Se si desidera attivare il risparmio energetico, nell'elenco a discesa **Modalità collegamento Ethernet** selezionare la voce **Auto**.
   c) Se si desidera impostare il sistema sul risparmio energetico in modo permanente, nell'elenco a discesa **Modalità collegamento Ethernet** selezionare la voce **100HDX** o **100FDX**.

      Nota:

      Per le modalità di collegamento Ethernet **100HDX**, **100FDX** e **1000FDX** potrebbe non essere possibile attivare il risparmio energetico.

   d) Fare clic su **Applica**.

4) Solo se è installata una UC Booster Card: selezionare la modalità di collegamento Ethernet per l'interfaccia LAN della UC Booster Card.

a) Nella struttura dei menu, fare clic su **Scheda applicazioni** > **LAN 2** o **LAN 1**, in base all'interfaccia LAN utilizzata per collegare la UC Booster Card all'infrastruttura LAN (riconoscibile dal segno di spunta nelle caselle di controllo **Interfaccia attivata**).

b) Se si desidera attivare il risparmio energetico, nell'elenco a discesa **Modalità collegamento Ethernet** selezionare la voce **Auto**.

c) Se si desidera impostare il sistema sul risparmio energetico in modo permanente, nell'elenco a discesa **Modalità collegamento Ethernet** selezionare la voce **100HDX** o **100FDX**.

Nota:

Per le modalità di collegamento Ethernet **100HDX**, **100FDX** e **1000FDX** potrebbe non essere possibile attivare il risparmio energetico.

---

d) Fare clic su **Applica**.

25.8 Monitoraggio e manutenzione di OpenScape Business

OpenScape Business offre varie funzioni per monitorare lo stato del sistema nonché per rilevare e correggere gli errori.

25.8.1 Test della connessione di rete per OpenScape Business X

Attraverso una richiesta ICMP (Internet Control Message Protocol), è possibile testare la connessione di rete tra un sistema di comunicazione OpenScape Business X e l'indirizzo di destinazione con l'aiuto di pacchetti eco.

I pacchetti eco possono essere inviati tramite le funzioni sia **Ping** che **Traceroute**. Le conferme di risposta vengono visualizzate insieme ai tempi variabili.

Tramite la funzione **Traceroute** i pacchetti eco ICMP vengono inviati con valori TTL (Time-To-Live) diversi, sempre crescenti.

25.8.1.1 Come inviare ping

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Manutenzione** > **Diagnosi IP**.

3) Nella struttura dei menu selezionare **Scheda madre** > **Richiesta ICMP** > **Ping**.

4) Nel campo **Indirizzo di destinazione** immettere l'indirizzo IP della destinazione desiderata.

5) Nel campo **Numero di richieste eco da inviare**, immettere il numero desiderato (predefinito = 3).
6) Fare clic su **Invia**.

   Vengono quindi visualizzate le conferme di risposta unitamente ai tempi variabili.

25.8.1.2 Come un test del traceroute

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Diagnosi IP**.
3) Nella struttura dei menu selezionare **Scheda madre** > **Richiesta ICMP** > **Traceroute**.
4) Nel campo **Indirizzo di destinazione** immettere l'indirizzo IP della destinazione desiderata.
5) Nel campo **Byte TOS**, immettere il valore desiderato (predefinito = 0).
6) Fare clic su **Invia**.

   Vengono quindi visualizzate le conferme di risposta unitamente ai tempi variabili.

25.8.2 SNMP (Simple Network Management Protocol)

Il Simple Network Management Protocol (SNMP) è un protocollo di rete che consente di comandare e monitorare componenti di rete (ad esempio router, server, switch, stampanti, PC) da una stazione centrale (console di gestione). In questo caso il protocollo regola la comunicazione fra i componenti monitorati e la stazione di monitoraggio.

SNMP descrive la struttura dei pacchetti dati che si possono inviare e il procedere della comunicazione. SNMP è stato concepito in modo che qualsiasi dispositivo di rete possa essere incluso nel monitoraggio. Nelle attività della gestione di rete tramite SNMP rientrano

- il monitoraggio dei componenti di rete,
- il controllo e la configurazione in remoto dei componenti di rete,
- l'individuazione e la segnalazione degli errori.

Per il monitoraggio vengono definiti i cosiddetti Agenti. Si tratta di programmi che vengono eseguiti direttamente sui componenti da monitorare. Questi programmi sono in grado di rilevare lo stato dei componenti e di effettuare autonomamente impostazioni o rilasciare azioni. Con il supporto di SNMP è possibile stabilire una comunicazione fra la console di gestione centrale e gli agenti attraverso la rete.

Nota: OpenScape Business supporta SNMPv2c, ma risponde anche a richieste snmpget SNMPv1.

Gestione database informazioni MIB

Il volume di dati amministrabili tramite SNMP viene definito in cosiddetti MIB. I MIB sono modelli di dati che descrivono i componenti di rete da gestire in modo prestabilito. Il MIB dei sistemi di comunicazione OpenScape Business X può essere scaricato tramite il WBM (Centro assistenza)

I sistemi di comunicazione sono dotati di un agente SNMP che consente di accedere a una serie di dati del sistema contenuti nel database di gestione MIB. Il MIB fornisce informazioni di base sul sistema, informazioni relative allo stato, dati riferiti agli eventi, nonché informazioni sull'hardware installato (slot) e sulle connessioni configurate (porte).

SNMP consente il monitoraggio e l'amministrazione centralizzata dei componenti di rete e dello stesso sistemi di comunicazione. Tramite questo è possibile

- comunicare con il sistema di comunicazione via TCP/IP.
- accedere ai dati da parte di applicazioni di gestione esterne.
- eseguire interventi di manutenzione in remoto.
- visualizzare lo stato operativo del sistema di comunicazione.
- la trasmissione degli errori relativi al servizio (trap).

Comunità

L'accesso ai dati SNMP (MIB) viene regolato tramite le comunità. Occorre distinguere fra comunità di lettura, di scrittura e comunità Trap. Dietro una comunità si nasconde sempre un indirizzo IP.

Ad esempio, per concedere a un PC l'accesso in lettura ai dati SNMP (MIB), l'indirizzo IP del PC deve essere inserito nell'elenco delle comunità di lettura. Per poter usufruire dell'accesso in lettura e scrittura, l'indirizzo IP del PC deve essere incluso nell'elenco delle comunità di scrittura.

Le comunità Trap consentono di gestire i destinatari dei messaggi di errore (Trap).

Trap

In caso di problemi al sistema di comunicazione vengono creati Trap che informano sulla natura dell'errore e dei guasti. Esistono diversi tipi di Trap:

- Trap di sistema = errore di sistema che richiede un intervento immediato.
- Trap di servizio/prestazione = informazioni su problemi di prestazioni che non richiedono interventi particolari.

I trap sono classificati in base all'effetto e possono essere richiamati da un amministratore con il profilo **Expert** tramite il WBM. Viene visualizzato un elenco di tutti i Trap ricevuti, con le seguenti informazioni:

Colonna della tabella	Significato
VarBind1 (Gravità)	Classe di effetto del Trap Sono possibili le seguenti voci: Critico: Messaggio d'errore. L'errore ha conseguenze problematiche. Major: messaggio di errore. L'errore può avere conseguenze problematiche. Minor: messaggio di errore. L'errore non causa problemi particolari. Avvertenza: messaggi su un possibile problema a una procedura o in uno stato, non si tratta di messaggi di errore. Eliminati Informazioni: semplici messaggi di stato, non di errore. Intermediate status Other traps
VarBind2 (Nome)	Nome del Trap
Nome generico	Denominazione generale, ad esempio un nome specifico dell'azienda
Nome specifico	Tipo di Trap (1 = Software, 2 = Hardware)
Enterprise	–
Tempo	Ora dell'errore
Indice	Numero elenco

La visualizzazione dei Trap viene aggiornata ogni 30 secondi. I Trap sono ordinati in base al momento in cui si sono verificati.

Facendo clic sul nome di un Trap vengono visualizzati i dettagli corrispondenti.

Codice SNMP	Evento:voci registro	Significato	Misure richieste	Nota
Classe di errore 01 - Messaggi generali				
	Riavvio del sistema	Riavvio forzato (ripristino) dell'intero sistema con CDB corrente.	Nessuno	
FP_EVT_ADM_002	ricarica dello slot occupato	ricarica dello slot occupato		
FP_EVT_ADM_003	riavvio del sistema	riavvio del sistema		
FP_EVT_ADM_010	Riavvio del sistema SNMP	Riavvio forzato dell'intero sistema tramite SNMP.	Nessuno	
FP_EVT_ADM_014	Modifiche al DB locale SNMP	Modifiche "in loco" al database.	Nessuno	

Codice SNMP	Evento:voci registro	Significato	Misure richieste	Nota
FP_EVT_ADM_015	Modifiche al DB remoto SNMP	Modifiche "remote" al database.	Nessuno	
FP_EVT_ADM_016	Risultato SNMP APSXF	Messaggio di conferma del trasferimento APS tramite SNMP.	Nessuno	
FP_EVT_ADM_017	Autenticazione SNMP non riuscita	Tentativo di accesso non autorizzato.	Controllare le impostazioni del firewall in OpenScape Business/ Manager E (Firewall di rete).	
FP_EVT_ADM_019	Allarme sensore	La temperatura nell'alloggiamento di OpenScape Business è troppo alta.	Controllare la ventola e l'alimentazione dell'aria nell'alloggiamento da 19'. Prendere nota della temperatura ambiente.	
FP_EVT_ADM_020	Limite buffer CDR raggiunto	Overflow nel buffer CDR (informazioni CDR).	Verificare che le interfacce (V.24, LAN), le porte e la connessione funzionino o leggere i dati delle chiamate.	
FP_EVT_ADM_024	applicazione non autorizzata	Tentativo di accesso tramite un'applicazione non autorizzata.	Controllare le impostazioni del firewall in OpenScape Business/ Manager E (Firewall di rete).	
FP_EVT_ADM_025	rientro manuale da HiPath Manager			
Classe di errore 02 - Messaggi di gestione delle licenze				
Classe di errore 09 - Messaggi del modulo hardware				
FP_EVT_HW_034	perdita di frame attiva (STMD)	perdita di frame attiva (STMD)		
FP_EVT_HW_035	perdita di frame disattiva (STMD)	perdita di frame disattiva (STMD)		
FP_EVT_HW_036	slip rilevato su (STMD)	Si è verificato un bit slip su una linea ISDN.	Controllare la linea S0. Se necessario, ricaricare la scheda o eseguire un riavvio forzato. Se l'errore persiste, impostare una traccia ISDN.	Il problema potrebbe essere causato da frequenze di clock interne ed esterne asincrone. Possibile perdita di dati/connessione interrotta.
FP_EVT_HW_039	errore del segnale di indicazione di allarme disattivato (TMS2M)	Visualizzazione allarmi: L'errore S2M è stato corretto.	Nessuno	

Codice SNMP	Evento:voci registro	Significato	Misure richieste	Nota
FP_EVT_HW_040	errore minuto degradato attivo (TMS2M)	errore minuto degradato attivo (TMS2M)		
FP_EVT_HW_041	errore minuto degradato disattivato (TMS2M)	errore minuto degradato disattivato (TMS2M)		
FP_EVT_HW_042	nessun errore di segnale attivo (TMS2M/STMD)	Visualizzazione allarmi: Si è verificato un errore S2M. Nessuna connessione fisica disponibile.	Controllare la linea e la scheda S2M. Se necessario, ricaricare la scheda o eseguire un riavvio forzato. Se l'errore persiste, impostare una traccia ISDN.	
FP_EVT_HW_043	nessun errore di segnale disattivato (TMS2M/STMD)	Visualizzazione allarmi: L'errore S2M è stato corretto.	Nessuno	
FP_EVT_HW_046	errore di secondi grave attivo (TMS2M)	errore di secondi grave attivo (TMS2M)		
FP_EVT_HW_047	errore di secondi grave disattivato (TMS2M)	errore di secondi grave disattivato (TMS2M)		
FP_EVT_HW_052	orologio può essere utilizzato come rif. (TMS2M/STMD)	orologio può essere utilizzato come rif. (TMS2M/STMD)		
FP_EVT_HW_053	orologio non può essere utilizzato come riferimento	orologio non può essere utilizzato come riferimento		
FP_EVT_HW_060	Errore alimentazione accesso attivo (SLMO)	Errore alimentazione accesso attivo (SLMO)		
FP_EVT_HW_063	Errore ELIC attivo (SLMO/SLMC)	Errore ELIC attivo (SLMO/SLMC)		
FP_EVT_HW_064	Errore ELIC disattivato (SLMO/SLMC)	Errore ELIC disattivato (SLMO/SLMC)		
FP_EVT_HW_067	Errore OCTAT attivo (SLMC)	Errore OCTAT attivo (SLMC)		
FP_EVT_HW_096	errore sconosciuto da LW	errore sconosciuto da LW		
Classe di errore 11 - Messaggi generali				
FP_EVT_DEV_041	L1 asincrono attivo	L1 asincrono attivo		
FP_EVT_DEV_042	L1 asincrono disattivato	L1 asincrono disattivato		
FP_EVT_DEV_043	Errore di sovraccarico attivo	Errore di sovraccarico attivo		

Codice SNMP	Evento:voci registro	Significato	Misure richieste	Nota
FP_EVT_DEV_044	Errore di sovraccarico disattivato	Errore di sovraccarico disattivato		
FP_EVT_DEV_045	Errore di controllo in tempo reale attivo	Errore di controllo in tempo reale attivo		
FP_EVT_DEV_046	Informazioni optiPoint	Informazioni optiPoint		
FP_EVT_DEV_048	Rilevato errore di livello 2	Rilevato errore di livello 2		
FP_EVT_DEV_049	Rilevato errore di livello 3	Rilevato errore di livello 3		
FP_EVT_DEV_052	Altri errori	Altri errori		
FP_EVT_DEV_057	NO TEI disponibile	NO TEI disponibile		
FP_EVT_DEV_058	Troppi errori L1	Troppi errori di livello 1.	Controllare le linee, il terminale e la porta. Potrebbe essersi verificato un cortocircuito.	
FP_EVT_DEV_059	Accesso non configurato	Accesso non configurato		
Classe di errore 16 - Messaggi del sistema operativo				
FP_EVT_GEN_002	Errore nel pool di rilascio	Errore nel pool di rilascio	Impostare una traccia utilizzando le informazioni di BLS (Back Level Support). Creare un dump dello stack. Salvare un'istantanea.	
FP_EVT_GEN_004	Errore nell'invio OSF	Errore nell'invio OSF	Impostare una traccia utilizzando le informazioni di BLS (Back Level Support). Creare un dump dello stack. Salvare un'istantanea.	
FP_EVT_GEN_005	Errore nel timer OSF	Errore nel timer OSF	Impostare una traccia utilizzando le informazioni di BLS (Back Level Support). Creare un dump dello stack. Salvare un'istantanea.	

Codice SNMP	Evento:voci registro	Significato	Misure richieste	Nota
FP_EVT_GEN_010	RESTARTED: ripristino manuale	RESTARTED: ripristino manuale	Impostare una traccia utilizzando le informazioni di BLS (Back Level Support). Creare un dump dello stack. Salvare un'istantanea.	
FP_EVT_GEN_011	RESTARTED: ricarica manuale	RESTARTED a causa della ricarica manuale	Impostare una traccia utilizzando le informazioni di BLS (Back Level Support). Creare un dump dello stack. Salvare un'istantanea.	
FP_EVT_GEN_012	RESTARTED: Spegnimento	RESTARTED a causa dello spegnimento	Impostare una traccia utilizzando le informazioni di BLS (Back Level Support). Creare un dump dello stack. Salvare un'istantanea.	
FP_EVT_GEN_013	Backup KDS non eseguito	Backup KDS non eseguito	Impostare una traccia utilizzando le informazioni di BLS (Back Level Support). Creare un dump dello stack. Salvare un'istantanea.	
FP_EVT_GEN_014	RESTARTED: rest sconosciuto. Mancata corrispondenza ind. HW	RESTARTED a causa di rest sconosciuto. Mancata corrispondenza ind. HW	Impostare una traccia utilizzando le informazioni di BLS (Back Level Support). Creare un dump dello stack. Salvare un'istantanea.	
FP_EVT_GEN_015	registrazione errore generale	registrazione errore generale	Impostare una traccia utilizzando le informazioni di BLS (Back Level Support). Creare un dump dello stack. Salvare un'istantanea.	

Codice SNMP	Evento:voci registro	Significato	Misure richieste	Nota
FP_EVT_GEN_020	CSTA: lunghezza fuori intervallo	CSTA: lunghezza fuori intervallo	Impostare una traccia utilizzando le informazioni di BLS (Back Level Support). Creare un dump dello stack. Salvare un'istantanea.	
FP_EVT_GEN_024	inattività rilevata dopo il riavvio	inattività rilevata dopo il riavvio	Impostare una traccia utilizzando le informazioni di BLS (Back Level Support). Creare un dump dello stack. Salvare un'istantanea.	
FP_EVT_GEN_030	superati CSTA mon. pts	superati CSTA mon. pts	Impostare una traccia utilizzando le informazioni di BLS (Back Level Support). Creare un dump dello stack. Salvare un'istantanea.	
Classe di errore 19 - Messaggi dei servizi di rete				
FP_EVT_NWS_011	Il client SNTP su PCS non può essere attivato	Il client SNTP su PCS non può essere attivato		
Classe di errore 20 - Messaggi di elaborazione delle chiamate				
FP_EVT_CP_002	RS232: DSR non pronto	L'interfaccia RS232/ V.24 non funziona.	Controllare l'interfaccia, la linea e l'applicazione.	
FP_EVT_CP_013	modalità non collegate	È stato superato il numero massimo di percorsi di connessione consentiti.	Utilizzare lo strumento di pianificazione del progetto per testare la configurazione del sistema. Impostare una traccia utilizzando le informazioni da BLS. Creare un dump dello stack. Salvare un'istantanea.	
Classe di errore 21 - Messaggi di Device Handler				
FP_EVT_DH_004	Porta fuori servizio	Porta fuori servizio		
FP_EVT_DH_005	Porta in servizio	Porta in servizio		

Codice SNMP	Evento:voci registro	Significato	Misure richieste	Nota
FP_EVT_DH_016	Nome in S0/S2M msg scartato	Nome in S0/S2M msg scartato		
FP_EVT_DH_017	msg troppo lungo L3S int->est	msg troppo lungo L3S int->est		
FP_EVT_DH_018	msg troppo lungo L3S est->int	msg troppo lungo L3S est->int		
FP_EVT_DH_022	Rilevamento automatico PRI DMS250 prot	Rilevamento automatico PRI DMS250 prot		
FP_EVT_DH_023	Rilevamento automatico PRI NI2 prot		Rilevamento automatico PRI NI2 prot	I
FP_EVT_DH_024	Rilevamento automatico PRI 4ESS prot		Rilevamento automatico PRI 4ESS prot	
FP_EVT_DH_026	overflow del modulo chiave	overflow del modulo chiave		
FP_EVT_DH_027	Limite B-chan raggiunto	Limite B-chan raggiunto		
Classe di errore 23 - Messaggi di Device Handler				
FP_EVT_NW_060	blocco del sistema, nessun buffer disponibile	Blocco del sistema, buffer libero non più disponibile.	Impostare una traccia utilizzando le informazioni da BLS. Creare un dump dello stack. Salvare un'istantanea.	
Classe di errore 26 - Messaggi di amministrazione scheda				
FP_EVT_PR_001	scheda fuori servizio	La scheda specificata non funziona.	Nessuno	
FP_EVT_PR_003	altro tipo di scheda rispetto al tipo di scheda precedente	Tipo di scheda incompatibile. Lo slot è già preassegnato con un diverso tipo di scheda.	Sostituire la scheda o usare Assistant T per eliminare il tipo di scheda preassegnato in modo che la nuova scheda venga riconosciuta.	
FP_EVT_PR_004	scheda in servizio	La scheda specificata è operativa.	Nessuno	
FP_EVT_PR_005	errore durante la lettura del database	errore durante la lettura del database		
Classe di errore 28 - Messaggi di ripristino				

Codice SNMP	Evento:voci registro	Significato	Misure richieste	Nota
FP_EVT_RC_008	APS mancante in EventLog B	APS mancante in EventLog B	Nessuno	La versione APS corrente viene immessa quando viene copiata la memoria del registro eventi B. Questo facilita l'analisi.
Classe di errore 30 - Messaggi del software della scheda				
FP_EVT_LW_095	nessuna connessione USBS al sistema	nessuna connessione USBS al sistema		
Messaggi relativi a Resource Manager				
FP_EVT_RM_001	Configurazione errori di Resource Manager	Configurazione errori di Resource Manager		
Messaggi relativi a UPM				
FP_EVT_UPM_010	UPM: riavviato	UPM: riavviato		

Codice SNMP	Evento:voci registro	Significato	Misure richieste	Nota
MSG_DLSC_BOOTSTRAP_OK	Il client DLS è stato avviato correttamente.	Il client DLS è stato avviato correttamente.		
MSG_STRC_STOP	Secure Trace arrestato.	Secure Trace arrestato.		
MSG_STRC_START	Secure Trace avviato per i protocolli.	Secure Trace attivati dall'utente per i protocolli menzionati.		
MSG_SPE_CERT_MISSING	Certificato SPE mancante.	Nessun certificato SPE installato.	Importare certificato SPE e chiave privata (file PKCS#12).	
MSG_SPE_CERT_AVAIL	Certificato SPE disponibile.	Il certificato SPE è ora disponibile.		
MSG_SPE_CERT_UPDATED	Il certificato SPE è stato aggiornato correttamente.	Il certificato SPE è stato aggiornato correttamente.		
MSG_SPE_CERT_EXPIRED	Certificato SPE scaduto.	Il periodo di validità del certificato SPE installato è scaduto.	Installare un nuovo certificato valido.	
MSG_SPE_CRL_EXPIRED	Il CRL SPE per una CA specifica è scaduto.	CDP inaccessibile o CRL recuperato è scaduto.	Importare un certificato CA SPE con CRL validi configurati in CDP.	
MSG_SPE_CRL_AGGIORNATO	L'elenco CRL SPE per CA è stato aggiornato correttamente.	L'elenco CRL SPE per CA è stato aggiornato correttamente.		
MSG_SPE_ALL_CRLS_UPTODATE	Tutti i CRL SPE sono nuovamente aggiornati.	Tutti i CRL SPE sono nuovamente aggiornati.		

Codice SNMP	Evento:voci registro	Significato	Misure richieste	Nota
MSG_MIKEY_REBOOT	Mikey Stack: asserzione non riuscita.	Mikey Stack: asserzione non riuscita.		
MSG_IPSEC_REBOOT	Errore irreversibile nello stack IPSec.	Errore irreversibile nello stack IPSec.		
MSG_CAT_H323_REBOOT		Riavviare con H.323		
MSG_CAT_HSA_REBOOT		Riavviare con HAS		
MSG_GW_SUCCESSFULLY_STARTED				
MSG_IP_LINK_FAILURE				
MSG_IP_LINK2_FAILURE		IP-Link 1 su/giù		
MSG_IP_LINK3_FAILURE				
MSG_NEW_SW_AVAILABLE				
MSG_ADMIN_REBOOT		Riavviare con WBM/CLI-Admin, aggiornamento software o ripristino dati		
MSG_SYSTEM_REBOOT		Riavvio automatico, ad esempio con Garbage Collection		
MSG_EXCEPTION_REBOOT		Riavviare con eccezione SW		
MSG_GW_OBJ_MEMORY_ESAURITO		Memoria esaurita		
MSG_TLS_POOL_SIZE_EXCEEDED		Nessun altro pool interno		
MSG_OAM_RAM_THRESHOLD_REACHED		Limite RAM raggiunto		
MSG_OAM_DMA_RAM_THRESHOLD_REACHED		Limite DRAM raggiunto		
MSG_OAM_THRESHOLD_REACHED		Limite raggiunto, ad esempio, per memoria flash o pool IP		
MSG_OAM_HIGH_TEMPERATURE_EXCEPTION		Limite di temperatura raggiunto (troppo caldo)		
MSG_HACKER_ON_SNMP_PORT_TRAP		Accesso non autorizzato alla porta SNMP		
MSG_DVMGR_LAYER2_SERVICE_TRAP		Canale B su/giù		
MSG_SSM_NUM_OF_CALL_LEGS_2BIG	Più di 2 chiamate Legs: non supportato. CSID: %x/%x	Non sono consentite più di due chiamate Legs per sessione. Ciò ha reso instabile il software. Viene eseguito il riavvio necessario.		

Codice SNMP	Evento:voci registro	Significato	Misure richieste	Nota
MSG_SSM_SESSION_CREATION_FAILED	Creazione della sessione non riuscita	La segnalazione non è più possibile perché non è stato possibile creare una sessione. Viene eseguito il riavvio necessario. Viene generato un trap SNMP.		
MSG_IPNCV_STARTUP_ERROR	Avvio IPNCV: Creazione di IPNCV Manager non riuscita	Impossibile avviare IPNCV. Viene generato un trap SNMP.	Creare un TR/MR	
MSG_IPNCV_STARTUP_SHUTDOWN	Avvio/arresto IPNCV: IPNCV Manager creato correttamente o avvio/ arresto IPNCV: Arresto di IPNCV Manager riuscito	IPNCV è stato avviato o arrestato correttamente. Viene generato un trap SNMP		
MSG_IPNCV_INTERNAL_ERROR	Errore IPNCV interno: %s	Errore software: rilevati dati interni non validi. Verrà generato un trap SNMP con il profilo IPNCV-Detailed.		
MSG_IPNCV_MEMORY_ERROR	Memoria IPNCV: %s	Overflow della memoria: viene generato un trap SNMP.	Riavviare il gateway. Creare un TR/MR.	
MSG_IPNCV_SIGNALING_ERROR	Errore di segnalazione IPNCV: %s	Errore software: trovati dati interni non validi.		
MSG_CAR_ALIVE_IP_CONNECTION_LOST	CAR: Tempo reale: connessione ip %d.%d. %d.%d persa	CAR: Tempo reale: Connessione IP persa.		
MSG_LIC_DATA_ACCEPTED		Dati della licenza accettati		
MSG_LIC_DATA_CORRUPTED		Dati della licenza incompleti		
MSG_LIC_DATA_NOT_ACCEPTED		Dati della licenza accettati		
MSG_SPE_CERT_MISSING	Nessun certificato SPE installato.	Certificato SPE mancante.	Installare il certificato SPE.	

Nota: Ci sono eventi SNMP non documentati in questa guida.

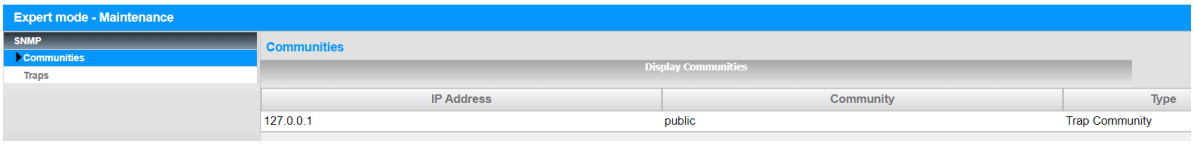
25.8.2.1 Come visualizzare tutte le comunità

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **SNMP**.
3) Nella struttura dei menu fare clic su **SNMP** > **Comunità**. Viene visualizzato un elenco di tutte le comunità e i dati corrispondenti (indirizzo IP, comunità, tipo).



25.8.2.2 Come aggiungere una comunità

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **SNMP**.
3) Selezionare la comunità desiderata:
   - Se si desidera aggiungere una comunità di lettura, nella struttura dei menu fare clic su **SNMP** > **Comunità** > **Comunità di lettura**. Fare clic sulla scheda**Aggiungi comunità di lettura**.
   - Se si desidera aggiungere una comunità di scrittura, nella struttura dei menu fare clic su **SNMP** > **Comunità** > **Comunità di scrittura**. Fare clic sulla scheda **Aggiungi comunità di scrittura**.
   - Se si desidera aggiungere una comunità Trap, nella struttura dei menu fare clic su **SNMP** > **Comunità** > **Comunità Trap**. Fare clic sulla scheda **Aggiungi comunità Trap**.
4) Nel campo **Indirizzo IP** immettere l'indirizzo IP della nuova comunità.
5) Nel campo **Comunità** indicare il nome della nuova comunità.
6) Fare clic su **Applica**, quindi su **OK**.

25.8.2.3 Come modificare una comunità

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **SNMP**.
3) Navigare nella struttura dei menu in **SNMP** > **Comunità** > **...** fino alla comunità desiderata.
4) Fare clic sulla scheda **Modifica comunità**.
5) Modificare la Comunità.

6) Fare clic su **Applica**, quindi su **OK**.

25.8.2.4 Come cancellare una comunità

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **SNMP**.
3) Navigare nella struttura dei menu in **SNMP** > **Comunità** > **...** fino alla comunità desiderata.
4) Fare clic sulla scheda **Cancella comunità**.
5) Fare clic su **Cancella** quindi su **OK**.

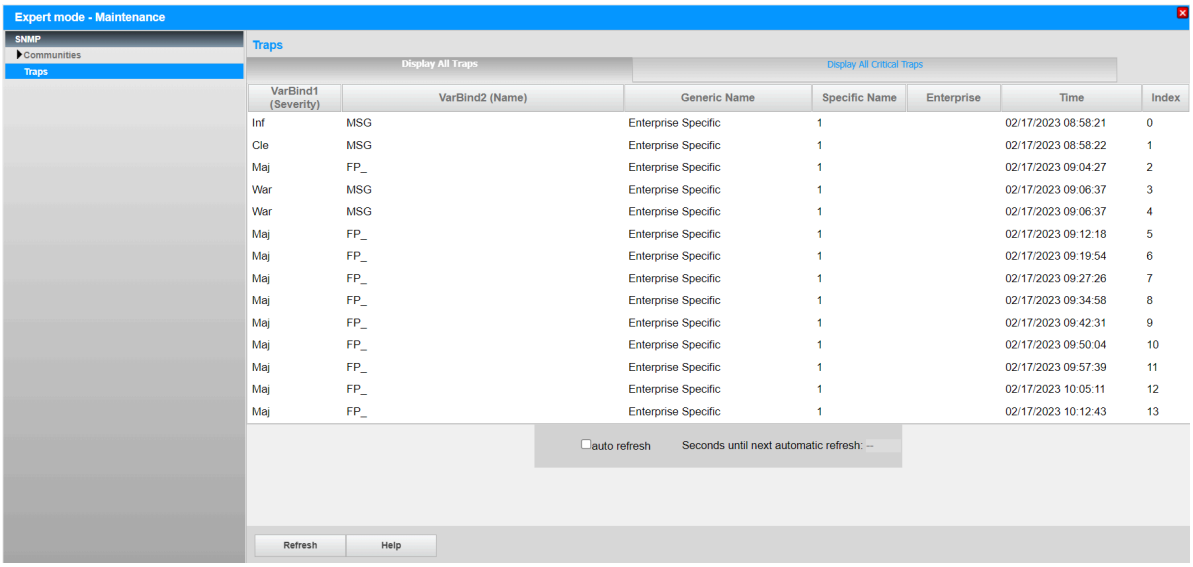
25.8.2.5 Come visualizzare i Trap

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **SNMP**.
3) Nella struttura dei menu fare clic su **SNMP** > **Trap**.
4) Selezionare una delle seguenti opzioni:
   - Se si vuole visualizzare l'elenco di tutti i Trap, fare clic sulla scheda **Mostra tutti i Trap**.



   - Se si vuole visualizzare l'elenco di tutti i Trap critici, fare clic sulla scheda **Mostra tutti i Trap critici**.

25.8.2.6 Come visualizzare i dettagli di un Trap

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **SNMP**.
3) Nella struttura dei menu fare clic su **SNMP** > **Trap**.
4) Fare clic sulla scheda **Trap Mostra tutte le porte utilizzate**. Viene visualizzato un elenco di tutti i Trap e dei dati corrispondenti.
5) Fare clic sul nome del Trap desiderato. Vengono visualizzati i dettagli di questo Trap.
6) Fare clic sulla scheda **Mostra tutti i Trap** per richiamare un elenco di tutti i Trap.

25.8.3 Azioni manuali

Mediante le azioni manuali si possono caricare diversi dati di registro (dati di diagnostica, registri di diagnostica).

La procedura guidata **Traccia** consente a un amministratore con il profilo **Advanced** di caricare dati di diagnostica (registri di diagnostica).

La **Modalità esperti** consente a un amministratore con il profilo **Expert** di caricare i registri di diagnostica.

Si possono caricare i seguenti protocolli:

Protocollo	Spiegazione	Esempio di applicazione
Registro di traccia	File di traccia standard, se sono attivi i profili di traccia. È possibile scegliere tra le seguenti opzioni: • **Intero protocollo**: vengono scaricati tutti i file di registro di traccia del sistema disponibili. • **Protocollo odierno**: vengono scaricati i registri di traccia del sistema dei dati del giorno (a partire dalle ore 00:00). • **Selezione propria**: **Da:** XXX **Fino a:** YYY: vengono scaricati i file di registro di traccia del sistema per il periodo indicato.	Nessuna applicazione particolare
Registro eventi	Azioni/eventi del sistema di comunicazione (reset, accensione/spegnimento, ecc.)	Nessuna applicazione particolare
Registro Admin	Messaggi sulle procedure di amministrazione del sistema di comunicazione (tentativi di login, ecc.)	Nessuna applicazione particolare
Protocolli licenza	Messaggi sui componenti del sistema di comunicazione che richiedono una licenza	Problemi con l'attivazione della licenza (impossibile attivare il file di licenza, ecc.)

Protocollo	Spiegazione	Esempio di applicazione
Traccia clienti	I messaggi per la traccia cliente vengono visualizzati in formato più dettagliato rispetto al protocollo Traccia (login remoto, login ITSP, ecc.)	Problemi con la connessione ITSP (Internet Telephony Service Provider) o con l'accesso remoto
Protocollo Framework	Messaggi di WBM	Problemi con la concessione licenza, durante il salvataggio (Backup), il ripristino (Ricarica) o con il WBM
Registro di diagnostica	Registri di diagnostica del sistema di comunicazione (FP/LDH)	Crash o arresto non controllato del sistema di comunicazione
Protocollo UC Suite	I messaggi della UC Suite del sistema di comunicazione (registri UC Suite, CSP e MEB) È possibile scegliere tra le seguenti opzioni: • **Intero protocollo**: vengono scaricati tutti i file di registro disponibili della UC Suite, CSP e MEB. • **Protocollo odierno**: vengono scaricati i file di registro della UC Suite, CSP e MEB relativi al giorno in corso (a partire dalle ore 00:00). • **Selezione propria**: **Da:** XXX **Fino a:** YYY: vengono scaricati i file di registro della UC Suite, CSP e MEB per il periodo indicato. Tutti i file di registro vengono riuniti in un file compresso. Per i registri OpenScape Business si applicano le seguenti indicazioni per i nomi dei file: file di registro UC Suite = `vs_jjjj_mm_tt.log`, file di registro CSP = `csptrace_jjjj_mm_tt.log`, file di registro MEB = `mebtrace_jjjj_mm_tt.log`. ***INFO***: i dati di diagnostica possono essere scaricati solo per l'uso con UC Booster Card OCAB. Quando si utilizza OpenScape Business UC Booster Server, è necessario scaricare i dati di diagnostica tramite il server stesso.	Problemi con la UC Suite e/o col client (myPortal for Desktop, myAttendant, ecc.)
Protocolli applicazioni	Messaggi della parte applicazioni del sistema di comunicazione (ad esempio, registri CSP) Un amministratore con il profilo **Expert** può, utilizzando la **Modalità esperti**, scegliere tra le seguenti opzioni: • **Intero protocollo**: vengono scaricati tutti i file di registro disponibili • **Protocollo odierno**: vengono scaricati i registri dei dati del giorno (a partire dalle ore 00:00). • **Selezione propria**: **Da:** XXX **Fino a:** YYY: vengono scaricati i file di registro per il periodo indicato. Tutti i file di registro vengono riuniti in un file compresso.	Problemi con la parte applicazioni del sistema di comunicazione

Protocollo	Spiegazione	Esempio di applicazione
Protocollo sistema-diagnostica	Registro di diagnostica del sistema di comunicazione	Nessuna applicazione particolare
Protocollo PPP	Messaggi al protocollo punto-punto	Problemi con le connessioni dial-in o dial-out
Protocollo CoreLog	I CoreLog vengono creati quando si esegue il reset (come i Memory Dump sul PC).	Crash o arresto non controllato di OpenScape Business

Dopo aver selezionato il protocollo desiderato, viene creato un file compresso che viene memorizzato in un'apposita directory.

25.8.3.1 Come effettuare il download dei dati diagnostica/Registri diagnostica

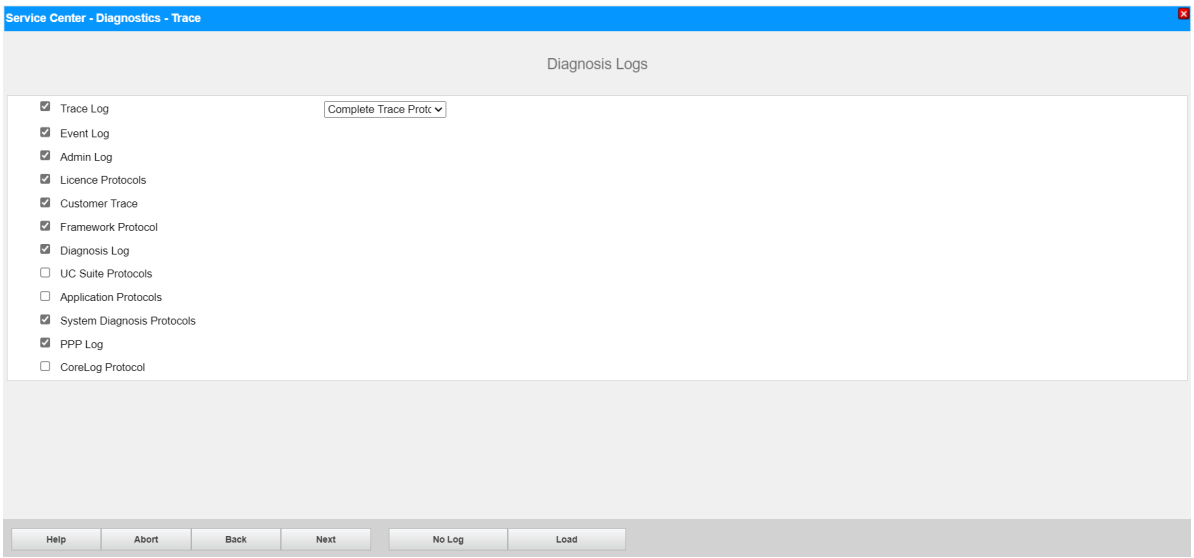
La procedura guidata **Traccia** consente di scaricare i dati di diagnostica (registri di diagnostica) dei sistemi di comunicazione.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Traccia**.
3) Fare clic su **Registri diagnostica**.



4) Selezionare le caselle di controllo dei registri da scaricare. Deselezionare le caselle di controllo dei registri che non si desidera scaricare.
5) Fare clic su **Carica**, quindi su **OK**. Viene visualizzata la finestra per il download del file.
6) Salvare il file nella cartella desiderata. Chiudere quindi la finestra che conferma il download del file.
7) Fare clic su **Avanti**, quindi su **Fine**.

25.8.4 Tracce

Le tracce consentono di registrare fasi di programma e risultati corrispondenti durante l'esecuzione del programma stesso. Unitamente ai dati di diagnostica consentono di risalire alle cause dell'errore verificatosi in un programma. Mediante Profili di traccia e Componenti di traccia viene configurato il livello di dettaglio delle tracce da visualizzare.

Suggerimento: L'attivazione delle tracce influenza negativamente le prestazioni del sistema e va eseguita solo da amministratori con esperti e in accordo con il servizio di assistenza competente.

In particolare, la traccia della console occupa importanti risorse del sistema e compromette le prestazioni del sistema di comunicazione.

Collegamento in rete

Per la diagnostica di sistemi di comunicazione collegati in rete, i dati di traccia di ogni singolo nodo devono essere rilevati separatamente. Non è possibile il rilevamento centralizzato di dati di traccia di sistemi di comunicazione in rete.

Configurazione formato traccia

La funzione Configurazione formato traccia consente a un amministratore con il profilo **Expert** di definire quali informazioni dell'intestazione inserire nel risultato della traccia e il formato dei dati della traccia.

Informazioni dell'intestazione da utilizzare per il risultato della traccia (impostazione predefinita - tutte le opzioni attive):

- Impostazioni globali del formato dell'intestazione della traccia

  Se questa opzione è attiva, è possibile selezionare se includere o meno le seguenti informazioni dell'intestazione.
- ID del sub-sistema
- Nome del task
- ID del task
- Ora
- Nome del modulo
- Numero della riga

Preparazione dei dati di traccia (formattazione):

- Formattazione completa con espansione dei parametri (predefinita) = grandi volumi di dati, prestazioni traccia normali. Impostazione predefinita
- Ristretto (tipi di messaggi binari, in particolar modo per Tracer X) = volumi di dati medi, prestazioni traccia rapide.
- Ristretto (soltanto espansione di tipi di dati elementari) = volumi di dati limitati, prestazioni traccia molto rapide.
- Traccia a prestazione ottimizzata senza espansione dei parametri = volumi di dati molto limitati, prestazioni traccia rapidissime.

Suggerimento:

Assicurarsi che le informazioni aggiuntive dell'intestazione e una formattazione eccessiva non riducano le prestazioni della traccia.

Interfacce di output traccia

Questa funzione consente a un amministratore con il profilo **Expert** di definire le interfacce per il risultato della traccia. È possibile attivare Traccia del file, Traccia tramite LAN o disattivare entrambe le interfacce.

Interfaccia di output traccia	Spiegazione	Impostazione predefinita
Traccia del file	**Attiva traccia del file** I messaggi della traccia vengono registrati in un file di registro nel sistema di comunicazione. Se l'opzione è attivata, vengono applicate le seguenti impostazioni: **Quota traccia max. (kbyte)**: Indica la dimensione massima della memoria Trace **Criteri per la gestione del raggiungimento della quota massima**. È possibile scegliere tra **Wrap Around (rimozione file della traccia meno recente)** e **Arresta temporaneamente file della traccia**. **Tempo fra la creazione di nuovi file della traccia (sec.):** 900 **Periodo di disponibilità dei file della traccia:** viene specificato il periodo corrente.	Abilitato
Traccia tramite LAN	**Attiva traccia tramite LAN** I messaggi della traccia vengono via interfaccia LAN. Se l'opzione è attivata, vengono applicate le seguenti impostazioni: **Timer =** 25 sec. (ritardo di trasmissione informazioni).	Non attivata

Registro di traccia

Se è selezionata l'opzione File della traccia come interfaccia di output, un amministratore con il profilo **Expert** può trasmettere o cancellare i file di registro risultanti su un PC.

Loopback digitale

I loopback digitali sono utilizzati per il test dei canali B delle interfacce S_0, S_{2M} e T1 di eventuali moduli esistenti. Il loopback digitale deve essere attivato solo su richiesta del provider di servizi.

La configurazione di loopback digitali è possibile solo con Manager E.

Visualizzatore eventi / Registro traccia cliente

Con la procedura guidata **Visualizzatore eventi**, un amministratore con il profilo **Advanced** può avviare la visualizzazione dell'evento (traccia cliente).

Inoltre i file di registro Traccia cliente possono essere trasmessi o eliminati su un PC.

Viene descritta la procedura per le seguenti funzioni configurabili tramite la procedura guidata:

- Come visualizzare o modificare il registro visualizzatore eventi / registro traccia cliente
- Come eseguire il download o aprire il registro visualizzatore eventi / registro traccia cliente
- Come eliminare il registro visualizzatore eventi / registro traccia cliente

Entrando in **Modalità Esperti**, un amministratore con il profilo **Expert** può attivare la visualizzazione del file di registro Traccia cliente. Inoltre i file di registro Traccia cliente possono essere trasmessi o eliminati su un PC.

Componente di traccia M5T

Questa funzione viene utilizzata per monitorare lo stack SIP tramite un amministratore con il profilo **Expert**. Per ognuno dei componenti traccia M5T, il livello di dettaglio della registrazione può essere definito in base ai livelli della traccia (da 0 = livello di dettaglio più basso a 4 = livello di dettaglio più elevato).

Secure Trace

Questa funzione viene utilizzata da un amministratore con il profilo **Expert** per registrare i flussi di dati d'uso e di segnalazione VoIP crittografati.

Se i servizio Crittografia segnalazione e payload (SPE) è attivato, vengono crittografati i flussi di dati d'uso e di segnalazione VoIP da e al sistema di comunicazione e tra telefoni IP.

Per assicurare l'esecuzione di analisi in caso di errore, per un periodo di tempo limitato è possibile trasmettere sulla LAN ulteriori informazioni di traccia (**Secure Trace**). In questo caso vengono generati file Secure Trace crittografati, la cui decrittazione e analisi può venire eseguita solo dal reparto Sviluppo.

Per limitare l'uso della funzione Secure Trace, sono state implementate le seguenti funzioni di sicurezza:

- Un tecnico dell'assistenza deve importare nel sistema di comunicazione in questione una cosiddetta chiave pubblica (certificato). Il certificato fa parte di un file X.509 e richiede che sia possibile creare un Secure Trace. Il file X.509 è viene messo a disposizione dal reparto Sviluppo. Il certificato contenuto è valido per un massimo di un mese.
- L'avvio e l'arresto di Secure Trace è protetto da una speciale password (passphrase). Questa password è nota solo al cliente.

Quindi, il certificato corrisponde alla chiave del tecnico dell'assistenza e la password a(passphrase) alla chiave del cliente. Per attivare la funzione di Secure Trace sono necessarie entrambe le chiavi.

Processo per la creazione di Secure Trace:

1) Un tecnico dell'assistenza rileva un problema nella LAN del cliente. Assieme al reparto Sviluppo, il tecnico dell'assistenza riconosce la necessità di generare un Secure Trace.
2) Il cliente viene informato della necessità e dovrà confermare di essere stato informato. Successivamente il cliente emette un ordine per la creazione

di una Secure Trace che specifica la data e l'ora di inizio e di fine del monitoraggio.

3) Un tecnico sviluppatore crea una coppia di chiavi costituita da una chiave pubblica e una privata. Con questa coppia di chiavi è possibile creare un'unica crittografia della traccia (Secure Trace). I certificati vengono utilizzati nel modo seguente

   - Il certificato con la chiave privata è rigorosamente riservato e può essere utilizzato solo da sviluppatori autorizzati.

     Per decrittografare i file Secure Trace è necessaria la chiave privata.
   - Il certificato contenente la chiave pubblica viene trasmesso al tecnico di manutenzione sotto forma di file X.509 in formato binario o PEM.

     Per poter generare un Secure Trace è richiesta l'importazione di questo certificato nel sistema di comunicazione.

4) Il tecnico informa il cliente dell'imminente avvio della generazione del Secure Trace. Il cliente è tenuto a informare gli utenti in questione.

   Nota: La registrazione di conversazioni e dati di connessione costituisce reato, a meno che l'utente in questione sia stato preventivamente informato a riguardo.

5) Il tecnico importa il certificato con la chiave pubblica nel sistema di comunicazione in questione.
6) Il cliente avvia Secure Trace immettendo la password (passphrase). I file Secure trace vengono creati.

   Gli avvii e gli arresti di Secure Trace vengono registrati dal sistema di comunicazione.
7) Dopo aver completato la generazione Secure Trace, una notifica informa il cliente che l'attività Secure Trace è conclusa. Il tecnico rimuove il certificato del sistema di comunicazione.
8) I file Secure Trace sono a disposizione per il settore Sviluppo.
9) Uno sviluppatore decrittografa i file Secure Trace utilizzando la chiave privata. Successivamente, viene eseguita l'analisi dei dati decrittografati.

   Nota: Terminata l'analisi, tutti i dati rilevanti devono essere distrutti in modo sicuro. Ciò comprende la distruzione della chiave privata, in modo che un'eventuale copia non autorizzata dei file di traccia non può più essere decrittografata.

Traccia dello stack H.323

Questa funzione consente a un amministratore con il profilo **Expert** di impostare la configurazione traccia dello stack H.323. Il livello di dettaglio della registrazione può essere definito in base ai livelli della traccia (da 0 = livello di dettaglio più basso a 4 = livello di dettaglio più elevato). Per l'output della Traccia dello stack H.323 è possibile selezionare le seguenti impostazioni:

Interfaccia di output traccia	Spiegazione	Impostazione predefinita
Traccia della console	**Attiva traccia della console** I messaggi della traccia dello stack H.323 vengono emessi sulla console.	Non attivata
Traccia del file	**Attiva traccia del file** I messaggi della traccia dello stack H.323 vengono registrati in un file di registro. Se l'opzione è attivata, vengono applicate le seguenti impostazioni: Dimensione max. del buffer di traccia = 50000 byte (quantità di informazioni conservate nella memoria temporanea) Dimensione max. del file di traccia = 1000000 byte (dimensioni massime del file di registro) Timer traccia = 60 sec. (ritardo con cui le informazioni vengono trascritte nei file di registro)	Non attivata

Attivando e/o disattivando i moduli H.323 si definisce per quali componenti di H.323 Stack Trace è necessario registrare le informazioni di processo e di stato. Lo stato di ciascun modulo H.323 viene visualizzato tramite il colore del punto elenco corrispondente (verde = modulo H.323 attivato, rosso = modulo H.323 disattivato).

Il registro di traccia dello stack H.323 può essere trasmesso o eliminato su un PC.

Traccia componente licenza

Questa funzione viene utilizzata da un amministratore con il profilo Expert per monitorare l'agente delle licenze (CLA) interno del sistema. Il livello di dettaglio della registrazione può essere definito in base ai livelli della traccia (Basso= livello di dettaglio inferiore (impostazione predefinita); Standard = livello di dettaglio medio; Tutto = livello di dettaglio maggiore).

Per impostazione predefinita, la traccia componente licenza è attivata (livello di traccia = basso).

La modifica dei livelli traccia influenza negativamente le prestazioni del sistema e va eseguita solo da amministratori esperti e in accordo con il servizio di assistenza competente.

Profili di traccia

I profili di traccia definiscono le informazioni da visualizzare e il livello di dettaglio corrispondente. A un profilo di traccia sono associati componenti di traccia. In questo modo viene definito per quali componenti del sistema registrare un profilo della traccia del processo e le informazioni di stato.

Sono disponibili profili di traccia predefiniti che coprono tutti gli scenari predefiniti. Inoltre un amministratore con il profilo **Expert** può definire i propri profili di traccia. Quando si inizia un profilo di traccia, la registrazione viene attivata tramite questo profilo. Quando si interrompe il profilo, la registrazione viene disattivata.

- La procedura guidata **Traccia** consente a un amministratore con il profilo **Advanced** di attivare/interrompere i profili di traccia. Lo stato di ciascun profilo di traccia viene visualizzato tramite il colore del punto elenco corrispondente (verde = profilo di traccia attivato, rosso = profilo di traccia disattivato). Selezionando **Avvia/Interrompi** è possibile attivare o avviare un profilo di traccia inattivo (punto elenco rosso) e disattivare o interrompere un profilo di traccia attivo (punto elenco verde).

  Carica traccia consente di trasmettere o aprire i file di registro risultanti su un PC.

  Cancella traccia consente di eliminare i file di registro risultanti.

  Viene descritta la procedura per le seguenti funzioni configurabili tramite la procedura guidata:

  – Come caricare il file di registro eventi traccia sistema
  – Come cancellare il file di registro traccia sistema
  – Come visualizzare tutti i profili di traccia
  – Come avviare o arrestare il profilo di traccia
  – Come effettuare il download dei dati diagnostica/Registri diagnostica
- Entrando in **Modalità esperti**, un amministratore con il profilo **Expert** può arrestare tutti i profili di traccia contemporaneamente e attivarli/interromperli singolarmente.

  Nella struttura dei menu, il colore dei punti elenco consente di distinguere lo stato del profilo di traccia (verde = profilo di traccia attivato, rosso = profilo di traccia non attivato). Selezionando **Avvia/Interrompi profilo di traccia** è possibile attivare o avviare un profilo di traccia inattivo (punto elenco rosso) e disattivare o interrompere un profilo di traccia attivo (punto elenco verde).

  Selezionando **Mostra profilo di traccia**, si possono visualizzare i dettagli del profilo di traccia desiderato: oltre al nome del profilo, indicazioni sulla protezione da scrittura e stato del profilo contengono informazioni sui problemi che possono richiedere l'uso del profilo di traccia. Inoltre vengono indicati i componenti che fanno parte del profilo di traccia.

Profilo di traccia	Esempio di applicazione
Actors_Sensors_Door-Opener	Informazione non disponibile al momento!
Basic	Informazione non disponibile al momento!
Calls_with_Analog_Subscriber_Trunks	Informazione non disponibile al momento!
Calls_with_ISDN_Subscriber_Trunks	Informazione non disponibile al momento!
Calls_with_System_Device_HFA	Informazione non disponibile al momento!
Calls_with_System_Device_Upn	Informazione non disponibile al momento!
CDR_Charging_data	Informazione non disponibile al momento!
CMI	Informazione non disponibile al momento!
CSTA_application	Informazione non disponibile al momento!
Display_problems	Informazione non disponibile al momento!
Gateway_Stream_detailed	Informazione non disponibile al momento!
Gateway_Stream_overview	Informazione non disponibile al momento!
IP_Interfaces	Informazione non disponibile al momento!

Profilo di traccia	Esempio di applicazione
Problema_licenza	Informazione non disponibile al momento!
Network_Call_Routing_LCR	Informazione non disponibile al momento!
Peripheral_cards	Informazione non disponibile al momento!
RAS_or_Internal_access	Informazione non disponibile al momento!
Ressources_MOH_Conferencing	Informazione non disponibile al momento!
SIP_Interconnection_Subscriber_ITSP	Informazione non disponibile al momento!
SIP_Registration	Informazione non disponibile al momento!
Smart_VM	Informazione non disponibile al momento!
UC Smart	Informazione non disponibile al momento!
Voice_Fax_connection	Informazione non disponibile al momento!
VPN	Informazione non disponibile al momento!
Web_based_Assistant_Expert_Mode	Informazione non disponibile al momento!

Componenti di traccia

In base ai componenti di traccia vengono registrate le informazioni di processo e di stato dei singoli componenti del sistema di comunicazione.

Tutti i componenti di traccia possono essere arrestati contemporaneamente o avviati/interrotti singolarmente da un amministratore tramite il profilo **Expert**. Avviando un componente di traccia si attiva la registrazione, disattivandolo la si interrompe. Il livello di dettaglio della registrazione può essere definito in base ai livelli della traccia (da 0 = livello di dettaglio più basso a 9 = livello di dettaglio più elevato).

Nella struttura dei menu, il colore dei punti elenco consente di distinguere lo stato del componente traccia (verde = componente traccia attivato, rosso = componente traccia non attivato). Selezionando **Avvia/Interrompi componente di traccia** è possibile attivare o avviare un profilo di traccia inattivo (punto elenco rosso) e disattivare o interrompere un profilo di traccia attivo (punto elenco verde).

La visualizzazione di un componente di traccia include il nome del sottosistema, l'indice dei componenti di traccia, il livello di traccia impostato, le informazioni di stato nonché l'attivazione corrente del componente. Se occorre modificare un componente di traccia, oltre a modificare il livello della traccia è necessario definire l'avvio o l'interruzione del componente.

25.8.4.1 Come caricare il file di registro eventi traccia sistema

La procedura guidata **Traccia** consente di scaricare i file di registro Traccia di sistema.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Traccia**.
3) Fare clic su **Registri diagnostica**.
4) Fare clic su **Nessun protocollo**, per deselezionare le caselle di controllo di tutti i registri.
5) Selezionare la casella di controllo **Registro di traccia**.
6) Selezionare una delle seguenti opzioni:
   - Se si desidera scaricare l'intero registro di traccia sistema disponibile, nell'elenco a discesa, selezionare **Registro completo**.
   - Se si desidera scaricare il registro di traccia del sistema del giorno, nell'elenco a discesa, selezionare **Protocollo odierno**.
   - Se si desidera scaricare il registro di traccia del sistema di un periodo specifico, nell'elenco a discesa selezionare **Selezione propria**. Nell'elenco a discesa **Da:** indicare la data di inizio del periodo desiderato e nell'elenco a discesa **Fino a:** la data di fine.
7) Fare clic su **Carica**, quindi su **OK**. Viene visualizzata la finestra per il download del file.
8) Salvare il file nella cartella desiderata. Chiudere quindi la finestra che conferma il download del file.
9) Fare clic su **Avanti**, quindi su **Fine**.

25.8.4.2 Come cancellare il file di registro traccia sistema

La procedura guidata **Traccia** consente di eliminare i file di registro Traccia di sistema.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Traccia**.
3) Fare clic su **Cancella traccia**, quindi su **OK**.
4) Fare clic su **Avanti**, quindi su **Fine**.

25.8.4.3 Come configurare impostazioni di traccia ai valori predefiniti

La procedura guidata **Traccia** consente di impostare i file di registro Traccia di sistema allo stato predefinito.

Prerequisiti

Si è connessi al WBM con il profilo **Advanced** o **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Traccia**.

3) Fare clic sul pulsante delle **impostazioni di traccia predefinite**, quindi su **OK** nel messaggio popup seguente che comunica il completamento corretto dell'azione.
4) Fare clic su **Avanti**, quindi su **Fine**.

Nota: Il tracciamento ampliato aumenta il carico generale del sistema e non dovrebbe pertanto essere sempre attivo. Ripristinare le impostazioni di traccia ai valori predefiniti facendo clic sul **pulsante delle impostazioni di traccia predefinite** non appena vengono create le tracce richieste**.**

Nota: Se le impostazioni di traccia ampliate sono attive, l'utente riceverà una notifica nella pagina iniziale del WBM nell'area delle **notifiche**. È disponibile anche un collegamento diretto alle impostazioni di traccia del Centro assistenza.

25.8.4.4 Come visualizzare tutti i profili di traccia

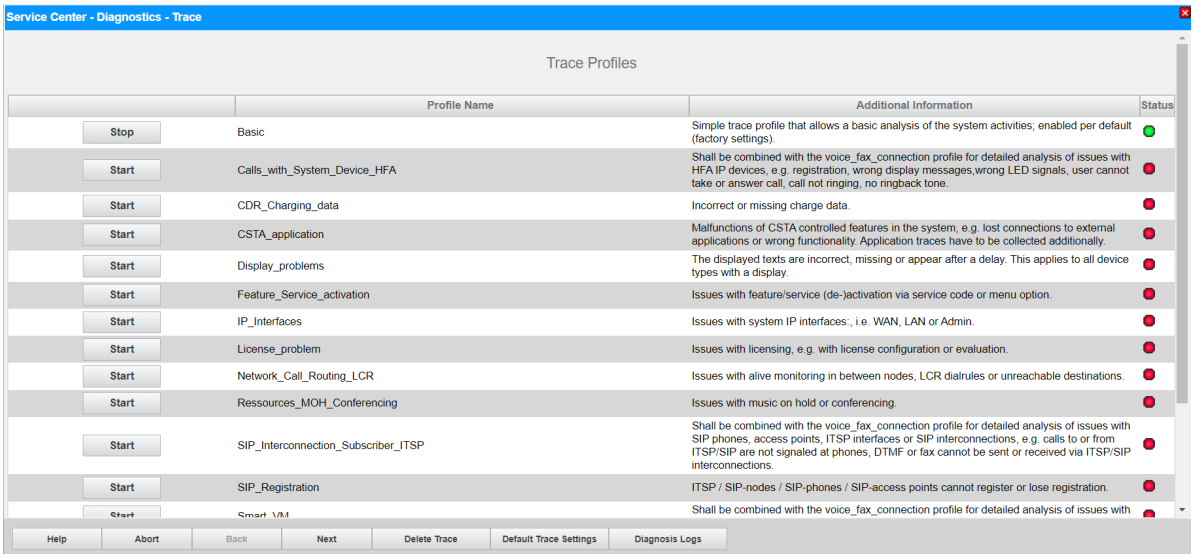
Con la procedura guidata **Traccia** è possibile ottenere informazioni sullo stato di tutti i profili di traccia.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Traccia**. Viene visualizzato un elenco di tutti i profili di traccia con l'indicazione dei profili avviati e non avviati.



3) Fare clic su **Avanti**, quindi su **Fine**.

25.8.4.5 Come avviare o arrestare il profilo di traccia

La procedura guidata **Traccia** consente di avviare e arrestare i profili di traccia.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Traccia**. Viene visualizzato un elenco di tutti i profili di traccia. Un punto elenco rosso contraddistingue i profili di traccia che possono essere avviati. Un punto elenco verde contraddistingue i profili di traccia che possono essere arrestati.
3) Selezionare una delle seguenti opzioni:
   - Se si desidera avviare un profilo traccia, fare clic su **Start**. Il colore del punto elenco che mostra lo stato del relativo profilo di traccia passa da rosso a verde.

     Nota: I profili di traccia avviati influenzano negativamente le prestazioni del sistema. Arrestare quindi tutti i profili traccia al termine delle attività di diagnostica, ad eccezione di quello **Predefinito**. Il profilo di traccia **Predefinito** deve restare attivo.
   - Se si desidera arrestare un profilo traccia, fare clic su **Arresto**. Il colore del punto elenco che mostra lo stato del relativo profilo di traccia passa da verde a rosso.
4) Fare clic su **Avanti**, quindi su **Fine**.

25.8.4.6 Come visualizzare o modificare la configurazione del formato della traccia

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È stata inviata una richiesta del servizio di assistenza competente per modificare la configurazione del formato della traccia.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Configurazione del formato della traccia**. Vengono visualizzate le impostazioni correnti della configurazione del formato traccia.
4) Modificare come necessario le impostazioni desiderate.
5) Fare clic su **Applica**, quindi su **OK**.

25.8.4.7 Come visualizzare o modificare le interfacce di output traccia

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È stata inviata una richiesta del servizio di assistenza competente per modificare le interfacce di output della traccia.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Interfacce di output della traccia**. Il Simple Network Management Protocol (SNMP) è un protocollo di rete che consente di comandare e monitorare componenti di rete (ad esempio router, server, switch, stampanti, computer) da una stazione centrale (Console di gestione).
4) Modificare come necessario le impostazioni desiderate.
5) Fare clic su **Applica**, quindi su **OK**.

25.8.4.8 Come visualizzare o modificare il registro visualizzatore eventi / registro traccia cliente

Con la procedura guidata **Visualizzatore eventi** è possibile avviare la visualizzazione di un evento (Traccia cliente) e modificare le impostazioni di aggiornamento.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Visualizzatore eventi**.
3) Fare clic sulla scheda **Visualizza**.
4) Selezionare l'impostazione desiderata:
   - Se il registro deve essere aggiornato automaticamente, selezionare la casella di controllo **Aggiornamento autom**.
   - Se il registro non deve essere aggiornato automaticamente, deselezionare la casella di controllo **Aggiornamento autom**.
5) Fare clic su **Aggiorna** come necessario per aggiornare manualmente il Registro traccia cliente.
6) Fare clic su **Fine**.

25.8.4.9 Come eseguire il download o aprire il registro visualizzatore eventi / registro traccia cliente

Con la procedura guidata **Visualizzatore eventi** è possibile trasferire o aprire il file di registro traccia cliente su un PC.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Visualizzatore eventi**.
3) Fare clic sulla scheda **Carica tramite HTTP**.
4) Fare clic su **Carica**, quindi su **OK**. Viene visualizzata la finestra per il download del file.
5) Selezionare una delle seguenti opzioni:
   - Se si desidera scaricare i file di registro, fare clic su **Salva con nome**. Salvare il file nella cartella desiderata e chiudere la finestra che conferma il download del file.
   - Se si desidera aprire i file di registro, fare clic su **Apri**. Successivamente viene visualizzato il contenuto del file di registro compresso.
6) Fare clic su **Fine**.

25.8.4.10 Come eliminare il registro visualizzatore eventi / registro traccia cliente

Con la procedura guidata **Visualizzatore eventi** è possibile cancellare il file di registro traccia cliente.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Visualizzatore eventi**.
3) Fare clic sulla scheda **Cancella registro eventi**.
4) Fare clic su **Cancella registro**, quindi su **OK**.
5) Fare clic su **Fine**.

25.8.4.11 Come mostrare componenti di traccia M5T

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Componenti di traccia M5T**. Viene visualizzato un elenco di tutti i componenti di traccia M5T e delle impostazioni correnti. Inoltre nella struttura dei menu vengono visualizzati i nomi di tutti i componenti di traccia M5T. Un punto elenco colorato contraddistingue lo stato di ciascun componente di traccia M5T.

25.8.4.12 Come avviare o arrestare un componente di traccia M5T

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È stata inviata una richiesta del servizio di assistenza competente per avviare o arrestare un componente di traccia M5T.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Componenti di traccia M5T**. Nella struttura dei menu viene visualizzato il nome di tutti i componenti di traccia M5T. Un punto elenco rosso contraddistingue i componenti di traccia M5T che possono essere avviati. Un punto elenco verde contraddistingue i componenti di traccia M5T che possono essere arrestati.
4) Nella struttura dei menu fare clic sul componente di traccia M5T desiderato.
5) Fare clic sulla scheda **Avvia/arresta componente traccia**.
6) Selezionare una delle seguenti opzioni:
   - Se si desidera avviare i componenti di traccia M5T, fare clic su **Avvio**, quindi su **OK**.
   - Se si desidera arrestare i componenti di traccia M5T, fare clic su **Arresto**, quindi su **OK**.

25.8.4.13 Come modificare componenti di traccia M5T

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È stata inviata una richiesta del servizio di assistenza competente per modificare i componenti di traccia M5T.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Componenti di traccia M5T**. Viene visualizzato un elenco di tutti i componenti di traccia M5T e delle impostazioni correnti.
4) Modificare le impostazioni desiderate.

5) Fare clic su **Applica**, quindi su **OK**.

25.8.4.14 Come avviare o arrestare Secure Trace

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Secure Trace**.
4) Fare clic sulla scheda **Avvia/arresta Secure Trace**.
5) Selezionare una delle seguenti opzioni:
   - Se si desidera avviare Secure Trace, procedere come segue:

     Nel campo **Passphrase di attivazione di Secure Trace** immettere la password per Secure Trace.

     Nel campo **Durata di Secure Trace (min.)** indicare il tempo di attivazione di Secure Trace in minuti.

     Selezionare la casella di controllo dei protocolli per i quali deve essere creato Secure Trace. Deselezionare la casella di controllo dei protocolli per i quali non deve essere creato alcun Secure Trace.

     Fare clic su **Attiva Secure Trace**, quindi su **OK**.
   - Se si desidera disattivare Secure Trace, fare clic su **Arresta Secure Trace**, quindi su **OK**.

25.8.4.15 Come controllare lo stato di Secure Trace

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Secure Trace**.
4) Fare clic sulla scheda **Stato di Secure Trace**. Viene quindi visualizzato lo stato corrente di Secure Trace.

25.8.4.16 Come modificare la password per Secure Trace

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Secure Trace**.
4) Fare clic sulla scheda **Modifica passphrase di Secure Trace**.
5) Nel campo **Passphrase corrente** immettere la password corrente per Secure Trace.
6) Nei campi **Nuova passphrase** e **Conferma nuova passphrase**, inserire la nuova password per Secure Trace, di lunghezza compresa tra cinque e dodici caratteri.
7) Fare clic su **Applica**.

25.8.4.17 Come importare il certificato per Secure Trace da un file X.509

Prerequisiti

È disponibile un file X.509 in formato binario o PEM.

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Secure Trace**.
4) Fare clic sulla scheda **Importa file X.509 per Secure Trace**.
5) Fare clic su **Sfoglia**, per selezionare il file X.509 desiderato.
6) Fare clic su **Apri**.
7) Fare clic su **Importa certificato da file**.

25.8.4.18 Come modificare o visualizzare la configurazione di traccia dello stack H.323

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È stata inviata una richiesta del servizio di assistenza competente per modificare la configurazione traccia dello stack H.323.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu, fare clic su **Tracce** > **Traccia dello stack H.323**.
4) Fare clic sulla scheda **Modifica configurazione di traccia dello stack H.323**. Vengono visualizzate le impostazioni correnti della configurazione di traccia dello stack H.323.
5) Modificare come necessario le impostazioni desiderate.
6) Fare clic su **Applica**, quindi su **OK**.

25.8.4.19 Come modificare i moduli H.323

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È stata inviata una richiesta del servizio di assistenza competente per modificare il modulo H.323.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu, fare clic su **Tracce** > **Traccia dello stack H.323**.
4) Fare clic sulla scheda **Modifica tutti i moduli H.323**.
5) Selezionare le impostazioni desiderate per **Traccia su**:
   - Se si desidera attivare la traccia per un modulo H.323 specifico, selezionare la casella di controllo del modulo H.323 desiderato. Deselezionare la casella di controllo del modulo H.323 per il quale deve essere disattivata la traccia.
   - Se si desidera disattivare la traccia per tutti i moduli H.323, fare clic su **Nessuno**.
6) Fare clic su **Applica**, quindi su **OK**.

25.8.4.20 Come caricare/aprire il registro di traccia dello stack H.323

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu, fare clic su **Tracce** > **Traccia dello stack H.323**.
4) Fare clic sulla scheda **Carica il registro di traccia dello stack H.323 tramite HTTP**.
5) Fare clic su **Carica**, quindi su **OK**. Viene visualizzata la finestra per il download del file.
6) Selezionare una delle seguenti opzioni:
   - Se si desidera salvare il file di registro traccia dello stack H.323, fare clic su **Salva con nome**. Salvare il file nella cartella desiderata e chiudere la finestra che conferma il download del file.
   - Se si desidera aprire il file di registro traccia dello stack H.323, fare clic su **Apri**. Il file viene quindi visualizzato nell'editor di testo.

25.8.4.21 Come cancellare il registro di traccia dello stack H.323

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu, fare clic su **Tracce** > **Traccia dello stack H.323**.
4) Fare clic sulla scheda **Cancella il registro di traccia dello stack H.323**.
5) Fare clic su **Cancella registro**, quindi su **OK**.

25.8.4.22 Come modificare la traccia componenti licenza

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

È stata inviata una richiesta del servizio di assistenza competente per modificare la traccia dei componenti della licenza.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Componenti licenza** > **CLA**.
4) Selezionare una delle seguenti opzioni:
   - Se si desidera interrompere la traccia componenti licenza, nell'elenco **Livello di traccia**, selezionare la voce **Off**.
   - Se si desidera utilizzare un livello di dettaglio basso per la registrazione di traccia, nell'elenco a discesa **Livello di traccia**, selezionare la voce **Basso**.
   - Se si desidera utilizzare un livello di dettaglio medio per la registrazione di traccia, nell'elenco a discesa **Livello di traccia**, selezionare la voce **Standard**.
   - Se si desidera utilizzare un elevato livello di dettaglio per la registrazione di traccia, nell'elenco a discesa **Livello di traccia**, selezionare la voce **Tutto**.
5) Fare clic su **Applica**.

25.8.4.23 Come visualizzare i dettagli di un profilo di traccia

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Profili di traccia**. Viene visualizzato un elenco di tutti i profili di traccia. Inoltre nella struttura dei menu vengono visualizzati i nomi di tutti i profili di traccia. Un punto elenco colorato contraddistingue lo stato di ciascun profilo di traccia.
4) Nella struttura dei menu fare clic sul nome del profilo di traccia desiderato. Vengono visualizzati i dettagli del profilo di traccia.

25.8.4.24 Come arrestare tutti i profili di traccia

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Profili di traccia**.
4) Fare clic sulla scheda **Arresta tutti i profili di traccia**.
5) Fare clic su **Arresta tutti** quindi su **OK**.

25.8.4.25 Come aggiungere un Profilo di traccia

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Profili di traccia**.
4) Selezionare una delle seguenti opzioni:
   - Se si desidera aggiungere un profilo di traccia vuoto, fare clic sulla scheda **Aggiungi profilo di traccia (profilo vuoto)**.
   - Se si desidera aggiungere un profilo di traccia che contenga i componenti di traccia di tutti i profili attualmente avviati, fare clic sulla scheda **Aggiungi profilo di traccia (con impostazioni aggiornate)**. Selezionare i componenti traccia e i rispettivi livelli da inserire nel nuovo profilo di traccia.
5) Nel campo **Nome del profilo** immettere il nome del nuovo profilo di traccia.
6) Fare clic su **Applica**, quindi su **OK**.

25.8.4.26 Come mostrare la componente di traccia

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Componenti traccia**.

4) Selezionare una delle seguenti opzioni:
   - Se si vuole visualizzare l'elenco di tutti i componenti di traccia, fare clic sulla scheda **Mostra tutti i componenti di traccia**.
   - Se si vuole visualizzare l'elenco di tutti i componenti di traccia avviati, fare clic sulla scheda **Mostra componenti di traccia avviati**.
   - Se si vuole visualizzare l'elenco di tutti i componenti di traccia arrestati, fare clic sulla scheda **Mostra componenti di traccia arrestati**.

25.8.4.27 Come visualizzare i dettagli dei componenti di traccia

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Componenti traccia**. Viene visualizzato un elenco di tutti i componenti di traccia. Inoltre nella struttura dei menu vengono visualizzati i nomi di tutti i componenti di traccia. Un punto elenco colorato contraddistingue lo stato di ciascun componente di traccia.
4) Nella struttura dei menu fare clic sul nome del componente di traccia desiderato. Vengono visualizzati i dettagli del componente di traccia.

25.8.4.28 Come avviare o arrestare un componente di traccia

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Componenti traccia**. Nella struttura dei menu vengono visualizzati i nomi di tutti i componenti di traccia. Un punto elenco rosso contraddistingue i componenti di traccia che possono essere avviati. Un punto elenco verde contraddistingue i componenti di traccia che possono essere arrestati.
4) Nella struttura dei menu fare clic sul componente di traccia desiderato.
5) Fare clic sulla scheda **Avvia/arresta componente traccia**.
6) Selezionare una delle seguenti opzioni:
   - Se si desidera avviare un componente di traccia, fare clic su **Avvio**, quindi su **OK**.
   - Se si desidera arrestare un componente di traccia, fare clic su **Arresto**, quindi su **OK**.

25.8.4.29 Come arrestare tutti i componenti di traccia

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Componenti traccia**.
4) Fare clic sulla scheda **Arresta tutti i componenti di traccia**.
5) Fare clic su **Arresta tutti** quindi su **OK**.

25.8.4.30 Come configurare impostazioni di traccia ai valori predefiniti

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Nella struttura dei menu fare clic su **Tracce** > **Componenti traccia**.
4) Fare clic sulla scheda delle **impostazioni di traccia predefinite**.
5) Fare clic sul pulsante delle **impostazioni di traccia predefinite**, quindi su **OK** nel messaggio popup seguente che comunica il completamento corretto dell'azione.

Nota: Il tracciamento ampliato aumenta il carico generale del sistema e non dovrebbe pertanto essere sempre attivo. Ripristinare le impostazioni di traccia ai valori predefiniti facendo clic sul **pulsante delle impostazioni di traccia predefinite** non appena vengono create le tracce richieste**.**

Nota: Se le impostazioni di traccia ampliate sono attive, l'utente riceverà una notifica nella pagina iniziale del WBM nell'**area delle notifiche. È disponibile anche un collegamento diretto alle impostazioni di traccia.**

25.8.4.31 Come modificare componenti di traccia

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.

3) Nella struttura dei menu fare clic su **Tracce** > **Componenti traccia**.
4) Fare clic sulla scheda **Modifica componenti di traccia**. Viene visualizzato un elenco di tutti i componenti di traccia e delle impostazioni correnti.
5) Modificare le impostazioni desiderate.
6) Fare clic su **Applica**, quindi su **OK**.

25.8.4.32 Come inoltrare automaticamente i file del registro di sistema

È possibile abilitare l'opzione per inoltrare automaticamente i file del registro di sistema a un sistema di gestione esterno/server syslog.

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione > Tracce > Inoltro Syslog**.
3) Inserire l'**Indirizzo IP** e la **Porta** del sistema di gestione a cui inoltrare il file syslog.
4) Fare clic su **Avvia** per salvare le modifiche della configurazione e avviare il processo.

   Se la connessione con il portale di gestione/server syslog è corretta, **Stato di connessione** ha un indicatore rotondo verde.

   Se la connessione con il server di gestione/syslog non è riuscita, **Stato di connessione** ha un indicatore rotondo rosso.
5) Fare clic su **Arresta** per disattivare il processo.

   Lo **Stato di connessione** è impostato su disattivato con un indicatore rotondo grigio.
6) Se si modificano le impostazioni di configurazione, fare clic su **Applica** per implementare le modifiche.

25.8.4.33 How to Start the Kernel Crash Data Service

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Your communication system has an V3 OCC mainboard (OCCLA, OCCMA(R), OCCMB(R)).
Make sure there is sufficient free space on the storage disk for the service to run correctly. The service requires a 200 MB of storage space. Disks affected are:

- SATA SSD 16GB (if no NVMe SSD is mounted)
- NVMe SSD

It is recommended to delete traces before starting the service, if you want to free up storage space.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Click on **Trace Components > Kernel Crash Data**.
4) Fare clic su **Avvia**.

The Kernel Crash Data service starts and a system restart is automatically initiated. The service retains status after system restart.

25.8.4.34 How to Stop the Kernel Crash Data Service

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Your communication system has an V3 OCC mainboard (OCCLA, OCCMA(R), OCCMB(R).

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Click on **Trace Components > Kernel Crash Data**.
4) Click on **Stop**.

The Kernel Crash Data service stops and a system restart is automatically initiated. The service retains status after system restart.

25.8.4.35 Come avviare Traccia server multimediale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Fare clic su **Media Server Trace**.
4) Seleziona un'opzione dall'elenco a discesa **Livello di traccia** per definire il livello di dettaglio della traccia.
5) Fare clic su **Avvia**.

Nota: Le tracce attive aumentano il carico generale del sistema e possono avere un impatto negativo sulle prestazioni del sistema. Pertanto, Traccia server multimediale dovrebbe essere disattivata non appena si terminano le attività di diagnostica.

25.8.4.36 Come arrestare Traccia server multimediale

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Tracce**.
3) Fare clic su **Media Server Trace**.
4) Fare clic su **Arresta**.

25.9 Trasferimento TCP

Un trasferimento TCP viene utilizzato per il monitoraggio e la valutazione del traffico dati su una rete IP.

Suggerimento: L'attivazione di un trasferimento TCP influenza negativamente le prestazioni del sistema e va eseguita solo da amministratori esperti e in accordo con il servizio di assistenza competente.

I file trasferimento TCP vengono salvati nel sistema di comunicazione. Per la diagnostica dei file, è necessaria la relativa applicazione.

I trasferimenti TCP vengono spesso utilizzati per

- creare per un breve periodo (ad esempio per una descrizione del problema riproducibile) una traccia LAN.
- consentire l'accesso remoto a una traccia LAN ai tecnici dell'assistenza autorizzati.

Vantaggi relativi al daemon RPCAP: funzionalità di accesso remoto, non richiede l'invio per e-mail di file traccia

Svantaggi rispetto al daemon RPCAP: le tracce a lungo termine non sono significative; spazio di memorizzazione limitato; nessun filtro di cattura regolabile; gestione più complessa per le numerose tracce singole

25.9.1 Come avviare il trasferimento TCP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Tracce** > **Trasferimento TCP**.
3) Fare clic su **Trasferimento TCP**.
4) Selezionare le impostazioni desiderate.

5) Fare clic su **Applica**, quindi su **OK**.

25.9.2 Come arrestare il trasferimento TCP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Tracce** > **Trasferimento TCP**.
3) Fare clic su **Termina trasferimento TCP**.
4) Fare clic su **OK**.

25.9.3 Come cancellare il trasferimento TCP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Tracce** > **Trasferimento TCP**.
3) Fare clic su **Pulizia del trasferimento TCP**.
4) Fare clic su **Applica**, quindi su **OK**.

25.10 Daemon RPCAP

Un Daemon RPCAP (Remote Packet Capture) viene utilizzato per il monitoraggio e l'analisi del traffico dati su una rete IP.

Suggerimento: L'attivazione di un daemon RPCAP influenza negativamente le prestazioni del sistema e va eseguita solo da amministratori esperti e in accordo con il servizio di assistenza competente.

Tramite il daemon RPCAP è possibile per le applicazioni esterne accedere in remoto a pacchetti TCP/IP dell'interfaccia LAN del sistema di comunicazione.

Un daemon RPCAP viene spesso impostato per tracce a lungo termine, in quanto i file traccia vengono salvati sul PC e non nel sistema di comunicazione.

Vantaggi relativi al trasferimento TCP: gestione più facile e veloce, supporto per tracce a lungo termine, numero e/o dimensioni dei file traccia liberamente definibile, funzionalità di traccia della rete LAN

Svantaggi rispetto al trasferimento TCP: traffico dati di rete raddoppiato e quindi maggiore carico sulle interfacce LAN del sistema di comunicazione; richiesta di autorizzazione speciale delle porte (firewall)

25.10.1 Come attivare il daemon RPCAP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Il daemon RPCAP è stato disattivato.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Tracce** > **rpcap Daemon**.
3) Selezionare le impostazioni desiderate.
4) Fare clic su **Applica**, quindi su **OK**.

25.10.2 Come disattivare il daemon RPCAP

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Il daemon RPCAP è stato attivato.

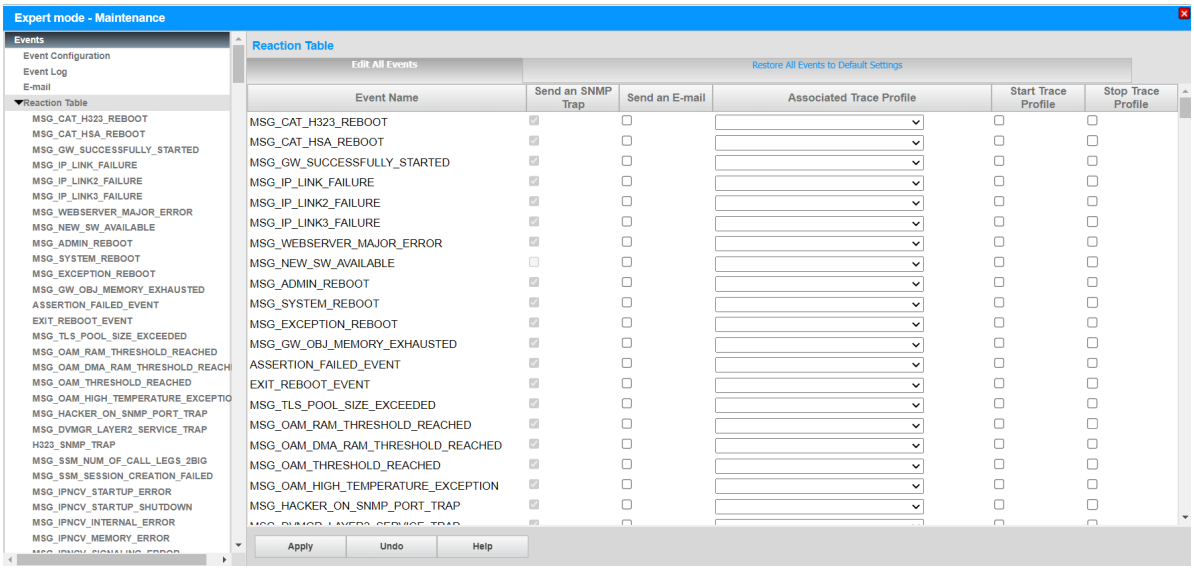
Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Tracce** > **rpcap Daemon**.
3) Fare clic su **Applica**, quindi su **OK**.

25.11 Eventi

Gli eventi informano su difetti/errori del sistema di comunicazione. Tutti gli eventi vengono memorizzati in un file di registro di dimensioni limitate. Se le dimensioni massime del file vengono superate, viene creato un nuovo file. Possono essere creati fino a sette file.

In base alle impostazioni della tabella delle reazioni e alla classe del problema, gli eventi possono determinare la creazione di un trap SNMP, il rilascio di e-mail e/o l'avvio/l'arresto del monitoraggio della traccia. Valutazione, configurazione e salvataggio dei registri evento hanno luogo tramite il WBM.



Per interpretare il file di registro eventi, il file deve essere scaricato ed estratto utilizzando WBM. Infine è possibile aprire il file con un editor di testo, modificarlo o stamparlo. Una volta trasmesso il file di registro eventi è possibile eliminarlo dalla memoria del sistema di comunicazione.

Gli eventi che determinano l'avvio di un'azione vengono definiti in base alle seguenti proprietà:

- Codice evento:

  Identifica un evento, quale ad esempio `MSG_ADMIN_LOGGED_OUT` = Informazione sulla disconnessione di un amministratore.
- Tipo evento:

  Di seguito sono elencati i diversi tipi di evento.

  – Informazioni: semplici messaggi di stato, non di errore.
  – Avvertenza: messaggi su un possibile problema a una procedura o in uno stato, non si tratta di messaggi di errore.
  – Minor: messaggio di errore. L'errore non causa problemi particolari.
  – Major: messaggio di errore. L'errore può avere conseguenze problematiche.
  – Critico: Messaggio d'errore. L'errore ha conseguenze problematiche.
  – Cleared: messaggio di errore. L'errore è già stato corretto dal sistema di comunicazione.
  – Indeterminate: messaggio di errore. La causa dell'errore non è ancora stata determinata con sicurezza.

- Testo evento

  Alcuni testi evento contengono variabili. Di norma sono codificate come segue:

  – %s: stringa
  – %u: numero decimale positivo o negativo
  – %f: numero a virgola mobile
  – %p: indice (indirizzo di memorizzazione)
  – %x: numero esadecimale (minuscolo)
  – %X: numero esadecimale (maiuscolo)
  – %c: singolo carattere
  – %d e %i: numero decimale positivo

Tabella delle reazioni

In base alla tabella delle reazioni un amministratore con il profilo **Expert** può definire separatamente per ciascun evento la modalità di reazione.

È possibile definire se creare e inviare un trap SNMP, il riavvio del sistema di comunicazione, l'invio di e-mail e/o l'avvio/l'arresto del profilo della traccia. Se l'evento è assegnato a un profilo di traccia, viene visualizzato il nome di tale profilo.

Impostazioni e-mail

In base a queste impostazioni, un amministratore con il profilo **Expert** può ricavare dati per l'invio di e-mail quando si verifica l'evento.

Registri di diagnostica

Il sistema di comunicazione registra azioni specifiche dei processi in un registro di diagnosi. Questi file di registro possono essere valutati per scopi di diagnostica da un amministratore con il profilo **Expert**.

Segnalazione di allarme per superamento della soglia di temperatura

Nel sistema di comunicazione sono memorizzati due valori critici di temperatura. Se la temperatura del sistema supera il primo valore, viene emesso un messaggio di attenzione, via Trap-SNMP o e-mail, che segnala che la temperatura del sistema è troppo elevata. Questo messaggio può inoltre essere visualizzato nel display di massimo 3 telefoni del sistema (UP0 e HFA), vedere Come definire le destinazioni per la segnalazione degli allarmi. Se viene superato il secondo valore, i moduli interessati dal surriscaldamento vengono arrestati in modo controllato (ad es. OpenScape Business Booster Card) o spenti (ad es. SLAV/SLAD). Per cancellare l'allarme e riportare in funzione i moduli è necessario spegnere e riaccendere il sistema.

Si può impostare quale delle 3 destinazioni (telefoni del sistema) deve ricevere la notifica del superamento della soglia di temperatura.

25.11.1 Come modificare la registrazione eventi tramite LAN

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Eventi**.
3) Nella struttura dei menu fare clic su **Eventi** > **Configurazione eventi**.
4) Selezionare l'impostazione desiderata:
   - Se è necessario trasferire la registrazione dell'evento tramite LAN, selezionare la casella di controllo **Attiva registrazione eventi tramite LAN**.
   - Se non si deve trasferire la registrazione dell'evento tramite LAN, deselezionare la casella di controllo **Attiva registrazione eventi tramite LAN**.
5) Fare clic su **Applica**, quindi su **OK**.

25.11.2 Come caricare il file di registro eventi

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Eventi**.
3) Nella struttura dei menu fare clic su **Eventi** > **Registro eventi**.
4) Fare clic sulla scheda **Carica tramite HTTP**.
5) Fare clic su **Carica**, quindi su **OK**. Viene visualizzata la finestra per il download del file.
6) Salvare il file nella cartella desiderata. Chiudere quindi la finestra che conferma il download del file.

25.11.3 Come cancellare il file di registro eventi

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Eventi**.
3) Nella struttura dei menu fare clic su **Eventi** > **Registro eventi**.
4) Fare clic sulla scheda **Cancella registro eventi**.
5) Fare clic su **Cancella registro**, quindi su **OK**.

25.11.4 Come modificare le impostazioni e-mail per gli eventi

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Inoltro e-mail deve essere configurato per tutti i sistemi per utilizzare l'opzione **Destinatario notifiche di emergenza**. Per ulteriori informazioni, vedere Come configurare l'invio di e-mail alla pagina 202

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Eventi**.
3) Nella struttura dei menu, fare clic su **Eventi** > **E-mail**.
4) Immettere come **Oggetto** il testo da visualizzare nel campo corrispondente del messaggio.

   Suggerimento: L'oggetto deve indicare chiaramente che si tratta di un'e-mail relativa a un evento.

5) Nei campi da **Destinatario 1** a **Destinatario 5**, immettere gli indirizzi e-mail dei destinatari.
6) Nel campo **Destinatario di emergenza**, inserire l'indirizzo e-mail di un responsabile della sicurezza in loco a cui viene inviata un'e-mail quando si seleziona un numero di emergenza.

   L'oggetto dell'e-mail è "Nuova chiamata di emergenza". Il numero di telefono e il nome del chiamante, se configurati, sono inclusi nell'e-mail e recuperati dal database del sistema.
7) Fare clic su **Applica**, quindi su **OK**.

25.11.5 Come visualizzare la tabella delle reazioni agli eventi

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Eventi**.
3) Nella struttura dei menu fare clic su **Eventi** > **Tabella delle reazioni**. Viene visualizzata la tabella delle reazioni con tutti i possibili eventi e le impostazioni corrispondenti.

25.11.6 Come modificare le impostazioni di reazione agli eventi

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Eventi**.
3) Nella struttura dei menu fare clic su **Eventi** > **Tabella delle reazioni**. Viene visualizzata la tabella delle reazioni con tutti i possibili eventi e

le impostazioni corrispondenti. Inoltre nella struttura dei menu vengono visualizzati i nomi di tutti gli eventi possibili.

4) Nella struttura dei menu fare clic sui nomi degli Eventi desiderati.

5) Fare clic sulla scheda **Modifica evento**. Vengono visualizzate le impostazioni delle reazioni all'evento desiderato.

> **Suggerimento:** Le impostazioni delle reazioni in **Riavvia gateway** e **Avvisa OpenScape** non possono essere modificate. Non è possibile modificare l'impostazione **Invia Trap SNMP** per tutti gli eventi.

6) Se possibile, selezionare l'impostazione per **Invia Trap SNMP**:
   - Se al verificarsi dell'evento si desidera inviare un Trap SNM, selezionare la casella di controllo **Invia Trap SNMP**.
   - Se al verificarsi dell'evento non si desidera inviare un Trap SNM, disattivare la casella di controllo **Invia Trap SNMP**.

7) Selezionare l'impostazione per **Invia e-mail**:
   - Se al verificarsi dell'evento si desidera inviare un'e-mail, selezionare la casella di controllo **Invia e-mail**.
   - Se al verificarsi dell'evento non si desidera inviare un'e-mail, disattivare la casella di controllo **Invia e-mail**.

8) Nell'elenco a discesa **Profilo di traccia assegnato** selezionare il profilo di traccia desiderato.

9) Selezionare l'impostazione per l'avvio o l'interruzione del profilo di traccia:
   - Se al verificarsi dell'evento si desidera avviare il profilo di traccia selezionato, selezionare la casella di controllo **Avvia profilo di traccia**.
   - Se al verificarsi dell'evento si desidera interrompere il profilo di traccia selezionato, selezionare la casella di controllo **Arresta profilo di traccia**.

10) Fare clic su **Applica**, quindi su **OK**.

25.11.7 Come modificare le impostazioni di reazione a più eventi

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.

2) Nella struttura di navigazione fare clic su **Manutenzione** > **Eventi**.

3) Nella struttura dei menu fare clic su **Eventi** > **Tabella delle reazioni**. Viene visualizzata la tabella delle reazioni con tutti i possibili eventi e le reazioni corrispondenti.

> **Suggerimento:** Le impostazioni delle reazioni in **Riavvia gateway** e **Avvisa OpenScape** non possono essere modificate. Non è possibile modificare l'impostazione **Invia Trap SNMP** per tutti gli eventi.

4) Modificare le impostazioni delle reazioni degli eventi desiderati nella tabella:
   - Se possibile, selezionare l'impostazione per **Invia Trap SNMP**:

     Se al verificarsi dell'evento si desidera inviare un Trap SNM, selezionare la casella di controllo **Invia Trap SNMP**.

     Se al verificarsi dell'evento non si desidera inviare un Trap SNM, disattivare la casella di controllo **Invia Trap SNMP**.
   - Selezionare l'impostazione per **Invia e-mail**:

     Se al verificarsi dell'evento si desidera inviare un'e-mail, selezionare la casella di controllo **Invia e-mail**.

     Se al verificarsi dell'evento non si desidera inviare un'e-mail, disattivare la casella di controllo **Invia e-mail**.
   - Nell'elenco a discesa **Profilo di traccia assegnato** selezionare il profilo di traccia desiderato.
   - Selezionare l'impostazione per l'avvio o l'interruzione del profilo di traccia:

     Se al verificarsi dell'evento si desidera avviare il profilo di traccia selezionato, selezionare la casella di controllo **Avvia profilo di traccia**.

     Se al verificarsi dell'evento si desidera interrompere il profilo di traccia selezionato, selezionare la casella di controllo **Arresta profilo di traccia**.
5) Fare clic su **Applica**, quindi su **OK**.

25.11.8 Come caricare/aprire registri di diagnostica

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Eventi**.
3) Nella struttura dei menu fare clic su **Eventi** > **Registri di diagnostica**.
4) Fare clic sulla scheda **Carica registri diagnostica**. Viene visualizzata una lista di tutti i registri disponibili con il nome file, le dimensioni del file in byte, l'ora dell'ultima modifica e gli attributi del file corrispondente.
5) In **Nome file**, fare clic sul nome del registro di diagnostica desiderato. Viene visualizzata la finestra per il download del file.
6) Salvare il file nella cartella desiderata. Chiudere quindi la finestra che conferma il download del file.

25.11.9 Come cancellare i registri diagnosi

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Eventi**.

3) Nella struttura dei menu fare clic su **Eventi** > **Registri di diagnostica**. Viene visualizzata una lista di tutti i registri disponibili con il nome file, le dimensioni del file in byte, l'ora dell'ultima modifica e gli attributi del file corrispondente.
4) Fare clic sulla scheda **Cancella registri diagnosi**.
5) Fare clic su **Cancella registro**, quindi su **OK**.

25.11.10 Come definire le destinazioni per la segnalazione degli allarmi

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Eventi**.
3) Nella struttura dei menu fare clic su **Eventi** > **Segnalazione allarme**.
4) Nell'elenco a discesa **Utente 1-3** selezionare le tre righe (telefoni di sistema con display, UP0 e HFA), che devono ricevere una notifica sul display in caso di superamento del valore critico della temperatura predefinito.
5) Fare clic su **Applica**, quindi su **OK**.

25.12 Dati di configurazione per funzioni diagnostiche

Per lo svolgimento di funzioni di diagnostica possono essere creati set di backup più piccoli, contenenti dati utili per la ricerca degli errori da parte del personale di assistenza. Diversamente dai normali set di backup, il volume di dati generato è notevolmente inferiore e quindi più facile da inviare ad esempio tramite e-mail.

I set di backup di diagnostica contengono fra l'altro i dati di configurazione del sistema di comunicazione e della applicazione UC (UC Smart o UC Suite). Non contengono invece i messaggi vocali, i messaggi fax e gli annunci.

Per il salvataggio dei set di backup di diagnostica possono essere utilizzati i seguenti supporti:

- **Periferica USB**

  Le informazioni possono ad esempio essere salvate su un disco USB o su una chiave USB collegati.

  Nota: Qualora per il backup vengano utilizzati un disco rigido USB, una partizione di un disco rigido USB o una chiavetta USB, questi devono essere formattati con FAT-32. A causa della limitazione del file system, le dimensioni massime del set di backup non devono superare i 4 GB. Altrimenti sarà necessario scegliere un supporto di backup alternativo. Un supporto USB formattato NTFS consente

solo la lettura. Qualora siano disponibili più partizioni, il salvataggio può essere eseguito solo sulla prima.

Se il salvataggio viene effettuato su un supporto USB avviabile, tale supporto dovrà essere rimosso dopo il backup.

- **HTTPS**

  I dati possono essere salvati tramite HTTPS sul disco rigido del client PC.
- **Disco rigido** (solo per OpenScape UC X3/X5/X8 con UC Booster Card (scheda applicazioni OCAB))

  I dati possono essere salvati sul disco rigido della scheda applicazioni OCAB.

Suggerimento: Non è possibile eseguire il backup sul disco rigido del sistema di comunicazione.

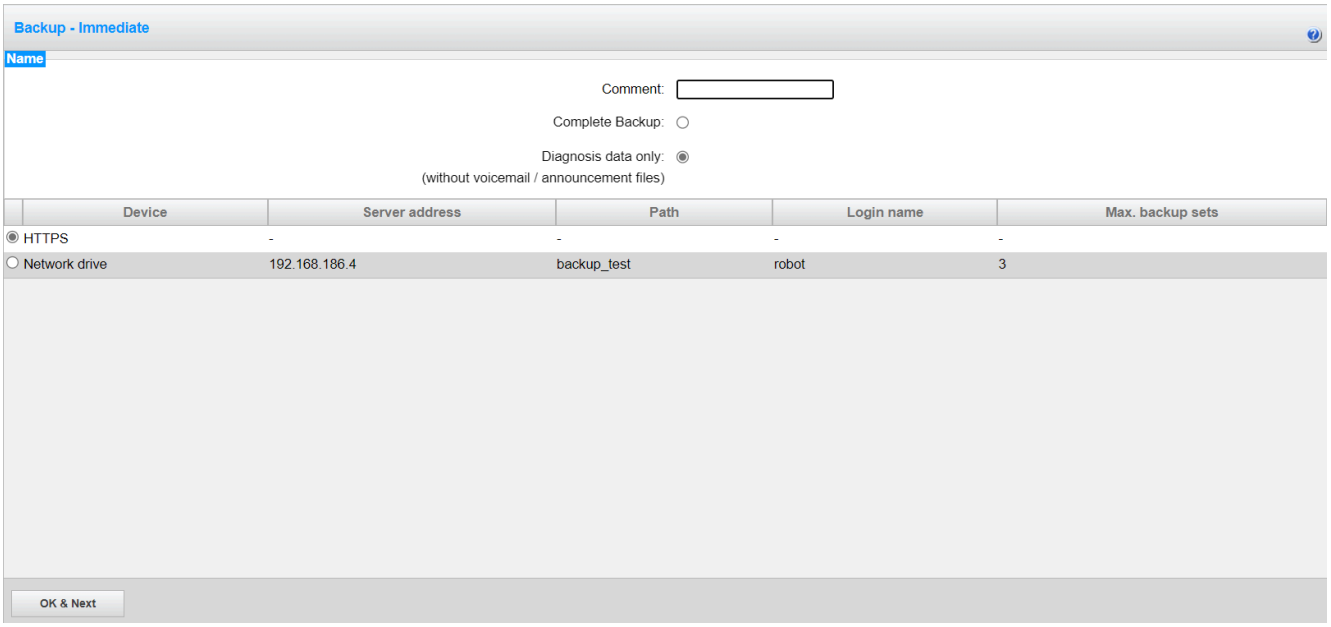
25.12.1 Come creare i dati di configurazione per le funzioni diagnostiche

Prerequisiti

Si è connessi a WBM con il profilo **Avanzato**.

Passo a passo

1) Nella barra di navigazione fare clic su **Backup dati**.
2) Nella struttura di navigazione fare clic su **Backup - dati** > **Backup - immediato**.



3) Selezionare la casella di controllo **Diagnostica**.

4) Selezionare la periferica sulla quale si desidera salvare il set di backup di diagnostica. Sono disponibili le seguenti opzioni:
   - Se si desidera salvare i dati su un disco rigido USB o su una chiave USB collegati, selezionare il pulsante di opzione **Periferica USB**.
   - Se si desidera salvare i dati tramite HTTPS sul disco rigido del client PC, selezionare il pulsante di opzione **HTTPS**.
   - Solo per OpenScape Business X3/X5/X8 con UC Booster Card (scheda applicazioni OCAB): Per salvare i dati sull'hard disk della scheda applicazioni OCAB, selezionare il pulsante di opzione **Hard Disk**.
5) Se necessario, immettere nel campo **Commento** un commento per il proprio set di backup di diagnostica. Non utilizzare dieresi e caratteri speciali.
6) Fare clic su **OK & Avanti**. Viene visualizzata una finestra a parte in cui è mostrato l'avanzamento del backup.
7) Il backup ha avuto esito positivo se viene visualizzato il messaggio `Backup completato`.
8) Se per il supporto di backup è stata attivata l'opzione **HTTPS**, è necessario salvare il set di backup di diagnostica e il corrispondente file di testo in una posizione a scelta. Per gli altri supporti di backup, questo avviene automaticamente. La finestra del browser deve restare aperta fino al termine dell'operazione di salvataggio del set di backup di diagnostica e del file di testo.

   Nota: Se per il backup si utilizza una **Periferica USB**, attendere fino a quando il LED di tale periferica non smette di lampeggiare. A questo punto il set di backup di diagnostica è stato interamente copiato su supporto USB. Rimuovere il supporto USB.
9) Fare clic su **Fine**.

Passaggi successivi

Il set di backup di diagnostica può ora essere inviato tramite e-mail all'assistenza tecnica competente a scopo di ricerca degli errori.

25.13 Card Manager

OpenScape Business è fornito con mezzi avviabili che contengono il software del sistema. Card Manager è uno strumento destinato al servizio assistenza per creare un nuovo software di sistema su una scheda SDHC vuota, un M.2 SATA SSD e hard disk UC Booster Card (HDD). A tal fine, è necessario il software del sistema di comunicazione sotto forma di file immagine compatibile.

Il software sulla scheda SDHC, M.2 SATA SSD o HDD è un software standard di sistema senza i dati del cliente. Non può essere utilizzato per gli aggiornamenti software o il backup dei dati dei clienti. Solo nel caso di una scheda SDHC è possibile includere un file di backup durante la creazione.

Card Manager può essere lanciato come un'immagine ISO in un DVD di avvio Linux, una chiavetta USB avviabile Linux o in un ambiente virtuale.

Il software Card Manager è disponibile tramite il Portale Partners

Esempi di applicazioni

- Prima della consegna del sistema, il software deve essere sostituito con la versione più recente dello stesso.
- Il dispositivo di stoccaggio è difettoso e deve essere sostituito con uno nuovo su cui non è ancora stato salvato alcun software.
- Il software utilizzato è difettoso e deve essere ricaricato. Durante il processo, tutti i dati dei clienti vanno persi.

  Se per il ripristino dei dati dei clienti è disponibile un set di backup, il software appena installato deve corrispondere alla versione software con cui è stato creato il set di backup, in questo modo le impostazioni mantenute nel set di backup possano essere supportate ed elaborate anche dal software installato.

25.13.1 Come utilizzare Card Manager per scrivere il software di comunicazione sull'M.2 SATA SSD

È possibile utilizzare Card Manager per scrivere il software di comunicazione di OpenScape Business V3 sull'M.2 SATA SSD.

Prerequisiti

La memoria viva del PC deve essere pari ad almeno 3 GB.

Sono disponibili un PC con un lettore DVD su sistema operativo Windows 10 e almeno 2 interfacce USB 2.0 o versione successiva.

Card Manager Tool V3 o superiore pienamente operativo su un PC.

È disponibile un adattatore USB SATA SSD. L'adattatore deve disporre di un supporto per tasto M e tasto B.

È disponibile un M.2 SATA SSD qualificato.

È disponibile un'immagine del SW di sistema nella versione corretta come file .tar. La versione SW deve corrispondere alla versione del sistema di destinazione. Deve essere esattamente la stessa versione utilizzata nel dispositivo di stoccaggio del sistema.

L'applicazione Card manager come file ISO su DVD.

Il file ISO di Card Manager deve essere masterizzato su un DVD.

Passo a passo

1) Salvare il file tar dell'immagine corrente su una chiavetta USB e avviare l'applicazione Card Manager dal file ISO del DVD.

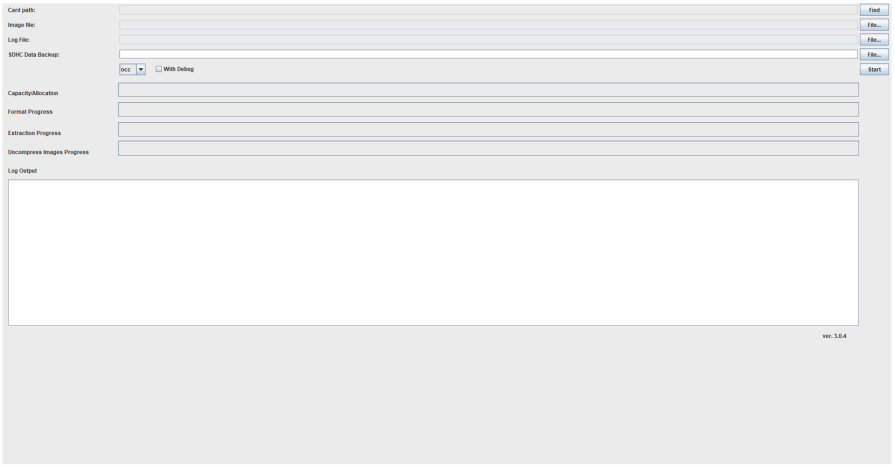
2) Collegare l'adattatore USB SATA SSD a un porta USB sul PC.

3) Inserire l'M.2 SATA SSD nell'adattatore e fare clic su **OK** sul pop-up per confermare la selezione.

Tutti i dati sull'SSD inserito saranno cancellati da Card Manager.

Non inserire altri dispositivi USB nel PC poiché saranno riconosciuti come mezzi di stoccaggio di OpenScape Business e tutti i dati saranno cancellati.

4) Sull'applicazione Card Manager, fare clic su **Trova** accanto a **Percorso scheda**.



5) Inserire una chiavetta USB con il file dell'immagine e fare clic su **File...** accanto a **File immagine** e selezionare il file tar dell'immagine archiviato sulla chiavetta USB.

6) Selezionare **OCCe** dal menu a tendina per la creazione dell'M.2 SATA SSD.

7) Come opzione, è anche possibile creare un file di registro dove memorizzare gli eventuali errori che si verificano durante l'esecuzione del programma. A tale scopo, fare clic su **File...**, accanto a **File di registro** e selezionare il percorso per il file di registro. Acquisire un nome per il file di registro e fare clic su **Salva**.

8) Fare clic su **Avvia**.

   Inizia il processo di scrittura ed è visualizzato il completamento di ogni tappa con la barra di avanzamento.

9) Fare clic su **OK** una volta ultimata l'installazione e rimuovere l'M.2 SATA SSD dall'adattatore.

10) Rimuovere l'adattatore dalla porta USB.

11) Spegnere il sistema di comunicazione.

12) Inserire il nuovo M.2 SATA SSD nel sistema di comunicazione spento.

13) Accendere il sistema di comunicazione. Il sistema si avvia con il nuovo M.2 SATA SSD e con la stessa versione software e configurazione ed è di nuovo operativo quando il LED verde lampeggia a impulsi di 1 Hz (0,5 sec acceso/0,5 sec spento).

Nota: Se l'M.2 SATA SSD è inserito in un sistema di comunicazione OpenScape Business, il sistema è avviato allo stato predefinito in origine, compreso l'indirizzo IP predefinito `192.168.1.2`.

Ripristinare un backup del sistema. Il backup deve avere la stessa versione inferiore del sistema installato.

25.13.2 Come utilizzare Card Manager per scrivere il software di comunicazione sulla scheda SDHC

È possibile utilizzare Card Manager per scrivere il software di comunicazione di OpenScape Business V3 su una scheda SDHC.

Prerequisiti

Sono disponibili un PC con un lettore DVD su sistema operativo Windows 10 e almeno 2 USB 2.0 o versione successiva.

Card Manager Tool V3 o superiore pienamente operativo su un PC.

È disponibile un lettore di schede SDHC USB.

È disponibile una scheda SDHC qualificata.

File di backup dei dati SDHC in opzione (file tar) archiviato su una chiavetta USB con l'immagine di sistema.

La protezione in scrittura della scheda SDHC è disattivata.

È disponibile un'immagine del SW di sistema nella versione corretta come file .tar. Può trattarsi di un file immagine piccolo (OCC) o grande (OCAB). La versione SW deve corrispondere alla versione del sistema di destinazione. Deve essere esattamente la stessa versione utilizzata sulla scheda SDHC attuale del sistema.

L'applicazione Card manager come file ISO su DVD.

Il file ISO di Card Manager deve essere masterizzato su un DVD.

Passo a passo

1) Salvare il file tar dell'immagine corrente su una chiavetta USB e avviare l'applicazione Card Manager dal file ISO del DVD.

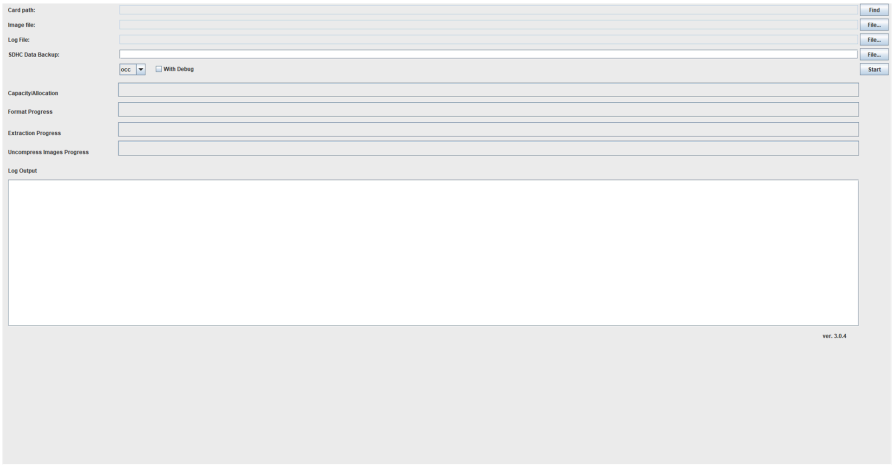
2) Collegare il lettore schede SDHC a un porta USB sul PC.

3) Rimuovere il lettore schede, inserire la scheda SDHC, inserire di nuovo il lettore schede e fare clic su **OK** sulla finestra popup. In **Percorso scheda** viene visualizzato il percorso per accedere alla scheda SDHC.

Tutti i dati sull'SSD inserito saranno cancellati da Card Manager.

Non inserire altri dispositivi USB nel PC poiché saranno riconosciuti come mezzi di stoccaggio di OpenScape Business e tutti i dati saranno cancellati.

4) Sull'applicazione Card Manager, fare clic su **Trova** accanto a **Percorso scheda**.



5) Inserire una chiavetta USB con il file dell'immagine e fare clic su **File...** accanto a **File immagine** e selezionare il file tar dell'immagine archiviato sulla chiavetta USB.

6) Selezionare **OCC** dal menu a tendina per la creazione della scheda SDHC.

7) Come opzione, è anche possibile creare un file di registro dove memorizzare gli eventuali errori che si verificano durante l'esecuzione del programma. A tale scopo, in **File di registro**, fare clic su **File...** e selezionare il percorso per il file di registro. Immettere il nome del file di registro e confermare con **Salva**.

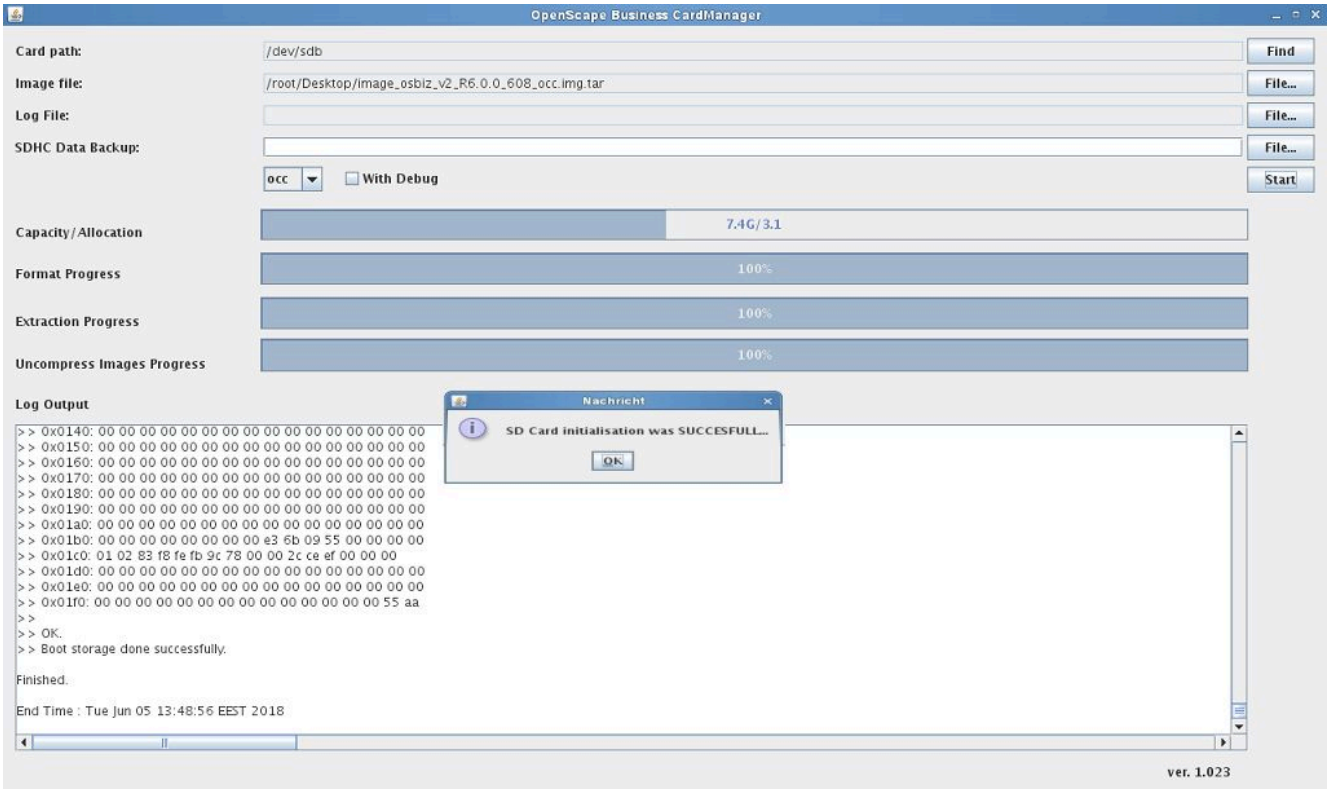
8) Come opzione, in **Backup dati SDHC** fare clic su **File...** e selezionare il file .tar con un file di backup dei dati della scheda SDHC specifico del cliente. In **Backup dati SDHC** viene visualizzato il percorso per accedere al file .tar.

9) Fare clic su **Avvia**.

   Inizia il processo di scrittura ed è visualizzato il completamento di ogni tappa con la barra di avanzamento.

Nota: Se il campo di testo (**Backup dati SDHC**) è compilato, Card Manager confronta innanzitutto la versione del file di backup della scheda SDHC con la versione del file di immagine del SW di sistema. In caso di incongruenza, viene visualizzato un messaggio di errore e il processo viene interrotto. Se le versioni sono congrue, Card Manager scrive l'immagine selezionata, quindi estrae il file .tar specificato nella scheda SDHC. Se

non è disponibile il backup dei dati SDHC, il campo di testo dovrebbe rimanere vuoto.



10) Fare clic su **OK** una volta completata l'installazione e rimuovere la scheda SDHC dal lettore schede.
11) Estrarre il lettore schede dalla porta USB.
12) Spegnere il sistema di comunicazione.
13) Inserire una nuova scheda SDHC nello slot SD del sistema di comunicazione spento.
14) Accendere il sistema di comunicazione. Il sistema si avvia con la nuova scheda SDHC e con le stesse versione software e configurazione ed è di nuovo operativo quando il LED verde lampeggia a impulsi di 1 Hz (0,5 sec acceso/0,5 sec spento).

Nota: Se la scheda SDHC è inserita in un sistema di comunicazione OpenScape Business, il sistema è avviato allo stato predefinito in origine, compreso l'indirizzo IP predefinito `192.168.1.2`.

25.13.3 Come utilizzare Card Manager per scrivere il software di comunicazione sull'hard disk OCAB

È possibile utilizzare Card Manager per scrivere il software di comunicazione di OpenScape Business V3 con OCAB su un hard disk OCAB.

Prerequisiti

Sono disponibili un PC con un lettore DVD su sistema operativo Windows 10 e almeno 2 interfacce USB 2.0 o versione successiva.

Card Manager Tool V3 o superiore pienamente operativo su un PC.

È disponibile un adattatore per hard disk OCAB. L'adattatore deve disporre di un supporto per tasto M e tasto B.

È disponibile un hard disk OCAB qualificato.

È disponibile un'immagine del software di sistema (OCAB) nella versione corretta come file .tar. La versione SW deve corrispondere alla versione del sistema di destinazione. Deve essere esattamente la stessa versione utilizzata nel dispositivo di stoccaggio del sistema.

L'applicazione Card manager come file ISO.

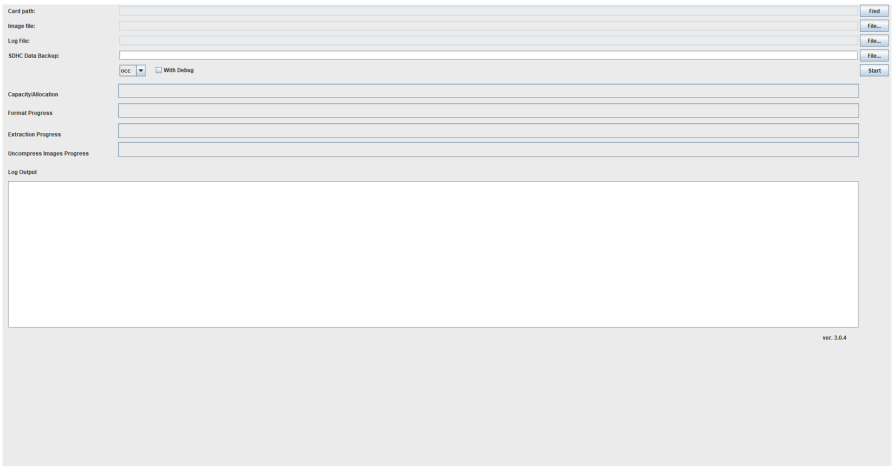
Il file ISO di Card Manager deve essere masterizzato su un DVD.

Passo a passo

1) Salvare il file tar dell'immagine corrente su una chiavetta USB e avviare l'applicazione Card Manager dal file ISO del DVD.
2) Collegare l'adattatore a un porta USB sul PC .
3) Inserire l'hard disk OCAB nell'adattatore e fare clic su **OK** sul pop-up per confermare la selezione.

   Tutti i dati sull'hard disk inserito saranno cancellati da Card Manager.

   Non inserire altri dispositivi USB nel PC poiché saranno riconosciuti come mezzi di stoccaggio di OpenScape Business e tutti i dati saranno cancellati.
4) Sull'applicazione Card Manager, fare clic su **Trova** accanto a **Percorso scheda**.



5) Inserire una chiavetta USB con il file dell'immagine e fare clic su **File...** accanto a **File immagine** e selezionare il file tar dell'immagine archiviato sulla chiavetta USB.
6) Selezionare **OCAB** dal menu a tendina per la creazione dell'hard disk OCAB.
7) Come opzione, è anche possibile creare un file di registro dove memorizzare gli eventuali errori che si verificano durante l'esecuzione del programma. A tale scopo, fare clic su **File...**, accanto a **File di registro** e

selezionare il percorso per il file di registro. Acquisire un nome per il file di registro e fare clic su **Salva**.

8) Fare clic su **Avvia**.

Inizia il processo di scrittura ed è visualizzato il completamento di ogni tappa con la barra di avanzamento.

9) Fare clic su **OK** una volta ultimata l'installazione e rimuovere l'hard disk OCAB dall'adattatore.

10) Rimuovere l'adattatore dalla porta USB.

11) Spegnere il sistema di comunicazione.

12) Montare il nuovo hard disk OCAB nella UC Booster Card e poi inserirlo nel sistema di comunicazione spento.

13) Accendere il sistema di comunicazione. Il sistema si avvia con il nuovo hard disk OCAB e con la stessa versione software e configurazione ed è di nuovo operativo quando il LED verde lampeggia a impulsi di 1 Hz (0,5 sec acceso/0,5 sec spento).

Nota:

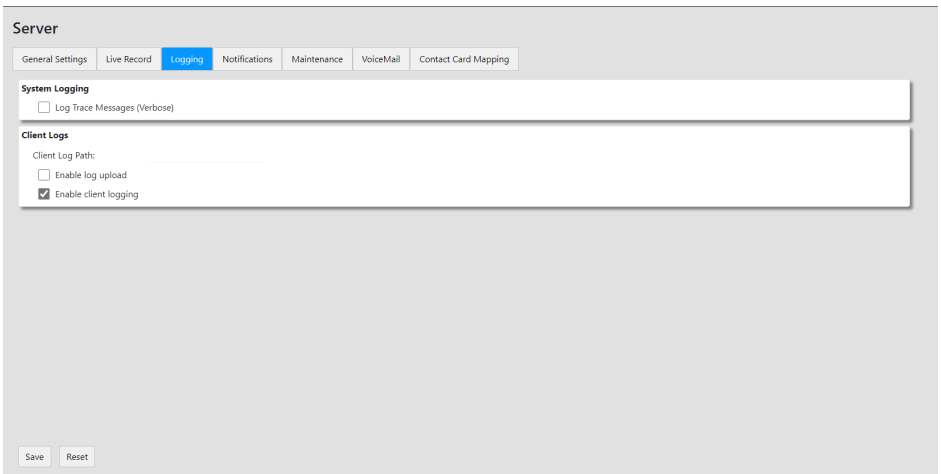
Sono persi tutti i dati dei media del cliente. È possibile effettuare un backup del sistema per recuperare questi dati.

25.14 Monitoraggio e manutenzione della UC Suite

Il WBM offre a un amministratore con il profilo **Expert** diverse funzioni per il monitoraggio e la manutenzione della UC Suite.

25.14.1 Logging

L'esecuzione della UC Suite viene monitorata internamente dal sistema. **System Logging** can be used to set whether logs should be created. In addition, a log of the activities of the UC Suite (e.g., the start of a UC Suite client) is maintained in **Client Logs**.



Registrazione sistema

La seguente registrazione sistema può essere attivata o disattivata:

Registrazione sistema	Impostazione predefinita
Registra messaggi traccia (estesi)	Non attivata

The results of the enabled system log are written daily to a log file with the designation `vs-yyyy-mm-dd.log` (e.g., `vs-2013-01-222.log`) and stored in the communication system under `/var/system/trace_log/vsl/log`.

Suggerimento: L'analisi dei file di registro può essere eseguita solo dal reparto Sviluppo.

Registri client

Client Logs are the log files of the UC Suite. Per ogni client UC Suite (myPortal for Desktop, myAttendant ecc.) e per ogni utente viene creata una cartella separata in cui vengono memorizzati i relativi file di registro. Qui vengono registrate le attività di un utente, ad esempio, l'avvio del client e le chiamate in arrivo e in uscita.

Suggerimento: La memorizzazione dei registri client è supportata solo per i client della UC Suite utilizzati con i sistemi operativi Microsoft Windows.

The path in which the `CC-Logs` directory with the subdirectories for the individual UC Suite clients is to be stored can be defined. È inoltre possibile selezionare se la directory deve essere salvata su ciascun PC client o su un PC o server centralizzato, sulla rete.

By default, the `CC-Logs` directory is stored in the following path: `<Drive>:\Documents and Settings/<PC User Name>/CC-Logs`

The retention period for **Client Logs** is 5 days. Non è possibile apportare modifiche.

The logging of the UC Suite activities in **Client Logs** is enabled by default. Administrators with the **Advanced** profile can disable logging on a station-specific basis by using the **User Directory** wizard. An administrator with the **Expert** profile can disable logging on a station-specific basis in **Expert Mode**.

A seconda dello scenario, i registri del client vengono salvati per impostazione predefinita su disco rigido della UC Booster Card (OCAB), dell'UC Booster Server o del sistema di comunicazione OpenScape Business S. An administrator with the **Expert** profile can disable the saving of client logs on the system hard disk in **Expert Mode**.

An administrator with the **Advanced** profile can use the **Trace** wizard to download the client logs (log files) of the UC Suite clients (myPortal for Desktop, myAttendant, etc.) used by the internal subscribers.

An administrator with the **Expert** profile can use the **Expert mode** wizard to download the client logs (log files) of the UC Suite clients (myPortal for Desktop, myAttendant, etc.) used by the internal subscribers.

25.14.1.1 Come attivare o disattivare la registrazione del registro di sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) In the navigation bar, click on **Expert Mode**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Click on **Server**, followed by **Logging**.
4) Select one of the following options, under the **System Logging** area:
   - If trace messages are to be recorded daily in a log file, select the **Log Trace Messages (Verbose)** check box.
   - If you do not want trace messages to be recorded in a log file, clear the **Log Trace Messages (Verbose)** check box).
5) Fare clic su **Salva**.

25.14.1.2 Come attivare o disattivare la registrazione di registri client a livello di sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) In the navigation bar, click on **Expert Mode**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Click on **Server**, followed by **Logging**.
4) Select one of the following options, under the **System Logging** area:
   - If client logs are to be recorded, select the **Enable client logging** check box.
   - If you do not want client logs are to be recorded, clear the **Enable client logging** check box.

   Suggerimento: La registrazione dei log dei client è supportata solo per i client della UC Suite utilizzati con i sistemi operativi Microsoft Windows.
5) Fare clic su **Salva**.

25.14.1.3 Come attivare o disattivare la registrazione di registri client per i singoli utenti

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione, fare clic su **Configurazione**.
2) Nella struttura di navigazione, fare clic su **Procedure guidate** > **UC Suite**.
3) Fare clic su **Modifica**, per avviare la procedura guidata **Rubrica utente**.
4) Selezionare l'utente desiderato nell'indice utenti e premere **Modifica**.
5) Nella struttura dei menu, fare clic su **Preferenze** > **Varie**.
6) Selezionare una delle seguenti opzioni:
   - Se è necessario tenere i registri client per l'utente desiderato, selezionare la casella di controllo **Registra messaggi di debug (estesi)**.
   - Se non è necessario tenere i registri client per l'utente desiderato, deselezionare la casella di controllo **Registra messaggi di debug (estesi)**.

   Suggerimento: La registrazione dei log dei client è supportata solo per i client della UC Suite utilizzati con i sistemi operativi Microsoft Windows.
7) Fare clic su **Salva**.
8) Se si desidera attivare o disattivare la registrazione dei registri client di un ulteriore utente, ripetere i passi da 4 a 7.

25.14.1.4 Come configurare il percorso dell'archivio per i file di registro del client

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Click on **Server**, followed by **Logging**.
4) In the field **Client Log Path:**, under the **Client Logs** area, enter the storage path in which the `CC-Logs` directory with the individual subdirectories of the UC Suite clients and their client log files are to be stored. Selezionare una delle seguenti opzioni:
   - If the `CC-Logs` directory is to be stored on every client PC, enter the following, for example: `<Drive>:\<Path>`.
   - If the `CC Logs` directory is to be stored on a central PC or server on the network, enter the following, for example: `\\<IP address>\<Drive>\<Path>`.

   Suggerimento: La memorizzazione dei registri client è supportata solo per i client della UC Suite utilizzati con i sistemi operativi Microsoft Windows.
5) Fare clic su **Salva**.

25.14.1.5 Come attivare o disattivare il salvataggio centralizzato dei registri client su disco rigido

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) In the navigation bar, click on **Expert Mode**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Click on **Server**, followed by **Logging**.
4) Select one of the following options, under the **Client Logs** area:
   - If you want client logs to be saved on the hard disk of the UC Booster Card (OCAB), the UC Booster Server or the OpenScape Business S communication system, select the **Enable log upload** check box.
   - If you do not want client logs to be saved on the hard disk of the UC Booster Card (OCAB), the UC Booster Server or the OpenScape Business S communication system, clear the **Enable log upload** check box.

   Suggerimento: La registrazione dei log dei client è supportata solo per i client della UC Suite utilizzati con i sistemi operativi Microsoft Windows.
5) Fare clic su **Salva**.

25.14.1.6 Come scaricare i registri client di tutti gli utenti interni

Con la procedura guidata **Traccia**, è possibile scaricare i registri dei client (file di registro) dei client UC Suite utilizzati dagli utenti interni (myPortal for Desktop, myAttendant ecc.). I registri dei client sono supportati solo per i client della UC Suite utilizzati con i sistemi operativi Microsoft Windows.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

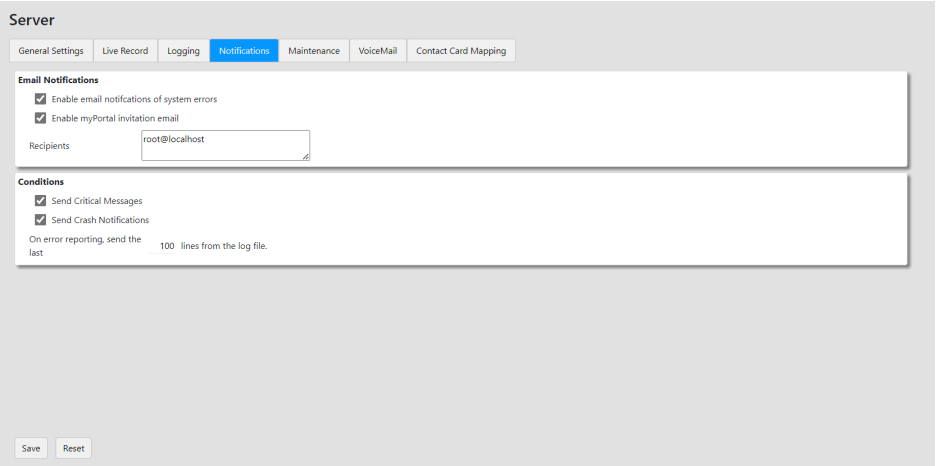
Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Diagnostica** > **Traccia**.
3) Fare clic su **Registri diagnostica**.
4) Fare clic su **Nessun protocollo**, per deselezionare le caselle di controllo di tutti i registri.
5) Selezionare la casella di controllo **Protocolli applicazioni**.

6) Selezionare una delle seguenti opzioni:
   - Se si desidera scaricare l'intero registro esistente, nell'elenco a discesa, selezionare **Intero protocollo**.
   - Se si desidera scaricare il registro del giorno, nell'elenco a discesa, selezionare **Protocollo odierno**.
   - Se si desidera scaricare il registro di un periodo specifico, nell'elenco a discesa selezionare **Selezione propria**. Nell'elenco a discesa **Da:** indicare la data di inizio del periodo desiderato e nell'elenco a discesa **Fino a:** la data di fine.
7) Fare clic su **Carica**, quindi su **OK**. Viene visualizzata la finestra per il download del file.
8) Salvare il file nella cartella desiderata. Chiudere quindi la finestra che conferma il download del file.
9) Fare clic su **Avanti**, quindi su **Fine**.

25.14.2 Avviso

E-mail notifications can be sent to the entered **Recipients** to provide advance warnings about critical disk usage levels for the hard disk, for example, or about errors.



The sending of e-mails can be linked to the following **conditions**:

Condizioni	Impostazione predefinita
Invia messaggi critici	Enabled
Invia avvisi sull'arresto imprevisto del sistema	Attivata

La funzione di invio di messaggi critici e avvisi relativi a crash di sistema deve essere attivata. Tali avvisi informano i destinatari su un possibile problema che deve essere comunicato al personale dell'assistenza tecnica competente.

È inoltre possibile definire quante delle righe finali di un file di registro devono essere incluse nel messaggio e-mail. Possono essere segnalati i seguenti tipi di errore di sistema (solo in inglese):

Errore di sistema
NULL monitor
Could not notify CallHandler (Impossibile inviare notifica a gestione chiamata)
Terminate call failed (Chiusura chiamata non riuscita)
Unable to load VM Structure from file (Impossibile caricare struttura VM da file)
Alsa stuck (Alsa bloccato)
Alsa cancel failed (Annullamento Alsa non riuscito)
MEN CallID 0
NULL alsa handle
Database connection failed (Connessione database non riuscita)
Rules engine logic failure (Errore logico motore regole)
Config schema format failure (Errore formato schema config)
90% Disk usage mark (segnalazione utilizzo disco 90%)
Main: Could not connect to the database !
Main: Could not load the configuration from the database!
Main: Could not open configuration file !
Main: Could not read the settings from the configuration file !
A segmentation fault was detected. (Rilevato errore di segmentazione)
Database logic error (Errore logico database)
Database schema error (Errore schema database)
ConnectionServer failed to start (Avvio server di connessione non riuscito)
MultisiteSync failed to start (Avvio MultisiteSync non riuscito)
Multisite failed to start (Avvio Multisite non riuscito)
TransferManager failed to start (Avvio gestore trasferimento non riuscito)
IPC failed to start (Avvio IPC non riuscito)
ConferenceManager failed to start (Avvio gestore conferenze non riuscito)
CallManager failed to start (Avvio gestore chiamate non riuscito)
MediaProcessing failed to start (Avvio MediaProcessing non riuscito)
Queues failed to start (Avvio code non riuscito)
Import failed to start (Avvio importazione non riuscito)
Data client failed to start (Avvio client dati non riuscito)
DirectoryClient failed to start (Avvio client directory non riuscito)
DirectoryServer failed to start (Avvio server directory non riuscito)
FV failed to start (Avvio FV non riuscito)
IM failed to start (Avvio IM non riuscito)
Switch failed to start (Avvio commutazione non riuscito)
No Switches (Nessuno switch)

Errore di sistema
Exchange Integration failed to start (Avvio integrazione Exchange non riuscito)
Outbound Fax failed to start (Avvio fax in uscita non riuscito)
SQL connection pool failed to start (Avvio pool connessione SQL non riuscito)
Task scheduler failed to start (Avvio pianificatore task non riuscito)
Trunks failed to start (Avvio linee non riuscito)
Unknown switch type (Tipo switch sconosciuto)
Users failed to start (Avvio utenti non riuscito)
MEB has been disconnected (MEB è stato scollegato)
MEB ACK timeout (Timeout MEB ACK)
Switch Heartbeat Timeout (Timeout Switch Heartbeat)

25.14.2.1 Come configurare le notifiche e-mail degli errori di sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Fare clic su **Server**, quindi su **Notifiche**.
4) Selezionare l'impostazione desiderata per le notifiche e-mail sotto l'area **Notifiche e-mail**:
   - Se si desidera ricevere le notifiche e-mail, attivare la casella di controllo **Abilita notifiche e-mail degli errori di sistema**.
   - Se non si desidera ricevere le notifiche e-mail, deselezionare la casella di controllo **Abilita notifiche e-mail degli errori di sistema**.
5) Nel campo **Destinatari**, inserire gli indirizzi e-mail delle persone a cui devono essere inviate le notifiche e-mail. I diversi indirizzi e-mail devono essere separati da una virgola `","` seguita da uno spazio `" "`.
6) Selezionare l'impostazione desiderata per i messaggi critici
   - Se si desidera ricevere le notifiche e-mail, per i messaggi critici, attivare la casella di controllo **Invia messaggi critici**.
   - Se non si desidera ricevere le notifiche e-mail per i messaggi critici, deselezionare la casella di controllo **Invia messaggi critici** casella di controllo.
7) Selezionare l'impostazione desiderata per le notifiche di arresti anomali
   - Se si desidera ricevere le notifiche e-mail per gli arresti anomali del sistema, attivare la casella di controllo **Invia notifiche arresti anomali**.
   - Se non si desidera ricevere le notifiche e-mail per gli arresti anomali del sistema, deselezionare la casella di controllo **Invia notifiche arresti anomali**.

8) Nel campo **Invia righe del file di registro**, inserire il numero di righe del file di registro da inviare con l'e-mail.
9) Fare clic su **Salva**.

25.14.3 Manutenzione

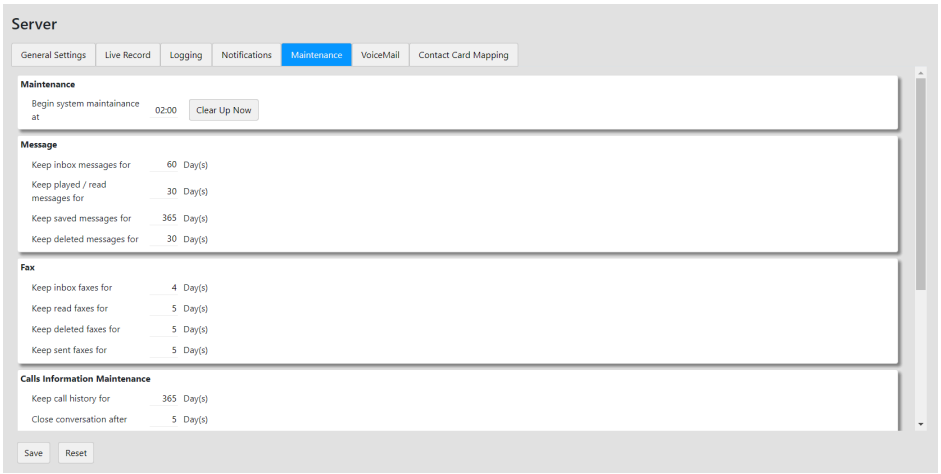
Con la manutenzione possono essere definiti i tempi di conservazione per messaggio, informazioni sulle chiamate nel diario, chiamate registrate tramite myAgent, fax e e-mail inviati e ricevuti per il Contact Center e file di registro.

È inoltre possibile impostare l'ora del giorno alla quale avrà luogo la cancellazione dei seguenti dati per i quali è trascorso il tempo di conservazione:

- Messaggi
- Informazioni sulle chiamate nel diario delle chiamate (cronologia chiamate)
- Chiamate registrate con myAgent (Contact Center)
- Fax e e-mail ricevuti e inviati per il Contact Center
- File di registro

Il valore predefinito è le 2:00.

Inoltre, è possibile avviare immediatamente la manutenzione del sistema e quindi la cancellazione immediata dei dati sopra indicati per i quali i periodi di conservazione indicati sono trascorsi. Ciò può essere ad esempio necessario se il disco rigido del sistema di comunicazione ha raggiunto un livello di riempimento critico.



For more information on **Message Maintenance**, see Voicemail Box .

For more information on **Maintaining Fax Messages**, see Fax Box .

For more information on **Calls Information Maintenance**: Call History, see Journal .

With **Calls Information Maintenance**: **Contact Center**, the calls recorded with myAgent and the received and sent faxes and e-mails for the Contact Center that have exceeded the set retention period are deleted. L'impostazione predefinita per la conservazione dei dati del Contact Center è 60 giorni.

Suggerimento: I tempi di conservazione per la manutenzione delle informazioni sulle chiamate sono indipendenti fra loro.

I rapporti del Contact Center si basano sulla cronologia chiamate. Se per la cronologia chiamate venisse impostato un tempo di conservazione minore rispetto a quello previsto per i dati del Contact Center, alcuni rapporti non sarebbero più disponibili.

During **Log File Maintenance**, the log files for which the set retention periods have expired are deleted. L'impostazione predefinita per la conservazione dei file di registro è 10 giorni.

25.14.3.1 Come configurare l'ora del giorno per la manutenzione

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Click on **Server** followed by **Maintenance**.
4) Enter the time at which the daily maintenance is to be performed in the **Begin system maintenance at** field, under the **Maintenance** area. All'ora impostata in questo campo, verrà avviata la cancellazione dei messaggi, delle informazioni di chiamata nel diario e dei file di registro che hanno superato i rispettivi tempi di conservazione previsti.
5) Fare clic su **Salva**.

25.14.3.2 Come configurare i tempi di conservazione dei file di registro

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Click on **Server** followed by **Maintenance**.
4) Enter the retention period in days in the **Keep log information for** field, under the **Log File Maintenance** area. Una volta trascorso il tempo di conservazione impostato in questo campo, i file di registro verranno eliminati.
5) Fare clic su **Salva**.

25.14.3.3 Come eseguire la manutenzione immediata del sistema

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Click on **Server** followed by **Maintenance**.
4) Click on **Clear Up Now**, under the **Maintenance** area.

   Suggerimento: I seguenti oggetti il cui periodo di conservazione è scaduto verranno eliminati: messaggi, informazioni sulle chiamate nel diario, chiamate registrate con myAgent, fax e e-mail ricevuti e inviati per il Contact Center e file di registro.

5) Click on **OK** to confirm the deletion.

25.14.3.4 Come configurare i tempi di conservazione dei dati Contact Center

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **OpenScape Business UC Suite**.
3) Click on **Server** followed by **Maintenance**.
4) Enter the retention period in days in the **Contact Center** field, under the **Calls Information Maintenance** area. Al superamento del periodo di conservazione qui definito, vengono eliminate le chiamate registrate con myAgent, i fax ricevuti e inviati e le e-mail per il Contact Center.
5) Fare clic su **Salva**.

25.15 Monitoraggio di UC Smart

Lo stato di aggiornamento di UC Smart può essere richiesto da un amministratore con il profilo **Expert** tramite il WBM.

25.15.1 Come controllare lo stato corrente di UC Smart

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

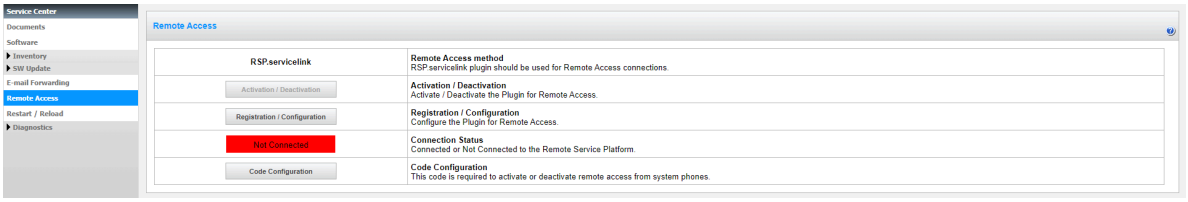
Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione, fare clic su **Applicazioni** > **UC Smart**.
3) Fare clic su **Stato**.

   Viene visualizzato lo stato corrente del server applicazioni e il numero di connessioni attive per ogni client UC.

25.16 Servizi di assistenza remoti

I vari servizi di assistenza remoti disponibili consentono a un tecnico dell'assistenza debitamente autorizzato di accedere in remoto al sistema di comunicazione e ai componenti collegati. In questo modo è possibile svolgere attività di manutenzione a costi convenienti e assistere gli utenti nella soluzione di problemi.



A causa del livello di sicurezza più elevato, occorre dare precedenza a RSP.servicelink sul servizio remoto. Per ulteriori informazioni, vedere: RSP.servicelink.

25.16.1 RSP.servicelink

Accesso remoto con RSP.servicelink (**R**emote **S**ervice **P**latform) offre a un tecnico dell'assistenza autorizzato di un partner di teleassistenza la possibilità di gestire a distanza il sistema di comunicazione e le relative applicazioni UC Booster in modo affidabile e sicuro. Per configurare RSP.servicelink, è necessaria solo una connessione a Internet, un browser Web, il Partner ID e la password del proprio partner di teleassistenza. RSP.servicelink assicura una connessione a banda larga altamente sicura.

RSP.servicelink è basato sulla tecnologia OpenVPN. Utilizza il protocollo SSL/TLS e la crittografia e fornisce un certificato client aggiuntivo del massimo livello di sicurezza. Nella documentazione, il termine RSP.servicelink è stato abbreviato in RSP.

Nota: RSP utilizza l'intervallo 100.64.0.1 - 100.127.255.254 per l'interfaccia tun0 quando RSP è attivo; ciò significa che, se è necessario accedere a un IP esterno all'interno di questo intervallo, è necessario aggiungere una route statica nel sistema Open Scape Business per instradare il traffico attraverso l'interfaccia desiderata.

In combinazione con OpenScape Business, RSP offre i seguenti importanti vantaggi:

- Elevata sicurezza tramite connessioni Internet in uscita

  L'instaurazione della connessione remota completa viene sempre avviata tramite il sistema di comunicazione. Ciò significa che il firewall della rete del cliente deve consentire solo una connessione HTTPS a un singolo indirizzo sul centro remoto (porta 443). Normalmente non è richiesta alcuna modifica delle politiche di sicurezza dei clienti o dei relativi firewall poiché questa porta è solitamente già aperta per le chiamante Internet in uscita nel firewall del cliente. In questo modo è garantita un'elevata sicurezza per la LAN del cliente.

  Con RSP l'amministratore del sistema di comunicazione mantiene il controllo della connessione remota tramite semplici attivazioni e disattivazioni dell'accesso. Con RSP.servicelink viene inoltre installato automaticamente un certificato client.
- Maggiore larghezza di banda

  Attraverso la connessione a Internet a banda larga, in caso di errore è possibile trasmettere rapidamente i dati di diagnostica e aumentare quindi la qualità del servizio.
- Configurazione semplice e a basso costo

  Il software del sistema di comunicazione contiene già un cosiddetto RSP.servicelink. All'attivazione del plugin del servizio, viene immesso il Partner ID e la password del partner di teleassistenza.

  Ogni partner di teleassistenza che utilizza RSP.servicelink dispone di un proprio Partner ID.

  Il plugin RSP.servicelink dovrebbe essere disattivato e riattivato quando si sta per eseguire l'aggiornamento di un software.
- Sicurezza futura

  RSP costituisce la base per i servizi futuri (servizi a valore aggiunto) quali ad esempio l'automatizzazione dei backup nonché delle funzioni di reporting e di monitoraggio.

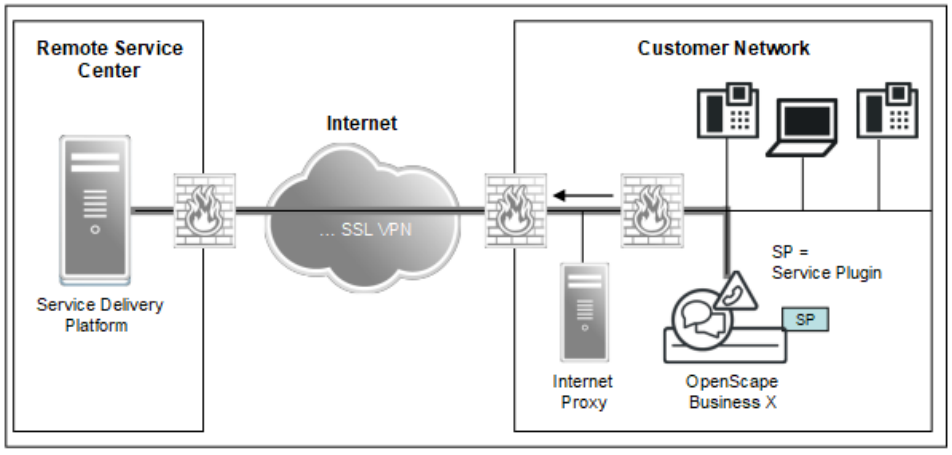


Figura 17: RSP - Panoramica per OpenScape Business X

RSP supporta gli standard dei servizi Web, quali il protocollo HTTPS (Hypertext Transfer Protocol Secure), SOAP (Simple Object Access Protocol) e XML (Extensible Markup Language).

La comunicazione tra i clienti e il centro di teleassistenza con RSP.servicelink avviene sempre mediante crittografia AES-256-CBC.

Plugin del servizio

Il plugin RSP.servicelink può essere abilitato o disabilitato singolarmente.

Il reset del plugin RSP.servicelink è necessario ad esempio dopo la sostituzione della scheda madre. Mediante reset, l'intera configurazione RSP viene eliminata e il plugin servizio è disattivato.

Nota: Se il sistema non è in modalità DTAG e il plugin RSP.servicelink è attivo, non è possibile modificare la configurazione delle impostazioni proxy. Il **pulsante Registrazione / Configurazione è disattivato.**

In modalità DTAG, se il plugin RSP.servicelink è attivo, premendo il pulsante Registrazione / Configurazione viene visualizzata direttamente la pagina delle impostazioni proxy con i pulsanti Interrompi/Fine. Ciò è possibile anche dal server remoto.

Gestione dispositivi (dispositivo gestito)

Nei sistemi di comunicazione senza UC Booster può essere consentito l'accesso remoto ad altri dispositivi alla LAN del cliente tramite la configurazione sul lato SIRA. I telefoni IP possono essere configurati sul lato SIRA utilizzando la funzione "Dispositivi gestiti".

Suggerimento: Non è possibile l'accesso remoto ad altri sistemi di comunicazione OpenScape Business disponibili sulla LAN del cliente. Ogni OpenScape Business deve essere configurato per l'accesso remoto.

Attivazione / Disattivazione

Per l'attivazione/la disattivazione del plugin servizio, è possibile procedere nei seguenti modi:

- Tramite la procedura guidata **Attivazione / Disattivazione**

  Per i plugin dei servizi RSP, è prevista una speciale procedura guidata per l'attivazione/la disattivazione.
- Inserendo un codice nel telefono di sistema (predefinito: attivazione con *996, disattivazione con #996)

  Per ragioni di sicurezza, per l'attivazione e la disattivazione tramite un telefono di sistema, è necessario inserire un PIN a 4 cifre oltre a un codice. La configurazione di questo PIN viene eseguita nel WBM del sistema di comunicazione da un utente con il profilo **Advanced**.

Backup e ripristina

Le credenziali RSP sono archiviate nel set di backup del sistema.

Se un nuovo sistema OpenScape Business viene configurato tramite clonazione o ripristino dei dati (migrazione) e il sistema originale aveva l'accesso RSP configurato, è necessario assicurarsi che il sistema clonato o ripristinato abbia attiva una configurazione RSP diversa.

È necessario disattivare o disinstallare l'RSP prima di clonare o eseguire il backup del sistema originale.

Se un certificato per la connessione a RSP viene utilizzato in più di un sistema, il certificato verrà revocato e nessuno dei sistemi OpenScape potrà connettersi al servizio RSP.

Premessa

- Accesso a Internet per il sistema di comunicazione o il proxy HTTP della LAN del cliente.
- Eventuale sblocco del firewall nella LAN del cliente per il registrar:
  - https://188.64.18.51
  - https://188.64.17.51
- Eventuale sblocco del firewall nella LAN del cliente per la VPN:
  - https://188.64.18.50
  - https://188.64.17.50
- Per la configurazione di Internet occorre specificare il router predefinito.

Nota: Nel caso in cui il sistema sia in modalità DTAG all'avvio del sistema e che si sia attivato l'accesso a Internet senza aver installato e configurato RSP.serviceplugin, uno script installerà, configurerà e attiverà automaticamente RSP.serviceplugin utilizzando il Partner ID e la password per DTAG (il nome del dispositivo sarà l'indirizzo MAC del sistema). Lo script sarà inoltre chiamato periodicamente ogni 10 minuti (ad esempio nel caso in cui non ci sia accesso a Internet dopo l'installazione iniziale del sistema). Lo script non attiverà automaticamente RSP.serviceplugin se l'utente lo ha disattivato manualmente.

25.16.1.1 Come installare, configurare e registrare il plugin RSP.servicelink

Con la procedura guidata **Registrazione / Configurazione** è possibile installare, configurare e registrare il plugin RSP.servicelink per l'accesso remoto al sistema di comunicazione tramite RSP.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Accesso remoto**.
3) Fare clic su **Registrazione / Configurazione**.
4) Se il plugin RSP.servicelink non è installato, fare clic su **Installa**, quindi su **OK & Avanti**.
5) Se il plugin RSP.servicelink è già installato, fare clic su **OK & Avanti**.
6) Se nella rete del cliente non viene utilizzato alcun server proxy, fare clic su **OK & Avanti**, in quanto non è necessaria la configurazione dei **Parametri proxy**. Saltare i due passaggi successivi.

7) Se nella rete del cliente viene utilizzato un server proxy, è necessario eseguire le impostazioni dei **Parametri proxy** in base alla rete del cliente:
   - Se nella rete del cliente è presente un proxy con protocollo HTTP, selezionare la casella di controllo **Usa stack HTTP Proxy**. Nel campo **Proxy HTTP Host** inserire il nome host e nel campo **Porta del proxy HTTP** inserire il numero di porta del server proxy. Se necessario, nel campo **Nome utente** e nel campo **Password** immettere nome utente e password per l'autenticazione del server proxy.
   - Se nella rete del cliente è presente un proxy con protocollo SOCKS, selezionare la casella di controllo **Usa stack SOCKS Proxy**. Nel campo **Proxy SOCKS host** inserire il nome host e nel campo **Porta del proxy SOCKS** inserire il numero di porta del server proxy. Se necessario, nel campo **Nome utente** e nel campo **Password** immettere nome utente e password per l'autenticazione del server proxy.

   Suggerimento: La necessità o meno dell'autenticazione, dipende dal tipo e dalla configurazione del server proxy.

8) Fare clic su **OK & Avanti**.
9) Solo se necessario, nel campo **Partner ID** modificare l'ID Partner assegnato.
10) Nel campo **Password** immettere la propria password.
11) Inserire il nome terminale. In SIRA Equipment Explorer (EqE) si trova il dispositivo e il relativo nome. L'indirizzo MAC di OpenScape Business è la voce predefinita.
12) Fare clic su **Fine**.

Nella colonna **RSP.servicelink**, la riga **Stato connessione** indica se la registrazione ha avuto esito positivo. In caso negativo, possono venire visualizzati i seguenti messaggi di errore:

- MAC già registrato:

  Soluzione: cancellare il dispositivo (= sistema di comunicazione OpenScape Business) dal SIRA Equipment Explorer e riconfigurarlo con la procedura guidata **Registrazione / Configurazione**.

  Nota: Con il nome terminale o l'indirizzo MAC, è possibile trovare il dispositivo sul SIRA Equipment Explorer. Il nome terminale o l'indirizzo MAC del sistema di comunicazione OpenScape Business si trova nel **Centro assistenza**, in **Accesso remoto**.

- Errore di configurazione:

  Soluzione: nella procedura guidata **Registrazione / Configurazione** inserire di nuovo il Partner ID e la password e uscire correttamente dalla procedura guidata.
- Credenziali errate:

  Soluzione: nella procedura guidata **Registrazione / Configurazione** inserire di nuovo il Partner ID e la password e uscire correttamente dalla procedura guidata.

25.16.1.2 Come attivare il plugin RSP.servicelink

Con la procedura guidata **Attivazione / Disattivazione** è possibile attivare il plugin RSP.servicelink per l'accesso remoto al sistema di comunicazione tramite RSP.

Prerequisiti

È disponibile e operativa una configurazione DNS.

È disponibile un router predefinito per l'accesso a Internet o, in alternativa, un server proxy nella rete del cliente.

Il plugin RSP.servicelink è disattivato.

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Accesso remoto**.
3) Nella colonna **RSP.servicelink**, fare clic su **Attivazione / Disattivazione** .
4) Fare clic su **Attiva**.

25.16.1.3 Come disattivare i plugin RSP.servicelink

Con la procedura guidata **Attivazione/Disattivazione** è possibile disattivare il plugin RSP.servicelink per l'accesso remoto al sistema di comunicazione.

Prerequisiti

Il plugin RSP.servicelink è attivato.

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Accesso remoto**.
3) Fare clic su **Abilita/Disabilita nella colonna RSP.servicelink**.
4) Fare clic su **Disattiva**.

25.16.1.4 Come reimpostare il plugin servizio RSP

Con la procedura guidata **Attivazione / Disattivazione** è possibile reimpostare il plugin del servizio RSP. In questo modo l'intera configurazione RSP viene eliminata e il plug-in servizio RSP disattivato.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Accesso remoto**.

3) Nella colonna **RSP.servicelink**, fare clic su **Attivazione / Disattivazione** .
4) Fare clic su **Ripristina predefinite**, quindi su **OK**.
5) Nella colonna **RSP.servicelink**, fare clic su **Attivazione / Disattivazione** .
6) Fare clic su **Disattiva**.
7) Sul server SIRA eliminare il dispositivo (= sistema di comunicazione OpenScape Business).

Nota: Con l'indirizzo MAC, è possibile trovare il dispositivo sul server SIRA. L'indirizzo MAC del sistema di comunicazione OpenScape Business si trova nel **Centro assistenza**, in **Inventory**.

25.16.1.5 Come configurare un PIN per l'attivazione e la disattivazione del plugin RSP.servicelink

Il PIN si utilizza per l'attivazione e la disattivazione del plugin RSP.servicelink tramite un telefono di sistema.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Accesso remoto**.
3) Nel campo **PIN** immettere il PIN a quattro cifre desiderato.
4) Fare clic su **Salva**, quindi su **OK**.

Passaggi successivi

L'attivazione del plugin di servizio primario tramite un telefono di sistema richiede l'inserimento del codice corrispondente (codice predefinito = *996) e quindi l'inserimento di un PIN a quattro cifre.

La disattivazione del plugin di servizio tramite un telefono di sistema richiede l'inserimento del codice corrispondente (codice predefinito = #996) e quindi l'inserimento di un PIN a quattro cifre.

25.16.2 Accesso remoto

Grazie all'accesso remoto è possibile consentire l'accesso dei tecnici dell'assistenza autorizzati al sistema di comunicazione OpenScape Business X tramite una connessione Internet. In questo modo è possibile ottenere supporto nello svolgimento delle attività di amministrazione o nel rilevamento degli errori.

Per consentire l'accesso a distanza al sistema di comunicazione è necessario attivare l'accesso remoto. È disponibile la modalità di accesso seguente:

Accesso remoto tramite connessione a Internet

Suggerimento: Quando si esegue l'accesso remoto mediante una connessione Internet sussiste un maggiore rischio per la sicurezza.

Per accedere tramite Internet il tecnico dell'assistenza necessita di una porta specifica (**Numero porta**) di accesso al sistema di comunicazione. Per impostazione predefinita, viene inserito il numero di porta 10099. Quando si utilizza un router esterno, è necessario configurare in tale router l'inoltro della porta per questo numero di porta.

Il numero di porta non deve venire bloccato da un eventuale firewall sul PC del tecnico dell'assistenza. La scelta del numero di porta deve essere concordata con il tecnico dell'assistenza.

Le applicazioni UC Booster (ad esempio UC Suite, OpenDirectory Service, Gate View) non possono essere amministrate tramite questo accesso remoto.

Per impedire l'accesso a distanza al sistema di comunicazione è necessario disattivare l'accesso remoto.

Nota: Per evitare l'accesso non autorizzato al sistema di comunicazione, è opportuno disabilitare l'accesso remoto al termine della procedura di amministrazione remota.

25.16.2.1 Come attivare l'accesso remoto tramite ISDN

La procedura guidata **Accesso remoto** consente di concedere ai tecnici dell'assistenza autorizzati l'accesso al sistema di comunicazione tramite la connessione a ISDN.

Prerequisiti

OpenScape Business X dispone di allacciamento a linea ISDN.

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Accesso remoto**.
3) Fare clic su **Accesso remoto**, per avviare la procedura guidata **Accesso remoto**.
4) Selezionare l'opzione **Accesso remoto: on**, per attivare l'accesso remoto.
5) Selezionare l'opzione **Accesso remoto tramite: ISDN**, per abilitare l'accesso remoto tramite ISDN.
6) Nel campo **Numero di telefono** immettere il numero interno da utilizzare per l'accesso remoto.
7) Nel campo **Numero di accesso** immettere il numero interno da utilizzare per l'accesso remoto.
8) Fare clic su **OK & Avanti**, quindi su **Fine**.

25.16.2.2 Come configurare un PC con Microsoft Windows Vista per l'accesso remoto tramite ISDN

Prerequisiti

Il PC è dotato di una scheda ISDN e dispone di una connessione esterna ISDN.

Per accedere al sistema di connessione OpenScape Business X3/X5/X8 viene utilizzata una connessione punto-punto. Sono disponibili il prefisso interurbano e il numero di telefono del sistema di comunicazione.

È stato abilitato l'accesso remoto tramite ISDN. È disponibile il numero di accesso da utilizzare per l'accesso remoto al sistema di comunicazione.

Sono disponibili il nome utente e la password per l'accesso al sistema di comunicazione.

Suggerimento: La seguente descrizione si riferisce a un PC con il sistema operativo Microsoft Windows Vista. La procedura da seguire per il sistema operativo Microsoft Windows XP è simile.

Passo a passo

1) Nel menu **Start** di Windows Vista, fare clic su **Connetti a**. Viene visualizzata la finestra **Connessione a una rete**.
2) Fare clic su **Configura connessione o rete**.
3) Fare clic sull'opzione di connessione **Connessione a una rete aziendale**, quindi su **Avanti**.
4) Fare clic su **Connetti direttamente tramite linea telefonica**.
5) Nel campo **Numero di telefono** indicare il codice di linea urbana (ad esempio `0`), il prefisso interurbano (ad esempio `089`), il numero di telefono del sistema (ad esempio `12345678`) e il numero di accesso (ad esempio `666`).

   La voce completa per l'esempio citato è la seguente: `008912345678666`
6) Nel campo **Nome destinazione** indicare una denominazione per questa connessione.
7) Selezionare la casella di controllo **Non collegare ora, configurare solo per uso successivo**.
8) Fare clic su **Avanti**.
9) Nel campo **Nome utente** immettere il nome utente per l'accesso al sistema di comunicazione.
10) Nel campo **Password** immettere la password per l'accesso al sistema di comunicazione.

    Nota: Come dati predefiniti per l'accesso al sistema di comunicazione vengono utilizzati il nome utente e la password predefiniti per l'accesso al sistema tramite il tool Manager E.

    ---
11) Fare clic su **Crea**.
12) Fare clic su **Connetti**.

È ora possibile l'accesso remoto al sistema di comunicazione.

Suggerimento: Per disattivare la connessione, fare clic su **Avvio** > **Connetti a**. Fare clic sul nome definito nella fase 6 della connessione (**Nome destinazione** e quindi su **Disconnetti**.

Per attivare la connessione, fare clic sulla descrizione definita al passo 6 (**Nome destinazione**) e quindi su **Collega**.

25.16.2.3 Come configurare un PC con Microsoft Windows 7 per l'accesso remoto tramite ISDN

Prerequisiti

Il PC è dotato di una scheda ISDN e dispone di una connessione esterna ISDN.

Per accedere al sistema di connessione OpenScape Business X3/X5/X8 viene utilizzata una connessione punto-punto. Sono disponibili il prefisso interurbano e il numero di telefono del sistema di comunicazione.

È stato abilitato l'accesso remoto tramite ISDN. È disponibile il numero di accesso da utilizzare per l'accesso remoto al sistema di comunicazione.

Sono disponibili il nome utente e la password per l'accesso al sistema di comunicazione.

Suggerimento: La seguente descrizione si riferisce a un PC con il sistema operativo Microsoft Windows 7.

Passo a passo

1) Nel menu **Start** di Windows 7, fare clic su **Pannello di controllo**.
2) Fare clic su **Rete e Internet**.
3) Fare clic su **Rete e centro condivisione**.
4) Fare clic su **Configura connessione o rete**.
5) Fare clic sull'opzione di connessione **Connessione a una rete aziendale**, quindi su **Avanti**.
6) Fare clic su **Connetti direttamente tramite linea telefonica**.
7) Nel campo **Numero di telefono** indicare il codice di linea urbana (ad esempio `0`), il prefisso interurbano (ad esempio `089`), il numero di telefono del sistema (ad esempio `12345678`) e il numero di accesso (ad esempio `666`).

   La voce completa per l'esempio citato è la seguente: `008912345678666`
8) Nel campo **Nome destinazione** indicare una denominazione per questa connessione.
9) Selezionare la casella di controllo **Non collegare ora, configurare solo per uso successivo**.
10) Fare clic su **Avanti**.
11) Nel campo **Nome utente** immettere il nome utente per l'accesso al sistema di comunicazione.

12) Nel campo **Password** immettere la password per l'accesso al sistema di comunicazione.

> **Nota:** Come dati predefiniti per l'accesso al sistema di comunicazione vengono utilizzati il nome utente e la password predefiniti per l'accesso al sistema tramite il tool Manager E.

13) Fare clic su **Crea**.
14) Fare clic su **Connetti**. Successivamente viene visualizzato il messaggio `Connessione stabilita`.
15) Fare clic su **Chiudi**.

È ora possibile l'accesso remoto al sistema di comunicazione.

> **Suggerimento:** Per disattivare la connessione, nella barra degli strumenti fare clic sull'icona **Connetti a**. Fare clic sul nome definito nella fase 8 della connessione (**Nome destinazione** e quindi su **Disconnetti**.
>
> Per attivare la connessione, fare clic sulla descrizione definita al passo 8 (**Nome destinazione**) e quindi su **Collega**.

25.16.2.4 Come accedere in remoto tramite Internet con indirizzo IP fisso

La procedura guidata **Accesso remoto** consente di concedere ai tecnici dell'assistenza autorizzati l'accesso al sistema di comunicazione tramite la connessione a Internet.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

È disponibile un Numero di porta che consente l'accesso tramite Internet al sistema di comunicazione per i tecnici dell'assistenza. Questo numero di porta non deve venire bloccato da un eventuale firewall sul PC del tecnico dell'assistenza.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Accesso remoto**.
3) Fare clic su **Accesso remoto**, per avviare la procedura guidata **Accesso remoto**.
4) Selezionare l'opzione **Accesso remoto: on**, per attivare l'accesso remoto.
5) Selezionare l'opzione **Accesso remoto tramite: Internet**, per abilitare l'accesso remoto tramite Internet.
6) Nel campo **Numero di porta** immettere il numero di porta da utilizzare per l'accesso remoto.

   Per impostazione predefinita, viene inserito il numero di porta 10099.

7) Fare clic su **OK & Avanti**. Viene visualizzato il messaggio `Accesso remoto attivato ...`. Il messaggio contiene l'URLtramite il quale è possibile accedere al sistema di comunicazione mediante il browser Web.
8) Fare clic su **Fine**.

25.16.2.5 Come accedere in remoto tramite Internet senza indirizzo IP fisso

La procedura guidata **Accesso remoto** consente di concedere ai tecnici dell'assistenza autorizzati l'accesso al sistema di comunicazione tramite la connessione a Internet.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

È disponibile un Numero di porta che consente l'accesso tramite Internet al sistema di comunicazione per i tecnici dell'assistenza. Questo numero di porta non deve venire bloccato da un eventuale firewall sul PC del tecnico dell'assistenza.

È disponibile un account DynDNS.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Accesso remoto**.
3) Fare clic su **Accesso remoto**, per avviare la procedura guidata **Accesso remoto**.
4) Selezionare l'opzione **Accesso remoto: on**, per attivare l'accesso remoto.
5) Selezionare l'opzione **Accesso remoto tramite: Internet**, per abilitare l'accesso remoto tramite Internet.
6) Nel campo **Numero di porta** immettere il numero di porta da utilizzare per l'accesso remoto.

   Per impostazione predefinita, viene inserito il numero di porta 10099.
7) Fare clic su **OK & Avanti** per applicare le impostazioni. Viene visualizzata la finestra **Configura account DynDNS**.
8) Nel campo **Nome utente** immettere il nome utente dell'account DynDNS attivo presso il provider DynDNS, nel caso questo non sia già visualizzato.
9) Nel campo **Password** e nel campo **Ripeti password** immettere la password dell'account DynDNS attivo presso il provider DynDNS, se questo non è già visualizzato.
10) Nel campo **Nome dell'host** immettere il nome host indicato dal provider DynDNS, senza nome di dominio, ad esempio `myhost` (se questo non è già visualizzato).
11) Nell'elenco a discesa **Nome del dominio** selezionare il provider DynDNS, ad esempio, `dyndns.org`, se questo non è già visualizzato. Il nome di dominio completo risulta `myhost.dyndns.org`.
12) Fare clic su **Test connessione**. Viene visualizzata la finestra **Test accesso DynDNS**.
13) Fare clic su **OK**. I dati di accesso DynDNS vengono comunicati al provider. Sono necessari circa 10 secondi.

14) Se il test ha esito positivo, viene visualizzato il messaggio `Accesso remoto attivato ...`. Il messaggio contiene l'URLtramite il quale è possibile accedere al sistema di comunicazione mediante il browser Web. Fare clic su **Fine**.
15) Se il test ha esito negativo, fare clic su **OK**. Verrà visualizzata la finestra **Accesso DynDNS** che fornisce informazioni sulle possibili cause degli errori. Fare clic su **OK**. Viene visualizzata la finestra **Configura account DynDNS**. Verificare ed eventualmente correggere i dati di accesso immessi (passaggi da 8 a 11). Procedere come descritto al passaggio 12.

25.16.2.6 Come disattivare l'accesso remoto

Con la procedura guidata **Accesso remoto** è possibile disattivare la funzione di accesso remoto.

Prerequisiti

Si è connessi a WBM con il profilo **Avanzate**.

Passo a passo

1) Nella barra di navigazione fare clic su **Centro assistenza**.
2) Nella struttura di navigazione fare clic su **Accesso remoto**.
3) Fare clic su **Accesso remoto**, per avviare la procedura guidata **Accesso remoto**. Viene visualizzato se è attivo l'accesso remoto tramite Internet e/o ISDN.
4) Selezionare l'opzione **Accesso remoto: off** per disattivare un accesso remoto.
5) Scegliere l'opzione di accesso remoto da disattivare:
   - Se si desidera disattivare l'accesso remoto tramite Internet, attivare il pulsante di opzione **Accesso remoto tramite: Internet**.
   - Se si desidera disattivare l'accesso remoto tramite ISDN, attivare il pulsante di opzione **Accesso remoto tramite: ISDN**.
6) Fare clic su **OK & Avanti**.
7) Se si desidera disattivare anche la seconda opzione di accesso remoto, fare clic su **Indietro**. Ripetere i passaggi 4 – 6.
8) Fare clic su **Fine**.

25.16.3 Utente online

Utente online consente di svolgere funzioni remote di controllo, verifica e monitoraggi oper i telefoni OpenStage tramite un PC con Windows. Con Utente online, è possibile riprodurre il comportamento di un telefono OpenStage sul PC.

Essenziale per consentire la comunicazione con un telefono OpenStage è che il software del telefono sia accompagnato da un cosiddetto "dongle".

Per l'accesso a un telefono OpenStage è necessario inserire in Utente online le seguenti informazioni:

- Tipo di telefono OpenStage

- Indirizzo IP del telefono OpenStage
- Password di amministratore del telefono OpenStage

Per informazioni sull'uso di Utente online, consultare la seguente documentazione: *OpenStage HUSIM Phone Tester User Guide*. Tale documento è accessibile sul portale intranet della documentazione tecnica dei prodotti, all'indirizzo `http://apps.g-dms.com:8081/techdoc/search_en.htm`.

Inoltre, il tool Manager E offre agli utenti online funzionalità di controllo remoto, test e monitoraggio dei telefoni OpenStage.

Nota: L'indirizzo IP del gateway in Utente online è lo stesso dell'indirizzo IP del sistema. L'indirizzo IP del gateway non è l'indirizzo IP del percorso predefinito.

25.16.3.1 Come avviare Utente online

Prerequisiti

Si è connessi al WBM con il profilo **Expert**.

Passo a passo

1) Nella barra di navigazione fare clic su **Modalità esperti**.
2) Nella struttura di navigazione fare clic su **Manutenzione** > **Utente online**. Viene visualizzata la finestra di registrazione dell'utente in linea.
3) Nell'elenco a discesa **Modello**, selezionare il modello del telefono OpenStage desiderato.
4) Nel campo **IP telefono** immettere l'indirizzo IP del telefono OpenStage desiderato.
5) Nel campo **Password** immettere la password di amministratore del telefono OpenStage desiderato. Per impostazione predefinita la password è `123456`.
6) Nell'elenco a discesa **Protocollo**, selezionare il protocollo di trasporto desiderato.
7) Selezionare una delle seguenti opzioni per il protocollo Internet versione IPv:
   - Se si desidera utilizzare il protocollo Internet Versione 4, selezionare l'opzione **IPv4**.
   - Se si desidera utilizzare il protocollo Internet Versione 6, selezionare l'opzione **IPv6**.
8) Nell'elenco a discesa **Number of Key modules** (Numero di moduli chiave) selezionare il numero di moduli aggiuntivi.
9) Per attivare l'accesso al telefono OpenStage desiderato, fare clic su **OK**.

Suggerimento: Per informazioni sull'uso degli utenti in linea, consultare la *OpenStage HUSIM Phone Tester User Guide*, disponibile all'indirizzo `http://apps.g-dms.com:8081/techdoc/search_en.htm`.

---

26 Migrazione

I sistemi OpenScape Business V1, V2 e i sistemi HiPath 3000 possono essere migrati/aggiornati a OpenScape Business V3.

I seguenti scenari di migrazione/upgrade sono supportati dal software OpenScape Business V3.

Nota: È fondamentale eliminare gli utenti Unify Phone attivi prima, ad esempio, delle migrazioni di sistema, per evitare discrepanze critiche tra il database OpenScape Business e il database cloud. Ulteriori informazioni sono disponibili in White paper Unify Phone di Unify Experts Wiki.

Nota: Vedere anche Come rimuovere o eliminare nuovi utenti Unify Phone alla pagina 1196.

Sistema OpenScape Business X con UC Booster Card o Booster Server

- Upgrade del software da OpenScape Business X V2 a V3 con «scheda madre V2»
- Migrazione hardware/software da OpenScape Business X V2 a V3 con «scheda madre V3»
- Migrazione hardware/software da OpenScape Business X V1 a V3 con «scheda madre V3»
- Migrazione hardware/software da OpenScape Business X V3 con «scheda madre V2» a V3 con «scheda madre V3»

Sistema OpenScape Business S

- Upgrade del software da OpenScape Business S V2 a V3

Rete OpenScape Business

- Migrazione/upgrade di una rete OpenScape Business da V2 a V3

HiPath 3000 con OpenScape Office HX

- Migrazione hardware di HiPath 3000 con OpenScape Office HX

HiPath 500

- Migrazione hardware da HiPath 500 a OpenScape Business X1 V3

Secondo il sistema sorgente, le licenze esistenti possono essere trasferite completamente o parzialmente. Lo stesso vale per il successivo uso dei moduli periferici e dispositivi terminali connessi.

Dopo la migrazione, il supporto software esistente per i sistemi OpenScape Business rimarrà immutato.

È possibile ridurre le operazioni di migrazione/upgrade per l'uso continuo delle licenze esistenti rispetto al trasferimento offline di una licenza connettendo il sistema OpenScape Business al server centrale delle licenze Unify e utilizzando la funzione **CLS Connect**.

In questa sezione sono utilizzati i seguenti termini:

Migrazione	in caso di modifica hardware/software
Upgrade	in caso di modifica puramente software
Scheda madre V2	termine utilizzato per la famiglia di schede madri introdotte con OpenScape Business.
Scheda madre V3	termine utilizzato per la famiglia di schede madri introdotte con il software V3.

Nota: Un prerequisito per tutti gli scenari di migrazione per l'aggiornamento da un sistema con scheda madre V2 a un sistema con scheda madre V3 è che l'amministratore carichi il set di backup tramite il dispositivo HTTPS. Altri dispositivi come disco rigido, FTP o unità di rete non sono supportati e il processo di migrazione non riuscirà.

Nota: Esistono due percorsi di migrazione validi a seconda della versione software del sistema OSBiz. Utilizzare un set di backup da un sistema hardware V2 sull'ultimo bind V2R7 oppure utilizzare lo stesso bind software V3 sia sulla scheda madre V2 che sui sistemi con scheda madre V3 per garantire la coerenza nel database.

Nota: Se un sistema OpenScape Office V3 MX/LX verrà sostituito con un sistema OpenScape Business, quest'ultimo dovrà essere ordinato come nuovo sistema.

26.1 Upgrade software dei sistemi OpenScape Business X

L'upgrade software dei sistemi OpenScape Business X comporta essenzialmente la sostituzione di alcuni componenti software.

Prima di eseguire l'upgrade del software di un sistema OpenScape Business X, si deve determinare la configurazione del sistema corrente e i componenti hardware/software e su licenza da sostituire, all'occorrenza.

Tabella 31: Upgrade software di OpenScape Business X - Checklist Hardware/Software

Componenti	Sostituito da
Componenti hardware	
Componenti software	
Software di sistema V2 su scheda SDHC	Software di sistema V3 (immagine dal server di download del software)
VPN su WAN nel sistema terminato	VPN nel router esterno terminato
XMPP	Nessuna soluzione di follow-up

Componenti	Sostituito da
myPortal Smart	myPortal @work
Componenti su licenza	
Licenze nel file di licenza	Trasferimento delle licenze in un nuovo file di licenza

26.1.1 Upgrade del software da OpenScape Business X V2 a OpenScape Business X V3

Durante l'upgrade del software di un modello OpenScape Business X dalla versione software V2 alla versione V3, viene sostituito solo il software del sistema; la scheda madre V2 ed eventuali UC Booster Card o UC Booster Server sono conservati. Le licenze esistenti e la configurazione del cliente sono mantenute. Il supporto software esistente rimarrà immutato dopo la migrazione.

Prima dell'upgrade software dalla versione V2 alla versione V3, se non esiste già, occorre configurare un accesso permanente al server delle licenze Unify (tramite Internet) nel sistema ed attivare la funzione **CLS Connect**. Ciò semplifica il trasferimento della licenza e accelera notevolmente la migrazione.

Premessa

Per l'upgrade del software e il trasferimento della configurazione del cliente esistente, il sistema deve funzionare con l'ultima versione software V2R7 prima dell'upgrade. Se necessario, aggiornare il sistema con l'ultima versione software. A tale scopo, il sistema deve avere uno stato di supporto software valido.

Per l'upgrade del software del sistema da V2 a V3, a seconda che la funzione CLS Connect venga utilizzata o no, sono richiesti i seguenti elementi:

- Licenza di migrazione SW OpenScape Business V3 (se non è utilizzata la funzione **CLS Connect**)

Limiti funzionali e restrizioni

Durante la migrazione, le licenze esistenti possono essere integralmente trasferite dalla scheda madre V2 esistente alla scheda madre V3. Il trasferimento della licenza senza attivare la funzione CLS Connect richiede la licenza di «upgrade SW» e una procedura molto più complessa, con un conseguente dispendio di tempo rispetto all'uso della funzione CLS Connect.

La configurazione del cliente e i dati del cliente sono trasferiti automaticamente dalla versione software V2 a V3 durante la procedura di upgrade.

I principali passaggi tecnici dell'upgrade del software sono descritti nei seguenti capitoli. Per il mantenimento delle licenze esistenti è effettuata una distinzione tra:

- Upgrade software per una licenza permanente con e senza CLS Connect
- Upgrade software con licenza PayGo

26.1.1.1 Upgrade software di sistemi con licenza permanente con CLS Connect

Eseguire i seguenti passaggi nell'ordine indicato.

Passo a passo

1) Preparare il sistema OpenScape Business
   a) Aggiornare il sistema esistente con la versione software V2R7.
   b) Impostare l'accesso al server delle licenze centrale (CLS) Unify nel sistema e testare la connessione
   c) Attivare **CLS Connect** nel sistema

2) Eseguire l'upgrade software.
   a) Eseguire l'upgrade a V3 con l'OpenScape Business Assistant.
   b) La configurazione del sistema è trasferita automaticamente a V3.
   c) Le licenze esistenti sono recuperate nella V3.

3) Generazione automatica del file di licenza da parte del CLS.
   Dopo il riavvio del sistema, il sistema indica al CLS che le licenze esistenti funzionano con la versione software V3.

26.1.1.2 Upgrade software di sistemi con licenza permanente senza CLS Connect

Eseguire i seguenti passaggi nell'ordine indicato.

Passo a passo

1) Preparare il sistema OpenScape Business.
   a) Aggiornare il sistema esistente con la versione software V2R7.

2) Creare un file di licenza di upgrade per il sistema V2 a livello del server delle licenze centrale (CLS)
   a) Attivare la licenza di upgrade SW per il sistema esistente.
   b) Generare un nuovo file di licenza per l'indirizzo MAC della scheda madre V2
   c) Scaricare il file di licenza dal CLS

3) Importare e attivare il file di licenza nel sistema OpenScape Business V2.

4) Eseguire l'upgrade software.
   a) Eseguire l'upgrade a V3 con l'OpenScape Business Assistant.
   b) La configurazione del sistema è trasferita automaticamente a V3.
   c) Le licenze esistenti nel sistema sono trasferite a V3

5) Riavviare il sistema dopo l'upgrade del software.

26.1.1.3 Upgrade software dei sistemi con licenza PayGo

Eseguire i seguenti passaggi nell'ordine indicato.

Passo a passo

1) Preparare il sistema OpenScape Business
   a) Aggiornare il sistema esistente con la versione software V2R7.

2) Rigenerare il file di licenza sul server delle licenze centrale (CLS)
   a) Rigenerare un nuovo file di licenza per l'indirizzo MAC della scheda madre V2.
   b) Scaricare il file di licenza dal CLS.
3) Importare e attivare il nuovo file di licenza nel sistema OpenScape Business V2.
4) Upgrade del software di OpenScape Business S
   a) Eseguire l'upgrade a V3 con l'OpenScape Business Assistant.
   b) La configurazione del sistema è trasferita automaticamente a V3.
   c) Il sistema è operativo dopo il riavvio.

26.2 Upgrade software da un UC Booster Server a OpenScape Business X V3

L'upgrade software da un UC Booster Server V2 alla versione V3 può essere eseguito in un solo passaggio.

L'upgrade software da un UC Booster Server V1 alla versione V3 deve essere eseguito in due passaggi. Prima eseguire l'upgrade da V1 a V2R7, poi da V2R7 a V3.

26.2.1 Come eseguire l'aggiornamento di UC Business Booster Server da V2 a V3

L'aggiornamento SW di UC Booster Server da V2 a V3 è necessario solo per i sistemi OpenScape Business X con scheda madre V2. I sistemi OpenScape Business X con scheda madre V3 non necessitano più di un UC Booster Server. In questo caso è necessaria la versione V2.7 del SW sull'UC Booster Server per migrare la configurazione e le licenze del cliente sulla scheda madre V3.

Prerequisiti

- Se necessario, controllare e aggiornare il sistema operativo Linux (vedere la *Nota tecnica di rilascio del software del sistema OpenScape Business V3*)
- UC Booster Server funziona con l'ultima versione SW V2R7 rilasciata prima dell'aggiornamento. Se necessario, aggiornare il sistema alla versione SW più recente.
- Aggiornare prima il sistema OpenScape Business X a cui è collegato l'UC Booster Server alla versione SW V3, comprese le licenze, come descritto in Upgrade del software da OpenScape Business X V2 a OpenScape Business X V3 alla pagina 1372
- Immagine SW dell'UC Booster Server V3

Prima di aggiornare il SW di UC Booster Server, determinare la configurazione del sistema e i componenti HW/SW e di licenza che potrebbero dover essere sostituiti.

Tabella 32: Migrazione di OpenScape Business S - Lista di controllo HW/SW

Componenti	Sostituito da
Componenti hardware	
PC Server	È possibile il riutilizzo. I requisiti HW devono essere verificati per le estensioni di OpenScape Business S[9]
Componenti software	
Sistema operativo SLES 12 o SLES 15	È possibile il riutilizzo. Infine è necessario un aggiornamento all'ultimo service pack[10]
XMPP	Nessuna soluzione di follow-up
myPortal Smart	myPortal @work
Componenti su licenza	
Licenze nel file di licenza (fa parte del file di licenza di OpenScape Business X)	Trasferimento delle licenze in un nuovo file di licenza
Applicazione CSTA (tramite scheda UC Booster/server)	Licenza CSTA per la connessione delle soluzioni esterne (non richiesta per UC Suite, TAPI 170 e TAPI 120)

Di seguito viene descritto l'aggiornamento del SW di OpenScape Business mantenendo il sistema operativo SLES.

Passo a passo

1) Eseguire l'aggiornamento del sistema OpenScape Business X alla versione V3.

Per i dettagli, vedere Upgrade del software da OpenScape Business X V2 a OpenScape Business X V3 alla pagina 1372.

2) Aggiornamento del SW di UC Booster Server alla V3

Per aggiornare il SW V2R7 alla versione V3, utilizzare la funzione di aggiornamento all'interno di OpenScape Business Assistant di UC Booster

9 L'HW del PC server esistente può essere utilizzato se la configurazione del sistema UC Booster Server rimarrà invariata dopo l'aggiornamento del SW. Se dopo l'aggiornamento del SW sono previste espansioni, potrebbe essere necessario adattare i requisiti hardware in base alle specifiche riportate nella *Guida all'installazione di OpenScape Business S, capitolo Prerequisiti*.

10 Il sistema operativo SLES installato sul PC server può essere adottato in caso di aggiornamento del SW di UC Booster Server. Tuttavia, deve essere aggiornato all'ultimo service pack rilasciato prima dell'aggiornamento del SW.

Se Novell ha interrotto il supporto SW per la versione SLES utilizzata, il cliente deve essere informato e, se necessario, deve essere commercializzato un aggiornamento SLES.

L'aggiornamento SLES potrebbe dover essere eseguito in più fasi per rilevare le installazioni OpenScape Business S esistenti, compresa la configurazione e i dati del cliente. Una chiave di aggiornamento SLES esistente rimane valida con un aggiornamento SLES. Tuttavia, prima dell'aggiornamento SLES, potrebbe essere necessario disattivare la registrazione presso Novell e quindi registrarla nuovamente per il nuovo sistema.

Server (vedere Aggiornamento del sistema di comunicazione alla pagina 1249).

3) Dopo l'aggiornamento del SW, eseguire un backup dei dati

   Eseguire il backup dei dati della versione V3 (vedere Salvataggio immediato alla pagina 1243)

26.3 Migrazione hardware/software dei sistemi OpenScape Business X a V3

Durante la migrazione dei sistemi OpenScape Business X, sono modificati sia i componenti HW, SW che su licenza.

Prima della migrazione di un sistema Business X, devono essere determinati la configurazione di sistema corrente, l'HW/SW, nonché i componenti su licenza da sostituire.

Nota: La scheda OCCLA con il sistema V3 può arrivare a 60 (+16) canali MEB. La migrazione alla nuova scheda consiste nel ripristino della configurazione OCC esistente. Se si desidera sfruttare i canali MEB aggiuntivi, è necessario riconfigurare il sistema utilizzando le apposite procedure guidate/ pagine WBM.

I moduli presenti nello slot 10 dei sistemi a parete OpenScape Business X5 non possono essere utilizzati con le schede madri V3. Questi moduli devono essere sostituiti da moduli/soluzioni successive.

Tabella 33: Migrazione di OpenScape Business X - Checklist HW/SW

Componente	Sostituito da
Componenti hardware	
«Scheda madre V2» esistente	Scheda madre V3 (di base o avanzata, secondo la configurazione)
UC Booster card / server (con UC Suite)	M.2 SSD supplementare
Modulo CMA	Modulo CMAe
Modulo EXMR per i dispositivi di annuncio esterni	Scheda madre V3 (audio in jack sul pannello frontale)
Interfacce S0 sulla scheda madre V2	Terminale S0 della scheda periferica S0
Schede X5W per slot 10 • SLCN16 • SLA16N • SLA24N	Sostituito da: • Connessione diretta cordless • SLAV16 • SLAV16 + SLAV8
500 telefoni Optipoint	Telefoni OpenScape Deskphone CP
400 telefoni Optipoint	
Componenti software	

Componente	Sostituito da
Software di sistema V2 su scheda SDHC	Software di sistema V3 (immagine a partire dal server di download del software)
VPN su WAN nel sistema terminato	VPN nel router esterno terminato
XMPP	Nessuna soluzione di follow-up
myPortal Smart	myPortal @work
Componenti su licenza	
Licenze nel file di licenza	Trasferimento delle licenze in un nuovo file di licenza
Applicazioni CSTA esterne (finora senza licenza, perché collegate alla scheda UC Booster / Server HW)	Licenza CSTA separata per la connessione delle soluzioni esterne (non richiesta per UC Suite, TAPI 170 e TAPI 120)

26.3.1 Migrazione da OpenScape Business X V2 a OpenScape Business X V3

Quando si esegue la migrazione di un modello OpenScape Business X dalla versione V2 alla versione V3, vengono sostituiti la scheda madre e il software di sistema. Le licenze esistenti e la configurazione del cliente possono essere trasferite. Il supporto software esistente continuerà senza modifiche dopo la migrazione.

Prima della migrazione, se non già esistente, configurare un accesso permanente al server licenze Unify (tramite Internet) nel sistema e attivare la funzione "CLS Connect". Ciò semplifica il trasferimento della licenza e riduce notevolmente i tempi di migrazione. Il cliente deve essere informato dell'accesso richiesto dal sistema OpenScape Business al CLS.

Premessa

Il sistema funziona con l'ultima versione SW rilasciata V2R7 prima dell'aggiornamento. Se necessario, aggiornare il sistema alla versione SW più recente. A tal fine, il sistema deve avere uno stato di supporto software valido.

Per la migrazione dalla V2 alla V3, a seconda che si utilizzino CLS Connect, UC Suite o applicazioni CSTA esterne, sono necessari i seguenti elementi:

- Scheda madre V3
- V3 SW su SSD M.2 SATA per l'archiviazione dei dati
- Stoccaggio dati in massa M.2 SSD 256 GB (facoltativo con l'applicazione UC Suite)
- Licenza di migrazione hardware OpenScape Business V3 (se non si utilizza CLS Connect)
- Licenza OpenScape Business CSTA (facoltativa)

Limiti funzionali e restrizioni

Le licenze esistenti possono essere trasferite completamente dalla scheda madre V2 esistente alla scheda madre V3 durante la migrazione. Il trasferimento della licenza senza attivare la funzione CLS Connect richiede

la licenza "Migrazione hardware" e una gestione molto più complessa e dispendiosa in termini di tempo rispetto all'utilizzo della funzione CLS Connect.

La configurazione e i dati del cliente vengono migrati dalla versione SW V2 alla versione V3 tramite un processo di backup/ripristino.

Le principali fasi tecniche della migrazione sono descritte nei seguenti argomenti. Al fine di mantenere le licenze esistenti, viene fatta una distinzione in merito alla gestione tra:

- Aggiornamento SW per licenza permanente con e senza CLS Connect
- Aggiornamento SW con licenza PayGo

Nota: Durante la migrazione dalla scheda madre V2 alla scheda madre V3, le porte EVM aggiuntive non vengono incluse nel gruppo di ricerca SmartVM. Ciò richiede una configurazione manuale, nel corso della quale dovrebbe essere applicata anche la restrizione COS.

Nota: Quando si esegue una migrazione hardware da un hardware V2 configurato con un indirizzo IP DSP non predefinito a un sistema hardware V3, l'indirizzo IP DSP verrà reimpostato al valore predefinito. Dopo la migrazione, l'amministratore deve riconfigurare manualmente l'indirizzo IP DSP e anche l'indirizzo IP FPGA in base alle esigenze specifiche del cliente.

26.3.1.1 Migrazione ai sistemi su licenza permanente V3 con CLS Connect

Per la migrazione, eseguire i seguenti passaggi nell'ordine indicato.

Passo a passo

1) Preparare il sistema OpenScape Business
   a) Aggiornare il sistema esistente con la versione software V2R7
   b) Impostare l'accesso al server delle licenze centrale (CLS) nel sistema e testare la connessione
   c) Attivare CLS Connect nel sistema

2) Generare il file di licenza sul server delle licenze centrale (CLS)
   a) Trasferire le licenze esistenti dall'indirizzo MAC della scheda madre V2 all'indirizzo MAC della scheda madre V3 con la funzione **Rigenera**
   b) Generare un nuovo file di licenza per l'indirizzo MAC della scheda madre V3

3) Eseguire il backup della configurazione del sistema V2 e dei dati del cliente.

4) Sostituire le schede madre
   a) Spegnere il sistema e tutti gli alimentatori
   b) Utilizzare un supporto dati V3 e se necessario uno stoccaggio dati di massa opzionale sulla scheda madre V3
   c) Rimuovere la scheda OCCB Voice Channel Booster dalla scheda madre V2 e inserirla nella scheda madre V3.
   d) Sostituire la scheda madre V2 con la scheda madre V3 nel sistema
   e) Alimentare di nuovo il sistema.

      Il sistema si avvia automaticamente.

5) Impostare i parametri di sistema di base con WBM dopo l'avvio
   a) Impostare la data e l'ora
   b) Impostare il pacchetto applicativo

      UC Smart per i sistemi senza UC o con UC Smart

      UC Suite per i sistemi con UC Suite
6) Ripristinare la configurazione del sistema
   a) Ripristinare il backup con la funzione di ripristino
   b) Importare il file di licenza appena creato

26.3.1.2 Migrazione ai sistemi su licenza permanente V3 senza CLS Connect

Per la migrazione, eseguire i seguenti passaggi nell'ordine indicato.

Passo a passo

1) Preparare il sistema OpenScape Business
   a) Aggiornare il sistema esistente con la versione software V2R7
2) Creare un file di licenza per la migrazione per il sistema V2 esistente a livello del server delle licenze centrale (CLS)
   a) Attivare la licenza di migrazione HW per il sistema esistente
   b) Generare un nuovo file di licenza per l'indirizzo MAC della scheda madre V2.

      A tale scopo, acquisire l'indirizzo MAC della scheda madre V3.
   c) Scaricare il file di licenza dal CLS
3) Importare il file di licenza nel sistema OpenScape Business V2.
4) Prendere nota del **Codice di conferma** visualizzato nell'OpenScape Business Assistant
5) Generare un nuovo file di licenza per la scheda madre V3 a livello del server delle licenze centrale (CLS)
   a) Creare un nuovo file di licenza per l'indirizzo MAC della scheda madre V3 sul CLS rigenerando l'indirizzo MAC della scheda madre V2 e il codice di conferma annotato in precedenza
   b) Cercare il sistema OpenScape Business con l'indirizzo MAC della scheda madre V3 nel CLS.
   c) Sbloccare il sistema OpenScape Business acquisendo e attivando il codice di conferma
   d) Rigenerare il file di licenza
   e) Scaricare il file di licenza appena generato dal CLS
6) Eseguire il backup della configurazione del sistema V2 e dei dati del cliente.

7) Sostituire le schede madre

a) Spegnere il sistema e tutti gli alimentatori

a) Utilizzare un supporto dati V3 e se necessario uno stoccaggio dati di massa opzionale sulla scheda madre V3

b) Rimuovere la scheda OCCB Voice Channel Booster dalla scheda madre V2 e inserirla nella scheda madre V3.

c) Sostituire la scheda madre V2 con la scheda madre V3 nel sistema

b) Alimentare di nuovo il sistema.

Il sistema si avvia automaticamente.

8) Impostare i parametri di sistema di base con WBM dopo l'avvio

a) Impostare la data e l'ora

b) Impostare il pacchetto applicativo

UC Smart per i sistemi senza UC o con UC Smart

UC Suite per i sistemi con UC Suite

9) Ripristinare la configurazione del sistema

a) Ripristinare il backup con la funzione di ripristino

10) Importare manualmente il nuovo file di licenza nel sistema V3 dopo l'avvio del sistema

26.3.1.3 Migrazione ai sistemi su licenza PayGo V3

Per la migrazione, eseguire i seguenti passaggi nell'ordine indicato.

Passo a passo

1) Preparare il sistema OpenScape Business

a) Aggiornare il sistema esistente con la versione software V2R7

2) Eseguire il backup della configurazione del sistema V2 e dei dati del cliente.

3) Rigenerare il file di licenza sul server delle licenze centrale (CLS)

a) Rigenerare un nuovo file di licenza per l'indirizzo MAC della scheda madre V3

Trasferire le licenze esistenti dall'indirizzo MAC della scheda madre V2 all'indirizzo MAC della scheda madre V3.

b) Scaricare il nuovo file di licenza dal CLS

4) Sostituire le schede madre

a) Spegnere il sistema e tutti gli alimentatori

b) Utilizzare un supporto dati V3 e se necessario uno stoccaggio dati di massa opzionale sulla scheda madre V3

c) Rimuovere la scheda OCCB Voice Channel Booster dalla scheda madre V2 e inserirla nella scheda madre V3.

d) Sostituire la scheda madre V2 con la scheda madre V3 nel sistema

e) Alimentare di nuovo il sistema.

Il sistema si avvia automaticamente.

5) Impostare i parametri di sistema di base con WBM dopo l'avvio
   a) Impostare la data e l'ora
   b) Impostare il pacchetto applicativo

      UC Smart per i sistemi senza UC o con UC Smart

      UC Suite per i sistemi con UC Suite
6) Ripristinare la configurazione del sistema
   a) Ripristinare il backup con la funzione di ripristino
7) Importare manualmente il nuovo file di licenza nel sistema V3 e attivare il file di licenza

26.4 Migrazione di un sistema OpenScape Business X V3 da una scheda madre V2 a una scheda madre V3

In questo caso, la scheda madre V2 esistente del sistema OpenScape Business e qualsiasi hardware UC Booster presente sono sostituiti con una scheda madre V3. Precedentemente, il sistema è stato aggiornato con la versione software V3, ad esempio, nel corso della manutenzione del software.

Le licenze esistenti e la configurazione del cliente possono essere trasferite. Il supporto di manutenzione software esistente rimarrà immutato dopo la migrazione.

Non sono più necessari un'eventuale UC Booster Card o un UC Booster Server in connessione con la scheda madre V3. A tale scopo, è utilizzato uno stoccaggio dati di massa supplementare sulla scheda madre V3.

In Tabella 33: Migrazione di OpenScape Business X - Checklist HW/SW alla pagina 1376 sono disponibili informazioni sui componenti sostituiti con la scheda madre V3 o interrotti senza sostituzione. È richiesta un licenza CSTA per una connessione esistente di applicazioni CSTA esterne. Questo requisito non è applicabile alla connessione di OpenScape TAPI 170 o TAPI 120.

Premessa

Il sistema funziona con l'ultima versione software V2R7 prima dell'upgrade. Se necessario, aggiornare il sistema con l'ultima versione software. A tale scopo, il sistema deve avere uno stato di supporto software valido.

Per la migrazione, secondo che le applicazioni CLS Connect, UC Suite o CSTA esterna siano utilizzate, sono richiesti i seguenti componenti:

- Scheda madre V3
- Software V3 su stoccaggio dati M.2 SATA SSD
- Stoccaggio dati in massa M2 SSD 256 GB (facoltativo con l'applicazione UC Suite)
- Licenza di migrazione HW OpenScape Business V3 (facoltativa)
- Licenza OpenScape Business CSTA (facoltativa)

Limiti funzionali e restrizioni

Durante la migrazione, le licenze esistenti possono essere integralmente trasferite dalla scheda madre V2 esistente alla scheda madre V3. Il trasferimento della licenza senza attivare la funzione CLS Connect richiede la licenza di migrazione HW e una procedura molto più complessa, con un conseguente dispendio di tempo rispetto all'uso della funzione CLS Connect.

La configurazione del cliente e i dati del cliente sono trasferiti attraverso una procedura di backup / ripristino.

Le principali tappe tecniche della migrazione sono descritte nei seguenti capitoli. Per ricordare le licenze esistenti è effettuata una distinzione tra:

- Upgrade software per una licenza permanente con e senza CLS Connect
- Upgrade software con licenza PayGo

Nota: Durante la migrazione dalla scheda madre V2 alla scheda madre V3, le porte EVM aggiuntive non sono incluse nel gruppo di ricerca SmartVM. Ciò richiede una configurazione manuale, nel corso della quale dovrebbe essere effettuata anche la restrizione COS.

La conversione di un KDS nella stessa versione software in un diverso tipo di sistema non è supportata da Manager E. Se si desidera utilizzare solo i dati KDS, è possibile provare i seguenti passaggi:

- Eseguire una migrazione completa del sistema dalla scheda madre V2 alla scheda madre V3.
- Scaricare il sistema di scheda madre V3 KDS con Manager E e memorizzalo localmente.
- Ricaricare il sistema della scheda madre V3.
- Caricare il sistema di scheda madre V3 precedentemente memorizzato KDS nel tuo sistema di scheda madre V3.

Il sistema della scheda madre V3 utilizzerà la configurazione del database KDS ed è possibile continuare con la configurazione UC manuale.

Nota: La migrazione del sistema della scheda madre V2 KDS al sistema della scheda madre V3 non è supportata, in quanto il database della scheda madre V2 non è compatibile con il database della scheda madre V3.

26.4.1 Migrazione ai sistemi su licenza permanente con scheda madre V3 con CLS Connect

Per la migrazione, eseguire i seguenti passaggi nell'ordine indicato.

Passo a passo

1) Preparare il sistema OpenScape Business
   a) Impostare l'accesso al server delle licenze centrale (CLS) nel sistema e testare la connessione
   b) Attivare CLS Connect nel sistema

2) Generare il file di licenza sul server delle licenze centrale (CLS)
   a) Trasferire le licenze esistenti dall'indirizzo MAC della scheda madre V2 all'indirizzo MAC della scheda madre V3 con la funzione **Rigenera**
   b) Generare un nuovo file di licenza per l'indirizzo MAC della scheda madre V3

3) Eseguire il backup della configurazione del sistema V3 e dei dati del cliente.

4) Creare un backup della configurazione del Booster Server se necessario.
5) Sostituire le schede madre
   a) Spegnere il sistema e tutte le alimentazioni
   b) Utilizzare un supporto dati V3 e se necessario uno stoccaggio dati di massa opzionale sulla scheda madre V3
   c) Rimuovere la scheda OCCB Voice Channel Booster dalla scheda madre V2 e inserirla nella scheda madre V3.
   d) Sostituire la scheda madre V2 con la scheda madre V3 nel sistema
   e) Alimentare di nuovo il sistema.

      Il sistema si avvia automaticamente.
6) Impostare i parametri di sistema di base con WBM dopo l'avvio
   a) Impostare la data e l'ora
   b) Impostare il pacchetto applicativo

      UC Smart per i sistemi senza UC o con UC Smart

      UC Suite per i sistemi con UC Suite
7) Ripristinare la configurazione del sistema
   a) Importare il file di licenza appena creato
   b) Ripristinare il backup del sistema e se necessario il backup del Booster Server con la funzione di ripristino

26.4.2 Migrazione ai sistemi su licenza permanente con scheda madre V3 senza CLS Connect

Per la migrazione, eseguire i seguenti passaggi nell'ordine indicato.

Passo a passo

1) Creare un file di licenza per la migrazione per la scheda madre V2 esistente a livello del server delle licenze centrale (CLS)
   a) Attivare la licenza di migrazione HW per il sistema esistente
   b) Generare un nuovo file di licenza per l'indirizzo MAC della scheda madre V2

      A tale scopo, deve essere acquisito l'indirizzo MAC della scheda madre V3.
   c) Scaricare il file di licenza dal CLS
2) Importare il file di licenza nel sistema OpenScape Business con la scheda madre V2.
3) Prendere nota del **Codice di conferma** visualizzato nell'OpenScape Business Assistant

4) Generare un nuovo file di licenza per la scheda madre V3 a livello del server delle licenze centrale (CLS)
   a) Creare un nuovo file di licenza per l'indirizzo MAC della scheda madre V3 sul CLS rigenerando l'indirizzo MAC della scheda madre V2 e il codice di conferma annotato in precedenza.
      a) Cercare il sistema OpenScape Business con l'indirizzo MAC della scheda madre V3 nel CLS.
      b) Sbloccare il sistema OpenScape Business acquisendo e attivando il codice di conferma
      c) Rigenerare il file di licenza
   b) Scaricare il file di licenza appena generato dal CLS.
5) Eseguire il backup della configurazione del sistema e dei dati del cliente.
6) Sostituire le schede madre
   a) Spegnere il sistema e tutti gli alimentatori
   b) Utilizzare un supporto dati V3 e se necessario uno stoccaggio dati di massa opzionale sulla scheda madre V3
   c) Rimuovere la scheda OCCB Voice Channel Booster dalla scheda madre V2 e inserirla nella scheda madre V3.
   d) Sostituire la scheda madre V2 con la scheda madre V3 nel sistema
   e) Alimentare di nuovo il sistema.

      Il sistema si avvia automaticamente.
7) Impostare i parametri di sistema di base con WBM dopo l'avvio
   a) Impostare la data e l'ora
   b) Impostare il pacchetto applicativo

      UC Smart per i sistemi senza UC o con UC Smart

      UC Suite per i sistemi con UC Suite
8) Ripristinare la configurazione del sistema dopo l'avvio
   a) Ripristinare il backup con la funzione di ripristino
9) Importare manualmente il nuovo file di licenza nel sistema V3 dopo l'avvio del sistema.

26.4.3 Migrazione ai sistemi su licenza PayGo con scheda madre V3

Per la migrazione, eseguire i seguenti passaggi nell'ordine indicato.

Passo a passo

1) Eseguire il backup della configurazione del sistema e dei dati del cliente.
2) Rigenerare il file di licenza sul server delle licenze centrale (CLS)
   a) Rigenerare un nuovo file di licenza per l'indirizzo MAC della scheda madre V3

      Trasferire le licenze esistenti dall'indirizzo MAC della scheda madre V2 all'indirizzo MAC della scheda madre V3.
   b) Scaricare il nuovo file di licenza dal CLS

3) Sostituire le schede madre
   a) Spegnere il sistema e tutti gli alimentatori
   b) Utilizzare un supporto dati V3 e se necessario uno stoccaggio dati di massa opzionale sulla scheda madre V3
   c) Rimuovere la scheda OCCB Voice Channel Booster dalla scheda madre V2 e inserirla nella scheda madre V3.
   d) Sostituire la scheda madre V2 con la scheda madre V3 nel sistema
   e) Alimentare di nuovo il sistema.

      Il sistema si avvia automaticamente.

4) Impostare i parametri di sistema di base con WBM dopo l'avvio
   a) Impostare la data e l'ora
   b) Impostare il pacchetto applicativo

      UC Smart per i sistemi senza UC o con UC Smart

      UC Suite per i sistemi con UC Suite

5) Ripristinare la configurazione del sistema dopo l'avvio
   a) Ripristinare il backup con la funzione di ripristino

6) Importare manualmente il nuovo file di licenza nel sistema V3 e attivare il file di licenza

26.5 Upgrade del software di OpenScape Business S

Prima di effettuare l'upgrade software di un sistema OpenScape Business S, occorre determinare la configurazione di sistema corrente e i componenti HW/SW e su licenza che devono essere eventualmente sostituiti.

Tabella 34: Migrazione di OpenScape Business S - Checklist HW/SW

Componenti	Sostituito da
Componenti hardware	
PC Server	È possibile riutilizzarlo. Devono essere verificati i requisiti hardware per le estensioni di OpenScape Business S.[11]
400 telefoni Optipoint	Telefoni OpenScape Deskphone CP
Componenti software	

[11] L'hardware del PC server esistente può essere utilizzato se la configurazione dell'UC Booster Server è immutata dopo l'upgrade software. Se sono pianificate espansioni dopo l'upgrade software, i requisiti hardware devono essere eventualmente adattati secondo le specifiche riportate in *Guida all'installazione di OpenScape Business S, capitolo Prerequisiti*.

Componenti	Sostituito da
Sistema operativo SLES12	È possibile riutilizzarlo. È eventualmente richiesto l'upgrade all'ultimo pacchetto di servizi[12]
Software di sistema V2 su scheda SDHC	Software di sistema V3 (immagine a partire dal server di download del software)
XMPP	Nessuna soluzione di follow-up
myPortal Smart	myPortal @work
Componenti su licenza	
Licenze nel file di licenza	Trasferimento delle licenze in un nuovo file di licenza
Applicazione CSTA (tramite UC Booster card / server)	Applicazione CSTA (tramite UC Booster card / server)

26.5.1 Upgrade del software da OpenScape Business S V2 a OpenScape Business S V3

Quando si esegue l'upgrade di un modello OpenScape Business S dalla versione software V2 a V3, è sostituito solo il software del sistema.

Le licenze esistenti e la configurazione del cliente sono recuperate. Il supporto software esistente rimarrà immutato dopo la migrazione.

In questo caso, non è richiesto ordinare componenti separati per l'upgrade software del sistema da V2 a V3.

La versione software V3 non supporta più alcune funzioni e componenti hardware. In Tabella 34: Migrazione di OpenScape Business S - Checklist HW/SW alla pagina 1385 sono disponibili informazioni sui componenti sostituiti nella versione V3 o interrotti senza sostituzione. Ciò dipende dall'espansione del sistema del cliente.

Premessa

Il sistema funziona con l'ultima versione software V2R7 prima dell'upgrade. Se necessario, aggiornare il sistema con l'ultima versione software. A tale scopo, il sistema deve avere uno stato di supporto software valido.

12 Il sistema operativo SLES installato sul PC server può essere adottato in caso di upgrade software di un sistema OpenScape Business S / UC Booster Server. Tuttavia, deve essere aggiornato all'ultimo pacchetto di servizi prima dell'upgrade software.

Se Novell ha sospeso il supporto software per la versione SLES utilizzata, informare il cliente e se necessario eseguire un upgrade SLES.

L'upgrade SLES deve essere eseguito in diversi passaggi per recuperare le installazioni esistenti di OpenScape Business S, compresa la configurazione e i dati del cliente. Una chiave di aggiornamento SLES esistente rimane valida con un upgrade SLES. Tuttavia, occorre annullare la registrazione presso Novell prima dell'upgrade SLES e poi registrarla di nuovo per il nuovo sistema.

Di seguito è descritto l'upgrade software di OpenScape Business conservando il sistema operativo SLES.

Prima dell'upgrade software dalla versione V2 alla versione V3, configurare un accesso permanente al server delle licenze Unify (tramite Internet) nel sistema ed attivare la funzione **CLS Connect**.

Limiti funzionali e restrizioni

Le licenze esistenti possono essere recuperate nel corso dell'upgrade software solo se è attivata la funzione CLS Connect.

La configurazione del cliente e i dati del cliente sono trasferiti automaticamente dalla versione software V2 a V3 durante la procedura di upgrade.

I principali passaggi tecnici della migrazione sono descritti nei seguenti capitoli. Per il mantenimento delle licenze esistenti è effettuata una distinzione tra:

- Upgrade software per una licenza permanente con e senza CLS Connect
- Upgrade software con licenza PayGo

Gestione tecnica dell'upgrade

I principali passaggi tecnici della migrazione sono descritti di seguito. Viene fatta distinzione tra:

- Upgrade per una licenza permanente con CLS Connect
- Upgrade con licenza PayGo

26.5.1.1 Upgrade a V3 ai sistemi su licenza permanente con CLS Connect

Per la migrazione, eseguire i seguenti passaggi.

Passo a passo

1) Preparare il sistema OpenScape Business V2
   a) Aggiornare il sistema esistente con la versione software V2R7
   b) Impostare l'accesso al server delle licenze centrale (CLS) nel sistema e testare la connessione
   c) Attivare CLS Connect nel sistema V2

2) Preparare il sistema operativo SLES

   Eseguire l'upgrade del sistema operativo con l'ultimo pacchetto di servizi della versione SLES utilizzata con OpenScape Business S.

3) Upgrade del software di OpenScape Business
   a) Eseguire l'upgrade a V3 con l'OpenScape Business Assistant.
   b) La configurazione del sistema è trasferita automaticamente a V3.
   c) Le licenze esistenti sono trasferite a V3.

4) Il file di licenza è generato automaticamente dal CLS.
   a) Dopo il riavvio del sistema, il sistema indica al CLS che le licenze esistenti funzionano con la versione software 3.
   b) Il server delle licenze genera automaticamente un nuovo file di licenza con l'informazione V3 e lo trasferisce a sua volta al sistema.

26.5.1.2 Upgrade a V3 ai sistemi su licenza PayGo

Per la migrazione, eseguire i seguenti passaggi.

Passo a passo

1) Preparare il sistema OpenScape Business
   a) Aggiornare il sistema esistente con la versione software V2R7
2) Preparare il sistema operativo SLES
   Eseguire l'upgrade del sistema operativo con l'ultimo pacchetto di servizi della versione SLES utilizzata con OpenScape Business S.
3) Rigenerare il file di licenza sul server delle licenze centrale (CLS)
   a) Rigenerare un nuovo file di licenza per il sistema V2.
   b) Scaricare il nuovo file di licenza dal CLS
4) Importare e attivare il nuovo file di licenza nel sistema OpenScape Business V2.
5) Upgrade del software di OpenScape Business
   a) Eseguire l'upgrade a V3 con l'OpenScape Business Assistant.
   b) La configurazione del sistema è trasferita automaticamente a V3.
   c) Il sistema è operativo dopo il riavvio.

26.5.2 Upgrade del software da OpenScape Business S V2 a OpenScape Business S V3

Eseguire i seguenti passaggi richiesti per la migrazione di un sistema OpenScape Business S V1 a OpenScape Business S V2.

Premessa

Prima della migrazione occorre verificare se le caratteristiche hardware e software del server Linux sono adeguate per OpenScape Business S V2. Può essere sufficiente un upgrade del server Linux (ad esempio, RAM aggiuntiva). Il sistema operativo SLES 64 bit Linux rilasciato per OpenScape Business V2 è un prerequisito. Per il passaggio di upgrade alla versione software V3 di OpenScape Business, è necessaria la versione SLES 64 bit per V3.

Se è necessario un nuovo server Linux, dopo l'installazione di Linux occorre installare il software di comunicazione OpenScape Business V1 S. È quindi possibile trasferire un backup dei dati V1 e continuare con il passo 1 della migrazione.

Limiti funzionali e restrizioni

Quando il sistema viene aggiornato da OpenScape Business V1 a OpenScape Business V2, non è possibile attivare o disattivare alcun ITSP tramite la procedura guidata per la telefonia Internet prima di aver eseguito un reset a LCR. Gli ITSP già configurati in OpenScape Business V1 continueranno a funzionare anche in OpenScape Business V3, senza necessità di resettare l'LCR. È possibile modificare gli ITSP già attivati ma non disattivarli. Per modificare le attivazioni/disattivazioni nella procedura guidata, eseguire un reset dell'LCR. Questo serve a riprodurre le modifiche necessarie per l'aumento degli ITSP da 4 a 8. Per reimpostare l'LCR, andare a **Modalità esperti** > **LCR** > **Flag LCR** e fare clic sul flag **Reset dati LCR**.

Procedura di upgrade

Eseguire i seguenti passaggi nell'ordine indicato.

1) **Aggiornamento del software OpenScape Business V1**

   Utilizzando il WBM, aggiornare il software OpenScape Business V1 alla versione V1 R3.3 o successiva (vedere Aggiornamento del sistema di comunicazione alla pagina 1249).
2) **Caricare il file di licenza di OpenScape Business V2**

   Caricare il file di licenza OpenScape Business V2 nel sistema OpenScape Business V1 e attivare le licenze (vedere Attivazione licenza (sistema indipendente) alla pagina 308).

   Può essere utilizzata la licenza per gli upgrade SLES gratuiti.
3) **Caricare il software corrente OS Biz V2**

   Con l'aiuto del WBM, caricare il software OpenScape Business V2 corrente nel sistema di comunicazione. I dati V1 vengono convertiti automaticamente in dati V3 durante la procedura (vedere Aggiornamento del sistema di comunicazione alla pagina 1249).
4) **Esecuzione del backup dei dati**

   Eseguire il backup dei propri dati V2 (vedere Salvataggio immediato alla pagina 1243).

26.6 Migrazione/upgrade della rete OpenScape Business V2 a V3

Durante la migrazione o l'upgrade di una rete OpenScape Business a V3, tutti i nodi devono essere aggiornati con la versione software V3. Per le funzioni di rete, non è rilevante se la versione software V3 è operativa su un sistema OpenScape Business X nella rete con una scheda madre V2 o una scheda madre V3.

Aggiornare ogni nodo di OpenScape Business della rete separatamente. I componenti richiesti per l'upgrade devono essere determinati per nodo secondo i sistemi individuali in conformità alle descrizioni fornite nei capitoli Upgrade software dei sistemi OpenScape Business X alla pagina 1371, Upgrade software da un UC Booster Server a OpenScape Business X V3 alla pagina 1374, Migrazione hardware/software dei sistemi OpenScape Business X a V3 alla pagina 1376 o Migrazione di un sistema OpenScape Business X V3 da una scheda madre V2 a una scheda madre V3 alla pagina 1381.

Le licenze per i nodi della rete V2 possono essere trasferite ai sistemi V3 grazie al server delle licenze centrale. Esistono diverse procedure per i sistemi con o senza la funzione **CLS Connect**. La procedura di licenza «Pay as yo go» non è supportata nella rete OpenScape Business.

La procedura richiesta per il trasferimento delle licenze con la funzione **CLS Connect** è notevolmente ridotta rispetto a una rete senza la funzione CLS Connect.

Importante: Eseguire l'upgrade dei nodi in una rete secondo la sequenza descritta per ogni scenario. È essenziale che tutti i nodi slave siano operativi con la versione software V3 prima che il nodo master possa essere migrato o aggiornato alla versione software V3.

Nel corso dell'aggiornamento della rete si avrà una rete eterogenea con software V2 e V3 durante il periodo di transizione. Durante questo intervallo di tempo, non è garantita

la piena funzionalità delle prestazioni della rete. In alcuni casi, i sistemi aggiornati / migrati funzioneranno in modo emergenza fino a quando il file di licenza non sarà aggiornato dal nodo master.

Le reti OpenScape Business possono essere realizzate in diverse combinazioni rispetto all'uso dei sistemi OpenScape Business X e S e le licenze dei sistemi nella rete. Le tappe più importanti per la migrazione o l'upgrade di una rete OpenScape Business e la rispettiva sequenza sono mostrati attraverso combinazioni tipiche.

La descrizione considera sempre che esista un file di licenza di rete nel CLS per la rete, attraverso il quale il nodo master fornisce a tutti i nodi slave le informazioni sulla licenza.

- **Rete composta solo da sistemi OpenScape Business X**
  - Scenario 1: Migrazione hardware soltanto nel nodo master, upgrade software in tutti i nodi slave
  - Scenario 2: Upgrade software di tutti i nodi di OpenScape Business X presenti nella rete
- **Rete composta dai sistemi OpenScape Business S e OpenScape Business X**
  - Scenario 3: OpenScape Business S è il nodo master e i sistemi OpenScape Business X sono i nodi slave
    - Scenario 3a: Upgrade software di tutti i nodi di OpenScape Business presenti nella rete
    - Scenario 3b: Upgrade software nel nodo master OpenScape Business S e migrazione dei nodi slave

26.6.1 Scenario 1: Migrazione hardware di un nodo master, upgrade software dei nodi slave

Durante la migrazione della rete, occorre distinguere tra la funzione **CLS Connect** e la procedura di trasferimento della licenza.

26.6.1.1 Migrazione/Upgrade con CLS Connect nel nodo master

Prerequisiti

- Tutti i nodi della rete funzionano con l'ultima versione software V2R7.x.
- A livello del server delle licenze centrale (CLS) è presente un file di licenza di rete per il nodo master della rete.
- La funzione **CLS Connect** è attivata nel nodo master. CLS Connect non deve essere attivato sui nodi slave.

Passo a passo

1) Eseguire l'upgrade di tutti i nodi slave alla versione software V3 (per maggiori dettagli, vedere Upgrade software dei sistemi OpenScape Business

X alla pagina 1371 o Upgrade software da un UC Booster Server a OpenScape Business X V3 alla pagina 1374)

a) Importare il software V3 con l'OpenScape Business Assistant (WBM) e aggiornare il sistema.
b) Le informazioni sulla configurazione e la licenza sono mantenute.

Il sistema non è operativo dopo l'avvio a causa del file di licenza non valido.

2) Generare un nuovo file di licenza di rete sul server delle licenze.
   a) Rigenerare il file di licenza di rete per il nodo master all'indirizzo MAC della scheda madre V3
   b) Scaricare il nuovo file di licenza di rete dal CLS
3) Migrare il nodo master alla scheda madre V3 (per maggiori dettagli, vedere Migrazione hardware/software dei sistemi OpenScape Business X a V3 alla pagina 1376)
   a) Configurazione del sistema di backup con WBM
   b) Sostituire la scheda madre
   c) Impostare la data e l'ora e il pacchetto applicativo con WBM
   d) Importare ed attivare il nuovo file di licenza di rete con WBM.
   e) Ripristinare la configurazione del sistema con WBM

   In questo caso, il file di licenza non viene cancellato.
4) Il nodo master trasferisce automaticamente le nuove informazioni sulla licenza ai nodi slave.

Nota: La trasmissione delle licenze ai nodi slave può richiedere fino a 15 minuti.

26.6.1.2 Migrazione/Upgrade senza CLS Connect nel nodo master

Prerequisiti

- Tutti i nodi della rete funzionano con l'ultima versione software V2R7.x.
- A livello del server delle licenze centrale (CLS) è presente un file di licenza di rete per il nodo master della rete.
- È disponibile la licenza di migrazione hardware per il nodo master
- Sono disponibili le licenze di upgrade software per ogni nodo slave

Passo a passo

1) Generare un nuovo file di licenza di rete sul server delle licenze.
   a) Suddividere il file di rete a livello del CLS in file di licenza individuali
   b) Generare un file di licenza per il nodo master

      Attivare la licenza di migrazione hardware per il nodo master
   c) Generare il file di licenza per i nodi slave

      Attivare la licenza di upgrade del software per ogni nodo slave individuale
   d) Eseguire la fusione dei file di licenza dei singoli nodi in un nuovo file di licenza di rete
   e) Scaricare il nuovo file di licenza di rete dal CLS
2) Eseguire l'upgrade dei nodi slave alla versione V3 (per maggiori dettagli, vedere Upgrade software dei sistemi OpenScape Business X alla pagina

1371 o Upgrade software da un UC Booster Server a OpenScape Business X V3 alla pagina 1374)

a) Importare il software V3 con l'OpenScape Business Assistant (WBM) e aggiornare il sistema.
b) Le informazioni sulla configurazione e la licenza sono trasferite automaticamente.

Il sistema non è operativo dopo l'avvio a causa del file di licenza non valido.

3) Migrare il nodo master alla V3 (per maggiori dettagli, vedere Migrazione hardware/software dei sistemi OpenScape Business X a V3 alla pagina 1376)

a) Configurazione del sistema di backup con WBM
b) Accendere la scheda madre
c) Impostare la data e l'ora e il pacchetto applicativo con WBM
d) Importare ed attivare il nuovo file di licenza di rete con WBM.
e) Ripristinare la configurazione del sistema con WBM (il file di licenza non è cancellato in questo caso)

4) Il nodo master trasferisce automaticamente le nuove informazioni sulla licenza ai nodi slave.

Nota: La trasmissione delle licenze ai nodi slave può richiedere fino a 15 minuti.

26.6.2 Scenario 2: Upgrade software di tutti i sistemi nella rete a V3

Durante l'upgrade del software di rete, l'uso della funzione **CLS Connect** o no definisce la procedura da seguire per il trasferimento della licenza.

26.6.2.1 Upgrade software con CLS Connect nel nodo master

Prerequisiti

- Tutti i nodi della rete funzionano con l'ultima versione software V2R7.x.
- A livello del server delle licenze centrale (CLS) è presente un file di licenza di rete per il nodo master della rete.
- La funzione **CLS Connect** è attivata nel nodo master. CLS Connect non deve essere attivato sui nodi slave.

Passo a passo

1) Eseguire la migrazione di tutti i nodi slave alla versione software V3 (per maggiori dettagli, vedere Upgrade software dei sistemi OpenScape Business X alla pagina 1371 o Upgrade software da un UC Booster Server a OpenScape Business X V3 alla pagina 1374)

a) Importare il software V3 con l'OpenScape Business Assistant (WBM) e aggiornare il sistema.
b) Le informazioni sulla configurazione e la licenza sono mantenute.

Il sistema non è operativo dopo l'avvio a causa del file di licenza non valido.

2) Eseguire l'upgrade del nodo master alla versione V3 (per maggiori dettagli, vedere Upgrade software dei sistemi OpenScape Business X alla pagina

1371 o) Upgrade software da un UC Booster Server a OpenScape Business X V3 alla pagina 1374

a) Importare il software V3 con l'OpenScape Business Assistant (WBM) e aggiornare il sistema.
b) La configurazione e le informazioni sulla licenza sono conservate.
c) Riavviare il sistema.

3) Le tappe successive sono automatiche (non è richiesto alcun intervento manuale)

a) Il nodo master si riferisce al CLS dopo l'avvio con la versione software 3.
b) Il CLS genera un nuovo file di licenza di rete.
c) Il CLS trasferisce il nuovo file di licenza di rete al nodo master.
d) Il nodo master trasferisce automaticamente le nuove informazioni sulla licenza ai nodi slave.

Nota: La trasmissione delle licenze ai nodi slave può richiedere fino a 15 minuti.

26.6.2.2 Upgrade software senza CLS Connect nel nodo master

Prerequisiti

- Tutti i nodi della rete funzionano con l'ultima versione software V2R7.x.
- A livello del server delle licenze centrale (CLS) è presente un file di licenza di rete per il nodo master della rete.
- Sono disponibili le licenze di upgrade software per ogni nodo

Passo a passo

1) Generare nuovi file di licenza di rete sul server delle licenze

a) Suddividere il file di rete a livello del CLS in file di licenza individuali
b) Generare un file di licenza per il nodo master

Attivare la licenza di upgrade software per il nodo master

c) Generare il file di licenza per i nodi slave

Attivare la licenza di upgrade del software per ogni nodo slave individuale

d) Eseguire la fusione dei file di licenza dei singoli nodi in un nuovo file di licenza di rete
e) Scaricare il nuovo file di licenza di rete dal CLS

2) Eseguire la migrazione di tutti i nodi slave alla versione software V3 (per maggiori dettagli, vedere Upgrade software dei sistemi OpenScape Business X alla pagina 1371 o Upgrade software da un UC Booster Server a OpenScape Business X V3 alla pagina 1374)

a) Importare il software V3 con l'OpenScape Business Assistant (WBM) e aggiornare il sistema.
b) La configurazione e le informazioni sulla licenza sono conservate.
c) Il sistema non è operativo dopo l'avvio a causa del file di licenza non valido.

Il sistema non è operativo dopo l'avvio a causa del file di licenza non valido.

3) Eseguire l'upgrade del nodo master alla versione V3 (per maggiori dettagli, vedere Upgrade software dei sistemi OpenScape Business X alla pagina

1371 o) Upgrade software da un UC Booster Server a OpenScape Business X V3 alla pagina 1374

a) Importare il software V3 con l'OpenScape Business Assistant (WBM) e aggiornare il sistema.
b) La configurazione e le informazioni sulla licenza sono conservate.
c) Importare il file di licenza di rete nel nodo master e attivare il file di licenza

4) Il nodo master trasferisce automaticamente le nuove informazioni sulla licenza ai nodi slave.

Nota: La trasmissione delle licenze ai nodi slave può richiedere fino a 15 minuti.

26.6.3 Scenario 3a: Upgrade software di tutti i nodi

In questo scenario, il nodo master è un sistema OpenScape Business S e i nodi slave sono sistemi OpenScape Business X.

Questo scenario è identico a Scenario 2: Upgrade software di tutti i sistemi nella rete a V3 alla pagina 1392

26.6.4 Scenario 3b: Upgrade software nel nodo master, migrazione hardware dei nodi slave

In questo scenario, i nodi slave sono migrati alla scheda madre V3 e alla versione software 3 con uno scambio HW/SW. Nel sistema OpenScape Business S il SW è aggiornato da V2 a V3. Per l'upgrade HW/SW della rete, l'uso della funzione CLS Connect definisce la procedura di trasferimento della licenza

26.6.4.1 Migrazione/Upgrade con CLS Connect nel nodo master

Prerequisiti

- Tutti i nodi della rete funzionano con l'ultima versione software V2R7.x.
- A livello del server delle licenze centrale (CLS) è presente un file di licenza di rete per il nodo master della rete.
- La funzione **CLS Connect** è attivata nel nodo master. CLS Connect non deve essere attivato sui nodi slave.
- Sono disponibili le schede madre V3 con il software V3.

Passo a passo

1) Eseguire la migrazione di tutti i nodi slave alla scheda madre V3 (per maggiori dettagli, vedere Migrazione hardware/software dei sistemi OpenScape Business X a V3 alla pagina 1376)

a) Ripristinare la configurazione del sistema con WBM
b) Sostituire le schede madre
c) Impostare la data e l'ora e il pacchetto applicativo con WBM
d) Ripristinare la configurazione del sistema con WBM

Il sistema non è operativo dopo l'avvio a causa del file di licenza non valido.

2) Eseguire l'upgrade del nodo master alla versione V3 (per maggiori dettagli, vedere Upgrade software dei sistemi OpenScape Business X alla pagina 1371 o) Upgrade software da un UC Booster Server a OpenScape Business X V3 alla pagina 1374
   a) Importare il software V3 con l'OpenScape Business Assistant (WBM) e aggiornare il sistema.
   b) La configurazione e le informazioni sulla licenza sono conservate.
   c) Riavviare il sistema.
3) Le tappe successive sono automatiche (non è richiesto alcun intervento manuale)
   a) Il nodo master si riferisce al CLS dopo l'avvio con la versione software 3.
   b) Il CLS genera un nuovo file di licenza di rete.
   c) Il CLS trasferisce il nuovo file di licenza di rete al nodo master.
   d) Il nodo master trasferisce automaticamente le nuove informazioni sulla licenza ai nodi slave.

Nota: La trasmissione delle licenze ai nodi slave può richiedere fino a 15 minuti.

26.6.4.2 Migrazione/Upgrade senza CLS Connect nel nodo master

Prerequisiti

- Tutti i nodi della rete funzionano con l'ultima versione software V2R7.x.
- A livello del server delle licenze centrale (CLS) è presente un file di licenza di rete per il nodo master della rete.
- È disponibile la licenza di upgrade software per il nodo master
- Sono disponibili le licenze di migrazione hardware per ogni nodo slave
- Sono disponibili le schede madre V3 con il software V3.

Passo a passo

1) Generare un nuovo file di licenza di rete sul server delle licenze.
   a) Suddividere il file di rete a livello del CLS in file di licenza individuali
   b) Generare un file di licenza per il nodo master
      Attivare la licenza di upgrade software per il nodo master
   c) Generare il file di licenza per i nodi slave
      Attivare la licenza di migrazione hardware per ogni nodo slave
   d) Eseguire la fusione dei file di licenza dei singoli nodi in un nuovo file di licenza di rete
   e) Scaricare il nuovo file di licenza di rete dal CLS
2) Eseguire la migrazione di tutti i nodi slave alla scheda madre V3 (per maggiori dettagli, vedere Migrazione hardware/software dei sistemi OpenScape Business X a V3 alla pagina 1376)
   a) Ripristinare la configurazione del sistema con WBM
   b) Sostituire le schede madre
   c) Impostare la data e l'ora e il pacchetto applicativo con WBM
   d) Ripristinare la configurazione del sistema con WBM

   Il sistema non è operativo dopo l'avvio a causa del file di licenza non valido.

3) Eseguire l'upgrade del nodo master alla versione V3 (per maggiori dettagli, vedere Upgrade software dei sistemi OpenScape Business X alla pagina 1371 o) Upgrade software da un UC Booster Server a OpenScape Business X V3 alla pagina 1374
   a) Importare il software V3 con l'OpenScape Business Assistant (WBM) e aggiornare il sistema.
   b) La configurazione e le informazioni sulla licenza sono conservate.
   c) Importare il file di licenza di rete nel nodo master e attivare il file di licenza
4) Il nodo master trasferisce automaticamente le nuove informazioni sulla licenza ai nodi slave.

Nota: La trasmissione delle licenze ai nodi slave può richiedere fino a 15 minuti.

26.7 Migrazione da HiPath 3000 a OpenScape Business V3

Questa sezione descrive la migrazione tecnica dei sistemi indipendenti HiPath 3000 / HiPath 500 V9 e dei sistemi HiPath 3000 collegati in rete a OpenScape Business V3 con schede madre V3.

Durante la migrazione dei sistemi HiPath 3000 a OpenScape Business X V3 con schede madre V3, secondo la configurazione hardware, può essere trasferita una parte dell'hardware del sistema con i terminali / client connessi.

Prima della migrazione di un HiPath 3000, devono essere determinati con verifiche successive la configurazione del sistema corrente, l'HW/SW, nonché i componenti su licenza da sostituire.

Verifiche generali

- **Controllo di compatibilità funzionale**

  Verificare quali caratteristiche non sono più supportate o sono cambiate rispetto a HiPath 3000 V9. Al capitolo Caratteristiche modificate/ abbandonate di HiPath 3000 e Interfacce alla pagina 1420 sono riportate le caratteristiche di HiPath 3000 che non saranno più supportate in OpenScape Business o che devono essere sostituite con nuove funzioni.
- **Verifica della versione software**

  Il sistema deve funzionare con la versione software V9 prima della migrazione. I sistemi con una versione software inferiore a V9 devono essere aggiornati e essere operativi con la versione software V9 prima della migrazione.
- **Verifica della messa a terra**

  Per tutti i sistemi di comunicazione OpenScape Business X, è obbligatoria la messa a terra con un conduttore di messa a terra supplementare!

Controllo compatibilità hardware

Per motivi tecnici, alcuni moduli e terminali non possono essere utilizzati nei sistemi di comunicazione OpenScape Business X. Al momento della migrazione da HiPath 3000 V9 a OpenScape Business V3, questi moduli e terminali devono essere rimossi. Se richiesto, sostituirli con le nuove versioni disponibili. The list of no longer supported modules and their successors can be found

in *OpenScape Business X3/X5/X8 Service Documentation* on section *Not Supported HW Components*.

- **Alimentazione**

  OpenScape Business 33xx / 35xx funzionano con un'alimentatore UPSC-D / DR o OCPSM. Eventuali alimentatori PSU rimanenti devono essere sostituiti con un'alimentatore OCPSM. Sono disponibili kit di upgrade PSU.
- **Periferiche**

  Verificare se le periferiche esistenti possono essere ancora utilizzate. I moduli che non sono più supportati o i dispositivi finali devono essere rimossi e sostituiti con le nuove versioni, se necessario.
- **Verifica del backplane**

  Nei sistemi HiPath 3550, lo slot 10 del backplane non è più indirizzato dalla scheda madre V3. I moduli periferici esistenti che utilizzano questo slot non funzionano più in OpenScape Business.
- **Verifica del telefono**

  I sistemi OpenScape Business V3 con schede madre V3 supportano dispositivi analogici, ISDN, SIP e OpenStage o OpenScape Deskphone IP / CP. I dispositivi Optiset E, Optipoint 4xx e Optipoint 5xx esistenti devono essere sostituiti.
- **Verifica dell'alloggiamento.**

  In seguito alla migrazione dei sistemi HiPath 33xx/35xx, è possibile che debbano essere sostituiti i coperchi dell'alloggiamento e installate delle ventole.

  Gli articoli corrispondenti sono disponibili su richiesta.

Altre verifiche

- **Piano di numerazione per i sistemi in rete**

  In reti puramente vocali è possibile utilizzare la numerazione aperta e chiusa. Se si utilizza la UC Suite, è necessario che la rete utilizzi un sistema a numerazione chiusa (funzionalità UC a livello di rete).

26.7.1 Migrazione da HiPath 33xx, 35xx, 3800 a OpenScape Business X3/ X5/X8 V3

Quando si effettua la migrazione di un sistema HiPath 33xx, 35xx o 3800 a OpenScape Business X V3, oltre al software di sistema, vengono sostituiti la scheda madre, i gruppi periferici definiti ed i dispositivi finali. Le licenze esistenti possono essere migrate con una licenza di upgrade. Può essere trasferita la configurazione del sistema. In seguito alla migrazione, il sistema OpenScape Business V3 ha un supporto software di 3 anni.

Per la migrazione da HiPath 3000 V9 a OpenScape Business V3 sono richiesti in generale i seguenti articoli:

- Scheda madre V3
- Software V3 su su SSD
- Stoccaggio dati in massa M2 SSD 256 GB (facoltativo con l'applicazione UC Suite)
- OpenScape Business Upgrade HiPath 3000 V9 (migrazione della licenza), o

- OpenScape Business Upgrade HiPath 3000 V8 (migrazione della licenza), o
- OpenScape Business Upgrade HiPath 3000 V7 (migrazione della licenza), o
- Licenza OpenScape Business CSTA (facoltativa)

Se necessario devono essere ordinati ulteriori componenti hardware e licenze. Ciò dipende dalla configurazione del sistema del cliente.

In *OpenScape Business X3/X5/X8, Documentazione di manutenzione*, nella sezione *Componenti HW non supportati*, si trovano informazioni su quali componenti sono stati sostituiti nella versione V3 o sono stati eliminati senza sostituzione. Si prega di notare che è richiesta un licenza CSTA per una connessione esistente di applicazioni CSTA esterne. Questo requisito non è applicabile alla connessione di OpenScape Business TAPI 170 o TAPI 120.

Premessa

Tutti i componenti hardware/software sono stati verificati per il riutilizzo.

Sono disponibili tutti i nuovi componenti hardware/software.

È stata ordinata una licenza di upgrade per l'upgrade da HiPath 3000 V7, V8 o V9 a OpenScape Business V3 ed è disponibile il LAC della licenza di upgrade per recuperare la nuova licenza dal server delle licenze.

Il sistema è stato aggiornato con la versione software V9 più recente per la migrazione software tecnica e il trasferimento della configurazione esistente del cliente.

È utilizzata la versione di Manager E più aggiornata.

Determinazione delle licenze OpenScape Business durante la migrazione

Le licenze esistenti nei sistemi HiPath 3000 possono essere trasferite al sistema OpenScape Business V3 attivando la licenza «OpenScape Business Upgrade HiPath 3000 (V7, V8 o V9)» nel server centrale delle licenze Durante il trasferimento della licenza è creato un nuovo file di licenza per il sistema OpenScape Business V3 con le seguenti licenze.

Tabella 35: Migrazione della licenza HiPath 3000

Licenza HP 3000	Licenza OpenScape Business	Commenti
	Licenza di base	Licenza appena creata con supporto software di 3 anni
	Licenza OpenDirectory Base	Appena creata
	Licenza Web Collaboration Connector	Appena creata
	Licenza utente TDM	Numero calcolato a partire a partire dalla configurazione del sistema[13]
Utente IP (ComScendo)	Licenza utente IP	Trasferimento 1:1 dal file di licenza HP 3000

Licenza HP 3000	Licenza OpenScape Business	Commenti
	Licenza utente TDM	Calcolata a partire dalla configurazione del sistema[13]
Canali S2M	Licenze di linea IP/S2M/ TI	Trasferimento 1:1 dal file di licenza HP 3000
Mobility Entry	Licenze utente Mobility	Trasferimento 1:1 dal file di licenza HP 3000

Determinazione delle licenze utente TDM nel file di licenza

Durante la conversione tecnica della configurazione del sistema HiPath 3000, il numero di utenti TDM attivi è determinato dal tool Manager E e scritto in un file di inventario (XML).

Il numero di licenze utente TDM è determinato dalle seguenti regole:

- 1x Licenza utente TDM per porta UP0 attiva - Telefono pronto (master/ slave), numero di telefono disponibile
- 1x Licenza utente TDM per telefono DECT registrato - numero di telefono disponibile
- 1x Licenza utente TDM per porta a/b attiva - (numero di telefono) per moduli inseriti
- 1x Licenza utente TDM per porta S0 attiva - (numero di telefono MSN) per moduli attivi

La migrazione della licenza utente TDM è eseguita offline a livello del CLS tramite il file di inventario XML.

Il server centrale delle licenze verifica se esiste un file di licenza per l'indirizzo MAC della scheda madre HiPath 3000.

Se è disponibile un file di licenza, la migrazione della licenza è eseguita a partire da questo file e dalle informazioni contenute nel file di inventario.

Se invece non è disponibile alcun file di licenza, l'upgrade di OpenScape Business è eseguito sulla base delle informazioni contenute nel file di inventario (XML)

Secondo la licenza di upgrade disponibile (V7, V8 o V9), vengono recuperate da OpenScape Business le seguenti percentuali di utenti TDM definiti.

- Upgrade da HiPath 3000 V4 o versione precedente a OpenScape Business V3:

  per le licenze di aggiornamento OpenScape Business a prezzo ridotto/ gratuite non viene calcolato alcun utente TDM
- Upgrade da HiPath 3000 V5, V6 o V7 a OpenScape Business V3:

  per le licenze di aggiornamento OpenScape Business a prezzo ridotto/ gratuite viene calcolato il 70% degli utenti TDM

[13] Determinato nel corso della descrizione della conversione tecnica; vedere di seguito.

- Upgrade da HiPath 3000 V8 a OpenScape Business V3:

  per le licenze di aggiornamento OpenScape Business a prezzo ridotto/ gratuite viene calcolato il 80% degli utenti TDM
- Upgrade da HiPath 3000 V9 a OpenScape Business V3:

  per le licenze di upgrade OpenScape Business a prezzo ridotto/gratuite viene calcolato il 100% degli utenti TDM.

Limiti funzionali e restrizioni

- La migrazione della licenza può essere effettuata solo alla V3. La migrazione della licenza a V2 non è supportata da Manager E.
- La migrazione della licenza di un sistema HiPath 3000 (scheda madre) può essere eseguita solo una volta e la scheda madre è bloccata per altre azioni dal CLS dopo la migrazione.
- Per poter migrare gli utenti di linee S2M e ComScendo, sul server centrale delle licenze deve essere disponibile un file di licenza HiPath 3000.
- Le licenze utente TDM generate durante la migrazione non possono essere trasferite ad altri sistemi o ad un account CLS.
- In OpenScape Business, le licenze utente e le licenze orientate all'utente UC vengono assegnate permanentemente agli utenti. Si noti che per gli utenti myAgent e myAttendant è disponibile il numero sufficiente di licenze. In OpenScape Business, le modifiche dello stato presenza di altri utenti da parte di utenti myAgent sono legate alla licenza myAttendant. Questa è acquistabile separatamente.
- In OpenScape Business la funzione Deskshare User (IP Moblity) richiede una licenza, diversamente da HiPath 3000. Ulteriori licenze utente IP devono essere disponibili e assegnate agli utenti Deskshare nel dialogo di licenza OpenScape Business Assistant.
- Per i seguenti prodotti e funzioni non sono eseguite migrazioni di licenza:
  - Canali B HG1500: modulo mancante, la funzionalità è integrata nella nuova scheda madre.
  - optiClient Attendant V8: non funziona con OpenScape Business.

    Prodotto di follow-up: OpenScape Business Attendant
  - optiClient BLF V1/V2: non funziona con OpenScape Business.

    Prodotto di follow-up: OpenScape Business BLF
  - HiPath TAPI 120/170 V2: non funziona con OpenScape Business.

    Prodotto di follow-up: OpenScape Business TAPI 120/170
  - Entry VoiceMail: modulo mancante, la funzionalità è integrata nella nuova scheda madre.

    Prodotto di follow-up: Smart Voicemail
  - Client di comunicazione myPortal entry Web Services installato sul Plug PC.
  - Stazione base: le licenze per gli utenti base non sono più necessarie.
  - Linea esterna ITSP: per l'uso dei canali ITSP per la telefonia Internet occorre acquistare licenze OpenScape Business.
  - Come in passato, non è richiesta alcuna licenza per linee S0, analogiche e CAS.
  - Per il collegamento in rete e la connessione di sistemi di terzi tramite linee trasversali è necessario acquistare in OpenScape Business una licenza di rete per nodo.

Gestione tecnica

Per la migrazione, eseguire i seguenti passaggi nell'ordine indicato:

1) **Scaricare il CDB di HiPath 3000 dal sistema**

   Con la versione più recente di Manager E, scaricare il CDB corrente di HiPath 3000 dal sistema HiPath 3000.

2) **Prendere nota delle impostazioni dell'HG1500 (opzionale)**

   Se è presente uno o più moduli HG1500, è necessario prendere nota delle impostazioni dell'HG1500 modificate rispetto a quelle predefinite, con l'aiuto dell'HG1500 WBM:

   - Routing IP
   - Routing PSTN
   - Firewall IP
   - Firewall MAC
   - Firewall applicaz.
   - Accounting IP
   - Mapping IP
   - SNMP

3) **Conversione del CDB di HiPath 3000**

   Con la versione più recente di Manager E, convertire il CDB corrente di HiPath 3000 nel CDB di OpenScape Business V3.

4) **Sostituire l'hardware**

   Sostituire la vecchia scheda madre dell'HiPath 3000 con la nuova scheda madre di OpenScape Business V3. Rimuovere tutti i moduli HG1500 e tutti i moduli e sottomoduli non più supportati. Tutti i sistemi di comunicazione OpenScape Business devono essere messi a terra con un conduttore di protezione supplementare.

5) **Esecuzione della prima installazione**

   Configurare il sistema di comunicazione tramite il WBM con la procedura guidata **Configurazione di base**. Prendere in considerazione anche le impostazioni HG1500 precedentemente trascritte.

6) **Carica CDB convertito**

   Caricare il CDB convertito con la versione più recente di Manager E nel sistema OpenScape Business V2. Il sistema OpenScape Business si riavvia automaticamente.

7) **Generare un nuovo file di licenza nel CLS**

   Generare nel CLS un nuovo file di licenza con il LAC della licenza di aggiornamento, il file di configurazione (file XML) e il Locking ID di OpenScape Business.

8) **Attivazione e assegnazione licenze**

   Attivare la licenza del sistema di comunicazione OpenScape Business entro 30 giorni utilizzando il file di licenza.

9) **Reset delle voci LCR**

   Se necessario, è possibile resettare le voci LCR configurate nel sistema HiPath 3000 (quali ad esempio piani di numerazione, tabelle delle rotte, regole di selezione) ripristinando le voci predefinite di OpenScape Business. Questa impostazione è disponibile nel WBM, utilizzando la procedura guidata **Installazione di base**.

26.7.1.1 Come caricare il CDB da HiPath 3000

Prerequisiti

È disponibile un sistema di comunicazione HiPath 3000 (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 o HiPath 3800).

Tutti i telefoni sono collegati e attivi.

L'ultima versione Manager E viene installata sul PC dell'Admin.

Il PC Admin è collegato con il sistema di comunicazione HiPath 3000.

Passo a passo

1) Dal PC Admin accedere a Manager E.
2) Nella barra dei menu, fare clic su **File** > **Trasmetti**.
3) Fare clic sulla scheda **Comunicazioni**.
4) Nell'area **Accesso**, selezionare l'opzione richiesta in base al tipo di collegamento del PC Admin al sistema.
5) Selezionare il pulsante di opzione **Leggere/scrivere CDB** quindi fare clic on **Sistema** > **PC**.
6) Fare clic su **OK**. Il CDB viene trasferito da HiPath 3000 a Manager E.
7) Terminato il trasferimento, fare clic su **OK**, quindi su **Chiudi**.
8) Nella barra dei menu, fare clic su **File** > **Salva database cliente con nome** in e salvare il CDB sul PC Admin in una directory a scelta.

Passaggi successivi

Come visualizzare le impostazioni dell'HG1500 alla pagina 1402

26.7.1.2 Come visualizzare le impostazioni dell'HG1500

Prerequisiti

Uno o più moduli HG1500 sono inseriti.

Si è connessi a Manager E.

Passo a passo

1) In Manager E, nello schema del sistema, fare clic sulla voce HG1500. Si apre il WBM dell'HG1500.
2) Prendere nota delle impostazioni modificate rispetto alle impostazioni predefinite. Le impostazioni HG1500 non vengono importate durante la conversione del CDB e devono essere nuovamente configurate in fase di messa in funzione di OpenScape Business in WBM.

Passaggi successivi

Come convertire il CDB di HiPath 3000 alla pagina 1403

26.7.1.3 Come convertire il CDB di HiPath 3000

Prerequisiti

È disponibile un sistema di comunicazione HiPath 3000 (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 o HiPath 3800).

Il PC Admin è collegato con il sistema di comunicazione HiPath 3000.

Passo a passo

1) Nella barra dei menu, fare clic su **File** > **Converti database cliente**.
2) Selezionare il CDB precedentemente memorizzato sul PC Admin e premere **OK**.
3) Come dati cliente, immettere il proprio **Nome** e **Numero di contratto**, quindi fare clic su **Avanti**.
4) Selezionare come **Versione** la voce **OpenScape Business V2** e fare clic su **Avanti**.
5) Confermare l'indicazione relativa ai moduli che non sono più supportati premendo **OK**.
6) Confermare la finestra che informa sul numero di utenti TDM per eseguire la migrazione e procedere con la migrazione premendo **Sì**.

   Il numero di utenti TDM da migrare è calcolato automaticamente.
7) Confermare l'indicazione dei moduli collegati premendo **Avanti**.
8) Nella barra dei menu fare clic su **File** > **Salva database cliente con nome** e salvare il CDB con un nome diverso sul PC Admin in una directory a scelta.
9) Chiudere Manager E.

Passaggi successivi

Come sostituire l'hardware con il sistema HiPath 3300/3500 alla pagina 1403 o

Come sostituire l'hardware con il sistema HiPath 3350/3550 alla pagina 1404 o

Come sostituire l'hardware con il sistema HiPath 3800 alla pagina 1406

26.7.1.4 Come sostituire l'hardware con il sistema HiPath 3300/3500

Prerequisiti

È disponibile e operativo un sistema di comunicazione HiPath 3000 (HiPath 3300 o HiPath 3500 montato su rack).

Scheda madre OpenScape Business V3 (OCCMRA o OCCMRB).



Attenzione:

Scossa elettrica per contatto con linee sotto tensione

Assicurarsi che per il sistema di comunicazione sia disponibile un conduttore di protezione aggiuntivo con la sezione minima richiesta (vedere la documentazione di manutenzione al capitolo Montaggio dell'hardware).

Passo a passo

1) Spegnere il sistema HiPath 3000, quindi scollegarlo dalla presa di rete.
2) Rimuovere tutti i connettori dalla scheda madre, ad esempio gli utenti analogici, le linee ISDN ecc.
3) Allentare le due viti di serraggio sul pannello frontale della scheda madre.
4) Allentare con le due chiavi per moduli (C39165-A7027-C26) la scheda madre dal backplane.
5) Estrarre con attenzione la scheda madre HiPath 3000 dal telaio portamoduli utilizzando entrambe le mani tirando in orizzontale, quindi riporla su una superficie conduttiva piana dotata di messa a terra.
6) Rimuovere dall'alloggiamento i moduli HG1500 eventualmente presenti. Gli slot HG1500 liberi possono essere utilizzati per moduli aggiuntivi.
7) Estrarre dall'alloggiamento tutti i moduli presenti e non supportati. Gli slot liberi possono essere utilizzati per moduli aggiuntivi.
8) Rimuovere tutti i sottomoduli inseriti nella scheda madre dell'HiPath 3000 e collegarli (se richiesti e supportati) sulla scheda madre di OpenScape Business V3.
9) Collegare l'M.2 SATA SSD con sistema SW e l'M.2 NVMe SSD opzionale sulla scheda madre V3.
10) Collegare i moduli opzionali come OCCBH o OCCBL.
11) Inserire con attenzione la scheda madre OCCMRA o OCCMRB orizzontalmente con entrambe le mani nello slot in cui prima era inserita la scheda madre di HiPath 3000.
12) Collegare i moduli opzionali come STRBR alla scheda madre V3.
13) Reinserire tutti i connettori nella scheda madre, ad esempio gli utenti analogici, le linee ISDN ecc.

Nota: Quando si utilizzano più di 2 porte a/b analogiche con HiPath 3300 o 3500, sono necessari 1 o 2 cavi adattatori a Y con OpenScape Business. È possibile collegare fino a 4 porte a/b mediante 2 connettori fisici RJ11. A causa di limitazioni di spazio, la nuova scheda madre dispone solo di 2 prese RJ11 a cui possono essere collegati 4 utenti a/b.

---

14) Collegare correttamente il sistema di comunicazione al conduttore di protezione.
15) Collegare di nuovo alla presa di rete e accendere il sistema.

Passaggi successivi

Come eseguire l'installazione iniziale alla pagina 1407

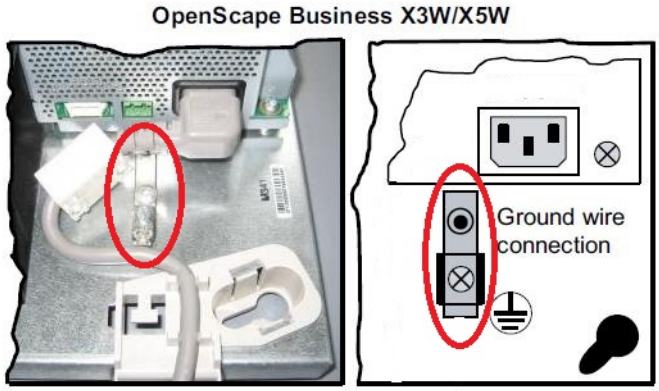
26.7.1.5 Come sostituire l'hardware con il sistema HiPath 3350/3550

Prerequisiti

È disponibile e operativo un sistema di comunicazione HiPath 3000 (HiPath 3350 o HiPath 3550).

Scheda madre OpenScape Business (OCCMA o OCCMB).

Nel caso di una migrazione da HiPath 3350/3550 a OpenScape Business X3W/X5W, il terminale di terra di protezione deve essere installato come mostrato nella figura di seguito. Successivamente il cavo di messa a terra deve essere collegato come descritto nella guida di installazione di OpenScape Business V2, OpenScape Business X3/X5/X8.



Attenzione:

Scossa elettrica per contatto con linee sotto tensione

Assicurarsi che per il sistema di comunicazione sia disponibile un conduttore di protezione aggiuntivo con la sezione minima richiesta (vedere la documentazione di manutenzione al capitolo Montaggio dell'hardware).

Passo a passo

1) Spegnere il sistema HiPath 3000, quindi scollegarlo dalla presa di rete.
2) Allentare l'alloggiamento e rimuoverlo.
3) Rimuovere la copertura.
4) Rimuovere tutti i connettori (edge connector) dalla scheda madre, ad esempio gli utenti analogici, le linee ISDN ecc.
5) Rimuovere il dispositivo di blocco del modulo.
6) Rimuovere con attenzione la scheda madre HiPath dal telaio portamoduli e riporla su una superficie conduttiva piana dotata di messa a terra.
7) Rimuovere dall'alloggiamento i moduli HG1500 eventualmente presenti. Gli slot HG1500 liberi possono essere utilizzati per moduli aggiuntivi.
8) Estrarre dall'alloggiamento tutti i moduli presenti e non supportati. Gli slot liberi possono essere utilizzati per moduli aggiuntivi.
9) Rimuovere tutti i sottomoduli inseriti nella scheda madre dell'HiPath 3000 e collegarli (se richiesti e supportati) sulla scheda madre di OpenScape Business.
10) Collegare l'M.2 SATA SSD con sistema SW e l'M.2 NVMe SSD opzionale sulla scheda madre V3.
11) Collegare i moduli opzionali come OCCBH o OCCBL.
12) Inserire con attenzione la scheda madre OpenScape Business OCCMA o OCCMB nello stesso slot in cui prima era inserita la scheda madre di HiPath 3000.

13) Collegare i moduli opzionali come STRBR alla scheda madre V3.
14) Reinserire tutti i connettori (edge connector) nella scheda madre, ad esempio gli utenti analogici, le linee ISDN ecc. Verificare che il connettore per le linee ISDN venga fatto passare prima attraverso il foro nel blocco di chiusura del nuovo modulo.
15) Chiudere il dispositivo di blocco del nuovo modulo.
16) Collegare correttamente il sistema di comunicazione al conduttore di protezione.
17) Rimontare l'alloggiamento e fissarlo.
18) Collegare di nuovo alla presa di rete e accendere il sistema.

Passaggi successivi

Come eseguire l'installazione iniziale alla pagina 1407

26.7.1.6 Come sostituire l'hardware con il sistema HiPath 3800

Prerequisiti

È disponibile e operativo un sistema di comunicazione HiPath 3800.

Scheda madre OpenScape Business OCCLA.

Attenzione:

Scossa elettrica per contatto con linee sotto tensione

Assicurarsi che per il sistema di comunicazione sia disponibile un conduttore di protezione aggiuntivo con la sezione minima richiesta (vedere la documentazione di manutenzione al capitolo Montaggio dell'hardware).

Passo a passo

1) Spegnere il sistema HiPath 3000, quindi scollegarlo dalla presa di rete.
2) Rimuovere tutti i connettori dalla scheda madre.
3) Estrarre con attenzione la scheda madre HiPath 3000 dal telaio portamoduli e riporla su una superficie conduttiva piana dotata di messa a terra.
4) Estrarre i moduli HG1500 eventualmente presenti dal telaio portamoduli. Gli slot HG1500 liberi possono essere utilizzati per moduli aggiuntivi.
5) Estrarre dal telaio portamoduli tutti gli eventuali moduli non più supportati. Gli slot liberi possono essere utilizzati per moduli aggiuntivi.
6) Rimuovere tutti i sottomoduli inseriti nella scheda madre dell'HiPath 3000 e collegarli (se richiesti e supportati) sulla scheda madre di OpenScape Business.
7) Collegare l'M.2 SATA SSD con sistema SW e l'M.2 NVMe SSD opzionale sulla scheda madre V3.
8) Collegare i moduli opzionali come OCCBH o OCCBL.
9) Inserire con attenzione la scheda madre OpenScape Business OCCLA nello stesso slot in cui prima era inserita la scheda madre di HiPath 3000.
10) Ricollegare tutti i connettori alla scheda madre.

11) Collegare correttamente il sistema di comunicazione al conduttore di protezione.
12) Collegare di nuovo alla presa di rete e accendere il sistema.

Passaggi successivi

Come eseguire l'installazione iniziale alla pagina 1407

26.7.1.7 Come eseguire l'installazione iniziale

L'installazione iniziale del sistema di comunicazione è descritta in Integrazione nella LAN del cliente).

L'installazione iniziale consiste nel configurare l'indirizzo IP del sistema, effettuare le impostazioni DHCP, quelle temporali e relative al paese.

Se il sistema HiPath 3000 comprende anche un HG 1500, alla prima installazione come indirizzo IP di OpenScape Business occorre usare l'indirizzo IP dell'HG 1500.

Terminata la prima installazione, il sistema di comunicazione si riavvia.

Passaggi successivi

Come caricare il CDB convertito nel nuovo sistema alla pagina 1407

26.7.1.8 Come caricare il CDB convertito nel nuovo sistema

Prerequisiti

L'hardware è stato sostituito.

Il PC Admin è collegato con il sistema di comunicazione OpenScape Business (tramite interfaccia LAN).

Il PC Admin è configurato in modo da poter ricevere l'indirizzo IP e la maschera di rete dal server DHCP di OpenScape Business.

Passo a passo

1) Dal PC Admin accedere a Manager E.
2) Nella barra dei menu, fare clic su **File** > **Apri database cliente**.
3) Selezionare il percorso di memorizzazione del CDB OpenScape Business convertito e fare clic su **OK**.
4) Confermare con **OK**.
5) Nella barra dei menu, fare clic su **File** > **Trasmetti**.
6) Fare clic sulla scheda **Comunicazioni**.
7) Nell'area **Accesso**, selezionare l'opzione **IP - HiPath** e nel campo Indirizzo IP indicare l'indirizzo IP del sistema di comunicazione OpenScape Business. Predefinito: `192.168.1.2`.
8) Attivare il pulsante di opzione **Sicurezza**.
9) Fare clic su **Modifica password**.
10) Inserire la vecchia password e quella nuova, quindi confermare con **OK**.
11) Selezionare il pulsante di opzione **Leggere/scrivere CDB**.

12) Selezionare le caselle **Addebiti** e **Hardware** e fare clic su **PC** > **Sistema**.
13) Fare clic su **OK**. Il CDB viene trasferito al sistema mediante Manager E.
14) Terminato il trasferimento del CDB, fare clic su **OK**, quindi su **Chiudi**.
15) Uscire da Manager E. Il sistema si riavvia automaticamente!

Passaggi successivi

Come generare un nuovo file di licenza alla pagina 1408

26.7.1.9 Come generare un nuovo file di licenza

Prerequisiti

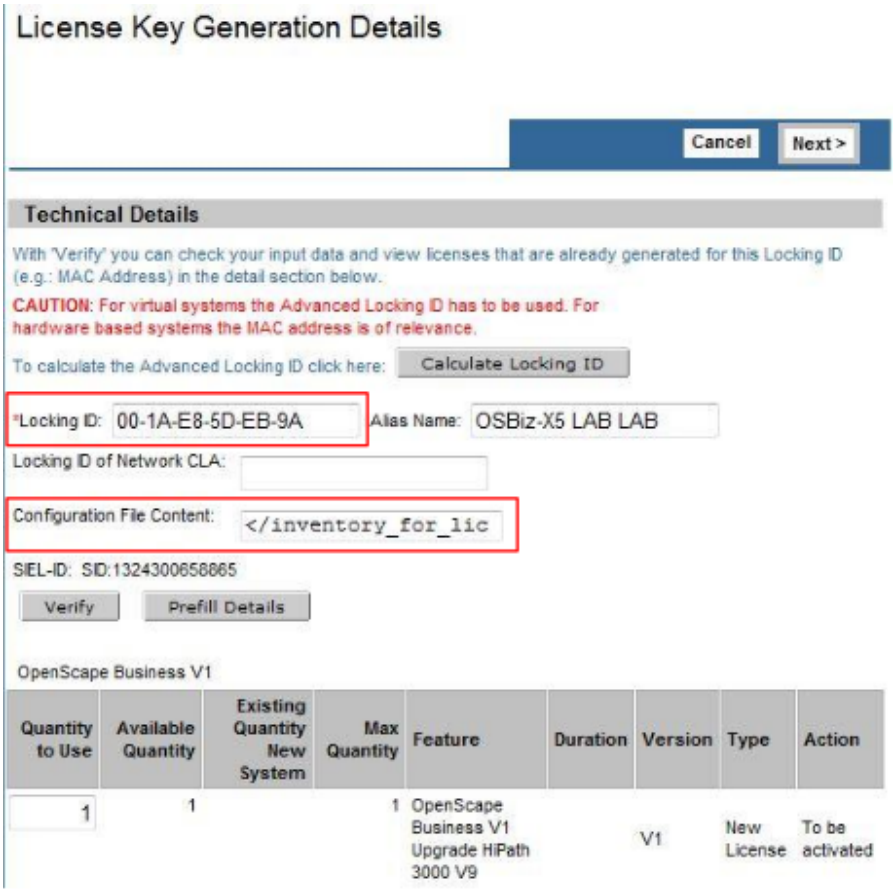
È disponibile il LAC della licenza di aggiornamento.

I dati di registrazione del cliente sono disponibili.

Passo a passo

1) Accedere al WBM con il profilo **Avanzato**.
2) Nella barra di navigazione fare clic su **Gestione delle licenze**.
3) Annotare il Locking ID di OpenScape Business, visualizzato sopra la tabella.
4) Nella struttura di navigazione fare clic su **Registrazione**.
5) Inserire i dati e fare clic su **OK & Avanti**.
6) Fare clic su **Esporta dati**. Viene generato un file di configurazione (file XML) utilizzando i dati di registrazione e le informazioni di inventario, ivi compreso il numero di utenti TDM collegati.
7) Salvare il file di configurazione in una cartella a scelta.
8) Accedere al CLS con nome utente e password.
9) Nella struttura dei menu fare clic su **Licenza** > **Genera chiave di licenza**.
10) Nel campo **LAC** specificare il LAC della licenza di upgrade, quindi fare clic su **Genera chiave**.

11) Selezionare la funzione **Aggiornamento a OpenScape Business V2 - HiPath 3000** e fare clic di nuovo su **Genera chiave.**



12) Nel campo **Locking ID**, immettere il Locking ID di OpenScape Business.

13) Aprire il file di configurazione con un editor di testo (ad esempio Notepad) e copiare l'intero contenuto del file di configurazione nel campo **Contenuto del file di configurazione**.

14) Fare clic su **Avanti** e seguire le istruzioni per generare un nuovo file di licenza.

Nota: La procedura e la migrazione della licenza nel CLS è possibile una sola volta. È opportuno quindi verificare che le informazioni siano corrette!

---

15) Salvare il nuovo file di licenza in una cartella a scelta.

Passaggi successivi

Come attivare il file di licenza offline alla pagina 1409

26.7.1.10 Come attivare il file di licenza offline

L'attivazione del file di licenza offline è descritta al capitolo Come attivare le licenze offline (indipendenti)

Passaggi successivi

Come assegnare le licenze alla pagina 1410

26.7.1.11 Come assegnare le licenze

L'assegnazione delle licenze è descritta in Assegnazione della licenza (indipendente) alla pagina 310.

26.7.1.12 Come resettare le voci LCR

L'installazione di base del sistema di comunicazione è descritta in Configurazione base alla pagina 155).

L'installazione base comprende la configurazione del numero del sistema, degli utenti, dell'accesso a Internet e della telefonia Internet.

Nella procedura guidata **Installazione di base**, nella finestra **Funzioni centrali per gli utenti**, si trova un pulsante di opzione aggiuntivo **Cancellazione dei dati LCR configurati e inizializzazione con dati LCR predefiniti**. Questo pulsante di opzione viene visualizzato solo se si carica nel sistema un CDB in precedenza convertito. Se questo pulsante di opzione è attivato, le voci LCR configurate nel sistema HiPath 3000 vengono eliminate e sostituite con le voci predefinite del sistema OpenScape Business.

Concetti correlati

Dati dell'utente alla pagina 159

26.7.2 Migrazione di un sistema HiPath 3000 con OpenScape Office V3 HX a OpenScape Business V3 con scheda madre V3

Durante la migrazione di sistemi HiPath 3000 con un server OpenScape Office HX connesso, non è richiesto il server esterno. La sua funzione è svolta dalla scheda madre V3 corrispondente del sistema OpenScape Business X.

La migrazione del sistema HiPath 3000 è effettuata come descritto in Migrazione da HiPath 33xx, 35xx, 3800 a OpenScape Business X3/X5/X8 V3 alla pagina 1397.

Le licenze OpenScape Office HX fanno parte integrante del file di licenza di HiPath 3000. Pertanto, sono trasferite anche alle licenze OpenScape Business nel corso della migrazione della licenza HiPath 3000.

Requisiti

Per poter effettuare la migrazione delle licenze OpenScape Business HX, deve essere disponibile sul server delle licenze centrale un file di licenza HiPath 3000.

Per le licenze HiPath 3000, la migrazione è eseguita come illustrato in Tabella 35: Migrazione della licenza HiPath 3000 alla pagina 1398. Per la migrazione della licenza OpenScape Office HX si applica la seguente procedura:

Tabella 36: Migrazione della licenza OpenScape Office HX

Licenza OpenScape Office HX	Licenza OpenScape Business	Commenti
Per licenza di base	1x licenza AutoAttendant	
Per utente OpenScape Office Standard:	1x Utente UC 1x Utente Voicemail 1x Utente Fax	Si applica alle licenze utente standard nelle licenze di base HX 5/10 e alle licenze di un singolo utente
Licenza OpenScape Office HX Voicemail	500 x Utente Voicemail	
myPortal for Outlook	Utente Groupware	Numero come sul file della licenza
myAttendant	myAttendant	Numero come sul file della licenza
myAgent	Utente myAgent	Numero come sul file della licenza
Fax Contact Center	Utente Fax Contact Center	Numero come sul file della licenza
E-Mail Contact Center	Utente E-Mail Contact Center	Numero come sul file della licenza
myReports	myReports	Numero come sul file della licenza
Application Launcher	Application Launcher	Numero come sul file della licenza
Connettore OpenDirectory	Connettore OpenDirectory	Numero come sul file della licenza

Limiti funzionali e restrizioni

La migrazione della licenza può essere effettuata solo alla V3. La migrazione della licenza a V2 non è supportata da Manager E.

La migrazione della licenza può essere eseguita solo una volta.

In OpenScape Business, le licenze utente e le licenze orientate all'utente UC vengono assegnate permanentemente agli utenti. Si noti che per gli utenti myAgent e myAttendant è disponibile il numero sufficiente di licenze.

In OpenScape Business, le modifiche dello stato presenza di altri utenti da parte di utenti myAgent sono legate alla licenza myAttendant. Questa è acquistabile separatamente.

Non è possibile trasferire annunci, immagini, caselle vocali, fax, diario, dati del contact center, configurazione dell'utente, profili, directory esterne, programmi da OpenScape Office HX a OpenScape Business V3 con scheda madre V3.

26.7.3 Migrazione di un sistema HiPath 3000 con OpenScape Office V3 HX a OpenScape Business V3 con UC Booster Server

La migrazione deve essere effettuata in due passaggi. Nella prima tappa, è eseguita la migrazione a V2. Alla tappa successiva, è eseguita la migrazione dei sistemi a V3.

Questo scenario di migrazione deve essere eseguito solo qualora sia necessario mantenere i dati cliente nel server OpenScape Office HX. Poiché la migrazione richiede molto tempo, deve essere impostato un nuovo UC Booster Server. Al termine della migrazione si avrà un sistema OpenScape Business X V3 con scheda madre V2 collegato a un UC Booster Server V3.

Alternativamente deve essere considerata una migrazione conforme a Migrazione di un sistema HiPath 3000 con OpenScape Office V3 HX a OpenScape Business V3 con scheda madre V3 alla pagina 1410 se sul server HX non devono essere conservati i dati del cliente.

Tappa 1 Migrazione di un sistema HiPath 3000 con OpenScape Office V3 HX a OpenScape Business V2

Con questa tappa, il sistema HiPath 3000 passa a OpenScape Business V2 e la funzione UC di OpenScape Office V3 HX è mappata a un server OpenScape Business UC Booster Server V2.

L'UC Booster Server deve essere installato da zero su una nuova base hardware e software. Le licenze e i dati del cliente possono essere trasferiti da OpenScape Office V3 HX all'UC Booster Server se è impostato prima con il software OpenScape Business Versione 1R2.2 e solo in questo caso sono trasferiti la seguente configurazione UC e i dati dell'utente:

- Annunci
- Immagini
- Casella vocale
- Fax
- Diario
- Dati del Contact Center
- Configurazione dell'utente
- Profili utente
- Rubrica esterna
- Pianificazioni

Le seguenti configurazioni UC e dati utente **non** vengono copiate e devono essere riconfigurate in UC Booster Server:

- Servizi Web (ad esempio XMPP, Web Collaboration, Mobility)
- Open Directory Service

Dopo il trasferimento delle licenze e dei dati del cliente, il server UC Booster Server deve essere aggiornato con la versione software V1R3.3 e successivamente aggiornato di nuovo con la versione software V2R7 più recente.

Per la migrazione/upgrade rispettare la seguente procedura nell'ordine indicato:

1) **Prendere nota degli ID degli agenti** (solo per l'uso del Contact Center)

   Prendere nota dell'assegnazione degli ID agente agli utenti della UC Suite, poiché questa assegnazione non viene considerata dalla migrazione.

L'assegnazione deve essere riconfigurata con la procedura guidata **Distribuzione delle chiamate** nel WBM del sistema di comunicazione OpenScape Business.

2) **Aggiornamento a OpenScape Office V3 HX**

   Se non è stato ancora eseguito, procedere ad aggiornare OpenScape Office HX V3 alla versione software V3 R3FR6.

3) **Creazione di un set di backup OpenScape Office V3 HX**

   Con il WBM di OpenScape Office V3 HX creare un set di backup su un supporto esterno.

   Per informazioni complete, consultare la Guida in linea di OpenScape Office Assistant.

4) **Aggiornamento di HiPath 3000**

   Eseguire l'upgrade da HiPath 3000 a OpenScape Business V1 come riportato nella descrizione della migrazione di un sistema indipendente (vedere Migrazione da HiPath 33xx, 35xx, 3800 a OpenScape Business X3/X5/X8 V3 alla pagina 1397). Le licenze di OpenScape Office V3 HX vengono trasferite a OpenScape Business in fase di migrazione sul server delle licenze. Il file di licenza contiene sia i dati della licenza per OpenScape Business X3/X5/X8 che quelli per la UC Suite.

5) **Impostazione dell'UC Booster Server e integrazione nella LAN del cliente**

   Sul nuovo PC server (server Linux) viene installato il sistema operativo Linux SLES 64 bit e successivamente il software di comunicazione (versione V1 R2.2). Per i dettagli, vedere le *Istruzioni di installazione del server Linux di OpenScape Business*.

6) **Attivazione di UC Booster**

   Attivare la funzionalità Booster UC nel WBM del sistema di comunicazione OpenScape Business (**Installazione di base** > **Installazione iniziale** > **Pacchetto con UC Suite su OpenScape Business UC Booster Server**) e inserire l'indirizzo IP del nuovo PC server (se possibile lo stesso indirizzo IP del precedente PC server). Assicurarsi che la UC Suite sia attiva sull'UC Booster Server.

   Per ulteriori informazioni, consultare la sezione "Installazione iniziale di OpenScape Business X3/X5/X8" in Come definire la soluzione UC alla pagina 153.

7) **Configurazione di UC Booster**

   Nel WBM dell'UC Booster Server, inserire l'indirizzo IP del sistema di comunicazione.

   Per ulteriori informazioni, consultare la sezione "Installazione iniziale di OpenScape Business UC Booster" in Comunicazione dell'indirizzo IP del sistema di comunicazione alla pagina 282.

8) **Conversione di un set di backup OpenScape Office V3 HX**

   Il set di backup di OpenScape Office V3 HX salvato su un supporto esterno deve essere convertito tramite uno script Linux in un set di backup per OpenScape Business V1. A tale scopo è necessaria la conoscenza dell'ambiente Linux. Successivamente, il set di backup convertito deve

essere caricato tramite il WBM nell'UC Booster Server. A questo punto saranno disponibili le configurazioni UC e i dati utente sopra indicati.

Sono disponibili maggiori informazioni su questa procedura in questa sezione in Come convertire un set di backup OpenScape Office V3 HX alla pagina 1414.

9) **Aggiornamento del software dell'UC Booster Server alla versione V2**

   Aggiornare prima l'UC Booster Server alla versione V1 R3.3 e successivamente alla nuova versione software OpenScape Business V2.

26.7.3.1 Come convertire un set di backup OpenScape Office V3 HX

Prerequisiti

OpenScape Business UC Booster Server è operativo.

Il set di backup OpenScape Office V3 HX si trova nel supporto esterno.

Passo a passo

1) Copiare il set di backup di OpenScape Office V3 HX dal supporto esterno al PC server (server Linux), nella seguente directory:

   ```
   /mnt/persistent/apollo/
   ```

2) Aprire un terminale sul PC server o connettersi con una shell SSH al PC server. È necessario disporre dei diritti di root.
3) Passare alla directory di backup con il seguente comando:

   ```
   cd /mnt/persistent/backup/
   ```

4) Richiamare lo script di conversione nel seguente modo:

   ```
   /opt/symappl/services/backup/script/migrate.sh /mnt/
   persistent/apollo/<nome del set di backup>
   ```

   ```
   /opt/symappl/services/backup/script/migrate.sh /mnt/
   persistent/apollo/BackupSet_130913-0400007.tar
   ```

5) Una volta eseguito lo script di conversione, è possibile usare per il ripristino il set di backup convertito.

26.7.4 Migrazione di una rete HiPath 3000 verso una rete OpenScape Business

Di seguito sono descritti i passaggi richiesti per la migrazione di una rete HiPath 3000 a una rete OpenScape Business.

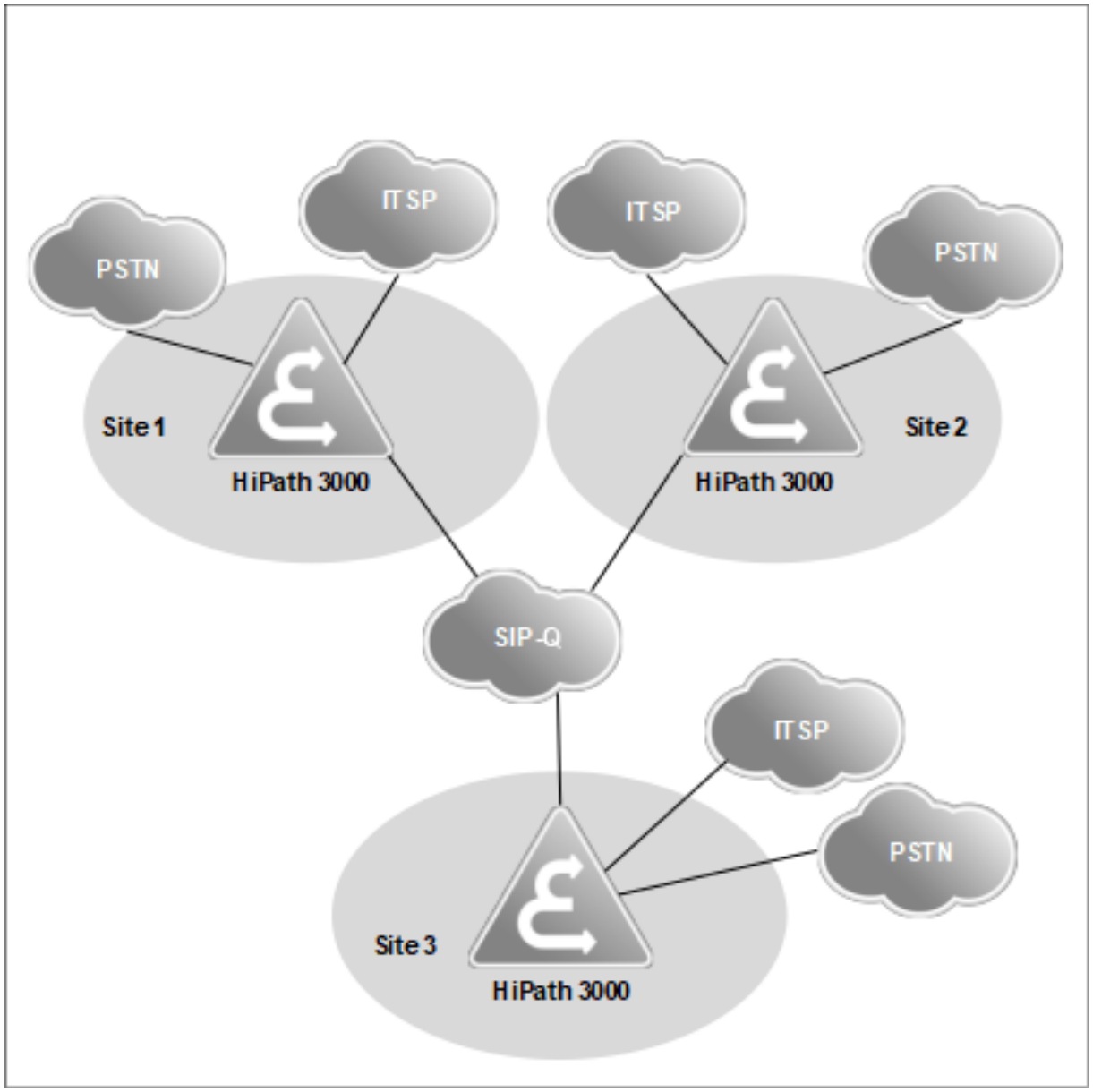


Figura 18: Sistema di reti HiPath 3000 V9

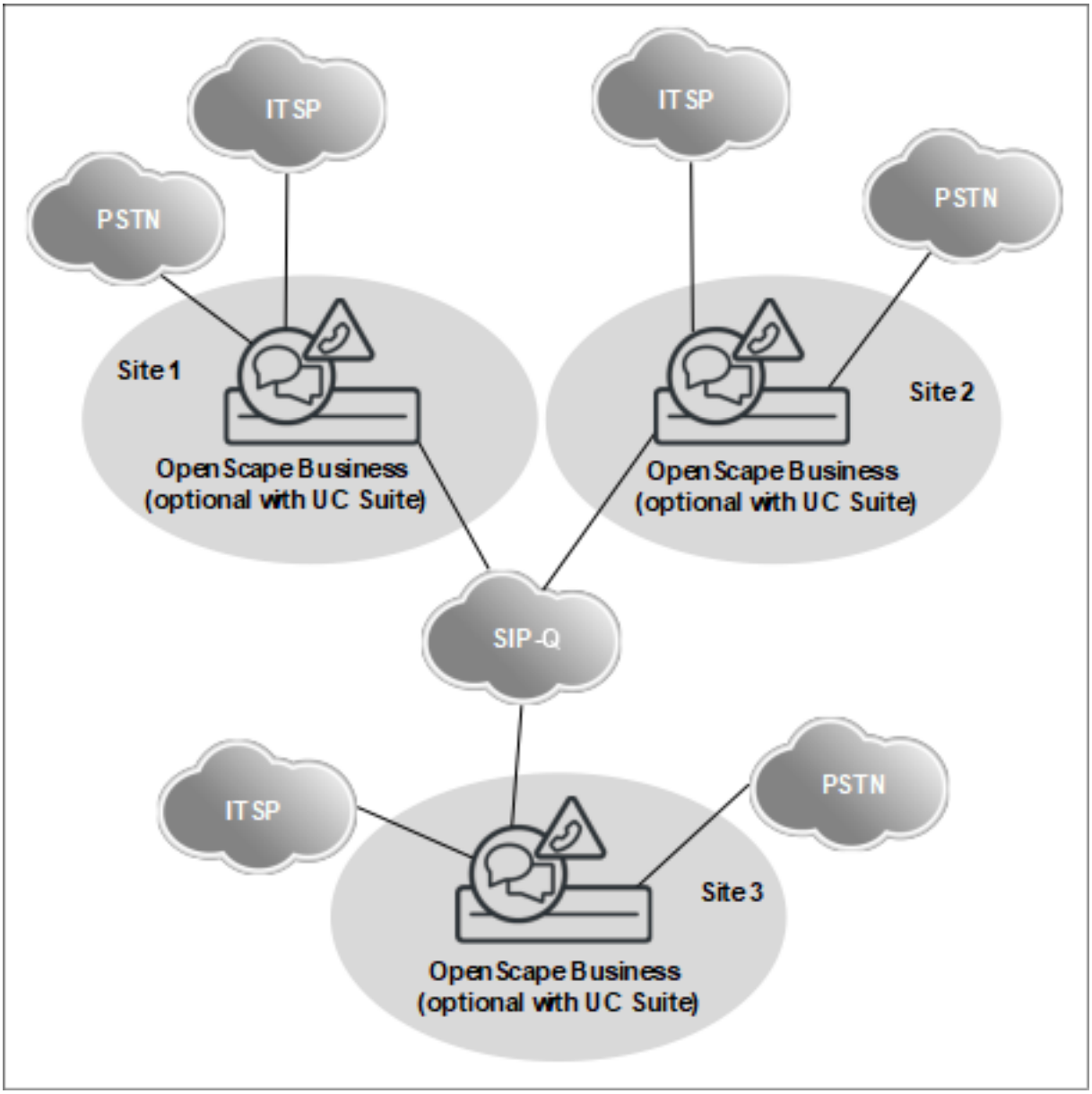


Figura 19: Sistema di reti OpenScape Business

Procedura di migrazione

Eseguire i seguenti passaggi nell'ordine indicato:

1) **Aggiornamento di HiPath 3000**

   Tutti i sistemi HiPath 3000 compresi nel sistema di reti devono essere aggiornati separatamente secondo la procedura descritta per la migrazione di un sistema indipendente (vedere 1.7.1).

2) **Modifica configurazione**

   Successivamente, i seguenti parametri di configurazione devono essere adattati utilizzando la Modalità esperti del WBM:

   - Voci LCR
   - Sistema Voicemail (gruppo di ricerca, codice selezione casella vocale)
   - Annunci

3) **Esecuzione della procedura di licensing**

   Una volta aggiornati tutti i sistemi, i singoli file di licenza vengono raggruppati nel CLS in una licenza singola a livello di rete.

26.7.5 Migrazione di un sistema di reti HiPath 3000 V9 con HiPath 5000 RSM

Una rete composta da HiPath 3000/5000 con un file di licenza di rete condiviso può essere suddivisa tramite il Server Centrale delle Licenze (CLS) in sistemi indipendenti con file di licenza individuali. Ogni sistema indipendente è migrato su OpenScape Business e ottiene una licenza separata.

Se richiesto, i sistemi OpenScape Business possono essere riuniti in un gruppo di reti con un file di licenza di rete unico nel CLS, dopo la migrazione

Le funzionalità di HiPath 5000 RSM sono state integrate in OpenScape Business, pertanto HiPath 5000 RSM non è più richiesto nel sistema di reti OpenScape Business.

Per la messa in rete dei sistemi OpenScape Business, devono essere disponibili inoltre le licenze di OpenScape Business Networking per nodo.

Per la telefonia Internet e le linee T1 sono richieste ulteriori licenze di linea.

Per la migrazione, rispettare la procedura descritta di seguito.

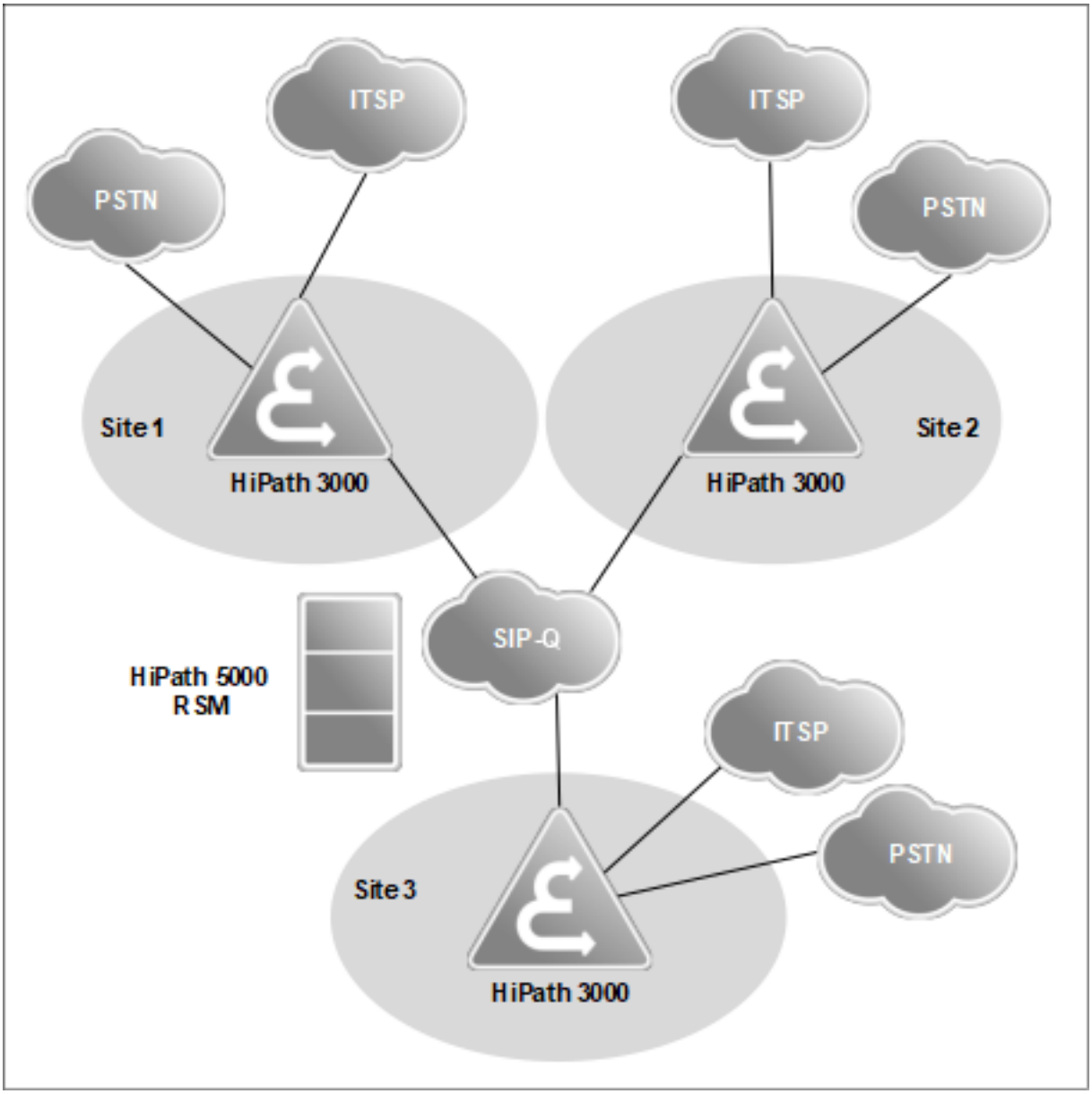


Figura 20: Sistema di reti HiPath 3000 V9

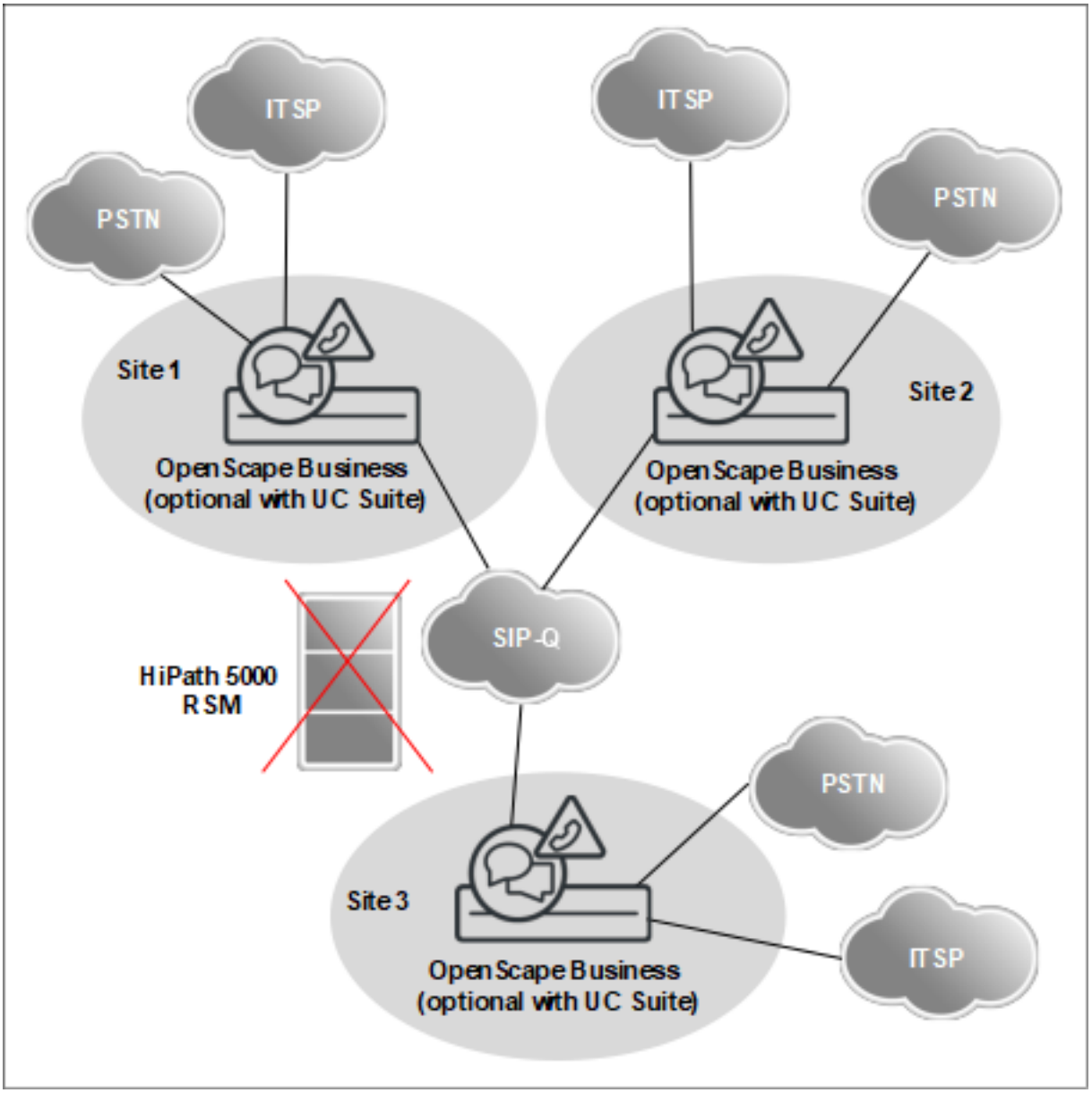


Figura 21: Sistema di reti OpenScape Business

Procedura di migrazione

Eseguire i seguenti passaggi nell'ordine indicato:

1) Rilascio concessione licenza a livello di rete

Un sistema di reti HiPath 3000 con HiPath 5000 RSM gestisce le licenze a livello di rete. Occorre dividere il file di licenza di rete in singoli file di licenza nel CLS e assegnare tali file ai Locking ID (indirizzi MAC) dei sistemi HiPath 3000 V9 prima di iniziare la migrazione effettiva a OpenScape Business.

- Assegnare innanzitutto le licenze del sistema di reti HiPath 5000 RSM ai singoli Locking ID dei nodi HiPath 3000. Suggerimento: creare un elenco in Excel con le assegnazioni corrispondenti delle singole licenze ai Locking ID dei sistemi HiPath 3000.
- Contattare la hotline licenze per richiedere che le licenze vengano suddivise secondo l'elenco Excel.

- Caricare le singole licenze di HiPath 3000 per il controllo del CLS. Non è richiesta l'attivazione delle licenze, ovvero l'importazione delle licenze nei sistemi HiPath 3000.

2) Eliminare HiPath 5000 RSM

Prima dell'aggiornamento dei sistemi HiPath 3000, assicurarsi che HiPath 5000 RSM sia spento.

3) Aggiornamento di HiPath 3000

Tutti i sistemi HiPath 3000 compresi nel sistema di reti devono essere aggiornati separatamente secondo la procedura descritta per la migrazione di un sistema indipendente. Vedere 1.7.1

4) Modifica configurazione

I seguenti parametri di configurazione devono essere adattati in un secondo momento utilizzando la Modalità esperti del WBM nei sistemi OpenScape Business.

- Voci LCR
- Sistema Voicemail (gruppo di ricerca, codice selezione casella vocale)
- Annunci

5) Esecuzione della procedura di licensing

Una volta aggiornati tutti i sistemi, i singoli file di licenza di OpenScape Business vengono raggruppati nel CLS in una licenza singola a livello di rete.

Nota: In caso di estensione a livello di rete della funzionalità UC, è necessario passare da una numerazione aperta a una chiusa per adeguare i numeri interni. Pertanto, la numerazione aperta deve essere disabilitata, mentre il numero del nodo deve essere eliminato e successivamente aggiunto come prefisso (ad esempio, numero interno esteso 87100 anziché 100 e 88100 anziché 100).

Differenze:

- La selezione dei partecipanti del proprio nodo viene eseguita con il numero interno esteso.

- Il numero di interno e il numero DID possono essere diversi, se necessario, ma i numeri DID non devono essere modificati.

26.7.6 Caratteristiche modificate/abbandonate di HiPath 3000 e Interfacce

Alcuni servizi e interfacce di HiPath 3000 sono stati adattati e ampliati in termini di funzioni per OpenScape Business.

Sostituzione della scheda MMC

Per ragioni tecniche, non è possibile la sostituzione della scheda SDHC / M.2 SATA SSD con il sistema acceso (procedura nota in HiPath 3000 come "Speed Update"). Inoltre, la scheda SDHC / M.2 SATA SSD di un sistema autorizzato A non può essere utilizzata per un altro sistema B perché la licenza è legata al locking ID della scheda madre A. Per utilizzare la scheda SDHC / M.2 SATA

SSD nel sistema B è necessario prima inizializzarla con il nuovo software utilizzando Card Manager.

Canali HG1500 DSP / canali B

Il modulo HG1500 non è più necessario. La funzione DSP è integrata in OpenScape Business sulla scheda madre V3 e tramite le schede opzionali Voice Channel Booster.

Indicare il numero di canali DSP richiesti. I canali DSP sono necessari per realizzare la transizione di rete da telefonia TDM a VoIP. OpenScape Business ha 8 canali DSP integrati sulla scheda madre V3. Per ampliare i canali DSP, è possibile usare il modulo DSP OCCB1/OCCBL (fino a 40 canali) o il modulo DSP OCCB3/OCCBH (fino a 120 canali).

Web Services entry level

La versione entry di Web Services non è più supportata. Il prodotto sviluppato da myPortal entry è chiamato myPortal @work e offre una gamma ampliata di funzioni. myPortal for Mobile è stato sostituito da myPortal to go (Web Edition). Per l'uso di myPortal to go non è più necessario il Plug PC

Entry VoiceMail

Il modulo Entry VoiceMail è stato abbandonato in OpenScape Business - Questa funzione è integrata come Smart Voicemail nella scheda madre di OpenScape Business. Gli utenti Smart Voicemail devono ottenere una licenza.

Casella vocale esterna

Se HiPath 3000 utilizza una soluzione voicemail esterna, quale Xpressions, le 10 porte EVM devono essere modificate da **Phonemail** a **Standard** in Manager E dopo la conversione del CDB.

Estensione delle funzionalità SIP

Rispetto a HiPath 3000 V9, sono state implementate le seguenti funzionalità SIP:

- Chiamata terminata altrove
- Indicazione messaggio in attesa per casella vocale
- Calling Name Presentation (CNIP)
- Squillo distintivo (chiamate interne/esterne)
- Controllo chiamate di terzi
- Deviazione delle chiamate su occupato/nessuna risposta/incondizionata (controllata dal portatile)

Linee SIP

Per la connessione a un server SIP esterno (ad esempio OpenScape Alarm Server, HiPath 4000, OpenScape Voice o UC Suite) sono disponibili altri fasci SIP nativo/SIP-Q in OpenScape Business (con HiPath 3000 solo un fascio SIP-Q). In questo modo, oltre ai classici fasci per la linea esterna, alla rete e all'ITSP, sono previste interfacce per linee SIP nativo/SIP-Q indipendenti per applicazioni certificate SIP (chiamate interconnessione SIP).

Vedere Connessione in rete di OpenScape Business

LCR

Le tabelle delle rotte da 1 a 15 sono intese per le voci predefinite o sono configurabili tramite procedura guidata. Durante la migrazione, le voci presenti in HiPath 3000 non vengono trasferite in questa tabella delle rotte. È necessaria una post-elaborazione manuale delle tabelle delle rotte.

Impegno automatico della linea

È possibile attivare le funzioni "LCR" o "Impegno automatico della linea" (selezione semplificata). Pertanto, per la migrazione viene automaticamente attivato "LCR" e disattivato "impegno automatico della linea(composizione semplificata)". Per disattivare "LCR" e attivare "Impegno automatico della linea (composizione semplificata)", occorre innanzitutto eseguire la procedura guidata "Installazione di base" e quindi attivare i relativi flag con Manager E (non per OpenScape Business X1, poiché non consente la gestione tramite Manager E).

Nota: La composizione semplificata non è supportata nelle applicazioni CSTA.

VoIP over PPP tramite ISDN

Non sono più supportate chiamate vocali instradate su linee a larghezza di banda ridotta

Supporto G.723

I codec G.723 non sono più supportati.

Babyphone (controllo stanza)

La funzione "Babyphone (controllo stanza)" non è più supportata. Poiché il "monitoraggio CSTA" è sempre attivo (un telefono di sistema può essere monitorato da un'applicazione, ad esempio myAgent o myPortal), non è più possibile attivare la funzione "controllo stanza" per quel telefono di sistema. Durante la conversione CDB con Manager E, il codice per l'attivazione del controllo stanza viene eliminato.

Numero di utenti base e telefoni DECT con OpenScape Business X3

Il numero di stazioni base di OpenScape Business X3 è stato aumentato da 3 a 7 rispetto a HiPath 33xx. Il numero di telefoni DECT di OpenScape Business X3 è stato aumentato da 16 a 32 rispetto a HiPath 33xx.

HiPath 3000 BS4

In OpenScape Business, non sono più richieste le licenze dell'utente base.

SSDP basato su Plug PC

SSDP è integrato in OpenScape Business. Il Plug PC non è più necessario.

Interfaccia di contabilità

Le interfacce dei dati contabili sono state modificate rispetto ad HiPath 3000.

Applicazioni V24

Le applicazioni V24 non sono più supportate.

Applicazioni CSTA

In OpenScape Business V3, per la connessione delle applicazioni CSTA è richiesta una scheda madre V3 o una UC Booster Card / Server in combinazione con una scheda madre V2. In un sistema di rete, nel nodo master deve esistere solo una scheda madre V3 / UC Booster Card / Server. Le applicazioni devono supportare il protocollo CSTAv3. Rispetto a HiPath 3000 sono state implementate modifiche del protocollo CSTA. Pertanto le applicazioni CSTA con HiPath 3000 V9 potrebbero non funzionare in modo compatibile ai sistemi OpenScape Business. Il protocollo CSTAv2 non è più supportato.

Nella versione software V3, è richiesta una licenza CSTA per utilizzare l'interfaccia CSTA, tranne per:

- Connessioni UC Booster Card CSTA in generale
- Connessioni OpenScape Business TAPI 120 o TAPI 170 CSTA in generale

Per l'interfaccia CSTA di OpenScape Business si applicano, rispetto all'interfaccia CSTA di HiPath 3000, le modifiche di seguito descritte.

- Con OpenScape Business, la connessione all'interfaccia CSTA è identica sia per i sistemi collegati in rete che per i nodi slave. L'interfaccia CSTA al nodo master in una rete fornisce funzioni avanzate. Viene realizzato solo tramite LAN. Le interfacce RS232(V.24) e S0 non sono più supportate.
- I componenti aggiuntivi hardware e software, quali provider di servizi CSTA servizi (CSP), moduli HG 1500 o il sistema HiPath 5000 RSM non sono più richiesti con OpenScape Business. Sono richiesti l'hardware UC Booster o la scheda madre V3.
- È fornita la licenza dell'interfaccia CSTA ad eccezione dell'UC Booster Card e delle connessioni TAPI 120/170.
- Per il collegamento di applicazioni esterne è possibile utilizzare un massimo di 4 collegamenti CSTA. Al momento della consegna, 3 delle 4 interfacce CSTA sono preconfigurate per l'uso di applicazioni interne di OpenScape Business. Queste possono opzionalmente essere utilizzate anche per il collegamento di applicazioni esterne.
- È stato migliorato il grado di protezione delle interfacce CSTA contro l'uso improprio. Il meccanismo di accesso è stato modificato.
- Il monitoraggio tramite CSTA è possibile solo se viene configurato un punto di monitoraggio con il numero MULAP. Non è possibile monitorare i singoli membri MULAP. Se si desidera che un'applicazione CSTA esegua il monitoraggio dei singoli membri MULAP, OpenScape Business non trasmetterà alcun evento CSTA all'applicazione. Questo si applica anche per i membri MULAP che fanno parte di un gruppo di ricerca.
- Le funzioni CSTA disponibili sono state ampliate. Per maggiori dettagli sull'interfaccia CSTA di OpenScape Business, consultare il relativo manuale.
- Il protocollo CSTA fase II non è più supportato.
- Le applicazioni CSTA compatibili con OpenScape Business devono essere testate in combinazione con OpenScape Business stesso e abilitate.

Applicazioni HiPath TAPI 120/170 V2

Per HiPath TAPI 120/170 V2, non è possibile trasferire le licenze esistenti. È necessario acquistare nuove licenze. HiPath TAPI 120/170 V2 deve essere disinstallato e al suo posto deve essere installato e configurato OpenScape Business TAPI 120/170 V1.

Le licenze TAPI sono configurabili in OpenScape Business, eliminando quindi la necessità di eseguire il licensing TAPI sul dispositivo TAPI. La licenza è

richiesta a partire dal primo utente TAPI (quindi anche TAPI120 non è più senza licenza per i primi 6 utenti). Il CMD (CSTA-Message Dispatcher) è integrato in OpenScape Business. Non è quindi più necessario un server Windows separato per il CMD. Il collegamento di applicazioni TAPI esterne è possibile sia in OpenScape Business che in OpenScape Business S. Per OpenScape Business è necessaria una scheda madre V3 o una UC Booster Card o un UC Booster Server. In un sistema di reti deve essere disponibile almeno un OpenScape Business S o una scheda madre V3 / UC Booster Card o UC Booster Server sul nodo master.

Per OpenScape Business TAPI 120/170 V2 V1 si applicano, rispetto a HiPath TAPI 120/170 V2, le modifiche di seguito descritte.

- L'accesso al sistema avviene esclusivamente tramite Ethernet LAN. Le interfacce RS-232 e S0 non sono più supportate.
- Nuova licenza comune TAPI su base "per utente" per TAPI 120 TSP e TAPI 170 TSP.
- Le licenze sono legate al Locking ID di OpenScape Business.
- Le licenze utente HiPath TAPI 120 TSP o HiPath TAPI 170 TSP non sono supportate dal nuovo meccanismo delle licenze.
- Nessuna compatibilità verso il basso con HiPath 3000 V8 o V9
- Per TAPI 170 TSP si applica quanto segue:
  - Per impostazione predefinita, l'accesso al sistema avviene tramite la porta 8800.
  - La configurazione dei dati di accesso CSTA nella finestra di configurazione è obbligatoria.
  - Supporto multi-nodo nella rete tramite CSP del nodo master centrale.
- Per TAPI 120 TSP si applica quanto segue:
  - Per impostazione predefinita, l'accesso al sistema avviene tramite la porta 8900.
  - Supporto per un nodo singolo, anche con collegamento al nodo master di una rete.

Ulteriori applicazioni esterne

Le applicazioni successive connesse esternamente a HiPath 3000 non possono funzionare più su OpenScape Business.

Applicazione HiPath 3000	Applicazione successiva per OpenScape Business	Commenti
optiClient Attendant	OpenScape Business Attendant	Nuova applicazione Nessuna possibilità di trasferimento di licenza
optiClient BLF V1/V2	OpenScape Business Attendant (OpenScape Business BLF)	Nuova applicazione Nessuna possibilità di trasferimento di licenza
HiPath TAPI 120/170	OpenScape Business TAPI 120/170	Nuova applicazione Nessuna possibilità di trasferimento di licenza

Applicazione HiPath 3000	Applicazione successiva per OpenScape Business	Commenti
Communication Clients di Entry WEB Services su Plug PC	Soluzione integrata UC	Nuova applicazione Nessuna possibilità di trasferimento di licenza
myPortal for Mobile/ Tablet	myPortal to go	Nuova applicazione Nessuna possibilità di trasferimento di licenza

Caratteristiche modificate/abbandonate di HiPath 5000 RSM

HiPath 5000 RSM non è più supportato. La funzionalità di HiPath 5000 RSM è stata integrata in OpenScape Business. Ciò significa che non è più richiesto un server separato

Tabella 37: Differenze tra HiPath 5000 RSM e OpenScape Business V3

Caratteristica	HiPath 5000 RSM	OpenScape Business
Concessione licenza a livello di rete, assegnazione delle licenze ai singoli nodi	Tutte le licenze di sistema della rete vengono combinate in una licenza a livello di rete in corrispondenza del CLS.	Tutte le licenze di sistema della rete vengono combinate in una licenza a livello di rete in corrispondenza del CLS.
Amministrazione di rete	DB Feature Server: tutti i nodi di una rete vengono uniti in un CDB rete tramite Manager E. Lo schema di numerazione è sincronizzato a livello di rete.	Tutti i nodi della rete sono registrati tramite l'OpenScape Business Assistant (WBM) utilizzando una procedura guidata di rete. Lo schema di numerazione è sincronizzato a livello di rete (numerazione chiusa).
Collegamento a nodi esterni e applicazioni esterne	Connessione SIP-Q di un massimo di 4 nodi esterni	Fino a 10 fasci di interconnessione SIP con 2 SIP-Q o fino a 10 SIP nativo o fino a 8 ITSP
Resilienza/Survivability	Survivability dell'utente per telefoni HFA con uso di numerazione chiusa	Survivability dell'utente per telefoni HFA con uso di numerazione chiusa (modifica da OpenScape Business S <-> OpenScape Business X3/X5/X8)
Backup / Ripristino	In tutta la rete	Locale
Funzione inventario	In tutta la rete	Locale

Caratteristica	HiPath 5000 RSM	OpenScape Business
Gestore presenze	Funzione a livello di rete con disponibilità di 5000 RSM	Funzione a livello di rete comprendente un CSP multinodo basato su OpenScape Business UC Booster Card, OpenScape Business UC Booster Server o OpenScape Business S. Prerequisito: numerazione chiusa.
TAPI 170 nel sistema indipendente	Il TAPI 170 nel sistema indipendente viene eseguito su un PC Windows con un proprio sistema di licensing (file di licenza separato per il TAPI 170).	Il sistema indipendente TAPI 170 viene eseguito su un PC Windows. La richiesta di licenza e l'erogazione dal database TAPI 170 viene eseguita mediante il DB SQL di OpenScape Business. Il collegamento di TAPI 170 viene effettuato tramite il CSP del sistema (OpenScape Business UC Booster Card, OpenScape Business UC Server Booster o OpenScape Business S)
TAPI 170 nel sistema di reti	TAPI 170 in esecuzione sul 5000 RSM con un proprio sistema di licensing (file di licenza separata per il TAPI 170). Il database TAPI 170 è ottenuto dal server DB Feature di 5000 RSM.	come sistema indipendente, tuttavia viene eseguito il collegamento del TAPI 170 sul multinodo CSP del nodo master (ovvero a livello di rete). Prerequisito: numerazione chiusa.

Reti miste

Non è supportato un sistema di reti misto costituito da OpenScape Business e OpenScape Office.

26.8 Migrazione tra sistemi OpenScape Business V3

Di seguito vengono descritte le diverse opzioni di migrazione tra i sistemi OpenScape Business X V3 con schede madre V2.

Nota: Questi scenari sono obsoleti (non validi) per i sistemi OpenScape Business X V3 con schede madre V3!

Aumento del numero di utenti UC Smart

È possibile scegliere tra le seguenti opzioni:

- Migrazione da **OpenScape Business X** (UC Smart) a **OpenScape Business X** con **UC Booster Card** (UC Smart)

  Utile per 50-150 utenti UC Smart. Vengono importati tutti i dati delle configurazioni e degli utenti. Nessuna importazione di dati in caso di downgrade. Per i nuovi utenti UC Smart, sono necessarie più licenze Utente UC Smart. OpenScape Business X1 non può essere espanso con la UC Booster Card.
- Migrazione da **OpenScape Business X** (UC Smart) a **OpenScape Business X** con **UC Booster Server** (UC Smart)

  Utile per 50-500 utenti UC Smart. Vengono importati tutti i dati delle configurazioni e degli utenti. Nessuna importazione di dati in caso di downgrade. Per i nuovi utenti UC Smart, sono necessarie più licenze Utente UC Smart.
- Migrazione da **OpenScape Business X** con **UC Booster Card** (UC Smart) a **OpenScape Business X** con **UC Booster Server** (UC Smart)

  Utile per 150-500 utenti UC Smart. Vengono importati tutti i dati delle configurazioni e degli utenti. Nessuna importazione di dati in caso di downgrade. Per i nuovi utenti UC Smart, sono necessarie più licenze Utente UC Smart.

Upgrade da UC Smart a UC Suite

È possibile scegliere tra le seguenti opzioni:

- Migrazione da **OpenScape Business X** (UC Smart) a **OpenScape Business X** con **UC Booster Card** (UC Suite)

  Non vengono importati i dati delle configurazioni e degli utenti. Per i client UC Smart disponibili è utile una licenza di upgrade ai client UC Suite. La conversione della soluzione di comunicazione alla UC Suite viene eseguita con il WBM utilizzando la procedura **Prima installazione**.
- Migrazione da **OpenScape Business X** (UC Smart) a **OpenScape Business X** con **UC Booster Server** (UC Suite)

  Non vengono importati i dati delle configurazioni e degli utenti. Per i client UC Smart disponibili è utile una licenza di upgrade ai client UC Suite. La conversione della soluzione di comunicazione alla UC Suite viene eseguita con il WBM utilizzando la procedura **Prima installazione**.
- Migrazione da **OpenScape Business X** con **UC Booster Card** (UC Smart) a **OpenScape Business X** con **UC Booster Server** (UC Suite)

  Non vengono importati i dati delle configurazioni e degli utenti. Per i client UC Smart disponibili è utile una licenza di upgrade ai client UC Suite. La conversione della soluzione di comunicazione alla UC Suite viene eseguita con il WBM utilizzando la procedura **Prima installazione**.
- **OpenScape Business S** - Migrazione da UC Smart a UC Suite

  Non vengono importati i dati delle configurazioni e degli utenti. Per i client UC Smart disponibili è utile una licenza di upgrade ai client UC Suite. La conversione della soluzione di comunicazione alla UC Suite viene eseguita con il WBM utilizzando la procedura **Prima installazione**.

- **OpenScape Business UC Booster Server** - Migrazione da UC Smart a UC Suite

  Non vengono importati i dati delle configurazioni e degli utenti. Per i client UC Smart disponibili è utile una licenza di upgrade ai client UC Suite. La conversione della soluzione di comunicazione alla UC Suite viene eseguita con il WBM utilizzando la procedura **Prima installazione**.

Aumento del numero di utenti UC Suite

È possibile scegliere tra le seguenti opzioni:

- Migrazione da **OpenScape Business X** con **UC Booster Card** (UC Suite) a **OpenScape Business X** con **UC Booster Server** (UC Suite)

  Utile per 150-500 utenti UC Suite. Vengono importati tutti i dati delle configurazioni e degli utenti. Nessuna importazione di dati in caso di downgrade. Per i nuovi utenti UC Suite, sono necessarie ulteriori licenze UC Suite User o Groupware User.

26.9 Migrazione dei moduli HW

Nei sistemi OpenScape Business X8 sono possibili le seguenti operazioni di migrazione hardware:

- Sostituzione di SLMO24N con SLMU
- Sostituzione di SLMO8N con SLMU
- Sostituzione di SLCN con SLMUC (SLMU + CMAe)

26.9.1 Sostituzione di SLMO24N con SLMU

È supportata una sostituzione di schede semplice. SLMO24N può essere rimossa dal sistema ed è possibile collegare la nuova SLMU. Tutte le porte configurate rimangono invariate. Non è necessario spegnere il sistema.

26.9.2 Sostituzione di SLM8N con SLMU

Poiché la scheda SLMU ha più porte rispetto a SLMO8, la scheda SLMO8 deve essere rimossa per amministrazione. Per rimuovere la scheda dal sistema, è necessario utilizzare l'utente online con la seguente finestra di dialogo:

```
Systemadministration 29- 4 - 1
```

e modificare il tipo di scheda in SLMUC.

Nota:

Se gli utenti sono configurati per UC Suite, vengono creati con le impostazioni predefinite. Tutti i dati precedenti (ad esempio messaggi vocali, fax, impostazioni utente) vengono persi.

Nota:

Nel caso in cui la scheda SLMO8 venisse sostituita con la scheda SLMU senza seguire la procedura descritta per la rimozione, le 16 porte aggiuntive della scheda SLMU potrebbero andare perse in quanto non sarebbe possibile configurarle. Ciò avviene se è già in funzione un'altra scheda che utilizza l'intervallo di porte di queste 16 porte. Se vi è una sola scheda SLMO8 nel sistema, sostituita da una scheda SLMU, tutte le porte saranno disponibili.

26.9.3 Sostituzione di SLCN con SLMUC (SLMU + CMAe)

Poiché la scheda SLMU ha più porte rispetto a SLCN, è necessario rimuovere SLCN per amministrazione prima dell'attivazione di SLMUC nello slot. Il procedimento da seguire per rimuovere la scheda è il seguente:

1) **Annullare la registrazione di tutti i ricevitori CMI dal relativo utente base**
2) **Rimuovere la scheda dal sistema**
3) **Rimuovere la scheda SLCN per utente online con la finestra di dialogo:**

   `Systemadministration 29- 4 - 1`

   e modificare il tipo di scheda in SLMUC.
4) **Installare la scheda SLMUC**
5) **Configurare il ricevitore usato**
6) **Registrare i ricevitori CMI**

   Tutti i telefoni DECT interessati (massimo 128) devono essere collegati per la nuova registrazione.

Nota:

Quando si sostituisce una scheda SLCN con SLMUC, è necessaria anche una copertura cieca per SLMUC al posto della copertura in plastica utilizzata per SLCN.

Nota:

Se gli utenti sono configurati per UC Suite, vengono creati con le impostazioni predefinite. Tutti i dati precedenti (ad esempio messaggi vocali, fax, impostazioni utente) vengono persi.

26.10 Migrazione da OpenScape Business X1 V2 a OpenScape Business X1W V3

Quando si esegue la migrazione di un modello OpenScape Business X1, è necessario sostituire l'intero sistema.

Le licenze esistenti possono essere rilevate. La configurazione del cliente non può essere rilevata e deve essere ripristinata manualmente dopo la migrazione. Il supporto software esistente continuerà invariato dopo la migrazione o verrà

adottata una nuova data di supporto software per la scheda madre V3 se valida oltre il 31/12/2026.

Prima della migrazione, è necessario configurare nel sistema l'accesso permanente al server delle licenze Unify (tramite Internet), se non già disponibile, e attivare la funzione "CLS Connect". Ciò semplifica il trasferimento della licenza e accelera notevolmente la migrazione. Il cliente deve essere informato dell'accesso richiesto dal sistema OpenScape Business al CLS.

Componenti dell'ordine richiesti

Per la migrazione del modello X1 a X1W con scheda madre V3, secondo che le applicazioni CLS Connect, UC Suite o CSTA esterna siano utilizzate, sono richiesti i seguenti componenti:

- Sistema X1W
- Software V3 su stoccaggio dati M.2 SATA SSD
- Stoccaggio dati in massa M2 SSD 256 GB (facoltativo con l'applicazione UC Suite)
- Licenza OpenScape Business Upgrade for OS Biz X1 (è sempre necessario)
- Licenza OpenScape Business CSTA (opzionale)

Limiti funzionali

Durante la migrazione, le licenze esistenti possono essere integralmente trasferite dal sistema X1 esistente al sistema X1W con scheda madre V3. Il trasferimento della licenza senza attivare la funzione CLS Connect richiede la licenza "Migrazione" e una procedura molto più complessa, con un conseguente dispendio di tempo rispetto all'uso della funzione CLS Connect.

I sistemi X1 con CLS Connect attivo non possono essere aggiornati ai sistemi X1W con scheda madre V3 tramite la funzione "Rigenerazione". La licenza "OpenScape Business Upgrade for OS Biz X1" deve essere sempre attivata, ma non è necessario inserire alcun codice di conferma durante il processo di aggiornamento.

L'aggiornamento del sistema OpenScape Business X1 PAYGO ai sistemi OpenScape Business X1W PAYGO non è supportato.

Nel caso in cui sul sistema vengano utilizzati client OpenScape Personal Edition e siano disponibili licenze corrispondenti, queste devono sempre essere rigenerate manualmente nel server licenze centrale per il nuovo ID di blocco (indirizzo MAC) della scheda madre V3, indipendentemente dal fatto che CLS Connect sia usato o meno.

La configurazione del cliente non può essere rilevata e deve essere ripristinata manualmente dopo la migrazione.

Gestione tecnica della migrazione

I principali passaggi tecnici della migrazione sono descritti di seguito. Viene fatta distinzione tra:

- Migrazione con licenza permanente
  - Migrazione con funzione CLS Connect attivata e connessione al server licenze centrale
  - Migrazione senza funzione CLS Connect e senza connessione al server centrale delle licenze

Ulteriori dettagli sulla gestione tecnica della migrazione sono contenuti nel manuale OpenScape Business Administrations.

26.10.1 Migrazione ai sistemi su licenza permanente X1W V3 con CLS Connect

Passo a passo

1) Generare i file di licenza sul server delle licenze centrale (CLS).
   a) Attivare la licenza "OpenScape Business Upgrade for OS Biz X1" sul sistema X1 con scheda madre V2. Durante il processo di attivazione fornire l'indirizzo MAC della scheda madre V3.
   b) Generare un nuovo file di licenza per l'indirizzo MAC del sistema X1W con scheda madre V3. Questo file di licenza include il supporto SW esteso.
   c) Trasferimento di eventuali licenze Personal Edition esistenti dall'indirizzo MAC della scheda madre V2 all'indirizzo MAC della scheda madre V3 utilizzando la funzione "Rigenera" e generazione di un nuovo file di licenza per le licenze Personal Edition.

2) Preparare il sistema OpenScape Business.
   a) Aggiornare il sistema esistente con la versione software V2R7.
   b) Impostare l'accesso al server delle licenze centrale (CLS) nel sistema e testare la connessione.
   c) Attivare CLS Connect nel sistema. Se è già stato fatto, il supporto SW verrà nuovamente esteso per 3 mesi.

3) Sostituzione del sistema X1
   a) Spegnere il sistema X1 e tutti gli alimentatori.
   b) Utilizzare un supporto dati V3 e se necessario uno stoccaggio dati di massa opzionale sul sistema X1W.
   c) Rimuovere CMAe e/o la scheda OCCB Voice Channel Booster dalla scheda madre V2 e inserirla nella scheda madre V3 X1W.
   d) Sostituire il sistema X1 con il sistema X1W.
   e) Collegare il cavo di messa a terra al sistema X1W.
   f) Collegare il telefono, la linea esterna, la LAN e, se applicabile, i cavi USB al sistema X1 W.
   g) Riaccendere gli alimentatori, il sistema si avvia automaticamente.

4) Impostare i parametri di sistema di base con WBM dopo l'avvio.
   a) Impostare la data e l'ora.
   b) Impostare il pacchetto applicativo.
      - UC Smart per i sistemi senza UC o con UC Smart
      - UC Suite per i sistemi con UC Suite
   c) Ripristinare la configurazione del sistema.
      - Configurazione manuale di X1W.
      - Importare i file di licenza appena creati.

26.10.2 Migrazione ai sistemi su licenza permanente X1W V3 senza CLS Connect

Passo a passo

1) Preparare il sistema OpenScape Business.
   a) Aggiornare il sistema esistente con la versione software V2R7.

2) Creare un file di licenza per la migrazione per X1 con scheda madre V2 a livello del server delle licenze centrale (CLS).
   a) Attivazione della "Licenza di migrazione X1" per il sistema esistente.
   b) Generare il nuovo file di licenza per l'indirizzo MAC della scheda madre V2. A tale scopo, deve essere inserito l'indirizzo MAC del sistema X1W nel CLS.
   c) Download del file di licenza dal CLS. Questo file di licenza include il supporto SW esteso.

3) Importare il file di licenza nel sistema OpenScape Business X1 con la scheda madre V2.

4) Annotare il "Codice di conferma" visualizzato in OpenScape Business Assistant.

5) Generare un nuovo file di licenza per il sistema X1W con la scheda madre V3 a livello del server delle licenze centrale (CLS).
   a) Creare un nuovo file di licenza per l'indirizzo MAC del sistema X1W con la scheda madre V3 sul CLS rigenerando l'indirizzo MAC di X1 con la scheda madre V2 e il codice di conferma annotato in precedenza.
      - Cercare il sistema OpenScape Business con l'indirizzo MAC del sistema X1W con la scheda madre V3 nel CLS.
      - Sblocco del sistema OpenScape Business acquisendo e attivando il codice di conferma.
      - Rigenerare il file di licenza.
   b) Scaricare il file di licenza appena generato dal CLS.

6) Sostituzione della scheda madre
   a) Spegnere il sistema e tutti gli alimentatori.
   b) Utilizzare un supporto dati V3 e se necessario uno stoccaggio dati di massa opzionale sul sistema X1W con la scheda madre V3.
   c) Rimuovere CMAe e/o la scheda OCCB Voice Channel Booster dalla scheda madre V2 e inserirla in X1W con la scheda madre V3.
   d) Sostituire la scheda madre del sistema X1 con V2 con la scheda madre del sistema X1W con V3.
   e) Collegare il cavo di messa a terra al sistema X1W.
   f) Collegare il telefono, la linea esterna, la LAN e, se applicabile, i cavi USB al sistema X1 W.
   g) Riaccendere l'alimentazione e il sistema si avvia automaticamente.

7) Impostare i parametri di sistema di base con WBM dopo l'avvio.
   a) Impostare la data e l'ora.
   b) Impostare il pacchetto applicativo.
      - UC Smart per i sistemi senza UC o con UC Smart
      - UC Suite per i sistemi con UC Suite
   c) Ripristinare la configurazione del sistema.
      - Configurazione manuale di X1W
   d) Importazione manuale del nuovo file di licenza nel sistema V3 dopo l'avvio del sistema.

27 Limiti di configurazione e capacità

I limiti di configurazione e le capacità si basano sui valori massimi in funzione del sistema di un singolo sistema. I valori massimi di un sistema all'interno di una rete possono essere diversi.

27.1 Valori massimi per utente

- I dati per i sistemi con schede madri V2 OCC sono disponibili in Tabella 38: Livello di espansione utenti con schede madri OCCx alla pagina 1433
- I dati per i sistemi con schede madri V3 OCC sono disponibili in Tabella 39: Livello di espansione stazioni/utenti con schede madri OCCSB/R, OCCMA/B o OCCLA alla pagina 1434
- I dati per sistemi OpenScape Business S Server sono disponibili in Tabella 40: Livello di espansione utenti con OpenScape Business S alla pagina 1435

Tabella 38: Livello di espansione utenti con schede madri OCCx

Utenti	X1	X3W/R	X5W/R	X8
Utenti max				
Massimo numero di utenti[15]	30	500	500	500
Utente IP				
Sistema Utenti IP (HFA)	20[16]	500	500	500
Utenti IP (SIP)	20[16]	500	500	500
Utenti TDM				
Numero massimo di utenti TDM[17] [21]	30	384	384	384
Utenti analogici (TDM)	4	20	68	384
Utenti master U_{P0} (TDM)[21]	8	24	56	384
Utenti slave U_{P0} (TDM) (incl. adattatori a/b e S0)	8	24	56	116
Utenti S0 ISDN (TDM)	2	36	52	128
Utenti DECT-CMI (TDM)	16	64	64	250
Utente Mobility				
Numero massimo di utenti mobility[18]	30	150	150	150
Utenti Mobility Entry	20	150	150	150
Utenti myPortal to go[19]	30	150	150	150
Utenti Skype for Business	30	150	150	150

Utenti	X1	X3W/R	X5W/R	X8
Altri utenti				
Utenti RAS	2	500	500	500
Utenti virtuali liberamente configurabili	30	250	250	250

Nota: Per ogni configurazione di sistema occorre verificare se la tensione di alimentazione nominale del sistema è sufficiente o se è necessaria un'alimentazione esterna (vedere *OpenScape Business - Requisiti di alimentazione di un sistema di comunicazione*).

Tabella 39: Livello di espansione stazioni/utenti con schede madri OCCSB/R, OCCMA/B o OCCLA

Utenti	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Stazioni massime								
Massimo numero di utenti[15]	30	30	500	500	500	500	500	500
Utente IP								
Sistema Utenti IP (HFA)	500	500	500	500	500	500	500	500
Utenti IP (SIP)	500	500	500	500	500	500	500	500
Utenti TDM								
Numero massimo di utenti TDM[17] [21]	384	384	384	384	384	384	384	384
Utenti analogici (TDM)	4	4	20	20	68	68	384	384

14 I valori sono scaglionati secondo la configurazione UC Booster: Booster Server / Booster Card / senza UC Booster

15 Somma di: Utenti IP (HFA), IP (SIP), Analogici, UP0 Master/Slave, DECT (CMI), ISDN S0, Mobility e Deskshare

16 Somma di utenti IP e utenti Deskshare (limitato dalla configurazione)

17 Somma di: Utenti analogici, UP0, DECT (CMI) e ISDN S0

18 Somma di: Partecipanti Mobility Entry, myPortal to go- Skype for Business

19 Il numero di connessioni VoIP simultanee dell'utente dipende da:

1) i canali DSP disponibili nel sistema per le chiamate gateway (transizione IP/TDM)

2) i canali proxy RTP interni disponibili nel sistema per le chiamate VoIP tramite internet.

20 Il numero di connessioni simultanee dipendenti dai canali DSP disponibili nel sistema per le chiamate gateway (transizione IP/TDM)

21 A seconda dei tipi di telefono e dei requisiti di potenza complessivi del sistema di comunicazione.

Utenti	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Utenti master/slave U_{P0} (TDM)[21]	8	8	24	24	56	56	384 master 116 slave	384 master 116 slave
Utenti S0 ISDN (TDM)	0	0	32	32	48	48	128	128
Utenti DECT-CMI (TDM)	16	16	64	64	64	64	250	250
Utente Mobility								
Numero massimo di utenti mobility[18]	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500 [22]	150/ 500[22]	500	500
Utenti Mobility Entry	150	20	150	150	150	150	150	150
Utenti myPortal to go[19]	150/ 500[22]	30	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500[22]	500	500
utenti myPortal for Teams[19]	150/ 500[22]	30	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500[22]	500	500
Utenti Skype for Business	150/ 500[22]	30	150/ 500[22]	150/ 500[22]	150/ 500[22]	150/ 500[22]	500	500

Tabella 40: Livello di espansione utenti con OpenScape Business S

Utenti	Server base (S)	Server standard (S)	Server avanzato (S)
Utenti max			
Massimo numero di utenti	50	500	1500
Utente IP			
Sistema Utenti IP (HFA)	50	500	1500
Utenti IP (SIP)	50	500	500
Utente Mobility			
Numero massimo di utenti mobility	50	250	500
Utenti Mobility Entry	50	150	150
Utenti myPortal to go	50	250	500
utenti myPortal for Teams	50	250	500
Utenti Skype for Business	50	250	500

22 I valori sono scaglionati secondo la versione della scheda: Base/Avanzata

27.2 Valori massimi per le linee

- I canali per tutti i tipi di linee (fascio, linea verticale, interconnessione, ecc.) nelle schede madri V2 OCC sono disponibili in Tabella 41: Livello di espansione canali di linea con schede madri OCCx alla pagina 1436.
- I canali per tutti i tipi di linee (fascio, linea verticale, interconnessione, ecc.) nelle schede madri V3 OCC sono disponibili in Tabella 42: Livello di espansione canali di linea con schede madri OCCSB/R, OCCMA/B o OCCLA alla pagina 1437
- I canali per tutti i tipi di linee (fascio, linea verticale, interconnessione, ecc.) in OpenScape Business S sono disponibili in Tabella 43: Livello di espansione canali di linea con OpenScape Business S alla pagina 1437

Tabella 41: Livello di espansione canali di linea con schede madri OCCx

	X1	X3W/R	X5W/R	X8
Canali di linea max				
Numero max. di canali di linea[23]	250	250	250	250
Canali di linea per la connessione del provider di servizi di telefonia, rete, computer esterno				
Canali trunk SIP (ITSP)	30	60[24]	60[24]	60[24]
Canali SIPQ (Rete)	100	100	100	100
ISDN S_0 - canali (BRI)	4	20	52	128
ISDN S_{2M} - canali (PRI)	-	30	30	80
ISDN CAS - canali (PRI)	-	30	30	180
Canali analogici (a/b)	-	X3R: 8 X3W: 16	X5R: 24 X5W: 48	120
Canali di linea per scopi interni				
Canali MEB per annunci interni[25]	0	16	16	16
Canali di linea MEB per UC Suite[26]	0	60 / 30 / 0[27]	60 / 30 / 0[27]	60 / 30 / 0[27]

23 Somma di: linea SIP, canali di linea ITSP, SIPQ, TDM e canali MEB senza (canali di annuncio MEB).

24 In rete con OpenScape Business S come gateway ITSP, sono possibili più di 60 canali

25 I canali MEB sono assegnati in modo dinamico dal sistema per gli annunci interni al sistema. Sono sempre inclusi nel numero massimo di canali di linea.

26 Per i sistemi con UC Suite, i canali MEB sono generati in modo dinamico per: Connessioni annunci e audiochiamate Voicemail, AutoAttendant, Fax, Call Me. Contano solo verso il numero massimo di canali di linea nei sistemi UC Suite.

27 I valori sono scaglionati secondo la configurazione UC Booster: Booster Server / Booster Card / senza UC Booster

Tabella 42: Livello di espansione canali di linea con schede madri OCCSB/R, OCCMA/B o OCCLA

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Canali di linea max								
Numero max. di canali di linea[23]	250	250	250	250	250	250	250	250
Canali di linea per la connessione del provider di servizi di telefonia, rete, computer esterno								
Canali trunk SIP (ITSP)	60/ 120[28]	60/ 120[28]	60/ 120[28]	60/ 120[28]	60/ 120[28]	60/ 120[28]	120	120
Canali SIPQ (Rete)	100	100	100	100	100	100	100	100
ISDN S_0 - canali (BRI)	-	-	16	16	48	48	128	128
ISDN S_{2M} - canali (PRI)	-	-	30	30	30	30	180	120
ISDN CAS - canali (PRI)	-	-	30	30	30	30	180	120
Canali analogici (a/b)	-	-	X3R: 8 X3W: 16	X3R: 8 X3W: 16	X5R: 24 X5W: 48	X5R: 24 X5W: 48	120	120
Canali di linea per scopi interni								
Canali MEB per annunci interni[25]	16	46	16	16	16	16	16	16
Canali di linea MEB per UC Suite[26]	0	30/60[28]	0	30/60[28]	0	30/60[28]	0	60

Tabella 43: Livello di espansione canali di linea con OpenScape Business S

	Server base (S)	Server standard (S)	Server avanzato (S)
Canali di linea max			
Numero max. di canali di linea[23]	250	250	250
Canali di linea per la connessione del provider di servizi di telefonia, rete, computer esterno			
Canali di linea SIP	180	180	180
Canali SIPQ (Rete)	100	100	100
Canali di linea per scopi interni			
Canali MEB per annunci interni[25]	16	16	16
Canali di linea MEB per UC Suite[26]	60	60	60

[28] I valori sono scaglionati secondo la versione della scheda: Base/Avanzata

27.3 Valori massimi delle risorse

Tabella 44: Livelli di espansione altre funzioni / risorse

	X1		X3		X5		X8	Server (S)
	Rack	**Parete**	**Rack**	**Parete**	**Rack**	**Parete**	**OCCL / OCCLA**	
Risorse di sistema								
Canali DSP								
DSP G.711 non criptato	8	8	128/ 48/ 8[34]	128/ 48/ 8[34]	128/ 48/ 8[34]	128/ 48/ 8[34]	128/ 48/ 8[34]	n/a
DSP G.711 + G.729 non criptato	8	8	104/ 40/ 8[34]	104/ 40/ 8[34]	104/ 40/ 8[34]	104/ 40/ 8[34]	104/ 40/ 8[34]	n/a
DSP G.711 criptato	6	6	102/ 38/ 6[34]	102/ 38/ 6[34]	102/ 38/ 6[34]	102/ 38/ 6[34]	102/ 38/ 6[34]	n/a
DSP G.711 + G.729 criptato	6	6	81/ 31/ 6[34]	81/ 31/ 6[34]	81/ 31/ 6[34]	81/ 31/ 6[34]	81/ 31/ 6[34]	n/a
DSP Fax T.38 (per gateway ISDN)[32]	3	3	12/ 6/ 3[34]	12/ 6/ 3[34]	12/ 6/ 3[34]	12/ 6/ 3[34]	12/ 6/ 3[34]	n/a
DSP Fax T.38 (per Fax UC Suite)[33]	-	-	8/ 6/ 0[34]	8/ 6/ 0[34]	8/ 6/ 0[34]	8/ 6/ 0[34]	8/ 6/ 0[34]	n/a
Canali proxy RTP								
Canali proxy RTP	30	30	60	60	60	60	60	180
Canali di linea MEB								
Canali di linea MEB in totale	**0**	**0**	**76/ 46/ 0[30]**	**76/ 46/ 0[30]**	**76/ 46/ 0[30]**	**76/ 46/ 0[30]**	**76/ 46/ 0[30]**	**76**
Canali di linea MEB per annunci	0	0	16/ 16/ 0[30]	16/ 16/ 0[30]	16/ 16/ 0[30]	16/ 16/ 0[30]	16/ 16/ 0[30]	16
Canali di linea MEB per UC Suite	-	-	60/ 30/ 0[30]	60/ 30/ 0[30]	60/ 30/ 0[30]	60/ 30/ 0[30]	60/ 30/ 0[30]	60
Musica su attesa e PPP								
Origini MOH [29] (G.711a, G.711u, G.729ab, G.729a)	4	4	4	4	4	4	4	32

29 Numero massimo di 16 connessioni simultanee per origine MOH

	X1		X3		X5		X8	Server (S)
	Rack	Parete	Rack	Parete	Rack	Parete	OCCL / OCCLA	
Canali PPP	8	8	8	8	8	8	8	n/a
Annunci								
Numero di dispositivi di annuncio per sistema	16	16	16	16	16	16	16	16
Dispositivi di annuncio tramite a/b	16	16	16	16	16	16	16	n/a
Annunci tramite Smart VM	6	6	6	6	6	6	6	6
Annunci tramite UC-Suite	16	16	16	16	16	16	16	16
Annunci prima della risposta (sistema, non UC Suite)								
Numero di chiamanti per i quali un annuncio può essere diffuso contemporaneamente	24	24	24	24	24	24	24	24
Destinatario DTMF								
Destinatario DTMF	16	16	16	16	16	16	16	per chiamata tramite ITSP

27.3.1 Dettagli sull'uso dei canali DSP

All'interno di OpenScape Business, i "canali DSP" vengono utilizzati per la conversione (transcodifica) dei flussi di dati. In linea di massima, è necessario in caso di transizione da IP a TDM o da TDM a IP per i dati vocali o di richiesta di crittografia dei dati vocali. Nel dettaglio:

30 I valori sono scaglionati secondo la configurazione UC Booster: Booster Server / Booster Card / senza UC Booster

31 Il valore dipende da UC Suite: Sistema con UC Suite / Sistema senza UC Suite

32 Valori applicabili a OpenScape Business come gateway ISDN. Da G.711 a T38 o viceversa senza UC Suite Fax

33 UC Suite generalmente è in grado di gestire fino a 8 connessioni fax contemporaneamente. Come gateway ISDN, OpenScape Business X3/X5/X8 può gestire da 3 a 12 fax simultanei, in funzione del modulo DSP. Entrambi i parametri in combinazione determinano il numero di connessioni fax T.38 o G.711 simultanee.

34 Valori scaglionati secondo la configurazione Voice Channel Booster: con OCCBH o OCCB3 / con OCCBL o OCCB1 / solo scheda madre

- Connessione vocale tra telefono IP e linea ISDN o analogica (trunk).
- Connessione vocale tramite linea IP SIP/ITSP e telefoni interni UP0/E, a/b o ISDN.
- Connessione vocale dalla linea IP o dall'utente IP a una conferenza interna. Qui è necessario un canale gateway per ogni linea/client IP coinvolti in una conferenza.
- Connessioni da telefoni UP0/E, a/b o ISDN o da linee ISDN/analogiche ad annunci, casella vocale, fax o conferenze di UC Suite.
- Connessioni vocali crittografate tra terminali e connessioni vocali crittografate su linee ITSP. Non è il caso della famiglia di schede madri V3, da OpenScape Business V3R4 in avanti.
- Le connessioni a Musica su attesa interna richiedono un canale DSP per il codec MoH configurato.

Per le seguenti connessioni non è necessario nessun canale DSP:

- Connessione tra utenti IP interni senza crittografia (payload diretto).
- Connessione tra ITSP e utenti IP senza crittografia.

I canali DSP vengono realizzati da un processore di segnale, il quale è integrato nella rispettiva scheda madre OCCL o OCCLA nei modelli X1, X3, X5 e X8.

A seconda del tipo di transcodifica, un unico processore di segnale può gestire più o meno canali DSP contemporaneamente. È supportata la seguente codifica (codec).

- **Per le connessioni vocali**
  - Conversione da IP (G.711) a TDM con G.711 o viceversa.
  - Conversione da IP (G.711) a TDM con G.711 o viceversa con crittografia (SPE).
  - Conversione da IP (G.729) a TDM con G.711 o viceversa.
  - Conversione da IP (G.729) a TDM con G.711 o viceversa con crittografia (SPE).
- **Per le connessioni fax**
  - Conversione da T.38 a G.711 quando si utilizza OpenScape Business come gateway ISDN.
  - Conversione da Fax G.711 a Fax T.38 o viceversa quando si utilizza la funzionalità Fax UC-Suite.

Se la capacità del processore di segnale integrato nella scheda madre non è sufficiente per realizzare il numero richiesto di canali DSP, è possibile estenderli utilizzando le schede opzionali "Voice Channel Booster" OCCBL o OCCBH disponibili.

Nella tabella 11 è riportato il numero massimo di canali DSP disponibili, a seconda della codifica. Ogni riga rappresenta il numero massimo di canali DSP simili, ma questi vengono assegnati dinamicamente dal sistema durante il funzionamento. Il numero di canali DSP attualmente occupati durante il funzionamento può essere determinato tramite OpenScape Business Assistant (WBM). Per ulteriori note sulla determinazione del numero di canali DSP richiesti, consultare il manuale di gestione.

27.3.2 Dettagli sull'uso dei canali proxy RTP

OpenScape Business utilizza un proxy RTP interno per tutte le connessioni VoIP tramite Internet. Il proxy offre un pool di canali RTP assegnati alle connessioni VoIP tramite Internet come segue.

- 1 canale proxy RTP per chiamata ITSP
- 1 canale proxy RTP per chiamata Unify Phone
- 1 canale proxy RTP per Dispositivo Sistema @Home in una chiamata
- 1 canale proxy RTP per dispositivo SIP @Home in una chiamata
- 1 canale proxy RTP per myPortal to go VoIP @Home in una chiamata
- 1 canale proxy RTP per myPortal @work VoIP @Home in una chiamata

Tra i diversi modelli OpenScape Business, è disponibile un numero diverso di canali proxy RTP. Vedere Tabella 44: Livelli di espansione altre funzioni / risorse alla pagina 1438

Esempi

- Una chiamata vocale in uscita esterna da un utente del sistema IP interno tramite una linea ITSP richiede un canale proxy RTP.
- Una chiamata vocale esterna dal Client myPortal to go VoIP tramite WiFi interno (campus) a un utente della rete pubblica tramite una linea ITSP richiede un canale proxy RTP. È utilizzato per la connessione tramite ITSP all'utente chiamato sulla rete pubblica.
- Una chiamata vocale esterna dal Client myPortal to go VoIP tramite WiFi pubblico a un utente della rete pubblica su una linea ITSP richiede due canali proxy RTP. È richiesto un canale proxy RTP per la connessione del client VoIP a OpenScape Business e un altro canale proxy RTP per la connessione tramite ITSP all'utente chiamato sulla rete pubblica.
- Una chiamata vocale esterna proveniente da una linea ITSP al Client myPortal @work VoIP nell'ufficio di casa richiede due canali proxy RTP. È richiesto un canale proxy RTP per la connessione da una linea ITSP al sistema OpenScape Business e un altro per la connessione da OpenScape Business tramite Internet al Client myPortal @work VoIP nell'ufficio di casa.

27.4 Valori massimi per funzione

I valori massimi qui indicati si riferiscono essenzialmente alla capacità del software OpenScape Business.

27.4.1 Connessione al provider di servizi

	X1W/R		X3W/R		X5W/R		X8W/R		Server (S)
	V2	V3	V2	V3	V2	V3	V2	V3	
Connessione ITSP (Internet Telephony Service Provider)									
Canali di linea SIP	30	120	60	120	60	120	60	120	180

	X1W/R		X3W/R		X5W/R		X8W/R		Server (S)
	V2	V3	V2	V3	V2	V3	V2	V3	
ITSP attivati simultaneamente	8	8	8	8	8	8	8	8	8
Route									
Route	16	16	16	16	16	16	16	16	16
Fascio di overflow per fascio	1	1	1	1	1	1	1	1	1

27.4.2 Utenti

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Numero telefonico utente/Numero selezione passante:					
Cifre per numero di telefono utente/numero interno	16 (predefinito = 3)	16 (predefinito = 3)	16 (predefinito = 3)	16 (predefinito = 3)	16 (predefinito = 3)

27.4.3 Livelli di espansione di UC Smart

- I livelli di espansione con schede madri V2 OCC sono disponibili in Tabella 45: Livello di espansione UC Smart con schede madri OCCx alla pagina 1442
- I livelli di espansione con schede madri V3 OCC sono disponibili in Tabella 46: Livello di espansione UC Smart con schede madri OCCSB/R, OCCMA/B o OCCLA alla pagina 1443
- I livelli di espansione con sistemi OpenScape Business S Server sono disponibili in Tabella 47: Livello di espansione UC Smart con OpenScape Business S alla pagina 1445

Tabella 45: Livello di espansione UC Smart con schede madri OCCx

	X1	X3W/R	X5W/R	X8
Utenti max UC Smart				
Numero massimo di utenti UC Smart (Account)	30	250/ 150/ 50[35]	250/ 150/ 50[35]	250/ 150/ 50[35]
Client UC Smart				
Numero di client UC attivi simultaneamente.[36]	30	500/ 300/ 150[35]	500/ 300/ 150[35]	500/ 300/ 150[35]
myPortal @work	30	250/ 150/ 50[35]	250/ 150/ 50[35]	250/ 150/ 50[35]
myPortal @work Chiamate parallele da VoIP a altre parti chiamate[37]	20	30	30	30

	X1	X3W/R	X5W/R	X8
myPortal to go[37]	30	150/ 150/ 50[35]	150/ 150/ 50[35]	150/ 150/ 50[35]
Deskphone CP 400/600/600E/ 700/700X/710 (modalità UC)	30	250/ 150/ 50[35]	250/ 150/ 50[35]	250/ 150/ 50[35]
OpenScape Business Attendant	8	8	8	8
Stato presenza				
Stato per utente	9	9	9	9
Annunci della casella vocale per stato presenza	1	1	1	1
Preferiti				
Preferiti per utente	100	100	100	100
Gruppi preferiti per utente	10	10	10	10
Registro chiamate				
Voci del diario chiamate per utente	100	100	100	100
Conferenza gestita da UC Smart (con UC Client)				
Numero di conferenze gestite	5	5	5	5
Numero di utenti per conferenza gestita	16	16	16	16
Canali per conferenze gestite	30	30	30	30

Tabella 46: Livello di espansione UC Smart con schede madri OCCSB/R, OCCMA/B o OCCLA

	X1W/R		X3W/R		X5		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Utenti max UC Smart								
Numero massimo di utenti UC Smart (Account)	150	150	150/500[39]	150/500[39]	150/500[39]	150/500[39]	500	500
Client UC Smart								

35 I valori sono scaglionati secondo la configurazione UC Booster: Booster Server / Booster Card / senza UC Booster

36 Somma di: myPortal @work, myPortal to go, CP 400/600/600E/700/700X/710 UC mode, Application Launcher, Business Attendant, TAPI 120 (WSI), Client WSI di terzi (Background: Diversi client con lo stesso account UC Smart possono connettersi al sistema)

37 Il numero di connessioni simultanee VoIP dell'utente dipende da:

1) i canali DSP disponibili nel sistema per le chiamate gateway (transizione IP/TDM)

2) i canali proxy RTP interni disponibili nel sistema per le chiamate VoIP tramite internet.

38 Il numero di connessioni simultanee dipendenti dai canali DSP disponibili nel sistema per le chiamate gateway (transizione IP/TDM)

	X1W/R		X3W/R		X5		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Numero di client UC attivi simultaneamente.[36]	150	150	150/500[39]	300/1000	150/500[39]	300/1000[39]	1000	1000
myPortal @work	150	150	150/250[39]	150/250[39]	150/250[39]	150/250[39]	250	250
myPortal @work Chiamate parallele da VoIP a altre parti chiamate[37]	150	150	30/70[39]	30/70[39]	30/70[39]	30/70[39]	70	70
myPortal to go[37]	150	150	150/500[39]	150/500[39]	150/500[39]	150/500[39]	500	500
myPortal for Teams	150	150	150/500[39]	150/500[39]	150/500[39]	150/500[39]	500	500
Deskphone CP 400/600/600E/ 700/700X/710 (modalità UC)	150	150	150/500[39]	150/500[39]	150/500[39]	150/500[39]	500	500
OpenScape Business Attendant	8	8	8	8	8	8	8	8
Stato presenza								
Stato per utente	9	9	9	9	9	9	9	9
Annunci della casella vocale per stato presenza	1	1	1	1	1	1	1	1
Preferiti								
Preferiti per utente	100	100	100	100	100	100	100	100
Gruppi preferiti per utente	10	10	10	10	10	10	10	10
Registro chiamate								
Voci del diario chiamate per utente	100	100	100	100	100	100	100	100
Conferenza gestita da UC Smart (con UC Client)								
Numero di conferenze gestite	5	5	5	5	5	5	5	5
Numero di utenti per conferenza gestita	16	16	16	16	16	16	16	16
Canali per conferenze gestite	30	30	30	30	30	30	30	30

[39] I valori sono scaglionati secondo la versione della scheda: Base/Avanzata

Tabella 47: Livello di espansione UC Smart con OpenScape Business S

	Server base (S)	Server standard (S)	Server avanzato (S)
Utenti max UC Smart			
Numero massimo di utenti UC Smart (Account)	50	500	1500
Client UC Smart			
Numero di client UC attivi simultaneamente.[36]	50	500	1500
myPortal @work	50	250	500
myPortal to go[37]	50	250	500
myPortal for Teams	50	250	500
Deskphone CP 400/600/600E/ 700/700X/710 (modalità UC)	50	250	500
OpenScape Business Attendant	8	8	8
Stato presenza			
Stato per utente	9	9	9
Annunci della casella vocale per stato presenza	1	1	1
Preferiti			
Preferiti per utente	100	100	100
Gruppi preferiti per utente	10	10	10
Registro chiamate			
Voci del diario chiamate per utente	100	100	100
Conferenza gestita da UC Smart (con UC Client)			
Numero di conferenze gestite	10	10	10
Numero di utenti per conferenza gestita	16	16	16
Canali per conferenze gestite	30	30	30

27.4.4 Livelli di espansione di Smart Voicemail

- I livelli di espansione con schede madri V2 OCC sono disponibili in Tabella 48: Livello di espansione Smart Voicemail con schede madri OCCx alla pagina 1446
- I livelli di espansione con schede madri V3 OCC sono disponibili in Tabella 49: Livello di espansione Smart Voicemail con schede madri OCCSB/R, OCCMA/B o OCCLA alla pagina 1446

- I livelli di espansione con sistemi OpenScape Business S Server sono disponibili in Tabella 50: Livello di espansione Smart Voicemail con OpenScape Business S alla pagina 1447

Tabella 48: Livello di espansione Smart Voicemail con schede madri OCCx

	X1	X3W/R	X5W/R	X8	Server (S)
Smart Voicemail					
Caselle Smart Voicemail	30	320	320	320	1500
Messaggi per casella vocale	100	100	100	100	100
Durata della registrazione per chiamata (minuti)	2	2	2	2	2
Capacità di registrazione totale in ore	32	32	32	32	32
Connessioni Voicemail simultanee (canali)	10	10	10	10	60
Annunci	16	16	16	16	16
Company/ Auto Attendant	100	100	100	100	100
Company/ Auto Attendant (attivi simultaneamente)	6	6	6	6	6

Tabella 49: Livello di espansione Smart Voicemail con schede madri OCCSB/R, OCCMA/B o OCCLA

	X1W/R		X3W/R	X5W/R		X8		
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Smart Voicemail								
Caselle Smart Voicemail	320	320	320/500[40]	320/500[40]	320/500[40]	320/500[40]	500	500
Messaggi per casella vocale	100	100	100	100	100	100	100	100
Durata della registrazione per chiamata (minuti)	2	4	4	4	4	4	4	4
Capacità di registrazione totale in ore	32	64	32	64	32	64	32	64
Connessioni Voicemail simultanee (canali)	30	30	30	30	30	30	30	30
Annunci	16	16	16	16	16	16	16	16
Company/ Auto Attendant	100	100	100	100	100	100	100	100
Company/ Auto Attendant (attivi simultaneamente)	6	6	6	6	6	6	6	6

Tabella 50: Livello di espansione Smart Voicemail con OpenScape Business S

	Server base (S)	Server standard (S)	Server avanzato (S)
Smart Voicemail			
Caselle Smart Voicemail	1500	1500	1500
Messaggi per casella vocale	100	100	100
Durata della registrazione per chiamata (minuti)	4	4	4
Capacità di registrazione totale in ore	64	64	64
Connessioni Voicemail simultanee (canali)	60	60	60
Annunci	16	16	16
Company/ Auto Attendant	100	100	100
Company/ Auto Attendant (attivi simultaneamente)	6	6	6

27.4.5 Livelli di espansione di UC Suite

- I livelli di espansione con schede madri V2 OCC sono disponibili in Tabella 51: Livello di espansione UC Suite con schede madri V2 alla pagina 1447
- I livelli di espansione con schede madri V3 OCC sono disponibili in Tabella 52: Livello di espansione UC Suite con schede madri OCCSB, OCCMA/B o OCCLA alla pagina 1450
- I livelli di espansione con sistemi OpenScape Business S Server sono disponibili in Tabella 53: Livello di espansione UC Suite con OpenScape Business S alla pagina 1454

Tabella 51: Livello di espansione UC Suite con schede madri V2

	X1	X3W/R	X5W/R	X8	Server (S)
Utenti max UC Suite					
Numero massimo di utenti UC Suite (Account)	-	250/ 150/ 0[41]	250/ 150/ 0[41]	250/ 150/ 0[41]	1500
Client UC Suite					
Numero di client UC attivi simultaneamente.[42]	-	500/ 150/ 0[41]	500/ 150/ 0[41]	500/ 150/ 0[41]	1500
myPortal for Desktop	-	500/ 150/ 0[41]	500/ 150/ 0[41]	500/ 150/ 0[41]	1500
myPortal for Outlook	-	500/ 150/ 0[41]	500/ 150/ 0[41]	500/ 150/ 0[41]	1500
myAgent (attivi simultaneamente)	-	64	64	64	64

40 I valori sono scaglionati secondo la versione della scheda: Base/Avanzata

	X1	X3W/R	X5W/R	X8	Server (S)
myAgent (configurabile)	-	192	192	192	192
myReports	-	1	1	1	1
myAttendant	-	20	20	20	20
myPortal @work	-	250/ 150/ 0[41]	250/ 150/ 0[41]	250/ 150/ 0[41]	250
myPortal @work Chiamate parallele da VoIP a altre parti chiamate[44]	-	30	30	30	60
myPortal to go[44]	-	150/ 150/ 0[41]	150/ 150/ 0[41]	150/ 150/ 0[41]	250
Deskphone 400/600/600E/700/700X/710	-	250/ 150/ 0[41]	250/ 150/ 0[41]	250/ 150/ 0[41]	250
OpenScape Business Attendant	-	8	8	8	8
Stato presenza					
Stato per utente UC Suite	-	9	9	9	9
Annunci della casella vocale per stato presenza	-	1	1	1	1
Diario delle chiamate (myPortal for Desktop / myPortal for Outlook)					
Durata dell'archiviazione nei client UC (giorni)	-	30 predefinito = 30	30 predefinito = 30	30 predefinito = 30	30 predefinito = 30
Durata dell'archiviazione nel sistema di comunicazione	-	365 predefinito = 30	365 predefinito = 30	365 predefinito = 30	365 predefinito = 30
Voci del Diario chiamate[46]	-	Abilitato[46]	Abilitato[46]	Abilitato[46]	Abilitato[46]
Voci del Diario chiamate myPortal for Desktop modern GUI	-	100 dopo l'avvio >100 durante il funzionamento	100 dopo l'avvio >100 durante il funzionamento	100 dopo l'avvio >100 durante il funzionamento	100 dopo l'avvio >100 durante il funzionamento
Casella vocale UC Suite					
Box VM	-	500/ 500/ 0[45]	500/ 500/ 0[45]	500/ 500/ 0[45]	1500
Gruppi VM	-	20/ 20/ 0	20/ 20/ 0	20/ 20/ 0	20
Messaggi per casella vocale[46]	-	n/a	n/a	n/a	n/a
Durata della registrazione per chiamata (minuti)	-	15	15	15	15
Durata della registrazione che può essere inoltrata via e-mail (minuti)[47]	-	~10	~10	~10	~10

	X1	X3W/R	X5W/R	X8	Server (S)
Capacità di registrazione totale (ore)[46]	-	n/a	n/a	n/a	n/a
Connessioni simultanee a voicemail (Canali MEB)	-	30	30	30	60
UC Suite AutoAttendant					
Personal Auto Attendant	-	20/ 20/ 0[41]	20/ 20/ 0[41]	20/ 20/ 0[41]	20
Posto operatore automatico azienda	-	1/ 1/ 0[41]	1/ 1/ 0[41]	1/ 1/ 0[41]	1
Chat Multiutente (Instant messaging)					
Interlocutori interni	-	illimitato	illimitato	illimitato	illimitato
Interlocutore esterno (XMPP)	-	-	-	-	-
Annunci per utente UC Suite					
Annunci di benvenuto	-	1/ 1/ 0[41]	1/ 1/ 0[41]	1/ 1/ 0[41]	1
Annunci basati sullo stato di presenza	-	1/ 1/ 0[41]	1/ 1/ 0[41]	1/ 1/ 0[41]	1
Annuncio Personal Auto Attendant	-	1/ 1/ 0[41]	1/ 1/ 0[41]	1/ 1/ 0[41]	1
Registrazione della chiamata UC Suite					
Durata della registrazione per chiamata/conferenza	-	Limitata dalla durata della chiamata	Limitata dalla durata della chiamata	Limitata dalla durata della chiamata	Limitata dalla durata della chiamata
Fax UC Suite					
Caselle Fax	-	500/ 150/ 0[41]	500/ 150/ 0[41]	500/ 150/ 0[41]	1500
Gruppi di caselle fax	-	60/ 60/ 0[41]	60/ 60/ 0[41]	60/ 60/ 0[41]	60
Utenti per gruppo di caselle fax	-	10/ 10/ 0[41]	10/ 10/ 0[41]	10/ 10/ 0[41]	10
Lunghezza del fax in pagine	-	500/ 500/ 0[41]	500/ 500/ 0[41]	500/ 500/ 0[41]	500
Fax T.38 simultanei	-	8/ 3/ 0[41]	8/ 3/ 0[41]	8/ 3/ 0[41]	8
Destinatari fusione fax	-	Abilitato	Abilitato	Abilitato	Abilitato
Conferenze UC Suite					
Conferenze simultanee UC Suite	-	5/ 5/ 0[41]	5/ 5/ 0[41]	5/ 5/ 0[41]	10
Partecipanti per conferenza UC Suite	-	16/ 16/ 0[41]	16/ 16/ 0[41]	16/ 16/ 0[41]	16
Utenti partecipanti esterni per conferenza UC Suite	-	15/ 15/ 0[41]	15/ 15/ 0[41]	15/ 15/ 0[41]	15
Numero max. canali per conferenze UC Suite	-	30/ 30/ 0[41]	30/ 30/ 0[41]	30/ 30/ 0[41]	60

	X1	X3W/R	X5W/R	X8	Server (S)
Numero di canali riservati per conferenze UC Suite Ad Hoc e Meet Me	-	20/ 20/ 0[41]	20/ 20/ 0[41]	20/ 20/ 0[41]	60
Connettività database esterno (LDAP)					
Connessioni database esterno di UC Server	-	10/ 10/ 0[41]	10/ 10/ 0[41]	10/ 10/ 0[41]	10

Tabella 52: Livello di espansione UC Suite con schede madri OCCSB, OCCMA/B o OCCLA

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Utenti max UC Suite						
Numero massimo di utenti UC Suite (Account)	-	50/ 500[48] 300 in caso di Contact Center	-	50/ 500[48]	-	500 300 in caso di Contact Center
Client UC Suite						
Numero di client UC attivi simultaneamente.[42]	-	100/ 1000[48] 600 in caso di Contact Center	-	100/ 1000[48] 600 in caso di Contact Center	-	1000 600 in caso di Contact Center

41 I valori sono scaglionati secondo la configurazione UC Booster: Booster Server / Booster Card / senza UC Booster

42 Somma di: myPortal Desktop, myPortal for Outlook, myAttendant, myAgent, myReports, myPortal @work, myPortal to go, myPortal for Teams, CP 400/600/600E/700/700X/710 UC mode (Background: Diversi client con lo stesso account UC Suite possono connettersi al sistema)

43 Il valore inferiore si applica ai sistemi con UC Suite Contact Center

44 Il numero di connessioni simultanee VoIP dell'utente dipende da

1) i canali DSP disponibili nel sistema per le chiamate gateway (transizione IP/TDM)

2) i canali proxy RTP interni disponibili nel sistema per le chiamate VoIP tramite internet.

45 La UC Booster Card supporta un massimo di 500 caselle VM, a prescindere dal limite di client UC Suite (150 utenti).

46 Il valore dipende dalla capacità di stoccaggio disponibile su HD / SSD. Non è implementato un limite rispetto all'utente.

1) Voicemail / Registrazioni: Un minuto di registrazione utilizza circa 1MB di memoria

2) Fax: Un fax standard (2 pagine DIN A4) corrisponde a circa 48 kB di memoria

Esempio: La dimensione della partizione di memoria per la registrazione di annunci vocali, messaggi vocali, registrazioni vocali e fax è di 20 GB per un disco rigido da 160 GB. Ciò corrisponde a un tempo di registrazione totale di circa 20.000 minuti.

47 In caso di registrazioni più lunghe, la registrazione è divisa e inviata in più file.

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
myPortal for Desktop	-	50/ 500[48] 300 in caso di Contact Center	-	50/ 500[48] 300 in caso di Contact Center	-	500 300 in caso di Contact Center
myPortal for Outlook	-	50/ 500[48] 300 in caso di Contact Center	-	50/ 500[48] 300 in caso di Contact Center	-	500 300 in caso di Contact Center
myAgent (attivi simultaneamente)	-	0/ 64[48]	-	0/ 64[48]	-	64
myAgent (configurabile)	-	0/ 192[48]	-	0/ 192[48]	-	192
myReports	-	0/ 1[48]	-	0/ 1[48]	-	1
myAttendant	-	4/ 20[48]	-	4/ 20[48]	-	20
myPortal @work	-	50/ 250[48] 300 in caso di Contact Center	-	50/ 250[48] 300 in caso di Contact Center	-	250 300 in caso di Contact Center
myPortal @work Chiamate parallele da VoIP a altre parti chiamate[44]	-	30/ 70[48]	-	30/ 70[48]	-	70
myPortal to go[44]	-	50/ 500[48] 300 in caso di Contact Center	-	50/ 500[48] 300 in caso di Contact Center	-	500 300 in caso di Contact Center
myPortal for Teams	-	50/ 500[48] 300 in caso di Contact Center	-	50/ 500[48] 300 in caso di Contact Center	-	500 300 in caso di Contact Center
Deskphone CP 400/600/600E/ 700/700X/710	-	50/ 500[48] 300 in caso di Contact Center	-	50/ 500[48] 300 in caso di Contact Center	-	500 300 in caso di Contact Center
OpenScape Business Attendant	-	8	-	8	-	8
Stato presenza						
Stato per utente UC Suite	-	9	-	9	-	9

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Annunci della casella vocale per stato presenza	-	1	-	1	-	1
Diario delle chiamate (myPortal for Desktop / myPortal for Outlook)						
Durata dell'archiviazione nei client UC (giorni)	-	30 predefinito = 30	-	30 predefinito = 30	-	30 predefinito = 30
Durata dell'archiviazione nel sistema di comunicazione	-	365 predefinito = 30	-	365 predefinito = 30	-	365 predefinito = 30
Voci del Diario chiamate[46]	-	Abilitato[46]	-	Abilitato[46]	-	Abilitato[46]
Voci del Diario chiamate myPortal for Desktop modern GUI	-	100 dopo l'avvio >100 durante il funzionamento	-	100 dopo l'avvio >100 durante il funzionamento	-	100 dopo l'avvio >100 durante il funzionamento
Casella vocale UC Suite						
Box VM	-	50/ 500[48]	-	50/ 500[48]	-	500
Gruppi VM	-	32	-	32	-	32
Messaggi per casella vocale[46]	-	n/a	-	n/a	-	n/a
Durata della registrazione per chiamata (minuti)	-	15	-	15	-	15
Durata della registrazione che può essere inoltrata via e-mail (minuti)[47]	-	~10	-	~10	-	~10
Capacità di registrazione totale (ore)[46]	-	n/a	-	n/a	-	n/a
Connessioni simultanee a voicemail (Canali MEB)	-	30/ 60[48]	-	30/ 60[48]	-	60
UC Suite AutoAttendant						
Personal Auto Attendant	-	20	-	20	-	20
Posto operatore automatico azienda	-	1	-	1	-	1
Chat Multiutente (Instant messaging)						
Interlocutori interni	-	illimitato	-	illimitato	-	illimitato

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Annunci per utente UC Suite						
Annunci di benvenuto	-	1	-	1	-	1
Annunci basati sullo stato di presenza	-	1	-	1	-	1
Annuncio Personal Auto Attendant	-	1	-	1	-	1
Registrazione della chiamata UC Suite						
Durata della registrazione per chiamata/conferenza	-	Limitata dalla durata della chiamata	-	Limitata dalla durata della chiamata	-	Limitata dalla durata della chiamata
Fax UC Suite						
Caselle Fax	-	50/ 500[48]	-	50/ 500[48]	-	500
Gruppi di caselle fax	-	60	-	60	-	60
Utenti per gruppo di caselle fax	-	10	-	10	-	10
Lunghezza del fax in pagine	-	500	-	500	-	500
Fax T.38 simultanei	-	3/ 8[48]	-	3/ 8[48]	-	8
Destinatari fusione fax	-	Abilitato	-	Abilitato	-	Abilitato
Conferenze UC Suite						
Conferenze simultanee UC Suite	-	5	-	5	-	5
Partecipanti per conferenza UC Suite	-	16	-	16	-	16
Utenti partecipanti esterni per conferenza UC Suite	-	15	-	15	-	15
Numero max. canali per conferenze UC Suite	-	30	-	30	-	30
Numero di canali riservati per conferenze UC Suite Ad Hoc e Meet Me	-	20	-	20	-	20
Connettività database esterno (LDAP)						
Connessioni database esterno di UC Server	-	10	-	10	-	10

[48] I valori sono scaglionati secondo la versione della scheda: Base/Avanzata

Tabella 53: Livello di espansione UC Suite con OpenScape Business S

	Server base (S)	Server standard (S)	Server avanzato (S)
Utenti max UC Suite			
Numero massimo di utenti UC Suite (Account)	150	500	1500
Client UC Suite			
Numero di client UC attivi simultaneamente.[42]	150	500	1500
myPortal for Desktop	50	500	1500
myPortal for Outlook	50	500	1500
myAgent (attivi simultaneamente)	0	64	64
myAgent (configurabile)	0	192	192
myReports	1	1	1
myAttendant	20	20	20
myPortal @work	50	250	500
myPortal @work Chiamate parallele da VoIP a altre parti chiamate[44]	30	60	60
myPortal to go[44]	50	250	500
myPortal for Teams	50	250	500
Deskphone CP 400/600/600E/ 700/700X/710	50	250	500
OpenScape Business Attendant	8	8	8
Stato presenza			
Stato per utente UC Suite	9	9	9
Annunci della casella vocale per stato presenza	1	1	1
Diario delle chiamate (myPortal for Desktop / myPortal for Outlook)			
Durata dell'archiviazione nei client UC (giorni)	30 predefinito = 30	30 predefinito = 30	30 predefinito = 30
Durata dell'archiviazione nel sistema di comunicazione	365 predefinito = 30	365 predefinito = 30	365 predefinito = 30
Voci del Diario chiamate[46]	Abilitato[46]	Abilitato[46]	Abilitato[46]

	Server base (S)	Server standard (S)	Server avanzato (S)
Voci del Diario chiamate myPortal for Desktop modern GUI	100 dopo l'avvio >100 durante il funzionamento	100 dopo l'avvio >100 durante il funzionamento	100 dopo l'avvio >100 durante il funzionamento
Casella vocale UC Suite			
Box VM	150	500	1500
Gruppi VM	32	32	32
Messaggi per casella vocale[46]	n/a	n/a	n/a
Durata della registrazione per chiamata (minuti)	15	15	15
Durata della registrazione che può essere inoltrata via e-mail (minuti)[47]	~10	~10	~10
Capacità di registrazione totale (ore)[46]	n/a	n/a	n/a
Connessioni simultanee a voicemail (Canali MEB)	60	60	60
UC Suite AutoAttendant			
Personal Auto Attendant	20	20	20
Posto operatore automatico azienda	1	1	1
Chat Multiutente (Instant messaging)			
Interlocutori interni	illimitato	illimitato	illimitato
Annunci per utente UC Suite			
Annunci di benvenuto	1	1	1
Annunci basati sullo stato di presenza	1	1	1
Annuncio Personal Auto Attendant	1	1	1
Registrazione della chiamata UC Suite			
Durata della registrazione per chiamata/ conferenza	Limitata dalla durata della chiamata	Limitata dalla durata della chiamata	Limitata dalla durata della chiamata
Fax UC Suite			
Caselle Fax	1500	1500	1500
Gruppi di caselle fax	60	60	60
Utenti per gruppo di caselle fax	10	10	10
Lunghezza del fax in pagine	500	500	500
Fax T.38 simultanei	8	8	8
Destinatari fusione fax	Abilitato	Abilitato	Abilitato
Conferenze UC Suite			
Conferenze simultanee UC Suite	10	10	10
Partecipanti per conferenza UC Suite	16	16	16

	Server base (S)	Server standard (S)	Server avanzato (S)
Utenti partecipanti esterni per conferenza UC Suite	15	15	15
Numero max. canali per conferenze UC Suite	60	60	60
Numero di canali riservati per conferenze UC Suite Ad Hoc e Meet Me	60	60	60
Connettività database esterno (LDAP)			
Connessioni database esterno di UC Server	10	10	10

27.4.6 Funzioni del telefono

	X1W/R	X3W/R	X5W/R	X8W/R	Server (S)
Lista dei chiamanti per telefoni del sistema (HFA)					
Liste dei chiamanti per sistema	650	650	650	650	1300
Liste dei chiamanti per utente nel sistema	1	1	1	1	1
Voci per lista chiamate	10	10	10	10	10
Cifre salvate per voce più codice del fascio	25 + (6)	25 + (6)	25 + (6)	25 + (6)	25 + (6)
Tasti per chiamata diretta (tasti DSS):					
Moduli aggiuntivi per sistema di comunicazione	250	250	250	250	250
Moduli aggiuntivi per telefono	2	2	2	2	2
Tasti per modulo aggiuntivo OpenStage	12	12	12	12	12
Tasti per modulo aggiuntivo OpenStage 15	18	18	18	18	18
Campi lampade di occupato (BLF) per sistema di comunicazione	12	25	25	25	25
Tasti per campi lampade di occupato	90	90	90	90	90
Selezione breve individuale (KWI)					
Voci nel pool di selezione breve personale per sistema di comunicazione	2000	2000	2000	2000	2000
Voci per utente	10	10	10	10	10
Cifre per voce (più codice del fascio)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)

	X1W/R	X3W/R	X5W/R	X8W/R	Server (S)
Selezione breve del sistema (KWZ)					
Voci nel pool di selezione breve personale per sistema di comunicazione	8000	8000	8000	8000	8000
Lunghezza in caratteri del nome	16	16	16	16	16
Cifre per voce (più codice del fascio)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Ripetizione della selezione					
Voci per OpenStage 20/ 20E/ 20G/ 40/ 40G	3	3	3	3	3
Voci per OpenStage 15	10	10	10	10	10
Voci per OpenStage 60/ 60G/ 80/ 80G	30	30	30	30	30
Voci per telefono senza display	1	1	1	1	1
Cifre salvate per voce	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Tonalità avviso di chiamata in attesa/Segnalazione della chiamata					
Chiamante in attesa per telefono	16				
Parcheggio					
Posizioni di parcheggio per sistema	10				
Richiamate					
Voci richiamata per telefono	5				
Testi di assenza/messaggi					
Testi di assenza per sistema	250	250	250	250	250
Messaggi per sistema	150	150	150	150	150
Testi di assenza + messaggi configurabili per sistema	10 + 10	10 + 10	10 + 10	10 + 10	10 + 10
Lunghezza in caratteri di un testo di assenza/messaggio configurabile	24	24	24	24	24
Testi di assenza ricevuti/ messaggi per telefono con display	5	5	5	5	5
Testi di assenza ricevuti/ messaggi per telefono senza display	1	1	1	1	1
Segnalaz. ampliata					

	X1W/R	X3W/R	X5W/R	X8W/R	Server (S)
utent. incl. segnal.chiam.	5				
Inoltro di chiamata (CF)					
Destinazioni AUL per telefono	4	4	4	4	4
Cifre per destinazione CFW esterna (più codice del fascio)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Destinazione AUL concatenate					5
Conferenze controllate dal sistema					
Conferenze del sistema simultanee per sistema	10	10	10	10	8
Utenti per conferenza	8	8	8	8	8
Utenti esterni per conferenza	7	7	7	7	7
Canali conferenza	32	32	32	32	20
Citofono/apriporta					
Connessioni tramite interfacce a/b per sistema	4	4	4	4	-
Cifre per codice	5	5	5	5	-
Prenotazione linea					
Voci simultanee per sistema	32	32	32	32	-

Nota: Per gli scenari di inoltro di chiamata sopra descritti, gli utenti possono acquisire solo una destinazione di inoltro per MSN. Possono essere inoltrati fino a 10 MSN.

In caso di connessione ITSP o ISDN configurata con numero di selezione passante, tale numero è 249.

27.4.7 Lavoro in team (Gruppi)

- Le informazioni sulle schede madri V2 OCC sono disponibili in Tabella 54: Dati per schede madri V2 alla pagina 1458
- Le informazioni sulle schede madri V3 OCC sono disponibili in Tabella 55: Dati per schede madri V3 alla pagina 1460
- Le informazioni sui sistemi OpenScape Business S Server sono disponibili in Tabella 56: Dati per OpenScape Business S alla pagina 1462

Tabella 54: Dati per schede madri V2

	X1	X3W/R	X5W/R	X8
Gruppi di risposta per assente				
Gruppi di risposta per sistema	32	32	32	32

	X1	X3W/R	X5W/R	X8
Utenti per gruppo di risposta per assente	32	32	32	32
Suoneria (gruppo configurabile dall'utente)				
Numero di estensioni nel gruppo suoneria	5	5	5	5
Chiamate di gruppo, gruppi di ricerca, Basic MULAP				
Totale chiamate di gruppo, gruppi di ricerca, Basic MULAP, Direttore MULAP e gruppi Casella vocale per sistema di comunicazione	800	800	800	800
Lunghezza del nome del gruppo	16	16	16	16
Numero di gruppi ai quali può essere assegnato un utente	32	32	32	32
Utenti per chiamata di gruppo, gruppo di ricerca, basic MULAP	20	20	20	20
Executive MULAP, gruppi Team, gruppi Top e gruppi Voicemail:				
Numero totale di gruppi Executive MULAP, Team e Top per	500	500	500	500
Utenti per direttore MULAP, gruppo Team, gruppo Top	10	10	10	10
Tasti MULAP per telefono	10	10	10	10
Gruppi casella vocale				
Numero di gruppi Voicemail	20	20	20	20
Utenti per gruppo casella vocale	20	20	20	20
Paginazione interna (Voice Paging)				
Paging simultanei per sistema di comunicazione	1	1	1	1
Destinatario del paging interno	20	20	20	20
Gruppi UCD				
Gruppi UCD per sistema	60	60	60	60
Annunci per gruppo UCD	7	7	7	7
Livelli di priorità per gruppo UCD	10	10	10	10
Chiamate in coda per gruppo UCD (ultimo gruppo max 72)	30	30	30	30
Agenti UCD				
ID agenti UCD per sistema di comunicazione	330	330	330	330
Agenti UCD attivi contemporaneamente per sistema di comunicazione	64	64	64	64

	X1	X3W/R	X5W/R	X8
Annunci UCD				
Chiamanti, per sistema di comunicazione, a cui è possibile trasmettere contemporaneamente un annuncio	8	8	8	8

Tabella 55: Dati per schede madri V3

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Gruppi di risposta per assente								
Gruppi di risposta per sistema	64	64	64/128[49]	64/128[49]	64/128[49]	64/128[49]	128	128
Utenti per gruppo di risposta per assente	32	32	32	32	32	32	32	32
Suoneria (gruppo configurabile dall'utente)								
Numero di estensioni nel gruppo suoneria	5	5	5	5	5	5	5	5
Chiamate di gruppo, gruppi di ricerca, Basic MULAP								
Totale chiamate di gruppo, gruppi di ricerca, Basic MULAP, Direttore MULAP e gruppi Casella vocale per sistema di comunicazione	800	800	800	800	800	800	800	800
Lunghezza del nome del gruppo	16	16	16	16	16	16	16	16
Numero di gruppi ai quali può essere assegnato un utente	32	32	32	32	32	32	32	32
Utenti per chiamata di gruppo, gruppo di ricerca, basic MULAP	20	20	20/32[49]	20/32[49]	20/32[49]	20/32[49]	32	32
Executive MULAP, gruppi Team, gruppi Top e gruppi Voicemail:								
Numero totale di gruppi Executive MULAP, Team e Top per	500	500	500	500	500	500	500	500
Utenti per direttore MULAP, gruppo Team, gruppo Top	10	10	10	10	10	10	10	10

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Tasti MULAP per telefono	10	10	10	10	10	10	10	10
Gruppi casella vocale								
Numero di gruppi Voicemail	20	20	20	20	20	20	20	20
Utenti per gruppo casella vocale	20	20	20	20	20	20	20	20
Paginazione interna (Voice Paging)								
Paging simultanei per sistema di comunicazione	1	1	1	1	1	1	1	1
Destinatario del paging interno	20	20	20/32[49]	20/32[49]	20/32[49]	20/32[49]	32	32
Gruppi UCD								
Gruppi UCD per sistema	60	60	60	60	60	60	60	60
Annunci per gruppo UCD	7	7	7	7	7	7	7	7
Livelli di priorità per gruppo UCD	10	10	10	10	10	10	10	10
Chiamate in coda per gruppo UCD (ultimo gruppo max 72)	30	30	30	30	30	30	30	30
Agenti UCD								
ID agenti UCD per sistema di comunicazione	330	330	330	330	330	330	330	330
Agenti UCD attivi contemporaneamente per sistema di comunicazione	64	64	64	64	64	64	64	64
Annunci UCD								
Chiamanti, per sistema di comunicazione, a cui è possibile trasmettere contemporaneamente un annuncio	8	8	8	8	8	8	8	8

[49] I valori sono scaglionati secondo la versione della scheda: Base/Avanzata

Tabella 56: Dati per OpenScape Business S

	Server base (S)	Server standard (S)	Server avanzato (S)
Gruppi di risposta per assente			
Gruppi di risposta per sistema	32	64	128
Utenti per gruppo di risposta per assente	32	32	32
Suoneria (gruppo configurabile dall'utente)			
Numero di estensioni nel gruppo suoneria	5	5	5
Chiamate di gruppo, gruppi di ricerca, Basic MULAP			
Totale chiamate di gruppo, gruppi di ricerca, Basic MULAP, Direttore MULAP e gruppi Casella vocale per sistema di comunicazione	800	800	800
Lunghezza del nome del gruppo	16	16	16
Numero di gruppi ai quali può essere assegnato un utente	32	32	32
Utenti per chiamata di gruppo, gruppo di ricerca, basic MULAP	32	32	32
Executive MULAP, gruppi Team, gruppi Top e gruppi Voicemail:			
Numero totale di gruppi Executive MULAP, Team e Top per	500	500	500
Utenti per direttore MULAP, gruppo Team, gruppo Top	10	10	10
Tasti MULAP per telefono	10	10	10
Gruppi casella vocale			
Numero di gruppi Voicemail	20	20	20
Utenti per gruppo casella vocale	20	20	20
Paginazione interna (Voice Paging)			
Paging simultanei per sistema di comunicazione	1	1	1
Destinatario del paging interno	20	20	20
Gruppi UCD			
Gruppi UCD per sistema	60	60	60
Annunci per gruppo UCD	7	7	7
Livelli di priorità per gruppo UCD	10	10	10
Chiamate in coda per gruppo UCD (ultimo gruppo max 72)	30	30	30
Agenti UCD			
ID agenti UCD per sistema di comunicazione	330	330	330

	Server base (S)	Server standard (S)	Server avanzato (S)
Agenti UCD attivi contemporaneamente per sistema di comunicazione	64	64	64
Annunci UCD			
Chiamanti, per sistema di comunicazione, a cui è possibile trasmettere contemporaneamente un annuncio	8	8	8

27.4.8 Routing delle chiamate

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Instradamento a minor costo (LCR)					
Cifre selezionate	24	24	24	24	24
Cifre verificate	24	24	24	24	24
Piani di composizione (max 10 campi per piano)	1000	1000	1000	1000	1000
Tabelle rotte	254	254	254	254	254
Rotte per tabella delle rotte	16	16	16	16	16
Regole di selezione per ogni fascio	254	254	254	254	254
Numero di fusi orari per giorno/settimana	8	8	8	8	8
Cifre per regola di composizione	40	40	40	40	40
Servizio notturno					
Utenti abilitati per sistema	5	5	5	5	5
Servizio d'emergenza E911 (solo per gli USA)					
Cifre per LIN (Location Identification Number)	16	16	16	16	16
Hotline a tempo/Hotline					
Destinazioni Hotline per sistema di comunicazione	6	6	6	6	6
Gruppi con restrizioni di traffico					
Gruppi con restrizioni di traffico per sistema	64	64	64	64	64

Partecipanti per schede madri V2

	X1	X3W/R	X5W/R	X8	Server (S)
myAttendant					

	X1	X3W/R	X5W/R	X8	Server (S)
myAttendant (UC Suite) per sistema	-	20	20	20	20
AutoAttendant (UC Smart)					
Company Auto-Attendant	100	100	100	100	100
AutoAttendant (UC Suite)					
Posto operatore automatico	-	20/ 20/ 0[50]	20/ 20/ 0[50]	20/ 20/ 0[50]	20
OpenScape Business Attendant					
OpenScape Business Attendant per sistema	-	8	8	8	8

Partecipanti per schede madri V3

	X1W/R	X3W/R	X5W/R	X8	Server (S)
myAttendant					
myAttendant (UC Suite) per sistema	4	4/20[51]	4/20[51]	20	20
AutoAttendant (UC Smart)					
Company Auto-Attendant	100	100	100	100	100
AutoAttendant (UC Suite)					
Posto operatore automatico	20	20/ 20/[51]	20/20[51]	20/20[51]	20
OpenScape Business Attendant					
OpenScape Business Attendant per sistema	8	8	8	8	8

27.4.9 Contact Center multimediale

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Code Contact Center					
Code d'attesa per sistema di comunicazione	-	50	50	50	50
Post- elaborazione					
Codici post-elaborazione	-	Abilitato	Abilitato	Abilitato	Abilitato
Agenti					
Agenti attivi simultaneamente	-	64	64	64	64
Agenti (configurabile)	-	192	192	192	192

50 I valori sono scaglionati secondo la configurazione UC Booster: Booster Server / Booster Card / senza UC Booster. Per le schede madri V3, è valido il valore più alto.

51 I valori sono scaglionati secondo la versione della scheda: Base/Avanzata

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Reporting storico					
myReports Clients attivi simultaneamente per sistema	-	1	1	1	1

27.4.10 Limiti di espansioni Mobility

Tabella 57: Dati per schede madri V2 OCC

	X1	X3W/R	X5W/R	X8
Postazioni per operatore remoto				
Postazioni per operatore remoto tramite VPN per sistema di comunicazione	10	10	10	10
Utenti Mobility				
Utenti Mobility Entry per sistema	30	150	150	150
myPortal to go (UC Smart): utenti per sistema	30	150/ 150/ 50[52]	150/ 150/ 50[52]	150/ 150/ 50[52]
myPortal to go (UC Suite): utenti per sistema	-	150/ 150/ 0[52]	150/ 150/ 0[52]	150/ 150/ 0[52]

Tabella 58: Dati per schede madri V3 OCC

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Postazioni per operatore remoto								
Postazioni per operatore remoto tramite VPN per sistema di comunicazione	10	10	10	10	10	10	10	10
Utenti Mobility								
Utenti Mobility Entry per sistema	150/500[53]	150/500[53]	150	150/500[53]	150/500[53]	150/500[53]	500	500
myPortal to go (UC Smart): utenti per sistema	150	150	150/500[53]	150/500[53]	150/500[53]	150/500[53]	500	500

[52] I valori sono scaglionati secondo la configurazione UC Booster: Booster Server / Booster Card / senza UC Booster

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
myPortal to go (UC Suite): utenti per sistema	-	50	-	50/500 300 in caso di Contact Center	-	50/500 300 in caso di Contact Center	-	500 300 in caso di Contact Center
myPortal for Teams (UC Smart): utenti per sistema	150	150	150/500[53]	150/500[53]	150/500[53]	150/500[53]	500	500
myPortal for Teams (UC Suite): utenti per sistema	-	50	-	50/500 300 in caso di Contact Center	-	50/500 300 in caso di Contact Center	-	500 300 in caso di Contact Center

Tabella 59: Dati per OpenScape Business S

	Server base (S)	Server standard (S)	Server avanzato (S)
Utenti Mobility			
Utenti Mobility Entry per sistema	50	150	150
myPortal to go (UC Smart): utenti per sistema	50	250	500
myPortal to go (UC Suite): utenti per sistema	50	250	500
myPortal for Teams (UC Smart): utenti per sistema	50	250	500
myPortal for Teams (UC Suite): utenti per sistema	50	250	500

27.4.11 Sicurezza

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Codice di blocco individuale					
Cifre per codice del telefono	5	5	5	5	5
Caratteri consentiti	0-9	0 – 9	0 – 9	0 – 9	0 – 9
Controllo della selezione					
Numero di liste consentite	6	6	6	6	6
Numero di liste negate	6	6	6	6	6

53 I valori sono scaglionati secondo la versione della scheda: Base/Avanzata

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Lista consentita, breve (10 voci di 32 cifre ciascuna)	5	5	5	5	5
Lista consentita, lunga (100 voci di 32 cifre ciascuna)	1	1	1	1	1
Lista negata, breve (10 voci di 32 cifre ciascuna)	5	5	5	5	5
Lista negata, lunga (50 voci di 32 cifre ciascuna)	1	1	1	1	1
Classi di servizio					
Classi di servizio per sistema	15	15	15	15	15
Dimensione matrice – giorno e notte – numero di linee	30	30	30	30	30
Liste consentite e negate	15	15	15	15	15
Gruppi utilizzati chiusi (gruppi ITR – Gruppi VBZ)					
Gruppi ITR per sistema	16	64	64	64	64
Dimensione matrice – giorno e notte – numero di linee	30	30	30	30	30
Liste consentite e negate	15	15	15	15	15

27.4.12 Connessione in rete di OpenScape Business

Connessione in rete di X1W/R, OpenScape Business X3R/X3W, OpenScape Business X5R/X5W, OpenScape Business X8, OpenScape Business S: Limiti di configurazione diversi per le reti possono essere richiesti tramite release specifica. Fare riferimento alle release di vendita correnti.

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Connessione in rete di OpenScape Business					
Sistemi di comunicazione collegati in rete (nodi)	8/32[54]	8/32[54]	8/32[54]	8/32[54]	8/32[54]
Utenti nella rete	1000	1000	1000	1000	1000

[54] I valori sono scaglionati secondo: Rete con UC Suite / Rete senza UC Suite

27.4.13 Application Connectivity

Tabella 60: Dati per schede madri V2 OCC

	X1	X3W/R	X5W/R	X8
Interfaccia CSTA				
Collegamenti CSTA tramite CSP per sistema	-	4/ 4/ 0[55]	4/ 4/ 0[55]	4/ 4/ 0[55]
Punti di monitoraggio per linee esterne o utenti	-	1500	1500	1500
TAPI 170 Middleware Server	-	4	4	4
TAPI 120 client (CSTA)	-	150/ 150/ 0[55]	150/ 150/ 0[55]	150/ 150/ 0[55]
Interfaccia Web Services (WSI)				
WSI - client attivi simultaneamente in totale	30	500/ 300/ 150[55]	500/ 300/ 150[55]	500/ 300/ 150[55]
myPortal @work	30	250/ 150/ 50[55]	250/ 150/ 50[55]	250/ 150/ 50[55]
myPortal to go	30	150/ 150/ 50[55]	150/ 150/ 50[55]	150/ 150/ 50[55]
DeskPhone CP 400/600/600E/ 700/700X/710 con WSI	30	150/ 150/ 50[55]	150/ 150/ 50[55]	150/ 150/ 50[55]
OpenScape Business Attendant	0	8/ 8/ 8[55]	8/ 8/ 8[55]	8/ 8/ 8[55]
OpenScape Business BLF	0	150/ 150/ 50[55]	150/ 150/ 50[55]	150/ 150/ 50[55]
Application Launcher	30	250/ 150/ 50[55]	250/ 150/ 50[55]	250/ 150/ 50[55]
TAPI 120 (modalità WSI)	30	0/ 0/ 30[55]	0/ 0/ 30[55]	0/ 0/ 30[55]
Applicazione di terze parti	Restante	Restante	Restante	Restante

Tabella 61: Dati per schede madri V3 OCC

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Interfaccia CSTA								
Collegamenti CSTA tramite CSP per sistema	-	-	4	4	4	4	4	4
Punti di monitoraggio per linee esterne o utenti	1650	1650	1650/3750[56]	1650/3750[56]	1650/3750[56]	1650/3750[56]	3750	3750

[55] I valori sono scaglionati secondo la configurazione UC Booster: Booster Server / Booster Card / senza UC Booster

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
TAPI 170 Middleware Server	4	4	4	4	4	4	4	4
TAPI 120 client (CSTA)	150	150	150/500[56]	150/500[56]	150/500[56]	150/500[56]	500	500
Interfaccia Web Services (WSI)								
WSI - client attivi simultaneamente in totale	150	300	150/500[56]	300/1000[56]	150/500[56]	300/1000[56]	1000	1000
myPortal @work	150	150	150/250[56]	150/250[56]	150/250[56]	150/250[56]	250	250
myPortal to go	150	150	150/500[56]	150/500[56]	150/500[56]	150/500[56]	500	500
myPortal for Teams	150	150	150/500[56]	150/500[56]	150/500[56]	150/500[56]	500	500
DeskPhone CP 400/600/600E/ 700/700X/710 con WSI	150	150	150/500[56]	150/500[56]	150/500[56]	150/500[56]	500	500
OpenScape Business Attendant	8	8	8	8	8	8	8	8
OpenScape Business BLF	150	150	150	150	150	150	150	150
Application Launcher	150	150	150/500[56]	150/500[56]	150/500[56]	150/500[56]	500	500
TAPI 120 (modalità WSI)	**Nota:** Eliminati gradualmente su schede madri V3 OCC. Supportato in V3 solo per schede madri V2.							
Applicazione di terze parti	Restante	Restante	Restante	Restante	Restante	Restante	Restante	Restante

Tabella 62: Dati per OpenScape Business S

	Server base (S)	Server standard (S)	Server avanzato (S)
Interfaccia CSTA			
Collegamenti CSTA tramite CSP per sistema	4	4	4
Punti di monitoraggio per linee esterne o utenti	3750	3750	3750
TAPI 170 Middleware Server	4	4	4

[56] I valori sono scaglionati secondo la versione della scheda: Base/Avanzata

	Server base (S)	Server standard (S)	Server avanzato (S)
TAPI 120 client (CSTA)	50	500	1500
Interfaccia Web Services (WSI)			
WSI - client attivi simultaneamente in totale	150	500	1500
myPortal @work	50	250	500
myPortal to go	50	250	500
myPortal for Teams	50	250	500
DeskPhone CP 400/600/600E/ 700/700X/710 con WSI	50	250	500
OpenScape Business Attendant	8	8	8
Application Launcher	50	250	500
TAPI 120 (modalità WSI)	0	0	0
Applicazione di terze parti	Restante	Restante	Restante

27.4.14 Accounting

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Registrazione centrale dei dettagli della chiamata					
Voci nel buffer dei dettagli chiamata per sistema	20000	20000	20000	20000	20000
Codice di addebito (CA):					
Voci di codici di addebito per sistema di comunicazione	1000	1000	1000	1000	1000
Cifre verificabili per codice del telefono	11	11	11	11	11
Caratteri consentiti	0-9	0-9	0-9	0-9	0-9

28 Modalità esperti

La **Modalità esperti** comprende menu e funzioni per la configurazione e la manutenzione del sistema.

28.1 Convenzioni di visualizzazione per le descrizioni dei parametri

Le descrizioni dei parametri seguono la struttura della Modalità esperti in WBM.

Voce di menu	A ogni voce di menu della Modalità esperti è assegnato a un argomento della Guida, che è possibile richiamare direttamente dal WBM (sensibile al contesto). Il titolo dell'argomento della Guida mostra il percorso della finestra WBM. Esempio: **Impostazioni di base** > **Sistema** > **Flag di sistema**
Scheda	Ogni scheda è assegnata a una tabella parametri nell'argomento della Guida. I parametri uguali di schede diverse vengono descritti nella stessa tabella parametri. In ogni tabella parametri è disponibile un elenco di schede per le quali i parametri sono validi. Esempio: • **Aggiungi indirizzo IP statico** • **Modifica indirizzo IP statico** • **Cancella indirizzo IP statico**
Area	Se le finestre del WBM sono organizzate in aree, si ritroverà la stessa struttura anche nella tabella parametri. La tabella parametri contiene per ogni area un'intestazione intermedia, seguita dai parametri di tale area.
Parametri	I parametri vengono descritti in tabelle parametri a due colonne. La colonna a sinistra riporta i nomi dei parametri, quella a destra fornisce una descrizione del parametro. I parametri il cui scopo è già di per sé chiaro vengono citati ma non spiegati. I valori consentiti e il valore predefinito, se disponibili, sono riportati al termine della descrizione.

Parametri (opzionale)	I parametri che non devono essere impostati sono riconoscibili dall'indicazione "opzionale".
Voce nell'elenco a discesa	Le voci dell'elenco a discesa non immediatamente comprensibili sono anche richiamate come parametro nella colonna di sinistra della tabella parametri. La voce è separata dal nome dell'elenco a discesa tramite i due punti. Esempio: **Algoritmo di crittografazione: AES**
Casella di controllo/pulsante di opzione/flag	La descrizione delle caselle di controllo/pulsanti di opzione/flag si riferisce sempre allo stato attivato.

28.2 Manutenzione

Le funzioni di manutenzione del sistema di comunicazione, ad esempio il caricamento della musica in attesa o l'aggiornamento delle immagini del software, sono raggruppate sotto la voce **Manutenzione**.

28.2.1 Configurazione

In **Configurazione** sono presenti funzioni quali il caricamento della musica su attesa (MoH) o la visualizzazione della configurazione hardware.

28.2.1.1 Configurazione > Musica su attesa > Carica nel gateway

Descrizione dei parametri delle schede:

- **Carica musica su attesa (MoH) tramite HTTP**

Parametri	Descrizione
Carica musica su attesa (MoH) tramite HTTP	
File musica su attesa giorno	Selezione del file MoH per il giorno dal file system locale. Formato file: vedi nota in WBM.
File musica su attesa notte	Selezione del file MoH per la notte dal file system locale. Formato file: vedi nota in WBM.
Carica	Caricamento dei file MoH selezionati nel sistema (richiesto riavvio). Attivazione con configurazione, Telefonia Centrale > Musica su attesa/ Annunci.

Descrizione dei parametri delle schede:

- **Carica file audio via HTTP**

Parametri	Descrizione
Carica file audio via HTTP	
File annuncio	Selezione del file WAV con l'annuncio dal file system locale. Formato file: vedi nota in WBM.
File audio già caricati	
File wave	Visualizzazione dei file annuncio caricati nel sistema di comunicazione
Elimina	Elimina il file annuncio
Carica	Caricamento nel sistema del file annuncio selezionato. Attivazione con configurazione, Telefonia Centrale > Musica su attesa/ Annunci.

28.2.1.2 Configurazione > Annunci > Caricamento sul gateway

Descrizione dei parametri delle schede:

- **Caricamento file audio tramite HTTP**

Parametri	Descrizione
Caricamento file audio tramite HTTP	
File annuncio	Selezionare il file WAV con l'annuncio dal file system locale. Formato del file: vedere nota in WBM.
File audio già caricati	
File Wave	Visualizza i file di annuncio caricati nel sistema di comunicazione
Elimina	Elimina il file dell'annuncio
Carica	Carica il file dell'annuncio selezionato nel sistema. Attivazione in Impostazioni, Telefonia centrale> Musica di attesa/Annunci.

28.2.1.3 Configurazione > Configurazione porta

Descrizione dei parametri della scheda:

- **Esportazione della configurazione**

Parametri	Descrizione
Esportazione della configurazione	
Nome file	Nome del file esportato.

Parametri	Descrizione
Azione	Esportare un file XML zippato (ad esempio per la successiva modifica in Excel) con i seguenti dati: nome, numero di telefono dell'utente, numero interno, tipo di stazione, licenze, linea di gruppo/di ricerca (no team/top), utenti virtuali, linee, gruppi di linee, caselle vocali.

28.2.1.4 Configurazione > SmartVM

Descrizione dei parametri delle schede:

- **Panoramica**

Parametri	Descrizione
Lingue Visualizzazione di tutte le lingue in cui è disponibile la guida utente. Viene utilizzata la seguente convenzione: aabb aa = codice della lingua a due cifre bb = codice internazionale a due cifre Il codice internazionale (bb), di regola, è uguale a quello del codice della lingua (aa).	
Informazioni su casella postale	
Numero di telefono	Visualizzazione del numero di telefono della casella vocale
Servizio	Visualizzazione del nome della casella vocale.
Messaggi	Visualizzazione del numero di nuovi messaggi/numero totale di messaggi.
Utilizzo caselle postali totale	Visualizzazione dell'utilizzo dello spazio di memorizzazione in percentuale.

28.2.1.5 Configurazione > SmartVM > Operazioni con casella postale

Descrizione dei parametri delle schede:

- **Esegui operazioni con casella postale**

Parametri	Descrizione
Reimposta la configurazione di tutte le caselle postali (elimina tutti i messaggi e gli annunci)	Se questa opzione è attivata, tutti gli annunci di benvenuto e i messaggi di tutte le caselle vocali di SmartVM vengono eliminati. Impostazione predefinita: funzione disattivata.
Indice	Visualizzazione dell'indice della casella vocale.
N° tel.	Visualizzazione del numero di telefono della casella vocale
Servizio	Visualizzazione del nome della casella vocale.

Parametri	Descrizione
Reimposta password	Se il flag è attivato, la password per la casella vocale viene riportata al valore predefinito `123456`. L'utente deve modificare la password al successivo utilizzo della casella vocale. Impostazione predefinita: funzione disattivata.
Inizializza caselle postali	Se questo flag è attivato, per tutte le caselle vocali selezionate, vengono eseguite le seguenti azioni: Mailbox standard: – Ripristino della password predefinita – Attivazione del flag **Registrazione** – Eliminazione messaggi in corso – Cancellazione degli annunci di benvenuto – Controllo degli annunci di benvenuto su manuale – Annuncio di benvenuto attivo: Annuncio 1 Mailbox AutoAttendant: – Ripristino della password predefinita – Il flag **Intercetta** dopo annuncio è disattivato – Cancellazione delle destinazioni di selezione breve – Cancellazione degli annunci di benvenuto – Controllo degli annunci di benvenuto su manuale – Annuncio di benvenuto attivo: Annuncio 1 Impostazione predefinita: funzione disattivata.

28.2.1.6 Configurazione > SmartVM > Operazioni su file

Descrizione dei parametri delle schede:

- **Backup**

Parametri	Descrizione
Backup	
Messaggi	Se questo flag è attivato, in aggiunta agli annunci di benvenuto, vengono salvati anche i messaggi della casella vocale selezionata. Impostazione predefinita: funzione disattivata.
Caselle postali disponibili	Lista di tutte le caselle vocali disponibili. È possibile inserire nella lista delle caselle vocali da salvare le singole caselle vocali o tutte le caselle vocali.
Caselle postali per backup	Lista delle caselle vocali da salvare.
Pulsanti	
Applica	Gli annunci di benvenuto (e i messaggi, se il flag **Messaggi** è attivato) delle caselle vocali da salvare vengono salvati in un file di backup (`*.tar`).

Descrizione dei parametri delle schede:

- **Dati degli annunci**

Parametri	Descrizione
Dati degli annunci	
Selezione casella postale	Scelta della casella vocale.
Annuncio 1 (giorno)	Visualizzazione dell'annuncio di benvenuto attualmente utilizzato. **Predefinito** significa che non sono disponibili per l'utente annunci di benvenuto singoli.
Annuncio 2 (notte)	Visualizzazione dell'annuncio di benvenuto attualmente utilizzato. **Predefinito** significa che non sono disponibili per l'utente annunci di benvenuto singoli.
Annuncio 3	Visualizzazione dell'annuncio di benvenuto attualmente utilizzato. **Predefinito** significa che non sono disponibili per l'utente annunci di benvenuto singoli.
Annuncio 4	Visualizzazione dell'annuncio di benvenuto attualmente utilizzato. **Predefinito** significa che non sono disponibili per l'utente annunci di benvenuto singoli.
Pulsanti	
Sfoglia	Navigazione fino al percorso di memorizzazione del file dell'annuncio di benvenuto.
Carica	In SmartVM è stato caricato un annuncio di benvenuto precedentemente salvato o un file wave. Il file Wave da caricare deve avere il seguente formato: PCM, 16 bit, 8khz, mono Durante il caricamento ha luogo la conversione del file Wave selezionato. A seconda delle dimensioni, l'operazione può durare alcuni minuti.
Salva	L'annuncio di benvenuto attualmente utilizzato viene salvato sul PC. Nel PC, gli annunci di benvenuto vengono salvati nel formato binario (file mva), pertanto non possono essere riprodotti o modificati.
Elimina	L'annuncio di benvenuto attualmente utilizzato viene eliminato da SmartVM.

Descrizione dei parametri delle schede:

- **Ripristino**

Parametri	Descrizione
Ripristino	
Messaggi	Sovrascrive non solo l'annuncio di benvento della casella vocale selezionata, ma anche i messaggi. Impostazione predefinita: funzione disattivata.

Parametri	Descrizione
Inclusione	Se il flag è attivato, vengono sovrascritti solo gli annunci di benevenuto delle caselle vocali selezionate che si trovano nei dati di backup. Inoltre, se il flag **Messaggi** è attivato, vengono aggiunti anche i messaggi contenuti nei dati di backup. I messaggi già esistenti vengono mantenuti. Se il flag è attivato, prima della riproduzione, tutti gli annunci di benvenuto e i messaggi delle caselle vocali selezionate in SmartVM vengono eliminati. Se solo selezionate caselle vocali che non contengono dati di backup, vengono eliminate anche queste! I messaggi di benvenuto contenuti nei dati di protezione vengono trasmessi. Se è attivata anche l'opzione **Messaggi**, vengono trasferiti anche i messaggi contenuti nei dati di backup. Impostazione predefinita: funzione disattivata.
Caselle postali disponibili	Elenco di tutte le caselle vocali esistenti nel file di backup. È possibile inserire nella lista delle caselle vocali da ripristinare singole caselle o tutte le caselle.
Caselle postali per backup	Lista delle caselle vocali da ripristinare.
Pulsanti	
Sfoglia	Navigazione nel percorso di memorizzazione del file di backup.
Carica	Vengono visualizzate le caselle vocali contenute nel file di backup. Facendo nuovamente clic sul pulsante, gli annunci e i messaggi delle caselle vocali selezionate vengono ripristinati.

28.2.1.7 Configurazione > Branding

Descrizione dei parametri della scheda:

- **Branding**

Parametri	Descrizione
Branding	Scelta del nome del prodotto.

28.2.1.8 Configurazione > Indirizzo IP del gateway

Descrizione dei parametri della scheda:

- **Modifica dell'indirizzo IP del gateway**

Parametri	Descrizione
Modifica dell'indirizzo IP del gateway	
Indirizzo IP del gateway	Input dell'indirizzo IP del sistema di comunicazione, ad esempio 192.168.1.2

28.2.2 Immagine del software

In **Immagine del software** sono riunite le funzioni che vengono utilizzate per aggiornare il software del gateway e le immagini dei telefoni.

28.2.2.1 Immagine del software > Software di sistema > Aggiornamento via Internet

Descrizione dei parametri delle schede:

- **Carica immagini software da server Web**

Parametri	Descrizione
Impostazioni del server Web	
URL dell'Immagine del software	Visualizzare e modificare dei collegamenti al server software, incluso il percorso del file immagine.
Nome utente	Nome utente per l'accesso al server proxy software.
Password	Password per l'accesso al server software.
Informazioni sull'aggiornamento del software	Attivazione dell'interrogazione presso il server software in relazione alla disponibilità di una nuova versione del software.
Ora inizio	Ora della Controllo. Valori consentiti: dalle 00.00 alle 24.00, valore predefinito: 02,00
Utilizza Proxy	Attivazione proxy, se usato.
Proxy HTTP	
Proxy HTTP	Immissione del collegamento al server proxy.
Porta del proxy HTTP	Immissione della porta del server proxy. Valore predefinito: 80
Nome utente	Nome utente per l'accesso al server proxy.
Password	Password per l'accesso al server proxy.
Instradamento statico dedicato	I clienti con una connessione WAN per linee SIP senza volume di dati Internet possono utilizzare la funzionalità **Instradamento statico dedicato** per eseguire un aggiornamento del software OSBiz tramite un'interfaccia LAN alternativa. L'indirizzo IP dinamico del server di aggiornamento viene rilevato automaticamente ed è quindi disponibile come voce di routing per questo processo. Per utilizzare questa opzione: • Attivare il flag **Instradamento statico dedicato**
Instradamento statico dedicato per aggiornamento software tramite interfaccia LAN	
Indirizzo IP del gateway di instradamento	Configurare l'indirizzo IP del gateway predefinito dell'interfaccia LAN - attraverso il quale è possibile una connessione a Internet - come indirizzo IP del gateway di instradamento.
Ultimo aggiornamento software	Indicazione di quando è stato eseguito l'ultimo aggiornamento software.
Pulsanti	
Predefinito	Riportare i valori modificati alle impostazioni predefinite.

28.2.2.2 Immagine del software > Software di sistema > Aggiornamento tramite Carica file

Descrizione dei parametri delle schede:

- **Carica immagini software tramite File Upload**

Parametri	Descrizione
Nome del file remoto (file system del PC)	Selezionare il percorso per il file immagine.
Pulisci lo spazio di archiviazione prima del trasferimento	Quando l'aggiornamento viene eseguito con questo flag attivo, i registri, le tracce, le immagini del software del telefono e i dump TCP vengono eliminati per liberare la memoria di archiviazione.
Attivazione del software	
Inizio dell'azione subito dopo la trasmissione	Il software viene scaricato nel sistema di comunicazione immediatamente, in background. Dopo due riavvii il software viene aggiornato.
Inizio dell'azione tra	Il software viene scaricato nel sistema di comunicazione immediatamente, in background. Il software verrà attivato una volta trascorso un tempo indicato. Immissione dell'intervallo in giorni, ore e minuti.
Inizio dell'azione il	Il software viene scaricato nel sistema di comunicazione immediatamente, in background. Il software verrà attivato nel momento indicato. Immissione di data e ora.
Ora del sistema locale	Visualizzazione della data e ora del sistema.
Versione delle immagini software di sistema correntemente utilizzate	Visualizzazione della versione del software del file immagine corrente.

28.2.2.3 Immagine del software > Software di sistema > Aggiornamento via supporto USB

Descrizione dei parametri delle schede:

- **Carica immagini software da chiave USB**

Parametri	Descrizione
Elenco di tutti i file di immagine compatibili esistenti	
Versione	Visualizzazione del numero versione dei file immagine rilevati sul supporto USB.
Carica	Selezionare il file immagine presente sul supporto USB da utilizzare per l'aggiornamento del software.
Nome file	Visualizzare dei nomi dei file immagine rilevati sul supporto USB.
Dimensione del file (MB)	Visualizzare della dimensione dei file immagine rilevati sul supporto USB.
Attivazione del software	

Parametri	Descrizione
Inizio dell'azione subito dopo la trasmissione	Il software viene scaricato nel sistema di comunicazione immediatamente in background e attivato. Per l'attivazione viene interrotto temporaneamente il funzionamento del sistema.
Inizio dell'azione tra	Il software viene scaricato nel sistema di comunicazione immediatamente, in background. Il software verrà attivato una volta trascorso un tempo indicato. Immissione dell'intervallo in giorni, ore e minuti.
Inizio dell'azione il	Il software viene scaricato nel sistema di comunicazione immediatamente, in background. Il software verrà attivato nel momento indicato. Immissione del momento con data e ora.
Ora del sistema locale	Visualizzazione della data e ora del sistema.
Versione delle immagini software di sistema attualmente utilizzate	Visualizzazione della versione software attiva.

28.2.2.4 Immagine del software > Immagini telefono > Carica

Descrizione dei parametri delle schede:

- **Caricamento del software del telefono**

Parametri	Descrizione
Nome del file remoto (sistema di file del PC)	Scelta del software del telefono (file immagine)
Immagini al momento installate	
Elimina	Le immagini del telefono vengono selezionate per l'eliminazione.
Nome file	Visualizzazione del nome del file immagine.
Tipo di dispositivo	Visualizzazione del tipo di carattere del telefono di sistema a cui appartiene il file immagine.
Versione	Visualizzazione della versione del file immagine.
Pulsanti	
Carica	L'immagine del telefono indicata viene caricata nel sistema di comunicazione.
Elimina	Le immagini del telefono selezionate vengono eliminate dal sistema di comunicazione.

28.2.2.5 Immagine del software > Immagini telefono > Distribuire

Descrizione dei parametri delle schede:

- **Distribuire il software dei telefoni**

Parametri	Descrizione
Immagini al momento installate	
Distribuire	Se si seleziona la casella di controllo, il software dei telefoni viene scaricato in tutti i telefoni di sistema collegati del tipo in questione.
Nome file	Visualizzazione del nome del file immagine.
Tipo di dispositivo	Visualizzazione del tipo di carattere del telefono di sistema a cui appartiene il file immagine.
Versione	Visualizzazione della versione del file immagine.
Tipo	Tipo di telefono di sistema.
Predefinito	Il software per telefoni configurato come predefinito viene automaticamente scaricato nei telefoni di sistema associati a questo tipo quando questi si connettono al sistema per la prima volta.

28.2.2.6 Immagine del software > Immagini telefono > Distribuzione per terminale

Descrizione dei parametri delle schede:

- **Distribuzione del software dei telefoni per terminale**

  Se l'utente è un utente Deskshare, la casella di controllo è visualizzata in grigio, quindi non è possibile distribuire un dispositivo a quell'utente.

Parametri	Descrizione
Immagini al momento installate	
N. chiamata	Numero del telefono di sistema.
Tipo di dispositivo	Tipo di telefono di sistema.
Indirizzo IP	Indirizzo IP del telefono di sistema; collegamento diretto al WBM del telefono di sistema.
Indirizzo MAC	Indirizzo MAC del telefono di sistema.
Versione software corrente	Versione software del telefono di sistema corrente.
Software disponibile per la distribuzione	Selezione delle immagini del telefono da scaricare nel telefono di sistema.

28.2.2.7 Immagine del software > Loghi immagine telefono > Carica

Un'immagine (ad esempio un logo aziendale) può essere caricata sul display dei telefoni di sistema (OpenStage 40/60/80 o varianti Telekom) e visualizzata allo stato inattivo (telefono agganciato). Per le specifiche del file del logo, vedere Loghi del telefono.

Descrizione dei parametri delle schede:

- **Carica immagine logo telefono**

Parametri	Descrizione
Nome del file remoto (sistema di file del PC)	Scelta del file con il logo del telefono.
Immagini logo attualmente installate	
Elimina	I file del logo telefono vengono selezionati per l'eliminazione.
Nome file	Visualizzazione del nome del file logo telefono.
Pulsanti	
Carica	Il file logo telefono indicato viene caricato nel sistema di comunicazione.
Elimina	I file logo telefono selezionati vengono eliminati dal sistema di comunicazione.

28.2.2.8 Immagine del software > Loghi immagine telefono > Distribuire

Un'immagine (ad esempio un logo aziendale) può essere caricata sul display dei telefoni di sistema (OpenStage 40/60/80 o varianti Telekom) e visualizzata allo stato inattivo (telefono agganciato). Per le specifiche del file del logo, vedere Loghi del telefono.

Descrizione dei parametri delle schede:

- **Distribuzione immagini logo telefono**

Parametri	Descrizione
Immagini logo attualmente installate	
Distribuire	Se la casella di controllo è selezionata, questo file del logo del telefono viene trasmesso al telefono del sistema selezionato.
Nome file	Visualizzazione del nome del file logo telefono.
Distribuisci ai workpoint con il tipo periferica selezionato	Indicazione se il logo del telefono deve essere trasferito a tutti i telefoni del sistema o solo a un tipo specifico di telefono del sistema.

28.2.3 Cordless

In **Cordless** sono riunite le funzioni relative alle stazioni base configurate.

28.2.3.1 Cordless > Base Stations

Descrizione dei parametri delle schede:

- **Stato utente base**

Parameters	Descrizione
Dati stazione base	

Parameters	Descrizione
Frequenza BS	Mostra le frequenze delle stazioni base selezionate. È possibile selezionare fino a 10 diversi canali di frequenza contemporaneamente (vedere la seguente tabella).
Base station	Numero della stazione base.
Versione SW	Versione software della stazione base.
Versione HW	Versione hardware della stazione base.
Stato	Stato delle porte associate: porta attiva Nessuna staz. base Bloccato Staz. base collegata, non attiva Staz. base collegata, non attiva 1. Porta aggiuntiva a... (n. della porta principale) 2. Porta aggiuntiva a... (n. della porta principale)
BS overload	Numero delle situazioni di Overload sull'interfaccia UP0/E.
Restart	Numero dei restart della stazione base.
Errore L1/L2	Numero degli errori L1/L2 che si sono verificati nella stazione base.
Rilascio anormale	Numero delle chiamate interrotte nella stazione base.
Chiamate per BS	Numero delle chiamate fatte attraverso la stazione base (sia in entrata e che in uscita).
Modo di salto	I sistemi Cordless della versione 2 lavorano sempre in "Modalità Fast Hopping". Possono essere ovvero utilizzate tutte le coppie di slot di tempo di frequenza. Sono perciò a disposizione 120 canali duplex. Nel caso di BS a Slow Hopping può solo essere impiegata ogni seconda frequenza - coppia di intervallo di tempo. Sono perciò a disposizione solo 60 canali duplex. Tutti i sistemi Cordless della versione 1 lavorano in "Modo Slow Hopping".
Numero BHO OK	Numero degli Intracell Handovers (Bearer Handovers BHO) riusciti, cioè dei cambi della frequenza portante e/o del timeslot all'interno di una cella. Non supportato da Hicom cordless EM versione 2.1 e versione 2.2. Il contatore non è implementato, ma il servizio del Bearer Handover è disponibile.
Numero BHO non OK	Numero degli Intracell Handover (Bearer Handovers BHO) non riusciti. Non supportato da Hicom cordless EM versione 2.1 e versione 2.2. Il contatore non è implementato, ma il servizio del Bearer Handover è disponibile.
Handover Intra SLC	Number of handover procedures within the SLC card. Il conteggio viene effettuato nella nuova stazione base.
Handover Inter SLC	Number of handover procedures between SLC cards. Il conteggio viene effettuato nella nuova stazione base.
SLC-wide	
Chiamate perse	Numero delle chiamate non connesse per mancanza di risorse.

Parameters	Descrizione
SLMUC Overload	Number of overload situations on the SLC board. The number of free pool elements on the SLC board falls below a minimum value. All incoming connections will be rejected by the SLC IWU until the overload situation returns to normal.
LR Roam	LR Roam conta ogni impegno di un portatile con una PMID standard e un SLC di stazionamento modificato. Numero dei messaggi Locate Request che hanno informato sul Roaming (cioè che l'attuale postazione del telefono portatile è cambiata). Ad ogni accensione il cellulare effettua una Locate Request. Se il cellulare viene disattivato ed attivato in un’altra cella radio questo contatore non scatta.
LR Async	LR Asinc conta ogni impegno di un portatile con una PMID standard e con SLC di stazionamento invariante. Numero di messaggi Locate Request che riferiscono l'asincronia dei livelli (cioè che l'attuale luogo di stazionamento del portatile è immutato). Il conteggio avviene però sempre sul SLC "home", quindi solo se il collegamento radio è effettivo oppure implementa il CHO con PMID standard. Per gli impegni delle linea, devono inoltre essere inoltre soddisfatti i criteri necessari per l'aggiornamento del luogo di stazionamento. Deve essere ovvero ricevuta una LOCATE Request o eseguite le misure di sicurezza, l’autentificazione (e codifica) per il collegamento.
Errore HDLC	Numero dei messaggi d'errore HDLC non critici che non sono stati segnalati al sistema di comunicazione (Overflow, Underrun, errore CRC).
Versione CMI	Qui viene visualizzata l'attuale versione Cordless.

Frequenza (canale)	**DECT**	Europa 1880 – 1900 MHz	America Latina 1910–1930 MHz
10	9	1881,792 MHz	1911,16 MHz
9	8	1883,520 MHz	1912,896 MHz
8	7	1885,24 MHz	1914,624 MHz
7	6	1886,976 MHz	1916,352 MHz
6	5	1888,704 MHz	1918,080 MHz
5	4	1890,432 MHz	1919,80 MHz
4	3	1892,160 MHz	1921,536 MHz
3	2	1893,88 MHz	1923,264 MHz
2	1	1895,616 MHz	1924,992 MHz
1	0	1897,344 MHz	1926,720 MHz

28.2.4 Stato porta/modulo

È possibile visualizzare lo stato di tutti i moduli e anche sbloccare e bloccare i moduli e le relative porte.

28.2.4.1 Stato porta/modulo > Stato modulo

Descrizione dei parametri delle schede:

- **Stato modulo**

Parametri	Descrizione
Slot	Numero di slot fisico.
Modulo	Descrizione del modulo.
Non collegato	Selezionato se il modulo non è inserito.
Difettoso	Selezionato se il modulo è difettoso (non caricato). È anche possibile che un modulo difettoso o non configurato non venga visualizzato.
Bloccato	Selezionato se almeno una porta di questo modulo è bloccata.
Libero	Selezionato se tutte le porte del modulo sono libere.
Occupato	Selezionato se almeno un utente o una linea di questo modulo è connessa, chiamata o in comunicazione.
Clock sorgente	Selezionato se il modulo fornisce il clock di riferimento.
Pulsanti	
Avvia	Viene avviato l'aggiornamento del display. Lo stato viene aggiornato ogni 3 secondi.
Arresta	Viene arrestato l'aggiornamento del display.

28.2.4.2 Stato porta/modulo > Fuori servizio

Descrizione dei parametri delle schede:

- **Porta fuori servizio**
- **Modulo fuori servizio**

Parametri	Descrizione
Accesso	Slot e porta a cui è collegato l'utente o la linea.
N° tel.	Il numero di telefono assegnato alla porta.
Servizio	Il nome associato all'utente o alla linea.
Stato	In funzione del fatto che alla porta siano collegati o no un terminale o una linea consentiti, tale porta può essere **attiva** o **non attiva**. Le porte possono anche essere allo stato **In funzione** (predefinito) o **Fuori servizio tramite lo strumento**, ovvero possono essere bloccate selezionando **Blocca modulo**. Lo stato **In funzione** non è identico ad **attivo**. Lo stato della porta può essere, ad esempio, **Attivo**, **In funzione** o anche **Non attivo**, **In funzione**.
Pulsanti	

Parametri	Descrizione
Bloccare selezione	Le porte selezionate vengono bloccate. Quando viene bloccata la porta $U_{P0/E}$, viene sempre bloccata la porta fisica associata. Ciò comporta che quando si sceglie una porta master, anche la relativa porta slave assume lo stato fuori servizio.
Rilasciare selezione	Le porte selezionate vengono sbloccate.
Blocca modulo	I moduli selezionati e le relative porte vengono bloccati. Quando si bloccano i singoli telefoni di un gruppo cordless viene bloccato sempre l'intero modulo e con esso anche tutti i relativi telefoni. Il blocco dei singoli cordless viene realizzato modificando il PIN dei cordless.
Abilita modulo	I moduli selezionati e le relative porte vengono sbloccati.

28.2.5 Tracce

In **Tracce** sono riunite le funzioni che vengono utilizzate per le tracce. L'amministratore può avviare e interrompere le tracce nonché modificarne le impostazioni.

28.2.5.1 Tracce > Configurazione formato traccia

La funzione Configurazione formato traccia consente di definire quali informazioni dell'intestazione devono essere contenute nel risultato della traccia e il formato dei dati della traccia.

Descrizione dei parametri delle schede:

- **Modifica configurazione di traccia**

Parametri	Descrizione
Dati di intestazione contenuti nell'output di traccia	
Impostazioni globali del formato dell'intestazione della traccia	Se il flag è attivato: se questa opzione è attiva, è possibile selezionare se includere o meno le seguenti informazioni sull'intestazione. Valore predefinito: Attivato
ID del sub-sistema	Se il flag è attivato: l'ID del sub-sistema è incluso nell'output di traccia. Valore predefinito: Attivato
Nome del task	Se il flag è attivato: il nome del attività è incluso nell'output di traccia. Valore predefinito: Attivato
ID del task	Se il flag è attivato: l'ID del task è incluso nell'output di traccia. Valore predefinito: Attivato
Tempo	Se il flag è attivato: le informazioni temporali vengono incluse nell'output di traccia. Valore predefinito: Attivato

Parametri	Descrizione
Nome del modulo	Se il flag è attivato: il nome del modulo è incluso nell'output di traccia. Valore predefinito: Attivato
Numero della riga	Se il flag è attivato: il numero della riga è incluso nell'output di traccia. Valore predefinito: Attivato
Preparazione dei dati della traccia	
Formattazione completa con espansione dei parametri (predefinita)	Modalità output predefinita: Tutti i tipi di dati sono ampliati. Output di traccia: normale (adatto per carichi di lavoro normali) Valore predefinito: Attivato
Ristretto (tipi di messaggi binari, in particolar modo per Tracer X)	In questa modalità di output limitata, i tipi di dati vengono mostrati in formato binario, ovvero lo stato in cui si trovavano al momento della traccia. Il formato binario è inteso per l'analisi con lo strumento X-Tracer. Output di traccia: veloce (adatto per carichi di lavoro medio-alti) Valore predefinito: Disattivato
Ristretto (soltanto espansione di tipi di dati elementari)	In questa modalità di output, vengono espansi solo tipi di dati elementari (ad esempio, integer, short, long, string). Output di traccia: molto veloce (adatto per carichi di lavoro elevati) Valore predefinito: Disattivato
Traccia a prestazione ottimizzata senza espansione dei parametri	In questa modalità di output, non viene eseguita alcuna espansione dei tipi di dati. In questo modo non viene generato alcun overhead per la formattazione Traccia. Output di traccia: velocissimo (adatto per carichi di lavoro molto elevati) Valore predefinito: Disattivato

28.2.5.2 Tracce > Interfacce di output traccia

Descrizione dei parametri delle schede:

- **Modifica interfacce di output traccia**

Parametri	Descrizione
Traccia del file	
Attiva traccia del file	Se il flag è attivato: i messaggi traccia vengono registrati in un file di registro nel sistema di comunicazione. Valore predefinito: Attivato
Quota traccia max. (kbyte)	Visualizzazione della dimensione massima della memoria Trace in Kbyte
Criteri per la gestione del raggiungimento della quota massima	Possibilità di scelta del comportamento del sistema al raggiungimento della quota traccia massima.

Parametri	Descrizione
Criteri per la gestione del raggiungimento della quota massima: Wrap Around (rimozione file della traccia meno recente)	Al raggiungimento della quota traccia massima, viene sovrascritto il file di registro traccia più vecchio. Valore predefinito: Attivato
Criteri per la gestione del raggiungimento della quota massima: Arresta temporaneamente file della traccia	Al raggiungimento della quota traccia massima, viene interrotto l'output di traccia. Valore predefinito: Disattivato
Tempo fra la creazione di nuovi file della traccia (sec.)	Visualizzazione del tempo in secondi trascorso il quale viene creato un nuovo file di registro traccia.
Intervallo di disponibilità dei file della traccia	Visualizzazione del periodo di disponibilità dei file di registro traccia.
Traccia tramite LAN	
Attiva traccia tramite LAN (XGracer)	I messaggi della traccia vengono via interfaccia LAN. Valore predefinito: Disattivato
Valore timer (sec.)	Visualizzazione del tempo in secondi trascorso il quale vengono trasferiti i dati di traccia.

28.2.5.3 TracceRegistro traccia

Descrizione dei parametri delle schede:

- **Carica via HTTP**
- **Cancella registro di traccia**

Suggerimento: La cancellazione dei dati del registro traccia non può essere annullata.

Parametri	Descrizione
Registro di traccia	
Registro completo	Tutti i file registro traccia disponibili vengono scaricati.
Protocollo odierno	Vengono scaricati i file di registro di traccia del giorno (a partire dalle ore 00:00).
Selezione propria	Vengono scaricati i file di registro di traccia per il periodo indicato.

28.2.5.4 Tracce > Loopback digitale

La configurazione di loopback digitali è possibile solo con Manager E.

I loopback digitali sono utilizzati per il test dei canali B delle interfacce S_0, S_{2M} e T1 di eventuali moduli esistenti. Il loopback digitale deve essere attivato solo su richiesta del provider di servizi.

Descrizione dei parametri delle schede:

- **Modifica loopback digitale**

28.2.5.5 Tracce > Registro traccia cliente

Tramite questa funzione è possibile avviare la visualizzazione degli eventi (Traccia cliente). I tipi di messaggi includono ad esempio messaggi di sistema, SIP, STUN e LDAP.

Descrizione dei parametri delle schede:

- **Visualizza**
- **Carica via HTTP**
- **Cancella registro di traccia**

Parametri	Descrizione
Aggiornamento autom.	Se il flag è attivato, viene eseguito l'aggiornamento automatico della visualizzazione del protocollo traccia cliente. Valore predefinito: Attivato
Secondi fino al prossimo aggiornamento	Tempo in secondi trascorso il quale viene eseguito l'aggiornamento del protocollo di traccia del cliente.

28.2.5.6 Tracce > Componenti di traccia M5T

Questa funzione consente il monitoraggio dello stack SIP.

Le modifiche alle impostazioni devono essere apportate solo se richiesto dal servizio di assistenza tecnica competente.

Descrizione dei parametri delle schede:

- **Modifica componenti di traccia M5T**
- **Avvia/arresta componente traccia**

Parametri	Descrizione
Nome pacchetto	Nome del componente traccia M5T
Livello di traccia	Livello di dettaglio della registrazione del componente Traccia del M5T (da livello traccia 0 = livello di dettaglio più basso a livello traccia 9 = livello di dettaglio più elevato) Valore predefinito: 0
Traccia su	Se il flag è attivato, viene eseguita la registrazione dei dati del componente di traccia del M5T. Valore predefinito: Disattivato
Crotch	Incremento dell'attivazione

28.2.5.7 TracceSecure Trace

Questa funzione viene utilizzata per la registrazione di flussi di dati d'uso e di segnalazione VoIP crittografati.

Per la registrazione crittografata dei dati di connessione è obbligatoria l'approvazione da parte del cliente. La registrazione può essere effettuata esclusivamente in collaborazione con il servizio di assistenza competente. Per informazioni sulla procedura, vedere Tracce (Secure Trace).

Nota: La registrazione di conversazioni e dati di connessione costituisce reato, a meno che l'utente in questione sia stato preventivamente informato a riguardo.

Descrizione dei parametri delle schede:

- **Modifica passphrase di Secure Trace**
- **Importazione di file X.509 per Secure Trace**

Parametri	Descrizione
Modifica passphrase di attivazione di Secure Trace	
Passphrase corrente	Password (passphrase) corrente per avviare e arrestare Secure Trace
Nuova passphrase	Nuova password (passphrase) per l'avvio e l'arresto di Secure Trace Valori consentiti: da 5 a 12 caratteri
Conferma nuova passphrase	Nuova password (passphrase) identica per l'avvio e l'arresto di Secure Trace Valori consentiti: da 5 a 12 caratteri
File certificato (PEM o binario)	Selezione del file X.509 che contiene il certificato da importare nel sistema di comunicazione. Dopo aver selezionato il file X.509, viene visualizzata l'impronta digitale del certificato da importare prima di importare il certificato nel sistema di comunicazione. ***INFO:*** l'importazione del certificato deve avvenire solo dopo la verifica delle impronte digitali.

28.2.5.8 Tracce > Secure Trace > Certificato Secure Trace

Questa funzione viene utilizzata per visualizzare i certificati Secure Trace importati.

Descrizione dei parametri delle schede:

- **Mostra certificato Secure Trace**

28.2.5.9 Tracce > Secure Trace > Impostazioni di Secure Trace

Questa funzione viene utilizzata per il controllo dello stato e l'avvio/arresto di Secure Trace.

Descrizione dei parametri delle schede:

- **Stato di Secure Trace**
- **Come avviare/arrestare Secure Trace**

Parametri	Descrizione
Stato corrente di Secure Trace	
Secure Trace è attiva	Stato di Secure Trace
Tempo di disattivazione automatica	Ora alla quale Secure Trace viene automaticamente disattivato.
Secure Trace per questi protocolli	Visualizzazione dei protocolli per i quali viene creato Secure Trace.
Parametri di avvio	
Passphrase di attivazione di Secure Trace	Password (passphrase) per l'avvio e l'arresto di Secure Trace
Durata di Secure Trace (min.)	Periodo di tempo in minuti durante il quale Secure Trace deve essere attivo. ***INFO:*** è obbligatorio inserire un valore.
Secure Trace per questi protocolli	
TC (TLS)	Se il flag è attivato, Secure Trace tiene in considerazione il protocollo TC (TLS). Valore predefinito: Disattivato
H.323 Core/HSA (TLS)	Se il flag è attivato, Secure Trace tiene in considerazione il protocollo H.323 Core/HSA (TLS). Valore predefinito: Disattivato
MMX (PEP)	Se il flag è attivato, Secure Trace tiene in considerazione il protocollo MMX (PEP). Valore predefinito: Disattivato
SIP Core/SSA (TLS)	Se il flag è attivato, Secure Trace tiene in considerazione il protocollo SIP Core/SSA (TLS). Valore predefinito: Disattivato
MSC (SRTP)	Se il flag è attivato, Secure Trace tiene in considerazione il protocollo MSC (SRTP). Valore predefinito: Disattivato

28.2.5.10 TracceTraccia dello stack H.323

Questa funzione consente di seguire la risoluzione dei problemi per i componenti che utilizzano il protocollo H.323.

Le modifiche alle impostazioni devono essere apportate solo se richiesto dal servizio di assistenza tecnica competente.

Descrizione dei parametri delle schede:

- **Modifica configurazione di traccia dello stack H.323**
- **Modifica tutti i moduli H.323**
- **Carica il registro di traccia dello stack H.323 tramite HTTP**
- **Cancella il registro di traccia dello stack H.323**

Parametri	Descrizione
Generale	
Livello di traccia	Livello di dettaglio della traccia (da livello traccia 0 = livello di dettaglio più basso a livello traccia 4 = livello di dettaglio più elevato) Valore predefinito: 2
Traccia della console	
Attiva traccia della console	Se il flag è attivato: i messaggi della traccia dello stack H.323 vengono trasmessi alla console. Valore predefinito: Disattivato
Traccia del file	
Attiva traccia del file	Se il flag è attivato: i messaggi della traccia dello stack H.323 vengono salvati in un file di registro. Valore predefinito: Disattivato
Dimensione max. del buffer di traccia (byte)	Dimensione max. del buffer di traccia in byte (quantità di informazioni conservate nella memoria temporanea)
Dimensione max. del file di traccia (byte)	Dimensione massima di file protocollo di traccia in byte
Timer di traccia (sec.)	Tempo in secondi trascorso il quale vengono scritti i dati di traccia nel file di registro.
Nome del modulo	Nome del modulo di traccia dello stack H.323
Traccia su	Se il flag è attivato: il modulo di traccia dello stack H.323 è attivo.

28.2.5.11 Tracce > Ascolto chiamate

Tramite questa funzione è possibile avviare e arrestare il monitoraggio delle interfacce di linea e utente.

Descrizione dei parametri delle schede:

- **Avvia/arresta protocollo**
- **Visualizza**
- **Carica via HTTP**

Parametri	Descrizione
Porta selezionata	Interfaccia di linea o utente per le quali occorre avviare o arrestare l'ascolto delle chiamate.
Nr.	Numero progressivo.

Parametri	Descrizione
Ora	Ora dell'evento.
Numero telefono/Accesso	Numero di telefono e interfaccia fisica.
Stato	Stato dell'interfaccia. Sono disponibili i seguenti stati dell'interfaccia: • Idle (interfaccia allo stato inattivo) • Call Initiated (interfaccia pronta) • Overlap Sending (invio cifre all'esterno) • Outgoing Call Proc (in composizione) • Call Request (attesa di un alert) • Call Present (interfaccia chiamata) • Active (interfaccia allo stato conversazione) • Metti in attesa (interfaccia in attesa) • Disconnect Indication (richiesta di concludere una conversazione attiva) • Direct (interfaccia in modalità chiamata diretta) • Intrusion (inclusione attivata) • Call Back A (richiamata utente A) • Call Back B (richiamata utente B) • Busy (interfaccia occupata) • Error (Errore) • Disconnect PI (attesa disconnessione di PI (Indicatore progresso)) • Sensor (il segnale viene inviato da un sensore) • Conference Master (master della conferenza) • Paging (cercapersone) • Help Dial (viene usata la composizione associata) • Remote (Iinterfaccia occupata tramite Remote Service o DISA) • ACD (distribuzione delle chiamate) • Unknown State (stato sconosciuto)

Parametri	Descrizione
Evento	Evento Sono disponibili i seguenti eventi: • Setup (linea: prenotazione in entrata o in uscita) • Setup Ackn (linea: conferma prenotazione) • Info (interfaccia della linea: Info (cifre numero di telefono)) • Call Proc (linea: composizione non valutata) • Progress (linea: informazioni supplementari per la creazione della connessione) • Alert (linea: composizione valutata) • Connect (linea: connessione canale B) • Connect Ackn (linea: conferma connessione canale B) • Disconnect (linea: richiesta di interruzione) • Release (linea: conferma interruzione) • Release Compl (linea: chiamata conclusa) • Monitor On (linea/interfaccia utente: ascolto chiamate avviato) • Monitor Off (linea/interfaccia utente: ascolto chiamate arrestato) • Off Hook (interfaccia utente: ricevitore sollevato) • On Hook (interfaccia utente: ricevitore riagganciato) • Digit (interfaccia utente: selezione delle cifre)
Aggiornamento autom.	Se il flag è attivato, viene eseguito l'aggiornamento automatico della visualizzazione dell'ascolto di una chiamata. Valore predefinito: Attivato
Secondi fino al prossimo aggiornamento	Tempo in secondi trascorso il quale viene eseguito l'aggiornamento dell'ascolto chiamate.

28.2.5.12 Tracce > Componente licenza

Questa funzione viene utilizzata per monitorare l'agente delle licenze (CLA) interno del sistema.

Le modifiche alle impostazioni devono essere apportate solo se richiesto dal servizio di assistenza tecnica competente.

Descrizione dei parametri delle schede:

- **Modifica dei componenti di traccia CLA**

Parametri	Descrizione
Nome pacchetto	Nome del componente traccia licenza.
Livello di traccia	Definizione del livello di dettaglio della registrazione del componente di traccia licenza Valore predefinito: Predefinito
Livello di traccia: bassa	Livello di dettaglio basso per la registrazione della traccia.
Livello di traccia: Predefinito	Livello di dettaglio medio per la registrazione della traccia.

Parametri	Descrizione
Livello di traccia: Tutti	Alto livello di dettaglio per la registrazione della traccia.
Livello di traccia: Off	Componente di traccia licenza arrestato.

28.2.5.13 Tracce > Profili di traccia

I profili traccia contengono componenti di traccia predefiniti per il monitoraggio di unità funzionali complete di un sistema di comunicazione.

Descrizione dei parametri delle schede:

- **Visualizza tutti i profili di traccia**
- **Aggiungi profilo di traccia (profilo vuoto)**
- **Aggiungi profilo di traccia (con impostazioni aggiornate)**
- **Arresta tutti i profili di traccia**
- **Avvia/arresta profilo di traccia**

Parametri	Descrizione
Nome del profilo	Nome del profilo traccia
Profilo avviato	Indicazione se il profilo di traccia è stato avviato.
Profilo di sola lettura	Indicazione se il profilo di traccia è di sola lettura (per impostazione predefinita, tutti i profili di traccia esistenti sono di sola lettura).
Componente di traccia	Nome del componente di traccia
Contenuto	Se il flag è attivato: il componente di traccia viene incluso nel nuovo profilo di traccia da aggiungere. Valore predefinito: Attivato
Livello	Livello di dettaglio della registrazione del componente di traccia (da livello traccia 0 = livello di dettaglio più basso a livello traccia 9 = livello di dettaglio più elevato)

28.2.5.14 Tracce > Componenti di traccia

In base ai componenti di traccia vengono registrate le informazioni di processo e di stato dei singoli componenti del sistema di comunicazione.

Descrizione dei parametri delle schede:

- **Mostra tutti i componenti di traccia**
- **Mostra componenti di traccia avviati**
- **Mostra componenti di traccia arrestati**
- **Modifica componenti di traccia**
- **Arresta tutti i componenti traccia**
- **Avvia/arresta componente traccia**
- **Impostazioni predefinite della traccia**

Parametri	Descrizione
Nome del sub-sistema	Nome del componente di traccia
Indice dei componenti di traccia	Numero progressivo
Livello di traccia	Livello di dettaglio della traccia (da livello traccia 0 = livello di dettaglio più basso a livello traccia 9 = livello di dettaglio più elevato)
Traccia su	Se il flag è attivato, viene eseguita la registrazione dei dati del componente di traccia.

28.2.5.15 Tracce > Trasferimento TCP

Un trasferimento TCP viene utilizzato per il monitoraggio e la valutazione del traffico dati su una rete IP. Per la diagnostica di file trasferimento TCP, è necessaria la relativa applicazione.

Descrizione dei parametri delle schede:

- **Stato trasferimento TCP**

Parametri	Descrizione
Avvia trasferimento TCP	Avvio del trasferimento TCP
Parametri iniziali	
Nome dell'interfaccia	Interfaccia per cui viene analizzato il traffico dati. Le interfacce disponibili vengono visualizzate in **Dettagli interfaccia**. Selezionando la voce **any**, viene eseguita la valutazione del traffico dati per tutte le interfacce disponibili. Valore predefinito: qualsiasi
Dimensione del pacchetto	Dimensione dei pacchetti di dati da registrare, in byte. La voce **0** significa che ogni pacchetto verrà completamente registrato. Valori consentiti: da 0 a 2000000000, valore predefinito: 0
Criteri finali	
Numero di pacchetti	Numero di pacchetti dati oltre il quale il trasferimento TCP viene interrotto.
Tempo fino alla conclusione (s)	Tempo in secondi trascorso il quale viene interrotto il trasferimento TCP.
Termina trasferimento TCP	Arresto del trasferimento TCP
Pulizia del trasferimento TCP	Elimina il file Trasferimento TCP salvato nel sistema di comunicazione
Aggiornamento autom.	Se il flag è attivato, viene eseguito l'aggiornamento automatico della visualizzazione dello stato. Valore predefinito: Attivato

28.2.5.16 Tracce > rpcap Daemon

Un Daemon RPCAP (Remote Packet Capture) viene utilizzato per il monitoraggio e l'analisi del traffico dati su una rete IP. Tramite il daemon RPCAP è possibile per le applicazioni esterne accedere in remoto a pacchetti TCP/IP dell'interfaccia LAN del sistema di comunicazione. Un daemon RPCAP viene spesso impostato per tracce a lungo termine, in quanto i file traccia vengono salvati sul PC e non nel sistema di comunicazione.

Nota: Attenersi alle istruzione i sicurezza indicate sulla scheda.

Descrizione dei parametri delle schede:

- **rpcap**

Parametri	Descrizione
Indirizzo Bind to	
Indirizzo IP (numerico o letterale)	Indirizzo IP dell'host, sul quale vengono eseguite le registrazioni. Valore predefinito: 0.0.0.0
Porta (scegliere una porta libera)	Porta dell'host attraverso la quale vengono eseguite le registrazioni.
LAN interna traccia	Se il flag è attivato, viene eseguita la registrazione del traffico dati tra due moduli attraverso l'interfaccia ETH9. Valore predefinito: Disattivato
Identificazione client per l'accesso	
Indirizzo IP (numerico o letterale)	Indirizzo IP del client remoto sul quale viene eseguito l'output della traccia. Valore predefinito: 0.0.0.0

28.2.5.17 Traces > Kernel Crash Data

The Kernel Crash Data service is used to automatically collect kernel crash data. It is available only on OSBiz X systems with V3 mainboards: OCCLA, OCCMA(R), OCCMB(R).

The service requires a 200 MB of storage space. Disks affected are:

- SATA SSD 16GB (if no NVMe SSD is mounted)
- NVMe SSD

It is recommended to delete traces before starting the service, if you want to free up storage space. If there is no sufficient space, service will not collect data.

Descrizione dei parametri delle schede:

- **Kernel Crash Data**

Parameters	Descrizione
Kernel Crash Data service	Status of the service: Verde: The service is enabled. Grey: The service is disabled.
Start	Starts the Kernel Crash Data service.
Stop	Stops the Kernel Crash Data service.

Upon starting or stopping the Kernel Crash Data Service, a system restart is automatically initiated. The service retains status after system restart.

With the service enabled, after a system restart with reason WATCHDOG or KERNEL_OOPS, kernel crash data are available in the oso diagnostic storage space. In order to collect kernel crash data, the **CoreLog Protocol** checkbox must be selected under **Service Center** > **Diagnostics** > **Trace** > **Diagnosis logs**.

After collecting the kernel crash data, the service must be disabled manually.

28.2.5.18 Tracce > Traccia server multimediale

Traccia server multimediale può essere utilizzato per registrare le informazioni di processo e stato del componente del server multimediale del sistema di comunicazione.

Descrizione dei parametri delle schede:

- **Modifica il componente di traccia server multimediale**

Parametri	Descrizione
Nome pacchetto	Nome del componente di traccia Valore predefinito: Media Server
Livello di traccia	Livello di dettaglio per la traccia (Nessuno, Non specificato, Predefinito, Irreversibile, Errore, Avviso, Informazioni, Imprevisto, Debug, Fine, Ottimo)
Stato traccia	Stato della traccia: Verde: La traccia è attivata. Grigio: La traccia è disattivata.
Avvia	Avvia la traccia del server multimediale.
Arresta	Arresta la traccia del server multimediale.

28.2.6 Eventi

In **Eventi** sono riunite le funzioni che vengono utilizzate per visualizzare e controllare gli eventi (Events). Fra queste, Configurazione eventi e Impostazioni e-mail.

28.2.6.1 Eventi > Configurazione eventi

Descrizione dei parametri delle schede:

- **Modifica configurazione eventi**

Parametri	Descrizione
Impostazioni del file eventi	
Dimensione max. del buffer eventi (byte)	Visualizzazione della dimensione massima del buffer eventi in byte
Dimensione max. del file eventi (byte)	Visualizzazione della dimensione massima del file di registro degli eventi in byte
Timer eventi (sec.)	Visualizzazione del tempo in secondi trascorso il quale viene creato un nuovo file di registro eventi.
Evento tramite LAN	
Attiva registrazione eventi tramite LAN	Se il flag è attivato: i messaggi registro eventi vengono tramite l'interfaccia LAN. Valore predefinito: Disattivato
Valore timer (sec.)	Visualizzazione del tempo in secondi trascorso il quale vi dati di registro eventi vengono trasmessi tramite l'interfaccia LAN.

28.2.6.2 Eventi > Registro eventi

Questa funzione viene utilizzata per scaricare o eliminare il file di registro degli eventi.

Descrizione dei parametri delle schede:

- **Carica via HTTP**
- **Cancellazione registro eventi**

28.2.6.3 Eventi > E-mail

Descrizione dei parametri delle schede:

- **Modifica impostazioni e-mail**

Parametri	Descrizione
Impostazioni e-mail	
Oggetto	Testo visualizzato nel campo oggetto dell'e-mail.
Indirizzi di posta elettronica dei destinatari	
Destinatario 1	Indirizzo di posta elettronica, al quale viene inviata un'e-mail al verificarsi di un evento.

Parametri	Descrizione
Destinatario 2	Indirizzo di posta elettronica, al quale viene inviata un'e-mail al verificarsi di un evento.
Destinatario 3	Indirizzo di posta elettronica, al quale viene inviata un'e-mail al verificarsi di un evento.
Destinatario 4	Indirizzo di posta elettronica, al quale viene inviata un'e-mail al verificarsi di un evento.
Destinatario 5	Indirizzo di posta elettronica, al quale viene inviata un'e-mail al verificarsi di un evento.
Destinatario notifiche di emergenza	
Destinatario emergenza	Indirizzo e-mail di un responsabile della sicurezza in loco a cui viene inviata un'e-mail quando si seleziona un numero di emergenza.

28.2.6.4 Eventi > Tabella delle reazioni

In base alla tabella delle reazioni è possibile definire separatamente per ciascun evento la modalità di reazione.

Descrizione dei parametri delle schede:

- **Modifica tutti gli eventi**
- **Riporta tutti gli eventi alle impostazioni predefinite**
- **Modifica evento**
- **Avvia/arresta profilo traccia associato**

Parametri	Descrizione
Nome dell'evento	Nome dell'evento
Invia Trap SNMP	Se il flag è attivato: quando si verifica l'evento viene inviato un trap SNMP.
Invia e-mail	Se il flag è attivato, viene inviata un'e-mail al destinatario indicato in **Modifica impostazioni e-mail** quando si verifica l'evento.
Profilo di traccia assegnato	Profilo di traccia che può essere avviato o arrestato al verificarsi di eventi.
Avvia profilo di traccia	Se il flag è attivato: il profilo di traccia selezionato viene avviato quando si verifica l'evento.
Arresta profilo di traccia	Se il flag è attivato: il profilo di traccia selezionato viene arrestato quando si verifica l'evento.
Riavvia gateway	Indica se al verificarsi dell'evento il sistema di comunicazione viene riavviato.
Riavvia gateway: Sì	Al verificarsi dell'evento, il sistema di comunicazione si riavvia.
Riavvia gateway: No	Al verificarsi dell'evento, il sistema di comunicazione non si riavvia.
Avvisa OpenScape	Indica se al verificarsi dell'evento viene inviato un messaggio al sistema di comunicazione.
Avvisa OpenScape: Sì	Il verificarsi dell'evento determina l'accesso al sistema di comunicazione.

Parametri	Descrizione
Avvisa OpenScape: No	Il verificarsi dell'evento non determina l'accesso al sistema di comunicazione.

28.2.6.5 Eventi > Registri di diagnostica

Qui vengono visualizzati i registri di diagnostica (file di registro) creati automaticamente in seguito a stati critici del sistema.

Descrizione dei parametri delle schede:

- **Carica registri diagnostica**
- **Come cancellare i registri diagnosi**

Parametri	Descrizione
Nome file	Nome dei registri di diagnostica memorizzati nel sistema di comunicazione (file di registro)
Dimensione (in byte)	Dimensione dei registri di diagnostica, in byte
Modificato	Data della modifica dei registri di diagnostica
Attributi	Attributi dei registri di diagnostica: • r = accesso in lettura • w = accesso in scrittura (write)

28.2.6.6 EventiSegnalazione allarmi

Qui vengono selezionati gli utenti (telefoni di sistema con display, UP0 e HFA) che riceveranno una notifica nel caso in cui la temperatura del sistema superi i 55 °C. Se viene superato 60 gradi Celsius, i moduli responsabili del surriscaldamento (ad esempio OCAB, SLAD60/16) vengono arrestati in modo controllato o spenti.

Descrizione dei parametri delle schede:

- **Modifica segnalazione di allarme**

Parametri	Descrizione
Porte di segnalazione allarme temperatura	
Utente 1	1° destinazione (utente con telefono di sistema).
Telefono 2	2° destinazione (utente con telefono di sistema).
Telefono 3	3° destinazione (utente con telefono di sistema).

28.2.7 Riavvia / Ricarica

Qui è possibile riavviare o ricaricare OpenScape Business o arrestare in modo controllato OpenScape Business X. Oltre a ciò è possibile attivare il riavvio dell'applicazione UC (UC Smart o UC Suite) o della UC Booster Card

(Application Board OCAB). Per consentire un arresto controllato di OpenScape Business X tramite un telefono di sistema, è possibile impostare un PIN. Nel caso di una connessione in rete, è possibile la sincronizzazione dei sistemi di comunicazione collegati in rete.

28.2.7.1 Riavvia / RicaricaRiavvia / Ricarica

Parametri	Descrizione
Sistema	
Riavvia sistema	Riavvio controllato di OpenScape Business • OpenScape Business S e OpenScape Business X: viene eseguito un riavvio controllato del sistema di comunicazione. Se OpenScape Business X3/X5/X8 è dotato di una UC Booster Card (scheda applicazioni OCAB), viene eseguito un riavvio controllato dell'applicazione UC (UC Smart o UC Suite). • OpenScape Business UC Booster Server (server applicazioni): viene eseguito un riavvio controllato della parte OpenScape Business e dell'applicazione UC (UC Suite).
Ricarica sistema	Ricarica di OpenScape Business: • OpenScape Business S e OpenScape Business X: viene ricaricato il sistema di comunicazione. Dopo l'inizializzazione, il sistema di comunicazione si trova nello stato base. Andranno perse tutte le impostazioni internazionali e del cliente (sigla internazionale del sistema = Germania). Il sistema di comunicazione ha l'indirizzo IP predefinito 192.168.1.2 e l'intervallo di indirizzi IP interni 192.168.3.xxx. La concessione delle licenze rimane invariata. • OpenScape Business UC Booster Server: viene ricaricata la sezione relativa a OpenScape Business. Dopo l'inizializzazione, tale sezione si trova nello stato base. Tutte le impostazioni della sezione OpenScape Business specifiche del cliente (ad esempio, l'indice utenti) sono state eliminate. La concessione delle licenze rimane invariata. Il sistema operativo non viene reimpostato.
Arresta sistema	Arresto controllato di OpenScape Business X: • OpenScape Business X3/X5: la successiva inizializzazione del sistema di comunicazione è possibile solo dopo aver scollegato e ricollegato il sistema alla presa di rete. • OpenScape Business X8: la successiva inizializzazione del sistema di comunicazione è possibile solo dopo aver scollegato e ricollegato tutte le fonti di alimentazione LUNA2.
Abilita/disabilita arresto	Definizione di un PIN per attivare lo spegnimento (spegnimento controllato del sistema di comunicazione) tramite un telefono di sistema

Parametri	Descrizione
Riavvia la scheda applicazioni	Riavvio controllato della scheda applicazioni OCAB, con applicazione UC (UC Smart o UC Suite): In caso di riavvio della scheda applicazioni OCAB, le connessioni a tutte le applicazioni attive, ad esempio myPortal for Desktop e myAttendant, vengono interrotte. Dopo l'inizializzazione, tutte le connessioni vengono automaticamente ripristinate.
Applicazioni	
Sincronizza rete	Sincronizzazione dei sistemi di comunicazione connessi in rete: Dopo la modifica dei numeri di telefono, numeri interni o nomi, i dati di tutti i sistemi di comunicazione collegati in rete vengono aggiornati mediante una sincronizzazione.
Riavvia applicazione UC	Riavvio controllato dell'applicazione UC (UC Smart o UC Suite): In caso di riavvio dell'applicazione UC, le connessioni a tutte le applicazioni attive, ad esempio myPortal for Desktop e myAttendant, vengono interrotte. Dopo l'inizializzazione, tutte le connessioni vengono automaticamente ripristinate.

28.2.8 SNMP

In **SNMP** sono riunite le funzioni che vengono utilizzate per la configurazione delle comunità e dei Trap. Tramite le comunità vengono regolate le autorizzazioni di accesso ai dati SNMP. In caso di problemi al sistema vengono creati Trap che informano l'amministratore sulla natura dell'errore e dei guasti.

28.2.8.1 SNMP > Comunità

Descrizione dei parametri delle schede:

- **Mostra comunità**

Parametri	Descrizione
indirizzo IP	Indirizzo IP del partner di comunicazione SNMP All'indirizzo 127.0.0.1 la comunicazione con gli indirizzi IP esterni è bloccata.
Comunità	Identificazione/password di accesso utilizzato per l'utente SNMP. ***INFO:*** per ragioni di sicurezza, si consiglia di non usare il valore predefinito **public**.
Tipo	Scelta del tipo.
Tipo: Comunità di lettura	Partner di comunicazione con accesso SNMP in lettura.
Tipo: Comunità di lettura	Partner di comunicazione con accesso SNMP in lettura e scrittura.
Tipo: Comunità Trap	Partner di comunicazione ai quali vengono inviati i messaggi di errore (trap).

28.2.8.2 SNMP > Comunità > Comunità di lettura

Descrizione dei parametri delle schede:

- **Mostra comunità di lettura**
- **Aggiungi comunità di lettura**

Parametri	Descrizione
indirizzo IP	Indirizzo IP del partner di comunicazione SNMP All'indirizzo 127.0.0.1 la comunicazione con gli indirizzi IP esterni è bloccata.
Comunità	Identificazione/password di accesso utilizzato per l'utente SNMP. ***INFO:*** per ragioni di sicurezza, si consiglia di non usare il valore predefinito **public**.

28.2.8.3 SNMP > Comunità > Comunità di scrittura

Descrizione dei parametri delle schede:

- **Mostra comunità di scrittura**
- **Aggiungi comunità di scrittura**

Parametri	Descrizione
indirizzo IP	Indirizzo IP del partner di comunicazione SNMP All'indirizzo 127.0.0.1 la comunicazione con gli indirizzi IP esterni è bloccata.
Comunità	Identificazione/password di accesso utilizzato per l'utente SNMP. ***INFO:*** per ragioni di sicurezza, si consiglia di non usare il valore predefinito **public**.

28.2.8.4 SNMP > Comunità > Comunità trap

Descrizione dei parametri delle schede:

- **Mostra comunità Trap**
- **Aggiungi comunità Trap**

Parametri	Descrizione
indirizzo IP	Indirizzo IP del partner di comunicazione SNMP All'indirizzo 127.0.0.1 la comunicazione con gli indirizzi IP esterni è bloccata.
Comunità	Identificazione/password di accesso utilizzato per l'utente SNMP. ***INFO:*** per ragioni di sicurezza, si consiglia di non usare il valore predefinito **public**.

28.2.8.5 SNMP > Trap

Descrizione dei parametri delle schede:

- **Mostra tutti i Trap**
- **Mostra tutti i Trap critici**

Parametri	Descrizione
VarBind1 (Gravità)	Classificazione dei trap: • Critical: messaggio di errore. L'errore ha conseguenze problematiche. • Major: messaggio di errore. L'errore può avere conseguenze problematiche. • Minor: messaggio di errore. L'errore non causa problemi particolari. • Avvertenza: messaggi su un possibile problema a una procedura o in uno stato. • Cleared: la causa del messaggio di errore è stata eliminata (ad esempio, la porta è di nuovo attiva) • Informazioni: semplici messaggi di stato, non di errore
VarBind2 (Nome)	Nome del Trap
Nome generico	Denominazione generale, ad esempio un nome specifico dell'azienda
Nome specifico	Tipo di trap: • 1 = Software • 2 = Hardware
Enterprise	(non utilizzato)
Tempo	Ora dell'errore
Indice	Numero progressivo

28.2.9 Registro Admin

Con **Registro Admin** l'amministratore può modificare la configurazione (ad es. la lingua) del registro di amministrazione.

28.2.9.1 Protocollo Admin > Configurazione

Descrizione dei parametri della scheda:

- **Modifica configurazione**

Parametri	Descrizione
Lingua del registro Admin	Impostazione della lingua desiderata per il registro Admin. Il registro Admin fornisce una panoramica delle modifiche eseguite sul sistema di comunicazione. Lingue disponibili: tedesco, inglese, francese, spagnolo, italiano, portoghese e olandese

28.2.9.2 Protocollo Admin > Dati del registro Admin

Descrizione dei parametri della scheda:

- **Carica via HTTP**

Parametri	Descrizione
Carica via HTTP	Salva il protocollo Admin del sistema di comunicazione. Il registro Admin consente di definire quando devono essere effettuate modifiche al sistema di comunicazione e da chi. Vengono registrati gli accessi al sistema di comunicazione.

28.2.10 Azioni

In **Azioni** sono riunite le funzioni che vengono utilizzate più di frequente dall'amministratore, ad esempio la cancellazione dei dati di registro.

28.2.10.1 Azioni > Azioni manuali > Registri di diagnostica

Descrizione dei parametri delle schede:

- **Carica dati tramite HTTP**

Parametri	Descrizione
Registro di traccia	Se il flag è attivato: vengono scaricati i file di registro di traccia del sistema. Sono disponibili le seguenti opzioni: • Registro di traccia completo: vengono scaricati tutti i file di registro di traccia del sistema disponibili. • Registro odierno: vengono scaricati i file di registro di traccia del sistema del giorno (a partire dalle ore 00:00). • Selezione propria: Da: XXX a: YYY: Vengono scaricati i file di registro di traccia del sistema per il periodo indicato. Valore predefinito: attivato, registro completo
Registro eventi	Se il flag è attivato: vengono scaricati i file di registro con informazioni su azioni/eventi del sistema di comunicazione (reset, attivazione/disattivazione ecc.). Valore predefinito: Attivato
Registro admin	Se il flag è attivato: vengono scaricati i file di registro con informazioni su attività amministrative (tentativi di accesso ecc.). Valore predefinito: Attivato
Protocolli licenza	Se il flag è attivato: vengono scaricati file di registro con messaggi sui componenti del sistema di comunicazione che richiedono una licenza. Valore predefinito: Attivato
Traccia cliente	Se il flag è attivato: vengono scaricati i file di registro con messaggi traccia cliente (accesso remoto, accesso ITSP ecc.). I messaggi per la traccia cliente vengono visualizzati in formato più dettagliato rispetto al protocollo Traccia. Valore predefinito: Attivato
Protocollo Framework	Se il flag è attivato: vengono scaricati file di registro con messaggi del WBM. Valore predefinito: Attivato

Parametri	Descrizione
Registro di diagnostica	Se il flag è attivato: vengono scaricati i registri di diagnostica del sistema di comunicazione. Valore predefinito: Attivato
Protocollo UC Suite	Se il flag è attivato: vengono scaricati file di registro con messaggi della UC Suite (registri UC Suite, CSP e MEB). Sono disponibili le seguenti opzioni: • Registro di traccia completo: vengono scaricati tutti i file di registro disponibili di UC Suite, CSP e MEB. • Registro odierno: vengono scaricati i file di registro di UC Suite, CSP e MEB relativi al giorno in corso (a partire dalle ore 00:00). • Selezione propria: Da: XXX a: YYY: Vengono scaricati i file di registro di traccia di UC Suite, CSP e MEB relativi al periodo indicato. Tutti i file di registro vengono riuniti in un file compresso. Il nome del file dei registri di OpenScape Business deve rispettare le convenzioni seguenti: file di registro del protocollo UC Suite = vs_aaaa_mm_gg.log, file di registro CSP = csptrace_aaaa_mm_gg.log, file di registro MEB = mebtrace_aaaa_mm_gg.log Valore predefinito: Disattivato
Protocolli applicazioni	Se il flag è attivato: vengono scaricati file di registro con messaggi della parte applicazioni del sistema di comunicazione (ad esempio, registri CSP. • Registro di traccia completo: Tutti i file di registro disponibili vengono scaricati. • Registro odierno: vengono scaricati i file di registro relativi al giorno in corso (a partire dalle ore 00:00). • Selezione propria: Da: XXX a: YYY: vengono scaricati i file di registro relativi al periodo indicato. Tutti i file di registro vengono riuniti in un file compresso. Valore predefinito: Disattivato
Protocolli diagnosi sistema	Se il flag è attivato: vengono scaricati i registri di diagnostica del sistema di comunicazione. Valore predefinito: Attivato
Protocollo PPP	Se il flag è attivato: vengono scaricati file di registro con messaggi sul protocollo punto-punto. Valore predefinito: Attivato
Protocollo CoreLog	Se il flag è attivato: vengono scaricati i file di registro con informazioni sullo stato più recente del sistema operativo. I CoreLogs vengono creati ad esempio al riavvio. Valore predefinito: Disattivato

28.2.10.2 Azioni > Azioni manuali > Manutenzione DLI

Descrizione dei parametri delle schede:

- **Manutenzione dispositivi DLI**

Parametri	Descrizione
Elimina dispositivo	Consente di selezionare il telefono di sistema da eliminare. Con questa operazione il telefono di sistema viene eliminato dal database DLI. **Nota:** Prima di effettuare qualsiasi intervento di manutenzione DLI (eliminazione), accertarsi che il dispositivo non venga più utilizzato.
N. chiamata	Numero del telefono di sistema.
Tipo di dispositivo	Tipo di telefono di sistema.
Indirizzo IP	Indirizzo IP del telefono di sistema; collegamento diretto al WBM del telefono di sistema.
Indirizzo MAC	Indirizzo MAC del telefono di sistema.
Versione software corrente	Versione software del telefono di sistema corrente.

28.2.10.3 Azioni > Azioni automatiche > Garbage Collection

Descrizione dei parametri delle schede:

- **Modifica azione**
- **Avvia/arresta azione**

Parametri	Descrizione
Azione attivata	Se il flag è attivato: qui è possibile eseguire periodicamente una pulizia della memoria del sistema di comunicazione. Al termine della pulizia della memoria, il sistema di comunicazione si riavvia. Valore predefinito: Disattivato
Ora di inizio dopo la mezzanotte	Ora dopo la mezzanotte in cui viene eseguita l'operazione di garbage collection. Esempio: nel campo **Ore** è stato inserito 3 e nel campo **Min.** 30. Ciò significa che l'azione Garbage Collection inizierà la mattina alle 3:30. Valore predefinito: 3 ore, 00 min.
Esegui azione i seguenti giorni della settimana	L'azione Garbage Collection viene eseguita nel giorno della settimana selezionato. Valore predefinito: Attivato

28.2.10.4 Azioni > Azioni automatiche > Notifica DLS

Descrizione dei parametri delle schede:

- **Modifica azione**
- **Avvia/arresta azione**

Parametri	Descrizione
Azione attivata	Se il flag è attivato: durante l'avvio del sistema di comunicazione, viene attivato l'accesso automatico a un server remoto DLS. Valore predefinito: Disattivato
indirizzo IP	Indirizzo IP del server DLS esterno Valore predefinito: 0.0.0.0
Porta	Porta del server DLS esterno Valore predefinito: 10444
Nome d'utente	Nome utente per l'accesso al server DLS esterno
Password	Password per l'accesso al server DLS esterno

28.2.10.5 Azioni > Azioni automatiche > Controllo di salute SDHC

Descrizione dei parametri delle schede

- Stato di salute SDHC

Parametri	Descrizione
Stato di salute SDHC	
Avvia controllo salute	Consente di attivare il controllo salute immediato della scheda
Avvia controllo salute il	Consente di indicare giorno, mese, anno e ora pianificati per il controllo salute della scheda.
File log Viene visualizzato il risultato degli ultimi controlli file.	
Stato/Azione consigliata Azioni consigliate per ogni stato di salute della scheda.	

28.2.11 Diagnostica piattaforma

Opzioni per la diagnostica della piattaforma (solo per lo sviluppo).

28.2.12 Diagnostica applicazione

Opzioni per la diagnostica dell'applicazione (solo per lo sviluppo).

28.2.12.1 Diagnostica applicazione > Impostazioni sviluppatore > Output console traccia

Opzioni per la diagnostica dell'applicazione (solo per lo sviluppo).

28.2.12.2 Diagnostica applicazione > Impostazioni sviluppatore > Accetta accesso in scrittura

Opzioni per la diagnostica dell'applicazione (solo per lo sviluppo).

28.2.12.3 Diagnostica applicazione > Scheda madre

Le modifiche alle impostazioni devono essere apportate solo se richiesto dal servizio di assistenza tecnica competente.

28.2.12.4 Diagnostica applicazione > Impostazioni sviluppatore > Profili Provider SIP

Descrizione dei parametri dei tag:

- Aggiungi profili Provider SIP
- Modifica profili Provider SIP

Questa pagina deve essere utilizzata da tecnici altamente qualificati durante la certificazione di un nuovo ITSP. Per ulteriori informazioni, fare riferimento ai documenti disponibili sul sito Unify Wiki all'indirizzo http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#How_to_get_a_new_VoIP_provider_released.

28.2.13 Diagnosi IP

Possibilità di diagnosi IP (solo per lo sviluppo).

28.2.13.1 Diagnosi IP > Scheda madre > Protocollo ARP

Questa funzione viene utilizzata per visualizzare i dati del protocollo di risoluzione dell'indirizzo ARP. La tabella delle mappature mostra l'allocazione degli indirizzi di rete agli indirizzi MAC.

Descrizione dei parametri delle schede:

- **Mostra protocollo ARP**

Parametri	Descrizione
indirizzo IP	Mostra gli indirizzi di rete attualmente collegati alla scheda madre del sistema di comunicazione.
Indirizzo MAC	Mostra l'indirizzo fisico corrispondente degli indirizzi di rete collegati
Tipo	Mostra l’assegnazione degli indirizzi. È possibile un'assegnazione fissa o dinamica.
Interfaccia	Descrizione interna delle interfacce LAN esistenti (ad esempio, eth0, eth1, eth2, eth3)

28.2.13.2 Diagnosi IP > Scheda madre > Richiesta ICMP > Ping

Utilizzando questa funzione, è possibile testare la connessione di rete tra il sistema di comunicazione e un indirizzo di destinazione liberamente selezionabile, con l'aiuto di un comando ping (richiesta eco).

Descrizione dei parametri delle schede:

- **Esegui ping**

Parametri	Descrizione
Parametri ICMP	
Indirizzo di destinazione	Indirizzo IP della destinazione la cui connessione di rete al sistema di comunicazione viene verificata mediante pacchetti di richiesta eco. Valore predefinito: 127.0.0.1
Numero di richieste eco da inviare	Numero di richieste eco da inviare per verificare la connessione di rete Valore predefinito: 3

28.2.13.3 Diagnosi IP > Scheda madre > Richiesta ICMP > Traceroute

Questa funzione utilizza richieste eco ICMP per determinare tramite quale router trasmettere i pacchetti di dati per l'indirizzo di destinazione richiesto.

Descrizione dei parametri delle schede:

- **Traceroute**

Parametri	Descrizione
Parametri ICMP	
Indirizzo di destinazione	Indirizzo IP della destinazione la cui rotta di traccia al sistema di comunicazione viene verificata mediante richieste eco ICMP. Valore predefinito: 127.0.0.1
Byte TOS	Indicazione se i byte TOS (Type Of Service) vengono inviati. I byte TOS forniscono informazioni sulla qualità di un servizio. Valori consentiti: da 0 a 255, valore predefinito: 0

28.2.14 Utente online

Strumento Web per il controllo remoto di telefoni OpenStage.

28.2.14.1 Utente online

L'applicazione Utente online apre il Java Husim Phone Tester (jHPT). Questo è uno strumento Web per il controllo remoto di telefoni OpenStage tramite Internet. Attraverso un'interfaccia Web, è possibile controllare un telefono di sistema trasmettendo le pressioni dei tasti effettive e le informazioni visualizzate

del sistema di comunicazione. Per il jHPT è disponibile una documentazione separata che può essere scaricata mediante la funzione Guida dei tool (in questa sede non viene fornita alcuna descrizione delle pagine jHPT).

28.3 Telefonia

In **Telefonia** sono raggruppate le funzioni per la configurazione della telefonia, quali ad esempio utente o Gestione chiamate (CM).

28.3.1 Impostazioni di base

In **Impostazioni di base** sono riunite funzioni quali Flag di sistema, impostazioni per Rubriche e Destinazioni di selezione breve, DynDNS, Quality of Service, Data e Ora, Addebiti.

28.3.1.1 Impostazioni di base > Sistema > Flag di sistema

Descrizione dei parametri delle schede:

- **Modifica flag di sistema**

Parametri	Descrizione
Interconnessione con DEV esterna on	Se il flag è attivato: in caso di deviazione di chiamata esterna, la chiamata viene passata immediatamente. Non fa differenza se si tratta di una chiamata interna o esterna (HKZ/ISDN). Se la deviazione di chiamata avviene tramite una linea ISDN e la destinazione di inoltro esterna si trova in un'altra rete (ad esempio rete GSM), l'instaurazione della connessione viene segnalata dalla linea ISDN tramite l'indicatore di avanzamento ISDN. Da questo momento vengono generati costi di connessione addebitati al chiamante. Valore predefinito: Disattivato
DEV su linea analogica permessa	Se il flag è attivato, le chiamate tramite linee esterne analogiche (HKZ) seguono la deviazione di chiamata esterna. Valore predefinito: Attivata
Inoltro chiamata dopo DEV alla destinazione esterna	Se il flag è attivato: se la destinazione di inoltro esterna non è raggiungibile, viene eseguito un inoltro di chiamata alla successiva destinazione specificata nella Lista destinazioni chiamata. Valore predefinito: Disattivato
Tono di conferenza	Se il flag è attivato: viene emesso un tono speciale ogni 20 secondi per ricordare ai partecipanti a una conferenza che sono impegnati in una conferenza. Valore predefinito: Disattivato

Parametri	Descrizione
Squillo di avviso in gruppi RPA	Se il flag è attivato: una chiamata per un membro di un gruppo di risposta viene segnalata visivamente (sul display) agli altri membri del gruppo. Se la chiamata non riceve una risposta entro quattro cicli di chiamata (4 x 5 secondi), gli altri membri del gruppo ricevono inoltre un tono di avviso. Valore predefinito: Attivata
Alzare il volume per i terminali optiPoint/ OpenStage	Se il flag è attivato: per i telefoni OptiPoint e OpenStage si passa a un piano di attenuazione alternativo che consente di alzare il volume dell'altoparlante. Valore predefinito: Disattivato
Cambio di terminali permesso	Se il flag è attivato: i telefoni di sistema possono essere spostati (per trasferimento/cambio numero) fisicamente senza dover modificare la configurazione logica (numero di telefono, nome, programmazione dei tasti ecc). Valore predefinito: Disattivato
Più di un partecipante esterno alla conferenza	Se il flag è attivato: più utenti esterni possono partecipare a una conferenza. Valore predefinito: Attivata
Prenotazione automatica della linea	Se il flag è attivato: un utente può prenotare una linea se non è disponibile alcuna linea esterna libera. Non appena si libera una linea, viene eseguita una richiamata ed è possibile stabilire la connessione esterna. Valore predefinito: Disattivato
Rip.ultimo nr. con PKZ	Se il flag è attivato: in caso di ripetizione della selezione, oltre al numero di telefono viene ripetuto anche il codice addebito eventualmente immesso in precedenza. Valore predefinito: Disattivato
Impegno automatico della linea	Quando questo flag è attivato, la composizione di una singola cifra in un telefono di sistema causa immediatamente l'impegno di una linea e viene composto il numero di chiamata richiesto. Non è necessario comporre il codice di accesso. Per comporre un utente interno, è necessario utilizzare una delle seguenti procedure: • Premere il tasto Interno (il tasto Muto diventa Interno se è attiva la composizione semplificata) e comporre il numero dell'utente • o premere il tasto DSS corrispondente. Questa funzione è disponibile solo se è stato configurato un solo fascio (vedere Fasci). Se Voce, ISDN o i telefoni a/b sono ancora collegati nel sistema di comunicazione, non è possibile utilizzare LCR con composizione automatica.
Usare per MSN solo numeri installati	Se il flag è attivato: su un bus S0 è possibile configurare numeri MSN (Multiple Subscriber Number) solo per numeri di telefono interni già presenti (a prevenzione dell'abuso dell'utilizzo). Valore predefinito: Disattivato

Parametri	Descrizione
Ottimizzazione delle rotte	Se il flag è attivato: nei sistemi di comunicazione collegati in rete viene realizzata una ottimizzazione del percorso. Questo flag deve essere attivato su tutti i sistemi di comunicazione appartenenti a una data rete. Esempio di due sistemi collegati in rete (sistema 1 e sistema 2): con una chiamata dall'utente A (sistema 1) all'utente B (sistema 2) e poi la deviazione di chiamata all'utente C (sistema 1), vengono occupate due linee. Grazie all'ottimizzazione delle rotte, la connessione di A a C viene passata automaticamente su una sola linea. Valore predefinito: Attivata
DTMF automatica	Se il flag è attivato: dopo ogni connessione in uscita andata a buon fine, si torna automaticamente alla modalità DTMF (modalità MFV). Ciò consente ad esempio l'interrogazione remota delle segreterie telefoniche. Valore predefinito: Attivata
Cercapersone con collegamento duplex	Se il flag è attivato, la chiamata diretta (paging) permette di collegarsi con un utente interno senza che questi sollevi il ricevitore. Sollevando il ricevitore si passa alla normale conversazione a due. Valore predefinito: Attivata
Tono di linea urbana	Se il flag è attivato: una connessione linea esterna o a un sistema di comunicazione collegato in rete viene attivata anche se non si riceve il segnale dall'utente chiamato. Valore predefinito: Disattivato
Rifiuto chiam.con add.al chiamante	Se il flag è attivato: le chiamate con addebito vengono automaticamente abilitate. Valore predefinito: Disattivato
Euroimpedenza	Se il flag è attivato, in Europa si applicano i seguenti valori di impedenza: le interfacce a/b per terminali analogici: impedenza d'ingresso = 270 Ohms + 750 Ohms || 150 nF, impedenza susseguente = 270 Ohms + 750 Ohms || 150 nF, livello relativo A/D = 0 dBr, livello relativo D/A = –7-7 dBr le interfacce a/b per linee analogiche: impedenza d'ingresso = 270 Ohms + 750 Ohms || 150 nF, impedenza susseguente = 270 Ohms + 750 Ohms || 150 nF, livello relativo A/D = 6-6 dBr, livello relativo D/A = –1-1 dBr Valore predefinito: Disattivato
Diversi annunci Phonemail giorno/notte	Se il flag è attivato: sui sistemi di comunicazione con Phonemail, è possibile attivare diversi annunci casella vocale per un utente, inviando sulla diversi numeri di telefono per tale utente alla casella vocale. A tal fine, è necessario che per questi utenti siano stati configurati inoltri diversi per l'utilizzo notturno e quello diurno. Valore predefinito: Disattivato

Parametri	Descrizione
Visualizzare codice internazionale / nazionale	Se il flag è attivato: consente di definire il formato di visualizzazione dei numeri di selezione breve nelle chiamate in entrata, quando nella memoria di selezione breve non è memorizzato il relativo numero breve. Per le chiamate in entrata, sul display del telefono viene visualizzato il numero di telefono completo (numero del sistema + selezione passante, inclusi prefisso interurbano e prefisso internazionale, se disponibile). Esempio: Il numero di selezione breve 06671234 è stato configurato senza nome. Prefisso interurbano = 02302, numero del sistema = 667, selezione passante = 1234. Per le chiamate in entrata dal 6671234, sul display viene visualizzato 023026671234. Valore predefinito: Disattivato
Cambio linea su chiamata diretta	Questo flag consente di definire il comportamento di un tasto per chiamata diretta quando è attiva una connessione voce su linea MULAP. Disponibile per la configurazione team/gruppo Team, Direttore/Segretaria / gruppo Top, Basic MULAP, Direttore MULAP. Dopo aver premuto un tasto per chiamata diretta viene eseguito un cambio linea. La chiamata viene messa in attesa e può essere ripresa solo su questo telefono. Valore predefinito: disattivato (non per USA e Canada), attivato (solo per USA e Canada)
Ripetizione automatica dell'ultimo nr. selez.	In caso di utente occupato viene eseguita la ripetizione automatica dell'ultimo numero selezionato. Il parametro di tempo Tempo ripetizione automatica ultimo nr. selez. consente di definire dopo quanto tempo diventa attiva la ripetizione della selezione. Valore predefinito: Disattivato
Nr. di tel. nodo con voicemail	Se il flag è attivato: nei sistemi di comunicazione collegati in rete, consente di definire se il numero di telefono del nodo deve essere fornito in fase di identificazione di un server di posta vocale centrale o di più di server di posta vocale decentrati. Il numero di telefono del nodo deve essere fornito per l'identificazione del o dei server di posta vocale. Valore predefinito: Disattivato
RPA alla richiamata	Se il flag è attivato: le richiamate e le prenotazioni vengono segnalate anche agli altri membri di un gruppo di risposta per assente e possono essere accettate da questi. Valore predefinito: Disattivato
CLIP impostabile	Se il flag è attivato: invece del numero di telefono, viene trasmesso all'utente esterno chiamato, e visualizzato sul display, il numero registrato in Clip/Lin. In caso di voce Clip/Lin vuota, viene inviato il numero di telefono. Valore predefinito: Attivata
Liste chiamanti presso l'utente di destinazione in caso di deviazione MULAP	Se il flag è attivato: in caso di trasferimento MULAP, le chiamate in entrata vengono inserite nella lista chiamate dell'utente di destinazione. Valore predefinito: Disattivato

Parametri	Descrizione
Inoltro di chiamata verso trasferimento Deflect call / Single step	Se il flag è attivato: se l'utente ha attivato una deviazione di chiamata verso una destinazione interna (Deflect Call), la chiamata viene segnalata a tale destinazione. Trascorso il tempo di inoltro chiamata, la chiamata viene segnalata ad una prima destinazione specificata nella Lista destinazioni chiamata, e successivamente alla seconda destinazione eventualmente specificata. Esempio: Per l'utente A è stata eseguita una Deflect Call all'utente B. il quale, nella sua Lista destinazioni chiamata, ha specificato come prima destinazione l'utente C e come seconda destinazione l'utente D. La chiamata viene segnalata all'utente C e, trascorso il tempo di inoltro chiamata, all'utente D. L'attivazione di questo flag ha senso solo se viene attivato anche il flag Rilevamento della destinazione mediante l'Elenco destinazioni chiamate per trasferimento Deflect call. Affinché questo flag abbia effetto, le funzioni di reindirizzamento avverranno in chiamata, deviazione e trasferimento a passaggio singolo e si applica principalmente alle chiamate gestite tramite UC (gruppi Posto operatore/UCD) a cui sono applicabili tali funzioni. Valore predefinito: Attivata
Rilevamento della destinazione mediante l'Elenco destinazioni chiamate per trasferimento Deflect call	Se il flag è attivato: se l'utente ha attivato una deviazione di chiamata verso una destinazione interna (Deflect Call), la chiamata viene segnalata a tale destinazione e, trascorso il tempo di inoltro chiamata, ad una ulteriore destinazione specificata nella Lista destinazioni chiamata. Esempio: Per l'utente A è stata eseguita una Deflect Call all'utente B. il quale, nella sua Lista destinazioni chiamata, ha specificato come prima destinazione l'utente C. Trascorso il tempo di inoltro chiamata, la chiamata viene segnalata all'utente C. Affinché questo flag abbia effetto, le funzioni di reindirizzamento avverranno in chiamata, deviazione e trasferimento a passaggio singolo e si applica principalmente alle chiamate gestite tramite UC (gruppi Posto operatore/UCD) a cui sono applicabili tali funzioni. Valore predefinito: Attivata
Tono di avviso durante la registrazione vocale	Se il flag è attivato, per OpenScape Business X si applica quanto segue: se durante una chiamata si attiva la registrazione vocale (Live Call Record) e il flag è impostato, viene emesso un tono di avviso corrispondente. Valore predefinito: Attivata
Numerazione E.164	Questo flag viene utilizzato per attivare o disattivare la connessione alla rete CDB di sistemi utente globali o estesi. Gli utenti possono essere raggiunti tramite un numero pubblico (il numero di chiamata E.164) in formato nazionale o internazionale (ad esempio, il numero di chiamante interno in formato ISDN), senza dover comporre prima un numero di nodo. Ogni utente è rappresentato da un proprio numero E.164, che può essere visualizzato in formato ottimizzato. Se il flag è attivato, il numero interno della chiamata viene trasferito in formato E.164. Se questo flag è impostato, gli utenti SIP vengono registrati con la versione lunga del numero di chiamata E.164 (numero di posizione + numero interno di chiamata interno, ad esempio, 4923026673665). Valore predefinito: Disattivato

Parametri	Descrizione
Funzionalità Key avanzata	Se il flag è attivato, una volta definito il tasto "Maiusc", solo i numeri di telefono senza supporto LED possono essere salvati al secondo livello, ora disponibile. È possibile programmare qualsiasi funzionalità tasti nel primo livello. La segnalazione LED è associata solo al primo livello. Valore predefinito: Disattivato
Numero chiamante in gruppi di risposta / gruppi di segnalazione chiamate / CFN / RNA	Se il flag è attivato: è possibile definire se il numero di telefono e il nome di un chiamante vengono mostrati a tutti i membri di un gruppo di risposta per assente, agli utenti inclusi nella segnalazione delle chiamate e alle destinazioni di inoltro di chiamata e di deviazione di chiamata. Numero di telefono e nome vengono visualizzati sul display. Valore predefinito: Attivata
Supporto SPE	Se il flag è attivato: il servizio di crittografia segnalazione e payload SPE è supportato. Vengono crittografati i flussi di dati d'uso e di segnalazione VoIP da e al sistema di comunicazione e tra telefoni di sistema OpenStage. Valore predefinito: Disattivato **Nota:** Se si desidera utilizzare il servizio cloud, Unify Video, occorre disattivare **Supporto SPE** per registrare la linea, a meno che non sia presente un certificato SPE importato nel sistema.
Tono di avviso SPE	Se il flag è attivato: se è disponibile supporto SPE e se viene utilizzato un telefono OpenStage 15, 20, 20 E o 20 G, un utente viene informato di una connessione non crittografata tramite visualizzazione sul display e con segnale acustico. L'attivazione del parametro utente Sicurezza payload è un prerequisito per utilizzare SPE tramite un utente. Quando si utilizza un telefono OpenStage 40, 40 G, 60, 60 G, 80 o 80 G, non viene emesso alcun bip. Lo stato della connessione (crittografato/in chiaro) viene visualizzato in modo permanente sul display. Valore predefinito: Disattivato **Nota:** Se si desidera desideri utilizzare il servizio cloud, Unify Video, occorre disattivare **Tono di avviso SPE** per registrare la linea, a meno che non sia presente un certificato SPE importato nel sistema.
Transito da SIP Prov. a SIP Prov.	Se il flag è attivato: con interfacciamenti ITSP sono consentite le connessioni di linea di transito. Le chiamate sulla linea di transito si svolgono quando una chiamata impegna due linee dello stesso sistema di comunicazione. Esempio: Una chiamata esterna viene inoltrata a un utente interno tramite un ITSP. L'utente interno trasferisce la chiamata di nuovo tramite un ITSP a una destinazione esterna. Ciò instaura una connessione di linea di transito all'interno del sistema di comunicazione. Per la durata della chiamata, due linee saranno occupate. Le connessioni di linea di transito sono consentite. Valore predefinito: Disattivato

Parametri	Descrizione
Selezione di * e # sulle interfacce di linea	Se il flag è attivato: è possibile l'attivazione e la disattivazione di servizi Centrex tramite linee IP (ITSP) e linee ISDN. Diversi provider mettono a disposizione servizi Centrex (Central Office Exchange), che possono essere attivati e disattivati mediante dei codici. Il codice deve essere immesso durante la selezione del numero (ad esempio dopo l'immissione del codice di linea). L'immissione inizia sempre con i simboli * (asterisco) o # (cancelletto). Poi si inserisce il codice vero e proprio (cifre da 0 a 9) e infine il carattere # (tasto cancelletto). Durante una conversazione non è possibile attivare o disattivare i servizi Centrex. L'attivazione e disattivazione dei servizi Centrex tramite linee IP (ITSP) e linee ISDN è possibile. Valore predefinito: Disattivato
Aggiungi codice del fascio per MEX	Si applica solo per le chiamate esterne effettuate tramite il servizio ITSP "Mobile Extension (MEX)". Se il flag è attivato, per le chiamate esterne, il sistema aggiunge automaticamente il codice di linea urbana al numero di telefono quando il numero è costituito da più di 7 cifre, poiché interpreta tale numero come un numero di telefono esterno. Se il numero di telefono è costituito da meno di 7 cifre, il codice di linea urbana non viene aggiunto perché il sistema interpreta il numero come numero interno. Se il flag è disattivato, il provider di servizi deve aggiungere il codice di linea urbana al numero di telefono per tutte le chiamate in uscita esterne. Valore predefinito: Disattivato
Suoneria CMI MWI	Se il flag è attivato, viene attivato il tono di avviso come segnalazione messaggio in attesa (MWI) per i telefoni DECT (CMI: Cordless Multicell integration). All'arrivo di nuovi messaggi nella casella vocale viene inviato un tono di avviso. Valore predefinito: Disattivato
Aggiornamento automatico software telefoni OpenStage TDM	Se questo flag è attivato, quando la versione software di un telefono TDM è meno recente rispetto alla versione software del sistema, il software del telefono viene automaticamente aggiornato. Valore predefinito: Attivata

Parametri	Descrizione
Limitare le connessioni di linea indirette dei gruppi secondo la Matrice Col	Se un'azienda ha filiali in diverse città, ogni filiale può avere una linea con il fornitore nazionale di telecomunicazioni. Queste filiali possono inoltre essere collegate tra loro attraverso linee private. Per motivi di regolamentazione nazionale (ad esempio, in India) può essere illegale effettuare la seguente connessione: un utente usa la linea privata dal proprio sistema di comunicazione a un sistema di comunicazione privato in un'altra città, quindi a un'altra linea di fornitura nazionale di telecomunicazione per raggiungere una destinazione esterna locale. Invece si consiglia di utilizzare direttamente una linea di fornitura nazionale di telecomunicazione per effettuare chiamate tra città. Questo requisito viene attuato come segue: • Le connessioni tra linee private possono essere limitate configurando la matrice VBZ. • Per le linee private che offrono funzionalità di inoltro chiamata, trasferimento e conferenza, è stato introdotto il flag "Limitare le connessioni di linea indirette dei gruppi secondo la Matrice VBZ". L'attivazione/ disattivazione di questo flag ha i seguenti effetti: – Attivata: le chiamate tra città con linee private sono limitate. – Disattivata: le chiamate tra città con linee private sono concesse. Valore predefinito: Disattivato
Numerazione aperta	
attiva	Se è impostata la numerazione aperta, un utente viene identificato grazie al numero del nodo, seguito da numero di telefono o di selezione passante. In questo modo è possibile assegnare lo stesso numero di telefono agli utenti di diversi nodi. In un collegamento in rete, questo flag è identico per tutti i sistemi. Valore predefinito: Disattivato
Numero del nodo	Registrare il numero del nodo in questo campo se la numerazione è aperta. Un utente può essere chiamato da altri nodi solo selezionando questo numero di nodo seguito dal numero di telefono utente. Se la somma delle cifre del numero di nodo e del numero di telefono dell’utente è superiore a 7, viene emesso un avviso. Valore predefinito: Disattivato
Permesso di transito	
Servizio di transito	Se il flag è attivato: sono consentite le connessioni di transito collegate a determinati servizi, quali ad esempio la deviazione di chiamata esterna, la trasferta e le applicazioni DISA. Non fa differenza se si tratta di connessioni sul linea TIE o da linea esterna a linea esterna. Valore predefinito: Attivata
Sel.passante transito lin. TIE	Se il flag è attivato: con connessioni incrociate (sistemi di comunicazione collegati in rete) sono consentite le connessioni di transito in selezione passante. Valore predefinito: Attivata

Parametri	Descrizione
Sel.passante transito lin.urbana	Se il flag è attivato: sono consentite le connessioni di transito in selezione passante con collegamenti da linea esterna a linea esterna. Valore predefinito: Disattivato
Interruttore speciale	
Non inviare CALL PROC	Questo flag deve essere attivato se il provider di servizi non deve ricevere alcun Call Proceeding Message (messaggio ISDN) dal sistema di comunicazione. Valore predefinito: Disattivato
Impegno linea ciclico, autom.	Se il flag è attivato, in caso di errore di connessione (ad esempio mancata conferma di ricezione) le chiamate in uscita impegnano ciclicamente nuove linee ISDN. I codici della linea o del fascio vengono incrementati. Valore predefinito: Attivata
Restrizione per le chiamate UC	
Restrizione per le chiamate UC	Se il flag è attivato, prima della composizione tutte le chiamate UC effettuate dal sistema (ad esempio tramite il servizio CallMe) vengono verificate per assicurarsi che l'utente UC che richiede il servizio disponga dell'abilitazione per quel tipo di chiamata. Se l'utente UC non dispone della necessaria abilitazione, la chiamata non viene eseguita. Valore predefinito: Disattivato

28.3.1.2 Impostazioni di base > Sistema > Temporizzazioni

Nella tabella sono elencati tutti i parametri temporali modificabili (colonna **Descrizione)**. Le colonne **Base**e **Fattore**consentono di impostare il valore del timer per ciascun parametro di tempo. Ne consegue che: Tempo effettivo = Base x Fattore. Se nella colonna **Fattore** viene specificato il valore 255, il timer diventa inattivo.

Descrizione dei parametri delle schede:

- **Modifica Temporizzazioni**

Parametri	Descrizione
NoFe tempo selez. cifre/ tempo attivaz. ricevitore DTMF	Il timer controlla la durata della connessione del ricevitore del codice con i terminali DTMF e perciò la condizione Pronto alla selezione. Allo scadere di tale timer, il ricevitore di codice viene rilasciato. Valori consentiti: 5-15 s
Tempo per l'attivazione di servizi NoFe	Questo timer viene attivato quando si preme il tasto R su un terminale. Il tasto R aiuta a distinguere se un utente vuole riprendere una prenotazione in attesa o se vuole attivare un servizio del tipo per esempio conferenza. Valori consentiti: 2-4 s
Tempo blocco di rimpegno linea	Questo timer viene attivato dopo il rilascio della linea e per tutta la durata dell'intervallo blocca un impegno immediato in uscita. Valori consentiti: 0-5 s

Parametri	Descrizione
Tempo di ritardo richiamata automatica	Questo timer è fatto partire se un terminale cambia il suo stato in riposo. Allo scadere di tale periodo viene verificato se è necessario effettuare una richiamata automatica. L'utente ha quindi la possibilità di effettuare altre chiamate. Valori consentiti: 0-60 s
Durata della prenotazione	Nel caso in cui la richiamata automatica non riceva risposta entro questo tempo, la chiamata viene terminata e la richiamata automatica viene posticipata. Valori consentiti: 15-60 s
Tempo di rinvio per richiamata	Se una richiamata automatica, causata da una trasferta rapida prima della risposta, non ottiene risposta entro questo lasso di tempo, viene inoltrata al posto operatore, premesso che sia stato attivato il presente criterio. Valori consentiti: 20-600 s
Tempo di chiamata durante la trasferta prima della risposta	Se non si risponde a una trasferta rapida prima della risposta (verso un utente occupato) entro il lasso di tempo qui definito, viene segnalata una richiamata presso l'utente che ha eseguito la trasferta. Valori consentiti: 30-600 s
Fine di selezione in caso di selezione incompleta (Austria)	Timer supervisore per selezione passante. Se allo scadere di questo tempo la selezione è incompleta, la selezione passante viene riconosciuta come incompleta o non selezionata (valido solo per l'Austria). Valori consentiti: 10-30 s
Tempo di fine selezione (nessuna selezione)	Se la selezione non viene attivata entro un determinato tempo, viene generata automaticamente una fine selezione. Valori consentiti: 5-15 s
Tempo tra il 1º e il 2º annuncio con sel.pass.fax	Fax/DID, selezione passante analogica, tempo dopo l'annuncio. Valore predefinito: 15 s
Tempo per parcheggio + passaggio a messa in attesa	La riattivazione di una chiamata in parcheggio deve avvenire entro un tempo massimo. Se la chiamata in parcheggio non riceve risposta (viene ripresa) entro questo tempo, l'apparecchio che ha messo in attesa la chiamata viene richiamato. Con la richiamata automatica, lo stato d'attesa e passa a quello attivo. Valori consentiti: 60-255 s
Fine selezione in caso di selezione incompleta	Se la selezione non viene proseguita entro un certo tempo, viene generata automaticamente una fine selezione. Valori consentiti: 10-20 s
Utente AB Tempo flash minimo	Per il riconoscimento di un flash è necessario determinare un tempo minimo nel quale il doppino deve essere aperto. Valore predefinito: 0 s

Parametri	Descrizione
NoFe Tempo flash massimo	Per il riconoscimento di un flash è necessario determinare un tempo massimo nel quale il doppino deve essere aperto. Valore predefinito: 0 s
Tempo per il rilascio di una richiamata dal PO	Nel caso in cui una richiamata automatica al posto operatore non riceva risposta entro questo tempo, la richiamata viene rilasciata. Valori consentiti: 30-180 s
HKZ tempo precedente al contatto NSA	Tempo di compressione per il contatto normalmente aperto del disco di composizione, utilizzato per evitare il rumore di composizione nella cuffia (prima dell'impulso). Valore predefinito: 0 s
HKZ tempo posteriore al contatto NSA	Tempo di compressione per il contatto normalmente aperto del disco di composizione, utilizzato per evitare il rumore di composizione nella cuffia (dopo l'impulso). Valore predefinito: 0 s
Tempo di masch.disturbo per chiamata	Tempo fino alla copertura dei disturbi di linea con composizione DP. Valore predefinito: 0 s
Fine selez. con selez. 1A	Indica il tempo trascorso il quale deve essere selezionata l’ultima cifra con il metodo 1A. Una cifra viene emessa dopo l'inserimento di quella successiva. L'ultima cifra viene emessa dopo la scadenza del timer o con la segnalazione di fine selezione (#) da parte dell'utente. Valori consentiti: 4-4,5 s
Tempo di post-conteggio degli addebiti	Sulle linee analogiche, quando viene rilasciata una linea, il sistema di comunicazione può analizzare le informazioni relative agli addebiti della chiamata in entrata (scatti). In questo intervallo la linea risulta bloccata per le connessioni in uscita. Valore predefinito: 0 s
Tempo di intercifra in selezione DP	Sono consentite pause tra le singole cifre mediante DP. Valore predefinito: 10 s
Tempo di controllo del segnale di linea	Indica il tempo di attesa per il tono di composizione. Se questo timer scade, il sistema presuppone un guasto della linea. Se questo tempo scade, nel sistema si verifica una caduta di linea. La linea viene segnata come "caduta ". Valore predefinito: 10 s
Tempo di pausa per DP	La selezione DP avviene mediante sequenze impulso-pausa, con il riconoscimento delle pause sulle linee DP. Valore predefinito: 0 s
Tempo impulso per DP	La selezione DP avviene mediante sequenze impulso-pausa. Riconoscimento di impulsi su linee DP. Valore predefinito: 0 s

Parametri	Descrizione
Tempo flash per PABX	Tempo di pausa richiesto perché il loop utente attivi le funzioni di controllo (ad esempio la consultazione) nel sistema. Valore predefinito: 0 s
Tempo flash per serv.l.urb.	Tempo di pausa richiesto perché il loop utente attivi le funzioni di controllo (ad esempio la consultazione) sulla linea analogica (HKZ). Valore predefinito: 0 s
Tempo minimo d'impulso con NoFe DP	La selezione DP avviene mediante sequenze impulso-pausa. Riconoscimento di impulsi da telefoni DP. Valore predefinito: 0 s
Tempo massimo d'impulso con NoFe DP	La selezione DP avviene mediante sequenze impulso-pausa. Riconoscimento di impulsi da telefoni DP. Valore predefinito: 80 ms
Tempo di trasmissione per segnali DTMF	Durata specifica di un paese dei caratteri DTMF. Valore predefinito: 80 ms
Tempo di pausa tra segnali DTMF	Pausa specifica di un paese tra i caratteri DTMF. Valore predefinito: 80 ms
MOH timer di ritardo	Agli utenti in stato di attesa, viene riprodotta una musica su attesa (Music on Hold), se configurata. L'attivazione della MOH avviene dopo il lasso di tempo impostato, per assicurare che l'attivazione di servizi - come ad esempio Conferenza - non interferisca con la MOH. Valori consentiti: 1-5 s
Tempo di pausa prima della selezione (solo per Sviluppo)	Se per le linee analogiche non è possibile o non si desidera eseguire alcun controllo del tono, la selezione può essere avviata automaticamente dopo questo intervallo. Valore predefinito: 3 s
Min. pausa addebiti	Tempo tra impulsi di addebito (scatti). Valore predefinito: 0 min.
Scatti in min	Durata degli impulsi di addebito. Valore predefinito: 0 min.
NSA tempo impulso	Disco di composizione, contatto di lavoro (linee DP). Valore predefinito: 0 s
NSA tempo imp. impegno	Disco di composizione, contatto di lavoro (linee DP). Valore predefinito: 0 s
Rilascio se non avviene la selezione	Se il numero non viene selezionato entro un determinato lasso di tempo dopo aver impegnato la linea, viene terminata la connessione. L'utente riceve un tono di occupato. Valori consentiti: 5-30 s

Parametri	Descrizione
DP NoFe Tempo minimo di interselezione	Tempo tra cifre composte nei telefoni DP. Valore predefinito: 0 ms
DTMF NoFe flash tempo di rimbalzo	Impedisce il rilevamento multiplo della pressione del pulsante Flash. Valore predefinito: 0 ms
Tempo di riposo DTMF	Tempo di attesa per evitare problemi con i segnali DTMF sulle linee in uscita. Valore predefinito 100 ms
Tempo di riposo flash (vedere la Guida)	Tempo di attesa dopo il flash sulle linee analogiche. Valore predefinito: 1 s
Lunghezza del ciclo per il ripristino	Tempo per il riavvio della rete analogica dopo il riconoscimento del tono di linea. Valore predefinito: 120 s
Durata della pausa	Indica la lunghezza della pausa che deve essere rispettata tra due cifre, se viene riconosciuto un segnale di pausa. Valori consentiti: 1-5 s
Tempo esclusione errori per chiamate in funzionamento PABX (vedere la Guida)	Tempo fino alla copertura dei disturbi di linea. Valore predefinito: 0 s
Fine selezione artificiale	Con la selezione esterna le cifre ricevute dopo una fine selezione artificiale sono interpretate come messa in consultazione. Valori consentiti: 5-15 s
Tempo ripetizione automatica ultimo nr. selez.	In caso di un utente occupato, dopo la scadenza del timer viene eseguita una ripetizione automatica dell’ultimo numero selezionato. È necessario prima selezionare l'opzione Ripetizione automatica dell'ultimo nr. selez. in Flags. Valori consentiti: 10-650 s
Disturbo per il primo cambio di polarità (Francia/ Spagna) (vedere la Guida)	Tempo fino alla copertura dei disturbi di linea. Valore predefinito: 0 ms
Tempo di ritardo annuncio prima di risposta	Questo timer regola il tempo di ritardo dopo il quale entra in funzione il risponditore. Valori consentiti: 1,5-30 s
Tempo tra riconoscimento tono e selezione su lin. urb. analogica	Determina il tempo fra il riconoscimento del tono di linea e la selezione della prima cifra attraverso il la linea analogica. Valori consentiti: 0-2 s
Pausa dopo la selezione del 2° codice di linea	Determina la lunghezza della pausa che intercorre dopo la selezione del 2° codice di linea o del prefisso internazionale. Passaggio al successivo nodo di commutazione. Valori consentiti: 1-5 s

Parametri	Descrizione
Tempo fino al tono di avviso nel transito con linee anal.	I collegamenti di transito sono controllati a seconda del tipo di protocollo. Ciò impedisce che una connessione rimanga tale per un tempo indefinito. Se almeno un tipo di record di questo collegamento di transito dispone di un riconoscimento di disimpegno, non avviene un controllo del tempo (per le eccezioni vedere la tabella riportata di seguito). Il tipo di record dati HKZ non prevede alcun riconoscimento del disimpegno, ma un'opzione hardware per il Silent Reversal. Si rende così possibile un riconoscimento di disimpegno con HKZ. La tabella per il monitoraggio del transito (quanto segue si applica a tipi di record specifici per USA) mostra per quali tipi di record viene effettuato il monitoraggio tramite timer. La durata del controllo può essere configurata. Se è in uso una linea analogica con Silent Reversal, occorre osservare che ci sono numeri telefono nel caso dei quali può non essere riconosciuta la risposta e quindi neanche la disconnessione. Generalmente questi numeri di telefono sono servizi annunci. In tal caso è necessario fornire al gestore di rete del sistema precise istruzioni in merito. Valori consentiti: 120 s-42 min
Tempo del segnale di avviso fino al rilascio...	In caso di controllo delle connessioni di transito, dopo la scadenza del timer di controllo viene emesso un segnale di avviso. Per poter terminare la chiamata, la connessione non viene terminata immediatamente bensì dopo il lasso di tempo specificato. Valori consentiti: 10-650
Tempo di rilascio per linee analogiche	La chiamata di una linea HKZ tramite selezione passante (DID) viene attivata allo scadere di questo tempo, se nel frattempo non è iniziata alcuna conversazione. Valori consentiti: 30 s-254 min
Dopo l'attesa viene attivato un segnale di avviso (solo Italia)	Trascorso questo lasso di tempo, le chiamate in stato d’attesa danno luogo ad un avviso di chiamata all’utente presso il quale sono in attesa. Valori consentiti: 30-180 s
LCR: Fine selezione artificiale	Tempo di attesa dalla digitazione dell'ultima cifra fino a quando il sistema non rileva il termine della composizione (LCR selezione in blocco). Valore predefinito: 5 s
Controllo di una chiamata UCD su una linea analogica	Tempo per il rilascio di una chiamata HKZ su un gruppo UCD, se non viene stabilita alcuna connessione. Valori consentiti: 10-3810 s
Controllo della trasferta senza consenso a un gruppo UCD (solo per Sviluppo)	In caso di trasferta di una conversazione su un gruppo UCD prima della risposta, viene avviato il timer. Se la chiamata trasferita non riceve risposta, allo scadere del timer viene eseguita una richiamata. Valori consentiti: 10-3810 s
Timer di ritardo per PO PC	Tempo per l'invio di un messaggio di aggiornamento al PC console posto operatore (Business Attendant). Valori consentiti: 300 ms

Parametri	Descrizione
Intervallo di tempo USBS	Per l'accesso tramite le porte S0, TA-S0, TA-RS232 e TA-API viene utilizzato il servizio User Signalling Bearer Service (USBS), basato su ETS 300 716. Valori consentiti: 1-60 s
Tempo di controllo del traffico di transito	In caso di attivazione di una connessione di transito, allo scadere di questo tempo appare una segnalazione sul display del posto operatore; quest'ultimo può eventualmente rilasciare le singole linee. In tal modo è possibile controllare periodicamente le connessioni di transito. Valori consentiti: 0-650 s
Tono speciale di occupato se l'utente dest. non risponde	Allo scadere di questo tempo, se l'utente interno chiamato non risponde, il chiamante riceve il tono speciale di occupato. Valori consentiti: 30-120 s
Tono speciale di occupato con linea impegnata senza selezione	Se un utente impegna una linea in uscita e non effettua alcuna selezione, allo scadere del tempo riceve un tono speciale di occupato. Valori consentiti: 20-60 s
Tempo di risposta a trasferta ad utente occupato.	Alla scadenza di questo timer l'utente A, che è stato trasferito dall'utente B ad un utente C occupato, viene ritrasferito a B. Valori consentiti: 15-180 s
Intervallo di segnalazione di errori	Con il tempo di segnalazione errori viene definito un intervallo entro un range di valori da 1 min. fino a 15 min. Le posizioni dopo la virgola vengono arrotondate al minuto intero, valori minori di 1 min. o maggiori di 15 min. vengono considerati come 15 min. Una volta scaduto l'intervallo gli errori della classe B registrati nel Registro eventi vengono trasmessi in modalità ciclica al Centro di assistenza remota. Valori consentiti: 60-900 s

28.3.1.3 Impostazioni di base > Sistema > Display

Descrizione dei parametri delle schede:

- **Modifica Display**

Parametri	Descrizione
Visualizzare il nome/nr. di tel.	È possibile configurare quale dei seguenti dati deve essere visualizzato sul display di tutti i telefoni collegati all'arrivo delle chiamate: solo numero di telefono o solo nome (se disponibile) o nome e numero di telefono contemporaneamente. Se un telefono non supporta queste impostazioni, ad es. la visualizzazione simultanea di nome e numero di telefono, viene visualizzato solo il numero di telefono. I telefoni OpenStage sono idonei alla visualizzazione del nome e del numero di telefono. Valore predefinito: Nome e numero di telefono

Parametri	Descrizione
nome visualizzato / algoritmo	Il supporto del nome completo è assicurato da tre campi: uno per il nome, uno per il cognome e un terzo per il nome visualizzato. Il campo Nome visualizzato può memorizzare fino a 16 caratteri, mentre i campi Nome e Cognome ne possono memorizzare fino a 32. È possibile utilizzare una delle seguenti opzioni dell'algoritmo nome visualizzato: • <cognome> <nome proprio> • <cognome> <iniziale nome.\> • <nome>, <cognome> • <iniziale nome.>, <cognome> • <cognome> Valore predefinito: <cognome> <nome proprio> **Importante:** Per gli utenti MULAP, l'opzione **<nome> <cognome>** non è riconosciuta in UC Suite. Se si usa questa opzione, il nome proprio e il cognome degli utenti UC Suite vengono visualizzati insieme nel campo del nome proprio nella rubrica utente UC e il campo del cognome resta vuoto. In questo caso, utilizzare il valore predefinito dell'opzione, dove si usa la virgola come separatore.
Trasferta prima della risposta	In caso di Trasferta prima della risposta viene visualizzato o il numero di telefono dell'utente che effettua la trasferta o il numero di telefono dell'utente trasferito. Una conversazione trasferita con Trasferta prima della risposta non può essere rifiutata dall'utente chiamato. Selezionando Utente trasferito, prima che avvenga il collegamento e dopo il rilascio, il display visualizza l'utente che effettua la trasferta. Selezionando Utente che effettua la trasferta, per l'intera durata del collegamento con il destinatario, il display visualizza l'utente che effettua la trasferta. Dopo che l'utente che trasferisce la chiamata rilascia la chiamata e fintantoché vi è il collegamento, il display cambierà dall'utente che trasferisce la chiamata all'utente trasferito. Valore predefinito: Utente trasferito
Richiamata	Se dopo aver trasferita una chiamata ha luogo una richiamata, presso il destinatario della trasferta stessa può essere visualizzato il numero dell'utente che ha trasferito la chiamata oppure il numero dell'utente dal quale è stata originata la richiamata. La chiamata trasferita viene visualizzata presso l'utente interno B. C riceve il tono di chiamata finché B non risponde o A non richiama. Questo punto consente di stabilire se sul display della destinazione di trasferimento B deve essere visualizzato l'utente A (Chiamante) o C (Destinazione della trasferta). Se l'utente A accetta una richiamata, sui display di entrambi gli utenti viene visualizzato non risponde. Valore predefinito: Destinazione della trasferta
Formato data/ora	La data può essere visualizzata in diversi formati. Valore predefinito: Europa - Formato 24 ore

Parametri	Descrizione
Lista delle chiamate, modo	Attivando Chiamate esterne e interne oppure Solo chiamate esterne tutte le chiamate che non hanno ricevuto risposta vengono salvate in una lista; tali numeri vengono poi richiamati in un secondo momento, tramite una procedura del sistema. Attivando Chiamate e conversazioni esterne vengono salvate nella lista delle chiamate anche conversazioni che hanno ricevuto risposta. Nella lista delle chiamate non avvengono cancellazioni di numeri di telefono, né per chiamate in entrata né per chiamate in uscita. Quando tutti i posti di memoria della lista delle chiamate sono stati assegnati, al momento del salvataggio di un nuovo numero viene sovrascritto quello più vecchio. Le chiamate che non hanno ricevuto risposta vengono visualizzate secondo quanto illustrato per il servizio Lista delle chiamate. Le chiamate che hanno ottenuto risposta vengono visualizzate secondo la normale funzionalità di salvataggio del numero di telefono fornita dalla lista delle chiamate. Le chiamate esterne in entrata trasferite tramite AutoAttendant ad utenti interni al momento occupati o che hanno attivato la deviazione di chiamata non vengono salvate nella lista delle chiamate. Valore predefinito: solo esterne
Disattiv.visualizzaz.del nr. di tel.	Se il flag è attivato: impedisce la visualizzazione del numero sulla linea ISDN. Presso l'interlocutore non viene in tal caso visualizzato il numero di telefono (il servizio deve essere attivato anche presso il gestore di rete). In alcuni scenari di chiamata un chiamante può essere impostato come "presentazione limitata" dal centralino. Se il flag è attivato, il numero di telefono del chiamate viene mostrato all'utente chiamato. Se il flag è disattivato, viene visualizzato il testo "Numero sconosciuto". Il flag dipende sempre dalle impostazioni di linea di ciascun provider. Valore predefinito: disattivato
Elenco telefonico interno	Gli utenti possono accedere ad un elenco telefonico online, che contiene nomi e numeri di telefono di tutti i derivati interni. I terminali con display specifici del sistema permettono all'utente di consultare l'elenco telefonico e di selezionare un numero a scelta fra quelli registrati. Nei terminali dotati di tastiera alfanumerica, quest'ultima può essere utilizzata per effettuare ricerche mirate. Nell'elenco selezionare l'opzione corrispondente: no: nessun accesso alla rubrica possibile; interno: accesso alla rubrica interna (utente, gruppi e destinazioni di selezione breve); LDAP: accesso alle informazioni nelle rubriche del server LDAP. A questo scopo, l'accesso LDAP deve essere configurato tramite LDAP; tutti: gli utenti possono scegliere tra accesso a una rubrica interna o a una rubrica LDAP. Valore predefinito: interno
Rubrica telefonica interna tramite Rubrica unificata	Se il flag è attivato, l'utente può cercare contatti in tutte le rubriche. Le richieste di ricerca vengono gestite come richieste per la Rubrica unificata. Se il flag non è attivo, le richieste di ricerca vengono gestite localmente dal sistema. Valore predefinito: Attivata
Interruttore	

Parametri	Descrizione
Visualizzare la durata della chiamata	In caso di chiamate in uscita, vengono visualizzate le informazioni sugli addebiti. Sui terminali UP0/E con display viene visualizzata la durata attuale della conversazione. Sulle linee analogiche il punto di avvio per il conteggio del tempo viene definito tramite timer (5 s dopo il termine della selezione), sulle linee digitali urbane con CONNECT. Il sistema di comunicazione non supporta l'indicazione della durata della conversazione sui terminali S0. Valore predefinito: disattivato
Sel.DTMF nascosta	I codici PIN immessi vengono mascherati con asterischi nel display dei telefoni di sistema. Valore predefinito: attivato
Indic. stato display per mess. inform	Questi messaggi informativi vengono visualizzati sul display dei telefoni di sistema. Valore predefinito: attivato
Inoltrare numero di tel. in modo trasparente	In caso di deviazione o inoltro di chiamata a un utente esterno, l'utente chiamato può visualizzare il numero di telefono del chiamante. In un sistema in rete l'opzione deve essere impostata nel nodo di attivazione di un collegamento di rete urbana. Requisito per l'attivazione di LM è il rilascio della funzione a pagamento Clip No Screening nella linea urbana. Questo flag funziona in modo alternato assieme al flag Disattiva nr. di tel. utente in Fasci. Valore predefinito: disattivato
SST con opzione di trasferimento (numero di trasferimento del chiamante)	Con il flag attivato, quando l'utente seleziona l'opzione di menu "Iniziare il trasferimento?" (durante una chiamata attiva), il trasferimento viene eseguito come Trasferimento a passaggio singolo (senza consultazione). Se l'utente sceglie di effettuare prima una consultazione (ad es.l'opzione "Richiesta di informazioni?") e trasferisce la nuova chiamata all'utente in attesa, la chiamata viene effettuata come un normale trasferimento nascosto (o trasferimento dopo una risposta). In caso di trasferimento a passaggio singolo, il numero del chiamante viene visualizzato presso la destinazione esterna quando il dispositivo mobile squilla; ciò significa che l'utente chiamato vede il numero del chiamante e non il numero dell'utente che trasferisce la chiamata quando questa viene trasferita da un dispositivo del sistema. Anche il flag "Inoltrare numero di tel. in modo trasparente" deve essere attivato. Valore predefinito: disattivato **Nota:** Se l'utente che effettua il trasferimento è un dispositivo esterno, la funzione CLIP no screening deve essere supportata e attivata dal provider di rete. In caso contrario, il DID predefinito del sistema sarà utilizzato dalla linea urbana o la chiamata verrà respinta dalla linea urbana.

28.3.1.4 Impostazioni di base > Sistema > DISA

Descrizione dei parametri delle schede:

- **Modifica DISA**

Parametri	Descrizione
DISA	
Selezione passante	Numero di telefono mediante il quale la funzione DISA è accessibile dall'esterno. Il numero di telefono può essere diverso per l'utilizzo interno ed esterno.
Modo di sicurezza	Per poter utilizzare le funzioni DISA, l'utente deve inserire una password. Le opzioni del Modo di sicurezza consentono di stabilire se, dopo l'immissione della password, l'utente deve attendere oppure inserire il simbolo cancelletto (#). Valore predefinito: a tempo
DISA interno	
Numero di telefono	DISA interno si riferisce all'uso press un altro nodo collegato alla rete IP.
Mobility Callback	
Selezione passante	Non è richiesta alcuna autenticazione se una chiamata riconosciuta come numero di telefono Mobility viene eseguita dall'esterno a un numero DID Mobility Callback. In questo caso si attiva direttamente il tono di selezione interno. A tale scopo, il terminale dell'utente esterno deve trasmettere il proprio numero di telefono Questo numero viene quindi confrontato con l'elenco Mobility.

28.3.1.5 Impostazioni di base > Sistema > Rinvio/PO/Hotline

Descrizione dei parametri delle schede:

- **Modifica rinvio/PO/Hotline**

Parametri	Descrizione
Posto di rinvio	
Giorno/notte	Numero di telefono del posto di rinvio. Il posto di rinvio può essere definito in modo separato per i servizi Giorno e Notte. Sussiste poi anche la possibilità di definire una destinazione a scelta quando si attiva il servizio notte (servizio notte variabile).
Posto di rinvio centrale	
Instradamento	Indice fascio per posto di rinvio centrale in sistemi di comunicazione connessi in rete
Numero di chiamata	Numero di telefono del punto di rinvio centrale in sistemi di comunicazione collegati in rete
Rinvio al posto di rinvio	

Parametri	Descrizione
su libero	La chiamata segue la procedura predefinita per le chiamate in entrata. Se la destinazione finale viene raggiunta e non risponde, il sistema esegue un controllo per verificare se applicare o meno un rinvio dopo il timeout. Se necessario, dopo il numero di squilli definito in Inoltro di chiamata viene chiamato il posto di rinvio. Da un gruppo di ricerca non vengono effettuati rinvii; la chiamata viene di nuovo inoltrata al primo apparecchio della linea con ricerca, dove vi resta. Valore predefinito: attivato
su occupato	Il flag su occupato consente di verificare se è possibile segnalare una chiamata in attesa. Se la chiamata in attesa non può essere segnalata (Rifiuto avviso di chiamata in attesa o criterio di rinvio), essa segue quanto specificato in Gestione chiamate/Routing delle chiamate. Se la chiamata non può essere segnalata a nessun apparecchio, viene controllato se deve avvenire il rinvio o la cancellazione (segnalazione B sulla linea urbana). Se un telefono analogico con rifiuto avviso di chiamata in attesa è occupato, la chiamata viene cancellata indipendentemente dal tipo di circuito. In caso di selezione passante DTMF e HKZ, il rinvio avviene sempre. Valore predefinito: disattivato
con selezione errata	Quando viene composto un numero di telefono errato, il sistema controlla se il rinvio deve avvenire. Nel caso di selezione passante DTMF il rinvio avviene sempre. Valore predefinito: attivato
Con selezione incompleta	Se il numero di telefono dell'utente selezionato è incompleto, dopo un determinato lasso di tempo viene richiamato il posto di rinvio. Detto lasso di tempo può essere impostato nel campo Fine selezione in caso di selezione incompleta in Temporizzazioni. Valore predefinito: attivato
In caso di richiamata senza risposta	Se dopo essere stata trasferita prima della risposta da A a B la chiamata non ottiene risposta da quest'ultimo, né da A a seguito di una richiamata, dopo un determinato lasso di tempo viene chiamato il posto di rinvio. Detto lasso di tempo può essere impostato nel campo Fine selezione in caso di selezione incompleta in Temporizzazioni. Se il flag non è attivato, dopo la scadenza del tempo impostato la chiamata viene disconnessa. Valore predefinito: disattivato
Al rifiuto	Se un utente interno rifiuta la chiamata con "Rifiuta chiamata in arrivo", la chiamata segue la procedura di Gestione chiamate/routing delle chiamate. Se la chiamata non può essere segnalata a nessun apparecchio, viene controllato se deve avvenire il rinvio o la cancellazione (segnalazione B sulla linea urbana). Valore predefinito: attivato
Intercettazione del blocco telefonico	

Parametri	Descrizione
Numero di chiamata	Se è attivata la chiave elettronica dell'apparecchio e viene selezionato un codice di accesso al fascio, la chiamata verrà immediatamente deviata verso la destinazione di rinvio registrata. In tal modo, se un utente seleziona un numero per il quale non è abilitato, la chiamata viene segnalata al numero di telefono utente qui assegnato. La funzione Rinvio con chiave elettronica può essere impostata singolarmente per ogni utente tramite i flag utente.
Autorizzazione del trunk commutato	
Autorizzazione del trunk commutato	In questo campo è necessario configurare una stazione con accesso al trunk illimitato, altrimenti non sarà possibile deviare la chiamata a una destinazione esterna.
Codice di posto	
Numero di telefono interno	Questo è il numero di telefono usato dagli apparecchi interni per raggiungere il posto di rinvio. Valori consentiti: Immissione di una cifra a scelta, a condizione che non sia già utilizzata nel piano di composizione.
Numero di telefono esterno	A questo numero di telefono viene raggiunto il posto di rinvio in selezione passante dalla rete del sistema (CorNet-N o CorNet-NQ).
Hotline	
Tempo di hotline	Se un utente solleva il ricevitore, la hotline viene chiamata automaticamente non appena scade il tempo di hotline. Tuttavia, questo accade solo se l'utente non immette nessuna cifra durante questo tempo. Il suddetto tempo viene specificato in secondi.
Nr. di tel. destinazione da 1 a 6	A livello di sistema è possibile inserire 6 destinazioni hotline, la cui scelta viene eseguita per utente (vedere Utenti/Modifica i parametri dell'utente)
Console posto operatore	
Chiam. in coda	Qui è possibile selezionare il numero massimo di chiamate in coda. Se il numero degli utenti nella coda di attesa del posto operatore raggiunge questo valore, le chiamate sono trasferite ad una destinazione di overflow. Valori consentiti: 1-15
Destinazione d'attesa	Nel campo Tempo di attesa, immettete il numero dei secondi, per i quali una chiamata può attendere nella coda. Allo scadere di tale intervallo, la chiamata viene inoltrata a una destinazione di overflow specificata tramite il Call Management.
Comm. rapidam.	Se questo flag è attivo, l'operatore può rispondere a una chiamata, quindi trasferirla a un altro utente premendo il relativo numero di selezione. La trasferta rapida è disponibile solo se è disattivato il flag del sistema **DTMF automatica**. Valore predefinito: disattivato

Parametri	Descrizione
Comm. senza selez.	Un utente abilitato (Posto operatore PO), ha la possibilità di assegnare una linea urbana non selezionata ad un utente interno con abilitazione alla linea urbana insufficiente, al fine di permettergli l'esecuzione di una sola chiamata esterna. Dopo la trasferta della linea commutata all'utente con abilitazione inadeguata, viene eseguito un controllo di selezione per mezzo di un'abilitazione alla linea urbana supplementare per linee commutate. Solo se questa abilitazione alla linea urbana supplementare è sufficiente, cioè se l'utente seleziona ad es. un numero valido in modo conforme alla lista dei nr. permessi/vietati per linee commutate, viene permesso il collegamento esterno in uscita. Su una linea commutata l'utente seleziona da solo il codice di impegno. Nel sistema di comunicazione, tramite un utente di riferimento, è possibile configurabile per ogni fascio un'abilitazione alla linea urbana per le linee commutate. L'utente di riferimento standard è la prima porta logica utente oppure il posto operatore. L'abilitazione standard per tutti i fasci è Abilitazione completa alla linea urbana. Valore predefinito: disattivato
Altri criteri	
Avviso chiamata in attesa su occupato	Se questo flag è attivato, per tutti gli utenti nel sistema di comunicazione è attiva la funzione "Avviso di chiamata in attesa". Valore predefinito: attivato
Attesa immediata per chiamate posto operatore	Importante solo in sistemi CorNet collegati in rete. Se il flag è impostato, all'utente B (sistema B), l'avviso di chiamata in attesa viene segnalato soltanto se proveniente dal posto operatore (sistema A). Tutti gli altri utenti del sistema A non possono effettuare avvisi di chiamata nel sistema B. Per gli utenti del sistema B si applica la condizione del rifiuto dell'avviso di chiamata in attesa (vedere la vista utente: Flag) per l'utente corrente. Se il flag non è impostato, gli avvisi di chiamata in attesa vengono segnalati a tutti gli utenti occupati che non hanno attivato la funzione di "Rifiuto dell'avviso di chiamata in attesa". Il flag deve essere impostato qualora si desideri che la chiamata giunta ad un utente in quel momento occupato da un posto operatore passi subito in stato di attesa e venga segnalata tramite avviso di chiamata. Se il flag non viene attivato, il posto operatore riceve il segnale di occupato e dopo alcuni secondi passa in stato di attesa. Valore predefinito: disattivato
Ignora per chiamate posto operatore	Se questo flag è attivato, il posto di rinvio è abilitato per la funzione "Inclusione". In questo modo è possibile inserirsi in una conversazione di un utente interno. Valore predefinito: attivato

28.3.1.6 Impostazioni di base > Sistema > LDAP

Descrizione dei parametri delle schede:

- **Modifica LDAP**

Parametri	Descrizione
Accesso LDAP	
Indirizzo IP del server LDAP	Indirizzo IP del server LDAP da cui devono essere recuperate le informazioni della rubrica.
Numero porta accessi LDAP	Numero porta per accedere a LDAP. Valore predefinito: 389
Nome utente/Password	Windows Server ADS non consente l'accesso anonimo In questo caso, inserire qui il nome utente e la password per la connessione LDAP. Valori consentiti: max. 48 caratteri
Parametro server LDAP	
Base DN	DN = Distinguished Name; Ricerca di base per le richieste di ricerca sul server LDAP (ASCII, 100 caratteri), ad esempio: ou=com, cn=unify, cn=de
Richiesta di ricerca	Esempio di richiesta di ricerca al server LDAP. È necessario inserire il carattere $ come segnaposto per il nome da ricercare. Tenere presente che un criterio di ricerca non può iniziare con un'espressione regolare. Valori consentiti: ASCII, 50 caratteri Valore predefinito: cn=$*
Attributo risultato Nome	Il nome attributo del risultato supporta solo il tipo di carattere ISO-8859-1 con valori dei codice compresi tra 0x20 e 0x80 (caratteri ASCII), oltre ai caratteri Ä, Å, Æ, Ñ, Õ, Ö, Ø, Ü, ß, ä, õ, ö, ü. La visualizzazione dei caratteri dipende dall'impostazione della lingua dell'utente e dal terminale utilizzato. Valori consentiti: ASCII, 24 caratteri Valore predefinito: cn
Attributo risultato Numero di telefono	Nell'attributo risultato Numero di telefono sono ammessi fino a 25 caratteri di selezione (0...9, *, #) e fino a 6 caratteri per la formattazione (+,(), spazio vuoto, -). Il numero di telefono deve presentare il formato canonico (ad es. +49 (89) 70070). Valori consentiti: ASCII, 25 caratteri Valore predefinito: numero di telefono
Ordina risultati ricerca	I risultati vengono visualizzati in ordine alfabetico per nome. Valore predefinito: attivato
Analisi numero di telefono LDAP	
Codice impegno LDAP	Il codice di impegno corrisponde al codice di fascio selezionato. Valore predefinito: 0 (codice predefinito del primo fascio)
Prefisso numero telefono LDAP	Il numero di telefono indicato viene anteposto al prefisso indicato. Valori consentiti: ASCII, 5 caratteri

Nota: Per visualizzare le risorse LDAP è necessario selezionare l'opzione appropriata in **Impostazioni di base** > **Visualizza** > **Rubrica interna** nel menu **Visualizza**. Per ulteriori informazioni vedere il capitolo 28.3.1.3 Impostazioni di base > Sistema > Display.

28.3.1.7 Impostazione di base > Sistema > Testi

Descrizione dei parametri delle schede:

- **Modifica Testi**

Parametri	Descrizione
Reimpostare sui valori predefiniti	Reimpostare i messaggi e i testi informativi sui valori preimpostati in una lingua specifica. Per eseguire il reset, selezionare una lingua nell'elenco a discesa.
Messaggi	Messaggi brevi che un utente può inviare a un altro utente. Di solito un sistema di comunicazione consente di configurare dieci testi di questo tipo, Ciascuno di questi testi standard può essere sovrascritto. Al massimo sono disponibili dieci messaggi per volta. Gli utenti vi possono accedere tramite l'opzione di menu "Inviare messaggio?" dal telefono di sistema. Gli utenti che dispongono di terminali dotati di tastiera alfanumerica possono inoltre creare messaggi personali; i messaggi predefiniti non possono essere tuttavia modificati. Valori consentiti: massimo 24 caratteri alfanumerici
Messaggi di risposta	Messaggi brevi che l'utente può inviare a un chiamante in caso di assenza. Ci sono 10 messaggi di testo predefiniti, Ciascuno di questi testi standard può essere sovrascritto. Gli utenti che dispongono di terminali dotati di tastiera alfanumerica possono inoltre creare messaggi personali; i messaggi predefiniti non possono essere tuttavia modificati. Se necessario, gli utenti possono aggiungere informazioni individuali ai messaggi esistenti. I testi che contengono due punti offrono all'utente la possibilità di completare il messaggio aggiungendo un numero o una data. Gli utenti vi possono accedere tramite l'opzione di menu "Messaggio di assenza on?" dal telefono di sistema. Valori consentiti: massimo 24 caratteri alfanumerici

28.3.1.8 Impostazioni di base > Sistema > Menu Flexible

I Menu Flexible consentono la personalizzazione delle opzioni del menu nel menu Servizio dei telefoni del sistema. Se la casella di controllo è selezionata, questa voce del menu non viene visualizzata nella **Lista di mascheramento**. Questa impostazione si applica a livello di sistema per tutti i telefoni di sistema. Le funzioni nascoste possono tuttavia essere attivate tramite un codice.

28.3.1.9 Impostazioni di base > Sistema > Destinazioni di selezione breve

Possono essere configurate o modificate manualmente fino a 8000 voci della rubrica. Le destinazioni di selezione breve sono numeri di selezione breve centralizzati (SPDC). Facendo clic su un nome colonna le voci vengono ordinate per la colonna corrispondente.

Descrizione dei parametri delle schede:

- **Cambia destinazione di selezione breve**

Parametri	Descrizione
Selezione breve	Numero selezionato dall'utente. I numeri di selezione breve devono contenere quattro cifre (`0000-7999`, utilizzare zeri iniziali).
Numero di telefono	Numero componibile della destinazione desiderata, ovvero con codice del fascio o di linea (ad esempio, 0, 9, 81 o 801). Valori consentiti: max. 31 cifre
Nome	Nome della destinazione di selezione breve memorizzato nella rubrica interna del telefono, visualizzato quando viene composta la destinazione corrispondente. Le chiamate in entrata (tramite CLIP) vengono confrontate con le destinazioni di selezione breve memorizzate e visualizzate come nome della destinazione di selezione breve, se è stato attivato il parametro Nome o Nome e numero di telefono. Valori consentiti: max. 16 caratteri
Cerca	Se nei campi di ricerca **Selezione breve**, **Numero di telefono** o **Nome** viene inserito un termine di ricerca e successivamente si preme il tasto Return, vengono visualizzati tutti i risultati che contengono il termine di ricerca. Immettendo `521` come numero di telefono verranno ad esempio trovati i numeri `+495213535` e `+498967521` oppure con `co` inserito come nome, verranno trovate le voci `Collins`, `Mcoin` e `Branco`. Se non si inserisce nulla in nessun campo di ricerca e si preme il tasto Invio, vengono visualizzate tutte le voci.
Pulsanti	
Applica	Aggiungere nuove voci o modificare quelle esistenti.
Annulla	Annullare le modifiche per le voci disponibili (prima di Applica).

Descrizione dei parametri delle schede:

- **Importa/esporta file csv/xml via HTTP**

Parametri	Descrizione
Importa file CSV/XML via HTTP	Le destinazioni di selezione breve possono essere importate in un file XML in formato UTF-8. I numeri di selezione breve già esistenti vengono cancellati prima dell'importazione. Un modello XML per l'importazione dei numeri di selezione breve è disponibile in **Centro assistenza** > **Documenti** > **Modelli CSV.**

Parametri	Descrizione
Esporta file XML via HTTP	Le destinazioni di selezione breve possono essere esportate in un file XML in formato UTF-8. Vengono sempre esportati tutti i record dati. **Nota:** L'importazione di numeri di selezione breve da file CSV non è più raccomandata ed è supportata solo per vecchi clienti.

28.3.1.10 Impostazioni di base > Sistema > Codici di servizio

Le diverse funzioni possono essere attivate e disattivate tramite telefono inserendo un codice di servizio. I codici di servizio predefiniti possono essere modificati, facendo tuttavia attenzione che l'assegnazione dei codici sia coerente.

In aggiunta, i due codici usati sui telefoni Dial Pulse e suoi dispositivi ISDN per sostituire i tasti * (asterisco, predefinito: `75`) e # (cancelletto, predefinito: `76`) possono essere cambiati (sostituzioni).

28.3.1.11 Impostazioni di base > Sistema > Password di registrazione HFA

Descrizione dei parametri delle schede:

- **Password di registrazione HFA**

Parametri	Descrizione
Per l'efficacia di questo parametro è essenziale che i telefoni di sistema utilizzino il DLI del sistema e che questo abbia implementato nei telefoni di sistema i parametri necessari.	
Modifica password di registrazione HFA Le password di registrazione HFA possono essere cambiate dall'amministratore	

Parametri	Descrizione
Imponi autenticazione per i dispositivi HFA	Nell'elenco a discesa sono disponibili le seguenti opzioni: • **No** (valore predefinito): nessuna autenticazione applicata Se questa opzione è selezionata, i campi della password sono disattivati. Facendo clic sul pulsante **Applica**, l'autenticazione è disattivata. • **Solo dispositivi non Deskshare con DLI** - la password verrà applicata solo ai client di sistema con DLI configurato. La password verrà impostata nel DB di sistema per detti dispositivi e verrà distribuita a quelli appropriati da DLI. • **Solo dispositivi Deskshare con DLI** - la password verrà applicata solo ai dispositivi Deskshare con DLI configurato. La password verrà impostata nel DB di sistema per detti dispositivi e verrà distribuita a quelli appropriati da DLI. • **Tutti i dispositivi non Deskshare** - la password verrà applicata a tutti i client di Sistema. La password verrà impostata nel DB di sistema per tutti detti dispositivi e verrà distribuita a quelli appropriati da DLI. Per i client di sistema senza DLI configurato, la password deve essere inserita manualmente in ciascuno di essi per poter entrare in servizio. • **Tutti i dispositivi Deskshare** - la password viene applicata per tutti i dispositivi attivati. La password verrà impostata nel DB di sistema per tutti detti dispositivi e verrà distribuita a quelli appropriati da DLI. Per i dispositivi Deskshare senza DLI configurato, la password deve essere inserita manualmente in ciascuno di essi per poter entrare in servizio.
Password	È necessario inserire la password in questo campo. La password deve avere almeno 8 caratteri e includere almeno 1 cifra e/o 1 lettera.
Confermare password	La password deve essere ripetuta in questo campo a scopo di verifica.

28.3.1.12 Impostazioni di base > Gateway

Descrizione dei parametri delle schede:

- **Modifica le proprietà del gateway**

Parametri	Descrizione
Generale	
Nome del cliente	Nome liberamente scelto del cliente, solo ai fini informativi (opzionale) Valori consentiti: max. 15 caratteri
Numero di contratto	Stringa liberamente scelta per scopi informativi (opzionale) Valori consentiti: illimitato

Parametri	Descrizione
Nome del sistema	Nome del sistema di comunicazione liberamente scelto. Questa stringa viene visualizzata nel display di tutti i telefoni di sistema. Valori consentiti: massimo 24 caratteri
Posizionamento del gateway	Stringa liberamente scelta per l'indicazione della posizione fisica del sistema di comunicazione. Queste informazioni consentono a un tecnico dell'assistenza di trovare il sistema di comunicazione, nel caso sia necessario l'accesso fisico al sistema stesso. (opzionale) Valori consentiti: illimitato
Indirizzo del contatto	Stringa liberamente scelta per l'indicazione della persona da contattare in caso di problemi con il sistema di comunicazione. (opzionale) Valori consentiti: illimitato
Sigla internazionale del sistema	Selezione del paese in cui verrà utilizzato il sistema di comunicazione; la modifica del codice del paese in cui viene utilizzato il sistema richiede un riavvio, che verrà eseguita automaticamente.
Indirizzo IP del gateway	Visualizzazione dell'indirizzo IP del sistema di comunicazione, ad esempio 192.168.1.2.
Maschera di rete del gateway	Visualizzazione della maschera di rete del sistema di comunicazione, ad esempio 255.255.255.0.
Prefisso internazionale	Indicazione del prefisso di composizione internazionale, ad esempio 00 per Germania o 011 per USA.
Prefisso nazionale	Indicazione del prefisso di composizione internazionale, ad esempio 0.
Brand	Selezione del prodotto acquistato (OpenScape Business o Octopus F X)
Posizionamento del gateway	
Prefisso internazionale	Indicazione del prefisso internazionale, ad esempio 39 per Italia.
Prefisso interurbano	Indicazione del prefisso interurbano: ad esempio 02 per Milano.
Numero PABX	Indica il numero del sistema (numero centrale senza selezione passante utente), ad esempio, 7007
Parametri rete	
ID nodo	Per ogni nodo di un sistema collegato in rete deve essere specificato un ID nodo univoco. In questo modo, i singoli nodi sono chiaramente identificabili nei sistemi collegati in rete. Valori consentiti: da 1 a 100
Tono interno	
Segnale continuo	Se questo flag è selezionato, il tono interno (segnale di linea) non è costituito da una sequenza di toni ma da un tono continuo. Il segnale di linea interno viene emesso non appena si solleva il ricevitore, senza che sia stata digitata alcuna cifra. Impostazione predefinita: funzione disattivata

28.3.1.13 Impostazioni di base > DynDNS > Servizio DynDNS

Descrizione dei parametri delle schede:

- **Mostra la configurazione di DynDNS**
- **Modifica la configurazione di DynDNS**

Parametri	Descrizione
Attiva DynDNS	Con il servizio DynDNS è possibile accedere al sistema di comunicazione da località diverse senza che sia noto l'indirizzo IP corrente del gateway. Il servizio DynDNS può essere attivato qui.
Dominio definito dall'utente	La casella di controllo deve essere selezionata se il provider DynDNS non è incluso nell'elenco **Nome del dominio**.
Nome d'utente	Nome utente dell'account DynDNS presso il provider DynDNS. Per la creazione di un account DynDNS, visitare il sito Web `http://www.dyndns.org/account/create.html`.
Password	Password dell'account DynDNS presso il provider DynDNS. Per motivi di sicurezza, durante l'insegnamento vengono visualizzati solo segnaposto.
Ripeti password	Ripetizione della password dell'account utente presso DynDNS-Service. Per motivi di sicurezza, durante l'insegnamento vengono visualizzati solo segnaposto.
Nome dell'host	Immissione del nome host registrato presso il provider DynDNS, senza il nome di dominio, ad es. myhost. Il nome di sub-dominio completo è composto dal nome host e dal nome di dominio, ad esempio myhost.dyndns.org.
Nome del dominio	Selezione del provider DynDNS da un elenco (ad esempio dyndns.org) o tramite immissione manuale del provider DynDNS (se **Dominio definito dall'utente** è stato attivato).

URL aggiornamento	Inserire l'URL aggiornamento di un provider DynDNS non incluso nell'elenco. La struttura dell'URL dipende dal provider DynDNS. Inoltre, completare con i parametri specifici per il cliente (nell'esempio contrassegnati in *corsivo*).
	Esempio di un URL aggiornamento:
	`http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`
	Esempio di un URL aggiornamento con autenticazione crittografata Base64:
	`https://<b64><username>:<pass></b64>@members.dyndns.org/nic/update?hostname=<domain>&myip=<ipaddr>&wildcard=NOCHG&mx=NOCHG&backmx=NOCHG`
	<b64>...</b64> per il parametro crittografato Base64

Ultimo aggiornamento	Ora dell'ultimo aggiornamento presso il servizio DynDNS.
Indirizzo IP in DynDNS	Indirizzo IP presso il fornitore DynDNS, al quale vengono deviate le interrogazioni dirette al proprio sottodominio DynDNS configurato.
Proprio indirizzo IP dinamico	Visualizzazione dell'indirizzo IP attuale del sistema di comunicazione assegnato dal provider di servizi Internet.

Parametri	Descrizione
Attiva Wildcard	Se questa opzione è attivata, ogni interrogazione per sotto-sottodomini quali qualsiasi.myhost.dyndns.org vengono istradate su myhost.dyndns.org.
Mail Exchanger	Il Mail Exchanger (MX Record) indica nel DNS a quali indirizzi IP o a quali nomi di dominio devono essere inviate le e-mail per il sub-dominio DynDNS configurato. La destinazione specificata deve essere un server di posta.
Backup MX	Se questa opzione è attivata, le e-mail che non possono essere inoltrate al Mail Exchanger indicato, ad esempio per temporanea indisponibilità, vengono inserite in un buffer dal servizio DynDNS e inviate una volta che Mail Exchanger torna disponibile.
Esegui aggiornamento con HTTPS	Se questa opzione è attivata, viene selezionata per l'aggiornamento la connessione protetta crittografata HTTPS.

28.3.1.14 Impostazioni di base > DynDNS > Ora di aggiornamento del nome di DNS

Descrizione dei parametri delle schede:

- **Modifica l’ora di aggiornamento**

Parametri	Descrizione
Aggiorna nome DNS	Questa opzione vale solo per la VPN. Allo scadere del tempo indicato in "Valore del timer per l'aggiornamento del nome DNS", il componente VPN verifica se il Nome DNS eventualmente utilizzato nella configurazione della VPN viene risolto nei nuovi indirizzi IP(VPN con indirizzi IP dinamici). In questo caso, la VPN viene riconfigurata con i nuovi indirizzi IP.
Valore del timer per l'aggiornamento del nome DNS (sec.)	Numero di secondi per l'intervallo tra due aggiornamenti. Valori consentiti: da 60 a 1800, valore predefinito: 180

28.3.1.15 Basic Settings > Quality of Service

Per il traffico dati IP, i pacchetti IP generati dal sistema di comunicazione stesso vengono suddivisi in cinque gruppi. Per quattro di questi gruppi è possibile definire con quale punto di codice devono essere contrassegnati i pacchetti. Al traffico restante non viene assegnata alcuna priorità (anche con a quello contrassegnato come "00").

Classe di priorità	Valore ToS binario	Valore ToS esadecimale
AF (Assured Forwarding)		
AF11	001-010-00	28
AF12	001-100-00	30
AF13	001-110-00	38
AF21	010-010-00	48
AF22	010-100-00	50

Classe di priorità	Valore ToS binario	Valore ToS esadecimale
AF23	010-110-00	58
AF31	001-010-00	68
AF32	011-100-00	70
AF33	011-110-00	78
AF41	100-010-00	88
AF42	100-100-00	90
AF43	100-110-00	98
EF (Expedited Forwarding)		
EF	101-110-00	B8
Best Effort (BE; massimo sforzo)		
BE	000-000-00	00
CS (Class Selector)		
CS3	011-000-00	60
CS4	100-000-00	80
CS5	101-000-00	A0
CS6	110-000-00	C0
CS7	111-000-00	E0
Inserimento manuale	xxx-xxx-00	0-63 (decimale)

Descrizione dei parametri delle schede:

- **Modifica la Quality of Service**

Parametri	Descrizione
Classe di priorità per dati di segnalazione	Segnalazione delle chiamate per connessione con H.323/SIP Valore predefinito: AF31
Classe di priorità per payload fax/modem	Payload dati, ad esempio per la rete IP con fax o modem Valore predefinito: EF
Classe di priorità per controllo di rete	Controllo rete, ad esempio trap SNMP Valore predefinito: CS7
Classe di priorità per payload voce	Voice Payload per telefonia IP (Voice over IP) Valore predefinito: EF

28.3.1.16 Impostazioni di base > Data e Ora > Data e Ora

Descrizione dei parametri delle schede:

- **Imposta Data e Ora**

Parametri	Descrizione
Data e Ora	
giorno	Scelta del giorno.
Mese	Scelta del mese.
Anno	Immissione dell'anno.
ORE:MM:SS	Immissione dell'ora nel formato 24 ore.

28.3.1.17 Impostazioni di base > Data e Ora > Impostazioni delle zone orarie

Descrizione dei parametri delle schede:

- **Modifica impostazioni dei fusi orari**

Parametri	Descrizione
Zona oraria	Fuso orario locale in cui si trova il sistema

28.3.1.18 Impostazioni di base > Data e Ora > Impostazioni di SNTP

Descrizione dei parametri delle schede:

- **Modifica impostazioni**

Parametri	Descrizione
Client SNTP Immissione dei dati di accesso per un server dell'ora esterno (SNTP) per la sincronizzazione del clock di sistema a livello di rete.	
Stato amministrativo del client SNTP	Attivare o disattivare la connessione del sistema di comunicazione al server SNTP Valore predefinito: non attiva
Indirizzo IP/nome DNS server di riferimento orario esterno	Indirizzo IP o Nome DNS del server SNTP. Valore predefinito: 0.de.pool.ntp.org
Tempo di polling del server dell'ora esterno	Intervallo per sincronizzare la data e l'ora con il server SNTP. Valore predefinito: 4 ore.

28.3.1.19 Impostazioni di base > Gestione della porta

Le porte indicate vengono utilizzate per identificare i protocolli di rete e servizi di rete appropriati. Qui è possibile modificare alcune delle porte utilizzate dal sistema di comunicazione. Ciò consente di personalizzare la comunicazione di rete per ogni rete del cliente se le porte sono già utilizzate per altri scopi. Se vengono apportate modifiche alla gestione delle porte, è di norma necessario

modificare contemporaneamente anche tutti i componenti (telefoni, impianti, ecc.) per garantirne la funzionalità.

Descrizione dei parametri delle schede:

- **Modifica impostazioni globali della gestione delle porte**

Parametri	Descrizione
Nome del registro	Servizio.
Numero di porta	Numero di porta del servizio (configurabile).
Tipo di porta	A titolo informativo viene visualizzato il tipo di porta; Single: porta singola; Min: limite inferiore per il range di porte.
Servizi	
CSP	Provider di servizi CSTA, porta IP per tutte le applicazioni che si desidera connettere con CSP. Valore predefinito: 8800
HFA	Controllo dei client HFA (porta del server CorNet-TC). Valore predefinito: 4060
HFA_EXT	Controllo dei client HFA (porta del server CorNet-TC) per DispositivoSistema@Home. Valore predefinito: 4062
HFA_TLS	CorNet-TC tramite TLS. Valore predefinito: 4061
HFA_TLS_EXT	CorNet-TC tramite TLS.per DispositivoSistema@Home. Valore predefinito: 4063
MEB_SIP	Media Extension Bridge, segnalazione delle chiamate per trunking SIPQ. Valore predefinito: 15060
RTP_MIN	Porte RTP/RTCP e T.38 (MediaBasePort). Valore predefinito: 29100
SIP	Segnalazione della chiamata per terminali SIP e per trunking in SIP. Valore predefinito: 5060
SIP_EXT	Segnalazione di chiamate per telefoni SIP e linee ITSP per Dispositivo SIP@Home. Valore predefinito: 5070
SIPS	Segnalazione sicura della chiamata per trunking SIPQ. Valore predefinito: 5061
SIP_TLS_SUB	Segnalazione sicura della chiamata per utenti SIP. Valore predefinito: 5062

Parametri	Descrizione
SIP_TLS_SUB_EXT	Segnalazione sicura delle chiamate per utenti SIP per Dispositivo SIP@Home. Valore predefinito: 5071
VSL_MULTISITE	Connessioni multisito. Valore predefinito: 8778

28.3.1.20 Impostazioni di base > Addebiti > Addebiti chiamata - Formato di output

Descrizione dei parametri delle schede:

- **Modifica formato di output**

Parametri	Descrizione
Formato del record di dati della chiamata	
Formato di output compresso	Valore predefinito: attivato
Mascheramento delle ultime 4 cifre	Per la tutela della privacy, vengono sostituite le ultime 4 cifre del campo numero di telefono con punti interrogativi. Valore predefinito: disattivato
Protocollo delle chiamate in entrata	Valore predefinito: disattivato
Messa a protocollo durata di chiam. on	Registrazione della durata della conversazione espressa in minuti e secondi. Valore predefinito: attivato
Protocollo di chiamata on	Per le chiamate in entrata, immediatamente dopo l'inizio della chiamata, viene creato un record della connessione, ad esempio, per trasmettere informazioni aggiuntive sul chiamante per un elenco chiamanti o un'analisi dei record su PC. Valore predefinito: disattivato
Output del MSN	Registrazione dei numeri MSN utilizzati (solo ISDN) Valore predefinito: disattivato
Formato decimale	(Non in USA) Il formato della visualizzazione degli addebiti deve essere configurato per i singoli paesi. In Germania, viene sempre utilizzato il formato decimale. Il formato decimale indica inoltre che il moltiplicatore è espresso in centesimi. Il moltiplicatore indica l'importo per il quale viene moltiplicata l'unità tariffaria per ottenere l'importo in denaro (ad esempio 0,06 euro anziché 6 centesimi). Valore predefinito: attivato
Emettere gli importi invece degli scatti	Vengono inseriti gli importi in denaro anziché le unità tariffarie (ad esempio 4,50 Euro anziché 75 unità). Valore predefinito: attivato

Parametri	Descrizione
In uscita senza collegamento	Chiamate delle chiamate in uscita senza risposta. Valore predefinito: disattivato
Output del numero LCR in uscita o del numero di telefono composto in entrata	Se questo flag è attivato, al record dei dati della chiamata viene aggiunto un ulteriore campo numero di telefono. Contiene: • per una chiamata in uscita: il numero di telefono LCR effettivamente inviato allo scambio in seguito alla conversione mediante LCR o • per una chiamata in arrivo: il numero interno dell'utente desiderato, ovvero il primo utente chiamato. Viene quindi generato un record della chiamata, anche se l'utente cui è destinata la chiamata è occupato. Il record della chiamata presenta lo stesso formato del record di dati creato per un utente libero, fatta eccezione per la durata della chiamata, che è impostata su "0". Valore predefinito: disattivato
Registrazione centrale dei dettagli della chiamata (CDRC)	
Output : nessuna	Nessuna trasmissione dei dati di connessione Valore predefinito: HTTP
Output: HTTPS	Trasmissione dei dati di connessione al Call Charge Manager o ad altro software di contabilità Valore predefinito: HTTP
Output: Client LAN-TCP	Trasmissione dei dati di connessione a un server esterno tramite TCP/IP Valore predefinito: HTTP
Client TCP	Definizione dell'indirizzo IP e del numero di porta di un server addebiti esterno. Se sono stati generati addebiti, il sistema di comunicazione avvia una connessione TCP/IP al server addebiti esterno. Una volta stabilita la connessione, vengono trasmessi i dati sugli addebiti; la connessione resta permanentemente aperta ed eventuali altri addebiti sostenuti vengono inviati.

28.3.1.21 Impostazioni di base > Addebiti > Addebiti - Coefficienti

Descrizione dei parametri delle schede:

- **Modifica fattori**

Parametri	Descrizione
Fattore di addebito per ogni fascio	Le informazioni sugli addebiti possono essere visualizzate sotto forma di unità tariffarie (scatti) o di unità monetarie (importo). Sono supportate entrambe le forme ma vengono visualizzate solo le unità di valuta. Per la trasmissione delle informazioni sotto forma di unità di costo, è usato un fattore di conversione. Questi fattori di addebito sono impostati per fascio e si applicano alle chiamate esterne e della rete, sia in entrata che in uscita.
Fasci	Visualizzazione dei fasci disponibili nel sistema

Parametri	Descrizione
Moltiplicatore	Tale moltiplicatore viene utilizzato per la conversione da unità tariffarie in importi in denaro. Valori consentiti: da 0 a 65534, valore predefinito: 6
Moltipl. ISDN	Fattore di conversione degli importi in denaro ricevuti o da versare in unità tariffarie e viceversa. Per i fasci con protocollo QSIG. Valori consentiti: da 1 a 65535, valore predefinito: 6
Valuta	Breve nome della valuta, ad esempio EUR. Questa opzione deve essere adattata al sistema di comunicazione collegato. La configurazione della stringa valuta è indipendente dalla stringa valuta visualizzata sui terminali. Nota: questo parametro è importante solo per i fasci con protocollo QSIG. Per altri protocolli, il parametro non ha alcun effetto e deve essere mantenuta l'impostazione predefinita. Valori consentiti: max. 3 caratteri
Importo in denaro	Nella colonna Importo in denaro viene definito se nel fascio vengono scambiati importi in denaro o unità tariffarie (scatti). Se questa opzione è attivata, viene inviato e ricevuto l'importo in denaro (vedere la colonna Moltipl. ISDN). In caso contrario, si inviano e ricevono le unità tariffarie. Questa opzione deve essere adattata al sistema di comunicazione collegato. Se gli impulsi di addebito vengono scambiati sul fascio, deve essere configurata come valuta una stringa vuota. Nota: questo parametro è importante solo per i fasci con protocollo QSIG. Per altri protocolli, il parametro non ha alcun effetto e deve essere mantenuta l'impostazione predefinita.
Avviso di addebito: Nessun addebito	Tramite il fascio non si ricevono addebiti (es. linee USA). Il parametro non è rilevante per i fasci con protocollo QSIG.
Avviso di addebito: Interim	Si ricevono gli addebiti solo durante la connessione, non al termine della connessione.
Avviso di addebito: Finale	Si ricevono gli addebiti solo al termine della connessione.
Avviso di addebito: Interim finale	Si ricevono gli addebiti durante una connessione e al termine della stessa.
Valuta	Codice valuta per la visualizzazione degli addebiti sui terminali.
Precisione di calcolo	La precisione di calcolo deve essere impostata in modo che la precisione del sistema di comunicazione sia almeno pari a quella degli importi in denaro inviati dal centralino. Se il numero massimo di decimali, cioè tre, non è sufficiente, ha luogo un arrotondamento automatico. Per i fasci con protocollo QSIG occorre selezionare "Sugli impulsi d'addebito".

28.3.1.22 Impostazioni di base > Addebiti chiamata > Addebiti chiamata - Codici di addebito

Descrizione dei parametri delle schede:

- **Modifica dei codici di addebito**

Parametri	Descrizione
Controllo	
Controllo: Nessun controllo	I codici di addebito inseriti non stati sottoposti a controllo. Questa opzione non può essere utilizzata in caso di fasci che prevedono una procedura di inserimento obbligatoria.
Controllo: Controllo liste	Viene verificata la validità dei codici di addebito inseriti mediante le liste PKZ.
Controllo: Esame del numero di cifre	Viene verificato il numero di cifre del codice di addebito inserito.
Numero delle cifre da controllare	Numero valido di caratteri per codice addebito. Valori consentiti: da 1 a 11, valore predefinito: 5
Liste PKZ	
Lista	Per la verifica degli elenchi è possibile inserire un massimo di 1.000 codici di addebito.
Codice d'addebito	Valori consentiti: max. 11 cifre

28.3.1.23 Impostazioni di base > Annuncio Player per messaggi vocali/Annunci

Descrizione dei parametri delle schede:

- **Modifica casella vocale/annuncio player**

Parametri	Descrizione
Casella vocale	
Prefisso	Numero di telefono per la casella vocale.
Player annuncio	
Numero di telefono	Numero di telefono del player (player annuncio).

28.3.1.24 Impostazioni di base > Implementazione parametri telefoni

Descrizione dei parametri delle schede:

- **Modifica parametri telefoni**

Parametri	Descrizione
Implementazione parametri telefoni Per l'efficacia di questo parametro è essenziale che i telefoni di sistema utilizzino il DLI del sistema e che questo abbia implementato nei telefoni di sistema i parametri necessari. I parametri dei telefoni di sistema vengono aggiornati non appena un telefono di sistema si riconnette al sistema o viene riavviato o dopo un riavvio del sistema. I singoli parametri possono essere configurati direttamente nel telefono di sistema o con il WBM del telefono di sistema. Le impostazioni per la porta Ethernet del PC e per la priorità codec non vengono sovrascritte dal DLI se sono state configurate direttamente sul telefono di sistema o con il WBM del telefono di sistema.	
attivare Implementazione parametri telefoni	Se questo flag è attivato, le opzioni seguenti sono attive per la modifica.
Distribuisci SW sui dispositivi a casa	Se questo flag è attivato, vengono concesse le autorizzazioni per l'aggiornamento del software tramite DLI per dispositivi HFA@Home.
Parametri telefoni Qui è possibile modificare le impostazioni telefoni seguenti.	
Porta PC	Se questo flag è attivato, la porta Ethernet del PC di tutti i telefoni di sistema attivi è attivata. Impostazione predefinita: funzione disattivata
L'impostazione codec è "banda ridotta preferita"	Se questo flag è attivato, per tutti i telefoni di sistema si applica la seguente priorità codec: G.729 - G.711 - G.722 Se questo flag è disattivato, si applica la seguente priorità codec: G.722 - G.711 - G.729 **Nota:** CP100 non supporta G.722 Impostazione predefinita: funzione disattivata
Mostra immagini chiamante	Se questo flag è attivato, l'immagine del chiamante viene visualizzata all'arrivo di una chiamata su telefoni di sistema con display a colori di grandi dimensioni, a condizione che sia stata caricata nel sistema con UC Smart o UC Suite. Impostazione predefinita: funzione disattivata
Applica le impostazioni parametri telefoni	
Applicare le impostazioni parametri telefono a tutti i telefoni	Se il flag è attivato, tutte le impostazioni locali amministrate vengono sovrascritte. Impostazione predefinita: funzione disattivata

Descrizione dei parametri delle schede:

- **Info terminale**

  Le informazioni seguenti per ciascun dispositivo vengono menzionate qui:

  Numero di telefono, Display, Tipo dispositivo, Indirizzo IP, Indirizzo MAC, Versione software corrente, Versione hardware, Porta PC, Impostazione Codec.

Descrizione dei parametri delle schede:

- **Modifica password amministratore**

  L'amministratore può configurare la password per accedere al WBM di un telefono.

Parametri	Descrizione
Per l'efficacia di questo parametro è essenziale che i telefoni di sistema utilizzino il DLI del sistema e che questo abbia implementato nei telefoni di sistema i parametri necessari.	
Modifica password amministratore La password predefinita può essere cambiata centralmente dall'amministratore per tutti i dispositivi collegati DLI.	
Password	È necessario inserire la password in questo campo. La password deve contenere almeno 6 caratteri.
Conferma password	La password deve essere ripetuta in questo campo a scopo di verifica.

Descrizione dei parametri delle schede:

- **Impostazioni di composizione canoniche**

  L'amministratore può distribuire in blocco le impostazioni di composizione canoniche a tutti i dispositivi Desk Phone CP HFA con DLI configurato.

  Tenere presente che i valori delle impostazioni di composizione canoniche, configurati in WBM, sovrascrivono sempre le impostazioni locali (del telefono).

Parametri	Descrizione
Impostazioni di composizione canoniche	
Prefisso internazionale	Obbligatorio - Codice interno per la posizione del telefono. Se non viene impostato, la conversione non avrà luogo. Lunghezza massima: 5 caratteri.
Cifra del prefisso nazionale	Necessario - Cifra del prefisso nazionale per la selezione PSTN all'interno del paese locale. Valore: Lunghezza massima: 5 caratteri.
Prefisso interurbano	Necessario - Codice area PSTN per la posizione del telefono. Lunghezza massima 6 caratteri.
Lunghezza minima del numero locale	Necessario - Lunghezza minima del numero locale PSTN. Intervallo: 0-50
Lunghezza massima numero interno	Opzionale - Lunghezza dei numeri dell'area locale PSTN. Un valore pari a 0 significa che questa nuova regola non verrà applicata. Intervallo: 0-50
Nodo aziendale locale	Opzionale - Prefisso della rete aziendale locale per un telefono come interno. Lunghezza massima 10 caratteri.

Parametri	Descrizione
Codice di accesso PSTN	Opzionale - Elenco di cifre per ottenere l'accesso PSTN. Lunghezza massima 10 caratteri.
Codice di accesso internazionale	Necessario - Elenco di codici di accesso PSTN per il gateway internazionale. Lunghezza massima 5 caratteri.
Codice operatore	Opzionale - Elenco dei numeri di interni per gli operatori. Lunghezza massima 50 caratteri.
Numeri di emergenza	Opzionale - Elenco dei numeri utilizzati per le chiamate di emergenza. Lunghezza massima 50 caratteri.
Cifre interno iniziali/Cifre iniziali	Opzionale - Elenco di cifre iniziali per l'estensione nella rete locale aziendale (definite dal nodo aziendale locale). Lunghezza massima 50 caratteri.
Numero di selezione previsto	Opzionale - Valore booleano per indicare quando un codice di accesso PSTN + cifra di prefisso nazionale viene mantenuto e non convertito nel codice di accesso internazionale. Vero/Falso con valore predefinito falso.
Composizione canonica	
Numeri interni	Elenco a discesa con le seguenti opzioni: Modulo impresa locale (predefinito), Aggiungi sempre nodo, Usa numeri esterni. Numero intero.
Numeri esterni	Elenco a discesa con le seguenti opzioni: Modulo pubblico locale (predefinito), Modulo pubblico nazionale, Modulo pubblico internazionale. Numero intero.
Codice di accesso esterno	Elenco a discesa con le seguenti opzioni: Non richiesto (impostazione predefinita), per i numeri esterni. Numero intero.
Codice gateway internazionale	Elenco a discesa con le seguenti opzioni: Usa codice nazionale (impostazione predefinita), Lascia come +. Numero intero.
Ricerca composizione canonica	
Codice locale 1-5	Opzionale - Un codice del nodo locale della rete aziendale. Lunghezza massima 10 caratteri.
Codice internazionale 1 - 5	Opzionale - Il codice internazionale equivalente al codice locale. Lunghezza massima 30 caratteri.

28.3.1.25 Impostazioni di base > Risparmio energia

Descrizione dei parametri delle schede:

- **Attivazione/disattivazione Risparmio energia**

Parametri	Descrizione
Risparmio energia La funzione Risparmio energia può essere attivata solo se l'interfaccia LAN del sistema si trova in Modo collegamento Ethernet **Auto**. In condizioni di risparmio energetico, l'interfaccia LAN del sistema passa automaticamente alla modalità Full duplex. Anche le interfacce LAN dell'infrastruttura collegata devono trovarsi in modalità Autosense.	
Attivazione/disattivazione Risparmio energia	Portare il sistema in condizioni di risparmio energetico.

Parametri	Descrizione
Inizio del LowPowerMode	Punto iniziale della condizione di risparmio energetico
Fine del LowPowerMode	Punto finale della condizione di risparmio energetico.
La larghezza di banda IP viene ridotta a 100 MBit/s FDX	Visualizza la velocità dati in condizioni di risparmio energetico.

28.3.1.26 Installazione di base> Dati di massa

- Descrizione dei parametri delle schede:

Parametri	Descrizione
Porta	Numero di porta. Campo non modificabile.
Validità	Esistono due tipi di convalida, il Controllo consistenza front end e il Controllo consistenza back end: a. Il **Controllo consistenza front end** convalida i dati presentati nei campi della procedura guidata dati di massa verificando la presenza di incoerenze e conflitti. Un'indicazione istantanea rossa viene visualizzata nel campo Validità sotto ai numeri corrispondenti. Passando con il mouse sull'indicazione viene visualizzato il conflitto preciso. b. Il **Controllo consistenza back end** convalida i dati presentati nella procedura guidata dati di massa confrontandoli con quelli non visibili ma presenti nel database del sistema. Fra questi, Gruppo, MULAP, Voicemail, Accesso nazionale e internazionale, Numeri VSL, Codice impegno e Codici di linea (ovvero, accesso alla linea esterna).
N. tel.	Numero di telefono interno dell'utente.
DID	MSN (Interno) dell'utente.
N. Dual Mode	Numero cellulare dell'utente.
N. Mobile UC	Numero cellulare personale dell'utente UC Smart o UC Suite. Il numero è in formato canonico, es.: +49 89 7007 100. Questo numero è visualizzato nella vista **I miei dati personali** dell'utente nella **Directory utente**.
Indirizzo e-mail	Indirizzo e-mail dell'utente.
Visualizzazione	Nome dell'utente liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome.
Nome	Nome proprio dell'utente liberamente scelto.
Cognome	Cognome dell'utente liberamente scelto.
Tipo di dispositivo	Il tipo di dispositivo assegnato all'utente. Campo non modificabile.
Tipo	Tipo di utente.
Tipo: **Senza porta**	Il numero di telefono non è assegnato ad alcun utente.
Tipo: **Client di sistema**	Un client di sistema è un utente IP che può utilizzare tutte le funzioni del sistema di comunicazione tramite CorNet-IP (in precedenza chiamato client di sistema HFA).

Parametri	Descrizione
Tipo: **Client SIP**	Un client SIP è un utente IP che utilizza il protocollo SIP. Tramite il protocollo SIP, può utilizzare solo un numero limitato di funzioni del sistema di comunicazione.
Tipo: **Utente Deskshare**	Un DeskShare User è un utente IP che può accedere a un altro telefono di sistema IP (Mobile Login) e può utilizzarlo come se fosse il suo (compreso il numero di telefono).
Fax N. tel	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'interno.
DID fax	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'esterno.
Accesso	Visualizzazione della porta fisica a cui è collegato il terminale.
Clip/Lin	Sequenza di cifre che viene mostrata per le chiamate esterne in uscita alla destinazione chiamata al posto del numero di telefono effettivo (ad esempio, per i servizi di emergenza E911 negli USA)
Stato	Visualizza lo stato del dispositivo. Attivo o inattivo.

28.3.2 Sicurezza

In **Sicurezza** sono riunite le impostazioni riferite alla sicurezza. Fra queste, le impostazioni per firewall, filtro, VPN ed SSL.

28.3.2.1 Sicurezza > Firewall delle applicazioni

Descrizione dei parametri delle schede:

- **Visualizza servizi**
- **Aggiungi servizio**
- **Elimina tutti i servizi**

Parametri	Descrizione
Firewall applicaz.	Il firewall delle applicazioni viene utilizzato per limitare l'accesso a servizi specifici come FTP o LDAP. È disabilitato per impostazione predefinita e può essere abilitato definendo le regole appropriate. I seguenti servizi possono essere bloccati o limitati a specifici indirizzi IP o intervalli di indirizzi IP dal firewall delle applicazioni: **Servizio/Porte** HTTPS / 443 Postgres / 5432 LDAP / 389 Manager E / 7000 ssh (bloccato per impostazione predefinita) / 22 FTP / 21, 40000 - 40040 OBSERVER/Il servizio OBSERVER consentiva l'accesso da un'applicazione OpenScape Observer che non è più supportata. Solo i servizi elencati possono essere bloccati tramite un menu di selezione in modalità Esperto. Le funzioni telefoniche come SIP, HFA ecc. non possono essere bloccate usando il firewall delle applicazioni. Un servizio può essere selezionato più volte; ogni volta è possibile specificare restrizioni IP diverse. **Nota:** Se abilitato, il firewall delle applicazioni non blocca i servizi per impostazione predefinita fino a quando non viene aggiunta una regola per quel servizio, a quel punto solo gli indirizzi IP inclusi nella regola possono accedere a quel servizio specifico. Il firewall delle applicazioni può limitare l'accesso alle funzioni inter-nodo quando il sistema è collegato in rete ad altri sistemi OpenScape Business. Ad esempio, la funzione di sopravvivenza richiede il servizio POSTGRES per funzionare correttamente; in questo caso, se viene aggiunta una regola per il servizio POSTGRES, è necessario aggiungere manualmente gli indirizzi IP degli altri nodi OpenScape Business collegati in rete alla regola POSTGRES per garantire il corretto funzionamento della funzione di sopravvivenza.
Nome regola	Nome della regola
Regola attivata	La regola è attivata.
Limite inferiore dell'intervallo di indirizzi IP di origine	Il limite inferiore degli indirizzi IP bloccati.
Limite superiore dell'intervallo di indirizzi IP di origine	Il limite superiore degli indirizzi IP bloccati.

28.3.2.2 Sicurezza > Client di distribuzione e licenze (DLSC)

Per utilizzare funzioni DLS, il sistema di comunicazione deve concedere al DLS esterno l'accesso ai dati di configurazione. Il sistema di comunicazione viene quindi utilizzato come client di distribuzione e licenze. Il server DLS esterno viene configurato selezionando il percorso > Scheda madre > Modo DHCP > Server DHCP > Impostazioni globali.

Descrizione dei parametri delle schede:

- **Configurazione base DLSC**
- **Contatta DLSC**
- **Reimposta bootstrap client DLSC**

Parametri	Descrizione
Stato	
Comunicazione protetta con client DLS	Visualizzazione dell'attivazione o disattivazione (0) della comunicazione sicura con il client DLS e del livello di protezione.
Client DLS	
Intervallo di tempo per la risposta alla richiesta di contatto	Valore predefinito: 0
PIN necessario per bootstrapping DLS	Elevato livello di sicurezza grazie al requisito di introduzione PIN su entrambi i lati
PIN bootstrap	Valori consentiti: min. 8 a max. 32 caratteri
Server DLS	
Indirizzo IP del server DLS	Immissione dell'indirizzo IP del server DLS esterno.
Porta del server DLS	Immissione porta del server DLS esterno Valore predefinito: 18443
Porta protetta del server DLS	Visualizzazione del numero di porta per una connessione sicura

28.3.2.3 Sicurezza > Client di distribuzione e licenze (DLSC) > Certificato del client DLSC

Descrizione dei parametri delle schede:

- **Informazioni sul certificato**

Parametri	Descrizione
Tipo di certificato	Utilizzato per assicurare un contatto iniziale sicuro tra il sistema di comunicazione e il DLS
Numero di serie del certificato	Visualizzazione del numero di serie rilevato.

Parametri	Descrizione
Numero di serie del certificato (hex)	Visualizzazione del numero di serie specificato in forma esadecimale.
Tipo di algoritmo della firma	Visualizzazione dell'algoritmo firma utilizzato Valori consentiti: sha256RSA, sha512RSA
Inizio della validità del certificato (GMT)	Visualizzazione dell'inizio della validità del certificato. La data viene intesa come ora di Greenwich (GMT).
Fine della validità del certificato (GMT)	Visualizzazione della fine della validità del certificato. La data viene intesa come ora di Greenwich (GMT).
Punto di distribuzione CRL	Visualizzazione dell'URL opzionale da cui possono essere distribuiti gli elenchi di revoche dei certificati (CRL)
Emesso da CA	L'autorità di certificazione che ha firmato il certificato
Paese (C)	Codice paese a due cifre
Organizzazione (O)	Il nome legale completo dell'azienda
Unità organizzativa (OU)	L'unità organizzativa è la succursale dell'azienda che sta ordinando il certificato
Nome generale (CN)	Nome di dominio completo (FQDN)
Richiedente	Visualizzazione della data del richiedente del certificato secondo le convenzioni previste dallo standard X.509 (ad esempio, campo Paese (C) DE per Germania)
Paese (C)	Codice paese a due cifre
Organizzazione (O)	Il nome legale completo dell'azienda
Unità organizzativa (OU)	L'unità organizzativa è la succursale dell'azienda che sta ordinando il certificato
Nome generale (CN)	Nome di dominio completo (FQDN)
Richiedente alternativo	Questa informazione opzionale effettua una distinzione tra il formato del nome DN (come i dati del richiedente) e qualsiasi altro formato (ad esempio un indirizzo IP). La maschera di immissione dipende dal formato selezionato
Dati dalla chiave pubblica	Dati chiave pubblica del certificato usati per la crittografia
Lunghezza della chiave pubblica	Valori consentiti: 1024, 1536, 2048
Chiave pubblica	Crittografia mediante chiave pubblica confermata da terzi secondo lo standard X.509. L'elevato livello di sicurezza deriva dal fatto che la chiave per la decodifica deve essere impostata singolarmente e viene salvata solo dall'utente.
Impronta digitale	La chiave pubblica utilizzata e l'impronta digitale vengono visualizzate in formato esadecimale.

28.3.2.4 Sicurezza > Client di distribuzione e licenze (DLSC) > Certificato CA del client DLSC

Descrizione dei parametri delle schede:

- **Informazioni sul certificato**

Parametri	Descrizione
Tipo di certificato	Utilizzato per assicurare un contatto iniziale sicuro tra il sistema di comunicazione e il DLS.
Numero di serie del certificato	Visualizzazione del numero di serie rilevato.
Numero di serie del certificato (hex)	Visualizzazione del numero di serie specificato in forma esadecimale.
Tipo di algoritmo della firma	Visualizzazione dell'algoritmo firma utilizzato. Valori consentiti: sha256RSA, sha512RSA
Inizio della validità del certificato (GMT)	Visualizzazione dell'inizio della validità del certificato. La data viene intesa come ora di Greenwich (GMT).
Fine della validità del certificato (GMT)	Visualizzazione della fine della validità del certificato. La data viene intesa come ora di Greenwich (GMT).
Punto di distribuzione CRL	Visualizzazione dell'URL opzionale da cui possono essere distribuiti gli elenchi di revoche dei certificati (CRL).
Emesso da CA	L'autorità di certificazione che ha firmato il certificato
Paese (C)	Codice paese a due cifre
Organizzazione (O)	Il nome legale completo dell'azienda
Unità organizzativa (OU)	L'unità organizzativa è la succursale dell'azienda che sta ordinando il certificato
Nome generale (CN)	Nome di dominio completo (FQDN)
Richiedente	Visualizzazione della data del richiedente del certificato secondo le convenzioni previste dallo standard X.509 (ad esempio, campo Paese (C) DE per Germania).
Paese (C)	Codice paese a due cifre
Organizzazione (O)	Il nome legale completo dell'azienda
Unità organizzativa (OU)	L'unità organizzativa è la succursale dell'azienda che sta ordinando il certificato
Nome generale (CN)	Nome di dominio completo (FQDN)
Richiedente alternativo	Questa informazione opzionale effettua una distinzione tra il formato del nome DN (come i dati del richiedente) e qualsiasi altro formato (ad esempio un indirizzo IP). La maschera di immissione dipende dal formato selezionato.
Dati dalla chiave pubblica	Dati chiave pubblica del certificato usati per la crittografia

Parametri	Descrizione
Lunghezza della chiave pubblica	Valori consentiti: 1024, 1536, 2048
Chiave pubblica	Crittografia mediante chiave pubblica confermata da terzi secondo lo standard X.509. L'elevato livello di sicurezza deriva dal fatto che la chiave per la decodifica deve essere impostata singolarmente e viene salvata solo dall'utente.
Impronta digitale	La chiave pubblica utilizzata e l'impronta digitale vengono visualizzate in formato esadecimale.
Tipo di certificato	Utilizzato per assicurare un contatto iniziale sicuro tra il sistema di comunicazione e il DLS.

28.3.2.5 Sicurezza > Crittografia segnalazione e payload (SPE)

Descrizione dei parametri delle schede:

- **Modifica impostazioni di protezione**

Parametri	Descrizione
Lunghezza minima delle chiavi RSA	Lunghezza minima delle chiavi RSA nei certificati. Più è elevato il valore, più sicura è la chiave Valori consentiti: 512, 1024, 2048 Predefinito: 1024
Convalida del certificato	Attiva o disattiva la convalida del certificato. È sconsigliabile disattivare tale convalida. Impostazione predefinita: opzione attivata
Verifica Subjectname	Mediante la verifica del nome oggetto nel certificato di un gateway è possibile verificarne l'identità. Il nome del soggetto contiene l'indirizzo IP o il nome DNS (DNS: Domain Name System) dei rispettivi gateway Impostazione predefinita: funzione disattivata
Verifica CRL	Con l'aiuto di un elenco revoche certificati (CRL: Certificate Revocation List) è possibile determinare se un certificato è stato revocato/annullato e perché. Se un'autorità di certificazione (CA: Autorità di certificazione) dichiara valido un certificato, inserisce il numero di serie nella sua lista. Durante la verifica del certificato, questo elenco può essere controllato tramite Internet presso l'autorità di certificazione (CA) Impostazione predefinita: funzione disattivata
Forza rinegoziazione sicura (RFC 5746)	Questo processo migliora la sicurezza quando si rinegozia il parametro crittografia delle connessioni TLS. Può essere utilizzato solo se è supportato da tutti i server collegati. (OpenScape Business, OpenScape 4000 e OpenScape Voice supportano il processo migliorato, HiPath 3000 non lo supporta). Impostazione predefinita: funzione disattivata

Parametri	Descrizione
Intervallo massimo di rinegoziazione chiavi (ore)	Questo intervallo determina per quanto tempo deve essere usata una chiave specifica per la crittografia dei dati delle segnalazioni e degli utenti. Trascorso questo intervallo, viene definita una nuova chiave Valori consentiti: da 6 a 48 Predefinito: 24

28.3.2.6 Sicurezza > Crittografia payload segnalazione e payload > Certificato SPE

Descrizione dei parametri della scheda:

- **Importa certificato SPE e chiave privata (file PKCS#12)**

Parametri	Descrizione
Password di decrittografia	Immissione della password che è stata utilizzata per la creazione del file PKCS#12.
File con certificato e chiave privata (formato PKCS#12 o PEM)	Scelta del file che contiene i dati del certificato da importare.

28.3.2.7 Sicurezza > Crittografia segnalazione/Crittografia Payload > Certificati SPE CA

È possibile ad esempio importare singolarmente fino a 16 certificati CA attendibili da un'autorità di certificazione PKI (RA/CA) del cliente.

Descrizione dei parametri della scheda:

- **Importa certificato CA attendibile per SPE (file X.509)**

Parametri	Descrizione
File con certificato (PEM o binari)	Scelta del file binario o PEM da importare.
Protocollo punto di distribuzione CRL (CDP)	Selezione del protocollo per elenchi CRL (elenchi di revoca dei certificati) Valori consentiti: LDAP o HTTP
CDP (senza ad esempio ldap://)	Un CDP è un'estensione del certificato opzionale. Un certificato ricevuto viene verificato solo rispetto ai CRL per cui è stato configurato il CDP.

28.3.2.8 Sicurezza > VPN

Descrizione dei parametri delle schede:

- **Mostra informazioni generiche**
- **Attivazione delle tabelle VPN configurate**
- **Attiva/disattiva IPSec**

Parametri	Descrizione
Algoritmo di crittografazione	Algoritmo di crittografazione utilizzato Valori consentiti: AES, 3DES
Algoritmi Hash	Hash di crittografia standardizzato per il calcolo di un valore di controllo univoco (firma digitale) Valori consentiti: MD5, SHA1, SHA2
Algoritmi a chiave pubblica	Procedura di crittografia asimmetrica Valori consentiti: RSA
Gruppi Diffie Hellman	Metodo per lo scambio di chiavi Valori consentiti: gruppo DH 2, Gruppo DH 5
Pulsanti	
Attiva subito	È possibile attivare le tabelle VPN. Leggere attentamente le avvertenze!
Attivazione/disattivazione IPsec	IPSec può essere attivato o disattivato. Leggere attentamente le avvertenze!

28.3.2.9 Sicurezza > VPN > CA Lightweight

Descrizione dei parametri delle schede:

- **Crea certificato CA**

Parametri	Descrizione
Nome del certificato	Nome del certificato da generale liberamente scelto
Numero di serie del certificato	Immissione di un numero di serie preimpostato dall'utente. Il numero deve essere un numero intero positivo.
Tipo di algoritmo della firma	Selezione dell'algoritmo di firma da utilizzare per questo certificato Valori consentiti: sha25RSA, sha512RSA
Lunghezza della chiave pubblica	Selezione della lunghezza della chiave da utilizzare per questo certificato Valori consentiti: 2048
Inizio della validità del certificato (GMT) Indicazione della data di inizio validità del certificato. La data viene intesa come ora di Greenwich (GMT).	
Fine della validità del certificato (GMT) Indicazione della data di fine validità del certificato. La data viene intesa come ora di Greenwich (GMT).	
Richiedente Immissione della data del richiedente del certificato secondo le convenzioni previste dallo standard X.509 (ad esempio, campo Paese (C) DE per Germania).	

Parametri	Descrizione
Richiedente alternativo Questa informazione opzionale effettua una distinzione tra il formato del nome DN (come i dati del richiedente) e qualsiasi altro formato (ad esempio un indirizzo IP). La maschera di immissione dipende dal formato selezionato. Se si seleziona un altro formato, è possibile configurare più di una voce SAN.	
Formato del nome di DN	Di solito viene fornito anche come Nome Generale RDN all'interno del campo Oggetto del certificato principale
Altro formato	Altri nomi, forniti come nomi generici
Estensione del nome alternativo del richiedente	Valori consentiti: nome DNS, indirizzo IP, indirizzo di posta elettronica, Uniform Resource Indicator, altro
Richiedente alternativo	Questa informazione opzionale effettua una distinzione tra il formato del nome DN (come i dati del richiedente) e qualsiasi altro formato (ad esempio un indirizzo IP). La maschera di immissione dipende dal formato selezionato. Se si seleziona un altro formato, è possibile configurare più di una voce SAN.
Tipo punto di distribuzione CRL	Valori consentiti: nome DNS, indirizzo IP, indirizzo di posta elettronica, Uniform Resource Indicator, altro
Punto di distribuzione del CRL	Visualizzazione di un URL da cui possono essere distribuiti gli elenchi di revoche dei certificati (CRL).
Crea certificato	

28.3.2.10 Sicurezza > VPN > Gestione certificati

Descrizione dei parametri delle schede:

- **Mostra certificato da file**

Parametri	Descrizione
Formato PKCS#12	Se il certificato è salvato in un file PKCS#12, è necessario attivare questo campo.
Password di decrittografia	Se è stato selezionato il campo Formato PKCS#12, è necessario inserire in questo campo la stessa password utilizzata per la creazione del file.
File con il certificato	Inserire in questo campo il percorso e il nome file del certificato. Se non si conosce con precisione il percorso di memorizzazione, fare clic su Sfoglia. Viene visualizzata una finestra di ricerca.

28.3.2.11 Sicurezza > VPN > Gestione certificati > Certificati CA attendibili > Certificati attivi

Descrizione dei parametri della scheda:

- **Importazione di certificato CA attendibile (X509)**

Parametri	Descrizione
Tipo di certificato	Utilizzato per assicurare un contatto iniziale sicuro tra il sistema di comunicazione e il DLS
Numero di serie del certificato	Visualizzazione del numero di serie rilevato.
Numero di serie del certificato (hex)	Visualizzazione del numero di serie specificato in forma esadecimale.
Tipo di algoritmo della firma	Visualizzazione dell'algoritmo firma utilizzato Valori consentiti: sha256RSA, sha512RSA
Inizio della validità del certificato (GMT)	Visualizzazione dell'inizio della validità del certificato. La data viene intesa come ora di Greenwich (GMT).
Fine della validità del certificato (GMT)	Visualizzazione della fine della validità del certificato. La data viene intesa come ora di Greenwich (GMT).
Punto di distribuzione CRL	Visualizzazione dell'URL opzionale da cui possono essere distribuiti gli elenchi di revoche dei certificati (CRL)
Emesso da CA	L'autorità di certificazione che ha firmato il certificato
Paese (C)	Codice paese a due cifre
Organizzazione (O)	Il nome legale completo dell'azienda
Unità organizzativa (OU)	L'unità organizzativa è la succursale dell'azienda che sta ordinando il certificato
Nome generale (CN)	Nome di dominio completo (FQDN)
Richiedente	Visualizzazione della data del richiedente del certificato secondo le convenzioni previste dallo standard X.509 (ad esempio, campo Paese (C) DE per Germania)
Paese (C)	Codice paese a due cifre
Organizzazione (O)	Il nome legale completo dell'azienda
Unità organizzativa (OU)	L'unità organizzativa è la succursale dell'azienda che sta ordinando il certificato
Nome generale (CN)	Nome di dominio completo (FQDN)
Richiedente alternativo	Questa informazione opzionale effettua una distinzione tra il formato del nome DN (come i dati del richiedente) e qualsiasi altro formato (ad esempio un indirizzo IP). La maschera di immissione dipende dal formato selezionato
Dati dalla chiave pubblica	Dati chiave pubblica del certificato usati per la crittografia
Lunghezza della chiave pubblica	Valori consentiti: 1024, 1536, 2048

Parametri	Descrizione
Chiave pubblica	Crittografia mediante chiave pubblica confermata da terzi secondo lo standard X.509. L'elevato livello di sicurezza deriva dal fatto che la chiave per la decodifica deve essere impostata singolarmente e viene salvata solo dall'utente.
Impronta digitale	La chiave pubblica utilizzata e l'impronta digitale vengono visualizzate in formato esadecimale.

28.3.2.12 Sicurezza > VPN > Gestione certificati > Certificati CA attendibili > Certificati configurati

Descrizione dei parametri della scheda:

- **Importazione di certificato CA attendibile (X509)**

Parametri	Descrizione
Nome del certificato	Immissione del nome che deve avere il certificato.
File con il certificato	Percorso e nome del file del certificato. Quando si fa clic su Sfoglia, viene visualizzata una finestra di ricerca in cui è possibile trovare la posizione del file.

28.3.2.13 Sicurezza > VPN > Certificati Peer

Descrizione dei parametri delle schede:

- **Crea richiesta del certificato (CSR)**
- **Importa certificato Peer (PKCS#12)**

Parametri	Descrizione
Nome della richiesta del certificato	È possibile creare un certificato Peer firmato CA (basato su un certificato CA). A tal fine è necessario che sia stato generato almeno un certificato. Il certificato creato viene salvato in un file PKCS#12. I file PKCS#12 (Personal Information Exchange Syntax Standard) memorizzano i certificati con chiave privata. Un file PKCS#12 contiene quindi i dati per la crittografia e la decrittografia personali.
Tipo di algoritmo della firma	Selezionare l'algoritmo di firma da utilizzare per questo certificato. Valori consentiti: sha25RSA, sha512RSA
Lunghezza della chiave pubblica	Valori consentiti: 2048
Richiedente	Dati del richiedente del certificato secondo le convenzioni previste dallo standard X.509 (ad esempio, campo Paese (C) DE per Germania).
Paese (C)	Codice paese a due cifre
Organizzazione (O)	Il nome legale completo dell'azienda

Parametri	Descrizione
Unità organizzativa (OU)	L'unità organizzativa è la succursale dell'azienda che sta ordinando il certificato
Nome generale (CN)	Nome di dominio completo (FQDN)
Richiedente alternativo	Questa informazione opzionale effettua una distinzione tra il formato del nome DN (come i dati del richiedente) e qualsiasi altro formato (ad esempio un indirizzo IP). La maschera di immissione dipende dal formato selezionato. Se si seleziona un altro formato, è possibile configurare più di una voce SAN.
Formato del nome di DN	Di solito viene fornito anche come Nome Generale RDN all'interno del campo Oggetto del certificato principale
Paese (C)	Codice paese a due cifre
Organizzazione (O)	Il nome legale completo dell'azienda
Unità organizzativa (OU)	L'unità organizzativa è la succursale dell'azienda che sta ordinando il certificato
Nome generale (CN)	Nome di dominio completo (FQDN)
Altro formato	Altri nomi, forniti come nomi generici
Estensione del nome alternativo del richiedente	Valori consentiti: nome DNS, indirizzo IP, indirizzo di posta elettronica, Uniform Resource Indicator, altro
Nome alternativo del richiedente	Questa informazione opzionale effettua una distinzione tra il formato del nome DN (come i dati del richiedente) e qualsiasi altro formato (ad esempio un indirizzo IP). La maschera di immissione dipende dal formato selezionato.
Importa certificato Peer [PKCS#12]	
Nome del certificato	Immissione del nome che deve avere il certificato.
Password di decrittografia	Password per la decrittografia del certificato Peer Valori consentiti: min. 7 e max. 32 caratteri
File con il certificato	Fare clic su Sfoglia. Viene visualizzata una finestra di ricerca.
Mostra impronta digitale del certificato	Fare clic su questo pulsante per verificare l'integrità del certificato.
Importa certificato da file	Fare clic su questo pulsante per importare un certificato.

28.3.2.14 Sicurezza > VPN > Servizi > Servizi attivi

Descrizione dei parametri della scheda:

- **Mostra servizi IPSec**

Parametri	Descrizione
Nome del servizio	Questo campo contiene il nome dei servizi configurati.
Stato nello stack IP	

Parametri	Descrizione
Porta di origine	Visualizzazione del numero di porta di origine. Se viene visualizzato "0", ciò corrisponde a una porta arbitraria o sconosciuta.
Porta di destinazione	Visualizzazione del numero di porta di destinazione. Se viene visualizzato "0", ciò corrisponde a una porta arbitraria o sconosciuta.
Protocollo IP	Visualizzazione del protocollo IP utilizzato per il trasferimento.
Regola 'pass' associata	Visualizzazione della regola "PASS" associata. L'assegnazione delle regole e dei servizi viene eseguita tramite le regole.
Regola 'deny' associata	Visualizzazione della regola "DENY" associata. L'assegnazione delle regole e dei servizi viene eseguita tramite le regole.

28.3.2.15 Sicurezza > VPN > Servizi > Servizi configurati

Descrizione dei parametri delle schede:

- **Mostra servizi IPSec**
- **Aggiungi servizio IPSec**
- **Modifica servizio IPSec**
- **Rinomina servizio IPSec**
- **Cancella servizio IPSec**

Parametri	Descrizione
Nome del servizio	Campo di input per il nome del servizio da configurare. Inserire una stringa in questo campo.
Porta di origine	Numero di porta da utilizzare per la trasmissione dei dati lato mittente. Se viene inserito "0", ciò corrisponde a una porta arbitraria o sconosciuta.
Porta di destinazione	Numero di porta da utilizzare per la trasmissione dei dati lato destinatario. Se viene inserito "0", ciò corrisponde a una porta arbitraria o sconosciuta.
Protocollo IP	Protocollo IP da utilizzare per la trasmissione Valori consentiti: ICMP, TCP, UDP
Nome del servizio	Campo di input per il nome del servizio da configurare.
Porta di origine	Numero di porta da utilizzare per la trasmissione dei dati lato mittente. Se viene inserito "0", ciò corrisponde a una porta arbitraria o sconosciuta.
Porta di destinazione	Numero di porta da utilizzare per la trasmissione dei dati lato destinatario. Se viene inserito "0", ciò corrisponde a una porta arbitraria o sconosciuta.
Protocollo IP	Selezionare il protocollo IP utilizzato per la trasmissione Valori consentiti: ICMP, TCP, UDP
Nome del servizio	Campo di input per il nome del servizio da configurare.
	L'eliminazione è possibile solo se al servizio non è assegnata alcuna regola.

28.3.2.16 Sicurezza > VPN > Tunnel > Tunnel attivi

Descrizione dei parametri delle schede:

- **Mostra dati generici dei tunnel**
- **Visualizza regole di tutti i tunnel**

Parametri	Descrizione
Nome del tunnel	Questo campo contiene il nome del tunnel configurato.
Stato nello stack IP	Visualizzazione stato nello stack IP. Valori consentiti: attivo/non attivo
Tipo di punto terminale del tunnel locale	Visualizzazione dell'indirizzo del punto terminale del lato invio del tunnel (possibilmente indicazione di un nome host o DNS).
Indirizzo del punto terminale del tunnel locale	Visualizzazione dell'indirizzo del punto terminale del tunnel locale.
Tipo di punto terminale del tunnel remoto	Visualizzazione del tipo di terminale del tunnel remoto.
Indirizzo del punto terminale del tunnel remoto	Visualizzazione del tipo di terminale del tunnel remoto. Visualizzazione dell'indirizzo di destinazione del tunnel remoto. Se si imposta l'indirizzo 0.0.0.0, il punto terminale del tunnel è sconosciuto. In tal caso, la creazione del tunnel deve avvenire sempre dal lato opposto (ad es. operatore remoto).
Durata proposta delle chiavi di sessione	Visualizzazione della validità accettata per la chiave di sessione (session key) da utilizzare. Una volta trascorso questo periodo, non sarà più possibile scambiare informazioni con questa sessione. In sostituzione di chiavi di sessione non più valide vengono negoziate automaticamente nuove chiavi di sessione.
Durata proposta della sessione di scambio delle chiavi	Visualizzazione della validità accettata per la sessione di scambio delle chiavi. Una volta scaduta la sessione di scambio delle chiavi, vengono negoziate automaticamente nuove chiavi per la sessione di scambio delle chiavi tramite IKE (protocollo di crittografia).
Regole associate: Regola di invio	Configurazione delle regola di invio in VPN> Regole
Regole associate: Regola di ricezione	Configurazione delle regola di ricezione in VPN> Regole
Dati del tunnel	
Nome del tunnel	Questo campo contiene il nome del tunnel configurato.
Stato nello stack IP	Visualizzazione stato nello stack IP. Valori consentiti: attivo/non attivo
Tipo di punto terminale del tunnel locale	Visualizzazione dell'indirizzo del punto terminale del lato invio del tunnel (possibilmente indicazione di un nome host o DNS).
Indirizzo del punto terminale del tunnel locale	Visualizzazione dell'indirizzo del punto terminale del tunnel locale.

Parametri	Descrizione
Tipo di punto terminale del tunnel remoto	Visualizzazione del tipo di terminale del tunnel remoto.
Indirizzo del punto terminale del tunnel remoto	Visualizzazione del tipo di terminale del tunnel remoto. Visualizzazione dell'indirizzo di destinazione del tunnel remoto. Se si imposta l'indirizzo 0.0.0.0, il punto terminale del tunnel è sconosciuto. In tal caso, la creazione del tunnel deve avvenire sempre dal lato opposto (ad es. operatore remoto).
Dati della regola	
Destinazione	Indicatore di stato nella Destinazione. Valori consentiti: invio/ricezione
Priorità	Visualizzazione della priorità per la sequenza di esecuzione. La massima priorità è indicata dal numero 1. Per ogni regola di un fascio occorre assegnare una priorità separata. La regola relativa a una direzione di trasmissione e quella per la direzione opposta devono sempre avere la stessa priorità. Le regole per il fascio opposto possono essere configurate solo con la voce di menu appropriata.
Azione per la regola	Indicazione di come i pacchetti IP devono essere gestiti secondo la regola: "pass" significa che i pacchetti IP vengono inoltrati; "deny" significa nessun pacchetto IP verrà trasmesso.
Crittografazione necessaria	Visualizzazione della crittografia per questa regola. Il metodo di crittografia è definito mediante il tunnel associato.
Stato della regola	Indicatore di stato nella regola. Valori consentiti: attivato/disattivato
Stato nello stack IP	Visualizzazione stato nello stack IP. Valori consentiti: attivo/non attivo
Indirizzo di origine Visualizzazione dell'indirizzo di origine e di destinazione nel formato corrispondente al tipo selezionato. L'indicazione dipende dal tipo di indirizzo selezionato. Se è possibile utilizzare qualsiasi indirizzo IP, viene visualizzato 0.0.0.0. Se come indirizzo di destinazione per l'invio di pacchetti in un tunnel viene inserito 0.0.0.0, è necessario disattivare l'interfaccia per la rete di destinazione NAT. In alternativa, per inviare i pacchetti attraverso un tunnel è possibile utilizzare un indirizzo IP compreso tra 0.0.0.1 e 255.255.255.254 è possibile inviare pacchetti in un tunnel.	
Tipo	Visualizzazione del tipo di l'indirizzo di origine e di destinazione (possibili opzioni: host, sottorete, intervallo di indirizzi IP e nome DNS).
Indirizzo (l'ultimo dell'intervallo)	Visualizzazione dell'indirizzo di origine e di destinazione nel formato corrispondente al tipo selezionato. La maschera di immissione dipende dal tipo di indirizzo selezionato. Se è possibile utilizzare qualsiasi indirizzo IP, viene visualizzato 0.0.0.0. Se come indirizzo di destinazione per l'invio di pacchetti in un tunnel viene inserito 0.0.0.0, è necessario disattivare l'interfaccia per la rete di destinazione NAT. In alternativa, per inviare i pacchetti attraverso un tunnel è possibile utilizzare un indirizzo IP compreso tra 0.0.0.1 e 255.255.255.254 è possibile inviare pacchetti in un tunnel.

Parametri	Descrizione
Maschera sub-rete / primo indirizzo dell'intervallo	Viene impostato nel caso in cui sia necessario configurare un intervallo di indirizzi di origine/destinazione per la trasmissione
Indirizzo di destinazione	
Tipo	Visualizzazione del tipo di l'indirizzo di origine e di destinazione (possibili opzioni: host, sottorete, intervallo di indirizzi IP e nome DNS).
Indirizzo (l'ultimo dell'intervallo)	Visualizzazione dell'indirizzo di origine e di destinazione nel formato corrispondente al tipo selezionato. La maschera di immissione dipende dal tipo di indirizzo selezionato. Se è possibile utilizzare qualsiasi indirizzo IP, viene visualizzato 0.0.0.0. Se come indirizzo di destinazione per l'invio di pacchetti in un tunnel viene inserito 0.0.0.0, è necessario disattivare l'interfaccia per la rete di destinazione NAT. In alternativa, per inviare i pacchetti attraverso un tunnel è possibile utilizzare un indirizzo IP compreso tra 0.0.0.1 e 255.255.255.254 è possibile inviare pacchetti in un tunnel.
Maschera sub-rete / primo indirizzo dell'intervallo	Viene impostato nel caso in cui sia necessario configurare un intervallo di indirizzi di origine/destinazione per la trasmissione
Dati del servizio Visualizzazione del servizio sul quale la crittografia viene limitata. Se la crittografia non deve essere limitata a un servizio, selezionare "Servizio qualsiasi".	
Nome del servizio	Campo di input per il nome del servizio da configurare.
Porta di origine	Visualizzazione del tunnel nella direzione di ricezione per la quale si applica questa regola. Da questo tunnel vengono recuperati i pacchetti IP ricevuti dalla rete. Se nel fascio di ricezione non deve essere assegnato alcun tunnel, selezionare l'opzione Nessuna assegnazione tunnel.
Porta di destinazione	Visualizzazione del tunnel nella in direzione di invio per la quale si applica questa regola. I pacchetti IP destinati alla rete vengono istradati attraverso questo tunnel. Se nel fascio di invio non deve essere assegnato alcun tunnel, selezionare l'opzione Nessuna assegnazione tunnel.
Protocollo IP	Selezionare il protocollo IP utilizzato per la trasmissione Valori consentiti: ICMP, TCP, UDP

28.3.2.17 Sicurezza > VPN > Tunnel > Tunnel configurati

Descrizione dei parametri delle schede:

- **Mostra dati generici dei tunnel**
- **Visualizza regole di tutti i tunnel**
- **Aggiungi tunnel/Modifica dati del tunnel**
- **Dati di scambio delle chiavi**

Parametri	Descrizione
	Il termine tunnel si riferisce al trasporto di pacchetti di dati crittografati fino a un punto terminale fisso. I tunnel attivi sono tunnel configurati dopo un'attivazione della configurazione. Nel complesso si possono configurare fino a 256 tunnel per gateway.

Parametri	Descrizione
Nome del tunnel	Questo campo contiene il nome del tunnel configurato.
Stato nello stack IP	Visualizzazione stato nello stack IP. Valori consentiti: attivo/non attivo
Tipo di punto terminale del tunnel locale	Visualizzazione dell'indirizzo del punto terminale del lato invio del tunnel (possibilmente indicazione di un nome host o DNS).
Indirizzo del punto terminale del tunnel locale	Visualizzazione dell'indirizzo del punto terminale del tunnel locale.
Tipo di punto terminale del tunnel remoto	Visualizzazione del tipo di terminale del tunnel remoto.
Indirizzo del punto terminale del tunnel remoto	Visualizzazione del tipo di terminale del tunnel remoto. Visualizzazione dell'indirizzo di destinazione del tunnel remoto. Se si imposta l'indirizzo 0.0.0.0, il punto terminale del tunnel è sconosciuto. In tal caso, la creazione del tunnel deve avvenire sempre dal lato opposto (ad es. operatore remoto).
Durata proposta delle chiavi di sessione	Visualizzazione della validità accettata per la chiave di sessione (session key) da utilizzare. Una volta trascorso questo periodo, non sarà più possibile scambiare informazioni con questa sessione. In sostituzione di chiavi di sessione non più valide vengono negoziate automaticamente nuove chiavi di sessione.
Durata proposta della sessione di scambio delle chiavi	Visualizzazione della validità accettata per la sessione di scambio delle chiavi. Una volta scaduta la sessione di scambio delle chiavi, vengono negoziate automaticamente nuove chiavi per la sessione di scambio delle chiavi tramite IKE (protocollo di crittografia).
Regole associate: Regola di invio	Configurazione delle regola di invio in VPN> Regole
Regole associate: Regola di ricezione	Configurazione delle regola di ricezione in VPN> Regole
Dati del tunnel	
Nome del tunnel	Questo campo contiene il nome del tunnel configurato.
Stato nello stack IP	Visualizzazione stato nello stack IP. Valori consentiti: attivo/non attivo
Tipo di punto terminale del tunnel locale	Visualizzazione dell'indirizzo del punto terminale del lato invio del tunnel (possibilmente indicazione di un nome host o DNS).
Indirizzo del punto terminale del tunnel locale	Visualizzazione dell'indirizzo del punto terminale del tunnel locale.
Tipo di punto terminale del tunnel remoto	Visualizzazione del tipo di terminale del tunnel remoto.
Indirizzo del punto terminale del tunnel remoto	Visualizzazione del tipo di terminale del tunnel remoto. Visualizzazione dell'indirizzo di destinazione del tunnel remoto. Se si imposta l'indirizzo 0.0.0.0, il punto terminale del tunnel è sconosciuto. In tal caso, la creazione del tunnel deve avvenire sempre dal lato opposto (ad es. operatore remoto).

Parametri	Descrizione
Dati della regola	
Destinazione	Indicatore di stato nella Destinazione. Valori consentiti: invio/ricezione
Priorità	Visualizzazione della priorità per la sequenza di esecuzione. La massima priorità è indicata dal numero 1. Per ogni regola di un fascio occorre assegnare una priorità separata. La regola relativa a una direzione di trasmissione e quella per la direzione opposta devono sempre avere la stessa priorità. Le regole per il fascio opposto possono essere configurate solo con la voce di menu appropriata.
Azione per la regola	Indicazione di come i pacchetti IP devono essere gestiti secondo la regola: "pass" significa che i pacchetti IP vengono inoltrati; "deny" significa nessun pacchetto IP verrà trasmesso.
Crittografazione necessaria	Visualizzazione della crittografia per questa regola. Il metodo di crittografia è definito mediante il tunnel associato.
Stato della regola	Indicatore di stato nella regola. Valori consentiti: attivato/disattivato
Stato nello stack IP	Visualizzazione stato nello stack IP. Valori consentiti: attivo/non attivo
Indirizzo di origine Visualizzazione dell'indirizzo di origine e di destinazione nel formato corrispondente al tipo selezionato. L'indicazione dipende dal tipo di indirizzo selezionato. Se è possibile utilizzare qualsiasi indirizzo IP, viene visualizzato 0.0.0.0. Se come indirizzo di destinazione per l'invio di pacchetti in un tunnel viene inserito 0.0.0.0, è necessario disattivare l'interfaccia per la rete di destinazione NAT. In alternativa, per inviare i pacchetti attraverso un tunnel è possibile utilizzare un indirizzo IP compreso tra 0.0.0.1 e 255.255.255.254 è possibile inviare pacchetti in un tunnel.	
Tipo	Visualizzazione del tipo di l'indirizzo di origine e di destinazione (possibili opzioni: host, sottorete, intervallo di indirizzi IP e nome DNS).
Indirizzo (l'ultimo dell'intervallo)	Visualizzazione dell'indirizzo di origine e di destinazione nel formato corrispondente al tipo selezionato. La maschera di immissione dipende dal tipo di indirizzo selezionato. Se è possibile utilizzare qualsiasi indirizzo IP, viene visualizzato 0.0.0.0. Se come indirizzo di destinazione per l'invio di pacchetti in un tunnel viene inserito 0.0.0.0, è necessario disattivare l'interfaccia per la rete di destinazione NAT. In alternativa, per inviare i pacchetti attraverso un tunnel è possibile utilizzare un indirizzo IP compreso tra 0.0.0.1 e 255.255.255.254 è possibile inviare pacchetti in un tunnel.
Maschera sub-rete / primo indirizzo dell'intervallo	Viene impostato nel caso in cui sia necessario configurare un intervallo di indirizzi di origine/destinazione per la trasmissione
Indirizzo di destinazione	
Tipo	Visualizzazione del tipo di l'indirizzo di origine e di destinazione (possibili opzioni: host, sottorete, intervallo di indirizzi IP e nome DNS).

Parametri	Descrizione
Indirizzo (l'ultimo dell'intervallo)	Visualizzazione dell'indirizzo di origine e di destinazione nel formato corrispondente al tipo selezionato. La maschera di immissione dipende dal tipo di indirizzo selezionato. Se è possibile utilizzare qualsiasi indirizzo IP, viene visualizzato 0.0.0.0. Se come indirizzo di destinazione per l'invio di pacchetti in un tunnel viene inserito 0.0.0.0, è necessario disattivare l'interfaccia per la rete di destinazione NAT. In alternativa, per inviare i pacchetti attraverso un tunnel è possibile utilizzare un indirizzo IP compreso tra 0.0.0.1 e 255.255.255.254 è possibile inviare pacchetti in un tunnel.
Maschera sub-rete / primo indirizzo dell'intervallo	Viene impostato nel caso in cui sia necessario configurare un intervallo di indirizzi di origine/destinazione per la trasmissione
Dati del servizio Visualizzazione del servizio sul quale la crittografia viene limitata. Se la crittografia non deve essere limitata a un servizio, selezionare "Servizio qualsiasi".	
Nome del servizio	Campo di input per il nome del servizio da configurare.
Porta di origine	Visualizzazione del tunnel nella direzione di ricezione per la quale si applica questa regola. Da questo tunnel vengono recuperati i pacchetti IP ricevuti dalla rete. Se nel fascio di ricezione non deve essere assegnato alcun tunnel, selezionare l'opzione Nessuna assegnazione tunnel.
Porta di destinazione	Visualizzazione del tunnel nella in direzione di invio per la quale si applica questa regola. I pacchetti IP destinati alla rete vengono istradati attraverso questo tunnel. Se nel fascio di invio non deve essere assegnato alcun tunnel, selezionare l'opzione Nessuna assegnazione tunnel.
Protocollo IP	Protocollo IP da utilizzare per la trasmissione Valori consentiti: ICMP, TCP, UDP
Nome del tunnel	Questo campo contiene il nome del nuovo tunnel configurato.
Abilita servizio remoto via VPN: (può essere attivato tramite codice servizio)	Selezionare questo campo se il tunnel VPN deve essere usato per l'amministrazione remota.
Tipo di punto terminale del tunnel locale	Selezionare il tipo di indirizzo del punto terminale per il lato di invio del tunnel (si possono immettere un nome host o un nome DNS).
Indirizzo del punto terminale del tunnel locale	Inserire l'indirizzo del mittente nel formato adattato al tipo di terminale.
Tipo di punto terminale del tunnel remoto	Tipo di indirizzo del terminale sul lato ricevente del tunnel (è supportata l'indicazione dell'indirizzo IP).
Indirizzo del punto terminale del tunnel remoto	Indirizzo del destinatario nel formato adattato al tipo di terminale. Se si imposta l'indirizzo 0.0.0.0, il punto terminale del tunnel è sconosciuto. In tal caso, la creazione del tunnel deve avvenire sempre dal lato opposto (ad es. operatore remoto).
Gestione della chiave di sessione	In Gestione della chiave di sessione viene immessa la procedura per lo scambio delle chiavi (automatica, con protocollo IKE).

Parametri	Descrizione
Algoritmi di crittografazione proposti	Quali algoritmi possono essere usati? Valori consentiti: AES, 3DES
Algoritmi Hash proposti	Quali algoritmi hash (algoritmi di verifica) devono essere utilizzati. Gli algoritmi selezionati vengono offerti dall'iniziatore della negoziazione IKE. Valori consentiti: MD5, SHA1, SHA2
Durata proposta delle chiavi di sessione	Durata validità della chiave di sessione (session key) da utilizzare. Una volta trascorso questo periodo, non sarà più possibile scambiare informazioni con questa sessione. In sostituzione di chiavi di sessione non più valide vengono negoziate automaticamente nuove chiavi di sessione
Durata proposta della sessione di scambio delle chiavi	Durata validità della sessione di scambio delle chiavi. Una volta scaduta la sessione di scambio delle chiavi, vengono negoziate automaticamente nuove chiavi per la sessione di scambio delle chiavi tramite IKE
Volumi di dati proposti delle chiavi chiavi di sessione	Volume massimo di dati per le chiavi di sessione (Session Key). Se il volume dati viene superato, vengono negoziate automaticamente nuove chiavi di sessione tramite IKE. Se si seleziona "illimitato" il volume dei dati non ha limite
Attiva 'Perfect Forward Secrecy'	Si consiglia di selezionare sempre questa opzione in quanto viene attivato un meccanismo di protezione avanzato per il trasferimento dei dati attraverso il tunnel
Metodo di autenticazione dei Peer di VPN	Metodo di autenticazione dell'utente VPN. Sono disponibili la firma digitale (autenticazione tramite certificati) e le chiavi pre-condivise (autenticazione tramite chiave manuale definita dall'utente)
Chiave precondivisa	Questo campo è disponibile solo se il metodo di autenticazione è impostato su Chiavi precondivise. Qui occorre inserire la password che deve essere usata dagli utenti VPN in entrambi i lati del tunnel. La password deve contenere almeno 12 caratteri.
Ripetizione della chiave precondivisa	Questo campo è disponibile solo se il metodo di autenticazione è impostato su Chiavi precondivise.
Elenco dei certificati CA	Queste opzioni sono disponibili solo se il metodo di autenticazione è impostato su Firma digitali. Gli utenti VPN possono utilizzare qualsiasi certificato di autenticazione rilasciato (firmato) da una delle autorità di certificazione selezionata
Gruppi Diffie Hellman proposti	Gli utenti VPN possono scambiarsi le chiavi con uno dei metodi selezionati

Nota: L'aggiunta/l'eliminazione di un tunnel VPN deve essere successivamente attivata selezionando "VPN> Attivazione delle tabelle VPN configurate".

28.3.2.18 Sicurezza > VPN > Regole > Regole attive

Descrizione dei parametri della scheda:

- **Mostra regole**

Parametri	Descrizione
Priorità	Visualizzazione della priorità per la sequenza sotto forma di cifra. La massima priorità è indicata dal numero 1. Per ogni regola di un fascio occorre assegnare una priorità separata. La regola relativa a una direzione di trasmissione e quella per la direzione opposta devono sempre avere la stessa priorità.
Servizio	Visualizzazione del servizio sul quale la crittografia viene limitata. Se la crittografia non è limitata a un servizio, viene visualizzato il messaggio "Servizio qualsiasi".
Azione per la regola	Indicazione di come i pacchetti IP devono essere gestiti secondo la regola: "pass" significa che i pacchetti IP vengono inoltrati; "deny" significa nessun pacchetto IP verrà trasmesso.
Crittografazione necessaria	Visualizzazione della crittografia. Il metodo di crittografia è definito mediante il tunnel associato.
Stato della regola	Indicatore di stato nella regola. Valori consentiti: Abilita/Disabilita
Stato nello stack IP	Visualizzazione stato nello stack IP. Valori consentiti: Abilita/Disabilita
Indirizzo di origine	
Tipo	Visualizzazione del tipo di indirizzo di origine. Valori consentiti: Host, Sub-rete, Intervallo di indirizzi IP, Nome DNS
Indirizzo (l'ultimo dell'intervallo)	Visualizzazione dell'indirizzo di origine e di destinazione nel formato corrispondente al tipo selezionato. La maschera di immissione dipende dal tipo di indirizzo selezionato. Se è possibile utilizzare qualsiasi indirizzo IP, viene visualizzato 0.0.0.0. Se come indirizzo di destinazione per l'invio di pacchetti in un tunnel viene inserito 0.0.0.0, è necessario disattivare l'interfaccia per la rete di destinazione NAT. In alternativa, per inviare i pacchetti attraverso un tunnel è possibile utilizzare un indirizzo IP compreso tra 0.0.0.1 e 255.255.255.254 è possibile inviare pacchetti in un tunnel.
Maschera sub-rete / primo indirizzo dell'intervallo	Viene impostato nel caso in cui sia necessario configurare un intervallo di indirizzi di origine/destinazione per la trasmissione
Indirizzo di destinazione	
Tipo	Visualizzazione del tipo di indirizzo di destinazione. Valori consentiti: Host, Sub-rete, Intervallo di indirizzi IP, Nome DNS
Indirizzo (il primo dell'intervallo)	
Maschera sub-rete / primo indirizzo dell'intervallo	Viene impostato nel caso in cui sia necessario configurare un intervallo di indirizzi di origine/destinazione per la trasmissione
Tunnel per la crittografazione	

Parametri	Descrizione
Tunnel lato di ricezione	Visualizzazione del tunnel nella direzione di ricezione per la quale si applica questa regola. Da questo tunnel vengono recuperati i pacchetti IP ricevuti dalla rete. Visualizzazione: nessuna assegnazione tunnel (se per la direzione di ricezione non è stato assegnato alcun tunnel).
Tunnel lato invio	Visualizzazione del tunnel nella in direzione di invio per la quale si applica questa regola. Da questo tunnel vengono recuperati i pacchetti IP ricevuti dalla rete. Visualizzazione: nessuna assegnazione tunnel (se per la direzione di invio non è stato assegnato alcun tunnel).

28.3.2.19 Sicurezza > VPN > Regole > Regole configurate

Le regole definiscono cosa accade a un pacchetto IP. L'azione regola Pass significa che il pacchetto IP continua ad essere trasportato. L'azione regola DENY significa che il pacchetto IP non viene più trasportato. È inoltre possibile scegliere se il pacchetto IP deve utilizzare un tunnel VPN (crittografato) o meno. Il sistema di comunicazione è in grado di gestire 640 regole, tra cui 6 regole predefinite e 634 liberamente assegnabili.

Descrizione dei parametri delle schede:

- **Mostra regole**
- **Aggiungi regola**
- **Modifica regola**
- **Aggiungi regola per direzione opposta**
- **Cancella regola**

Parametri	Descrizione
Priorità	Visualizzazione della priorità per la sequenza sotto forma di cifra. La massima priorità è indicata dal numero 1. Per ogni regola di un fascio occorre assegnare una priorità separata. La regola relativa a una direzione di trasmissione e quella per la direzione opposta devono sempre avere la stessa priorità.
Servizio	Visualizzazione del servizio sul quale la crittografia viene limitata. Se la crittografia non è limitata a un servizio, viene visualizzato il messaggio "Servizio qualsiasi".
Azione per la regola	Indicazione di come i pacchetti IP devono essere gestiti secondo la regola: "pass" significa che i pacchetti IP vengono inoltrati; "deny" significa nessun pacchetto IP verrà trasmesso.
Crittografazione necessaria	Visualizzazione della crittografia. Il metodo di crittografia è definito mediante il tunnel associato.
Stato della regola	Indicatore di stato nella regola. Valori consentiti: attivato/disattivato
Stato nello stack IP	Visualizzazione stato nello stack IP. Valori consentiti: Abilita/Disabilita
Indirizzo di origine	

Parametri	Descrizione
Tipo	Visualizzazione del tipo di indirizzo di origine. Valori consentiti: Host, Sub-rete, Intervallo di indirizzi IP, Nome DNS
Indirizzo (l'ultimo dell'intervallo)	Visualizzazione dell'indirizzo di origine e di destinazione nel formato corrispondente al tipo selezionato. La maschera di immissione dipende dal tipo di indirizzo selezionato. Se è possibile utilizzare qualsiasi indirizzo IP, viene visualizzato 0.0.0.0. Se come indirizzo di destinazione per l'invio di pacchetti in un tunnel viene inserito 0.0.0.0, è necessario disattivare l'interfaccia per la rete di destinazione NAT. In alternativa, per inviare i pacchetti attraverso un tunnel è possibile utilizzare un indirizzo IP compreso tra 0.0.0.1 e 255.255.255.254 è possibile inviare pacchetti in un tunnel.
Maschera sub-rete / primo indirizzo dell'intervallo	Viene impostato nel caso in cui sia necessario configurare un intervallo di indirizzi di origine/destinazione per la trasmissione
Indirizzo di destinazione	
Tipo	Visualizzazione del tipo di indirizzo di destinazione. Valori consentiti: Host, Sub-rete, Intervallo di indirizzi IP, Nome DNS
Indirizzo (il primo dell'intervallo)	
Maschera sub-rete / primo indirizzo dell'intervallo	Viene impostato nel caso in cui sia necessario configurare un intervallo di indirizzi di origine/destinazione per la trasmissione
Tunnel per la crittografazione	
Tunnel lato di ricezione	Visualizzazione del tunnel nella direzione di ricezione per la quale si applica questa regola. Da questo tunnel vengono recuperati i pacchetti IP ricevuti dalla rete. Visualizzazione: nessuna assegnazione tunnel (se per la direzione di ricezione non è stato assegnato alcun tunnel).
Tunnel lato invio	Visualizzazione del tunnel nella in direzione di invio per la quale si applica questa regola. Da questo tunnel vengono recuperati i pacchetti IP ricevuti dalla rete. Visualizzazione: nessuna assegnazione tunnel (se per la direzione di invio non è stato assegnato alcun tunnel).

28.3.2.20 Sicurezza > VPN > Public Key Infrastructure (PKI)

Il server PKI si riferisce a un server in grado di rilasciare, distribuire e verificare i certificati digitali. I certificati emessi nell'ambito di una PKI (Public Key Infrastructure)vengono utilizzati per la protezione delle comunicazioni. Quando si utilizzano certificati (firme digitali), viene eseguito un tentativo di scaricare il CRL tramite l'URL PKI configurato nel server PKI.

Descrizione dei parametri delle schede:

- **Mostra server PKI**
- **Aggiungi server PKI**

Parametri	Descrizione
Nome del server PKI	Inserire un nome facilmente riconoscibile per il server.

Parametri	Descrizione
Tipo di server PKI	Selezionare l'attività dal server (le opzioni possibili sono LDAP e Registrazione).
URL del server PKI	Inserire l'URL del server (ad esempio: LDAP://139.21.92.144:389).

28.3.2.21 Sicurezza > SSL > Creazione certificati

L'accesso amministrazione è crittografato e utilizza HTTPS e il protocollo TLS 1.2. I certificati consentono di autentificare la connessione. Per impostazione predefinita, viene utilizzato un certificato autofirmato. Per aumentare la sicurezza, è possibile utilizzare un certificato specifico del cliente rilasciato da un'autorità di certificazione (CA). Il sistema di comunicazione si autentica rispetto al client Admin con il supporto di certificati generati o importati da WBM. Nel browser questi certificati possono essere importati come attendibili, per evitare che vengano visualizzati avvisi del browser nelle connessioni al server SSL.

Descrizione dei parametri delle schede:

- **Crea certificato CA**
- **Crea certificato autofirmato**

Parametri	Descrizione
Nome del certificato	Nome del certificato da generare.
Numero di serie del certificato	Numero di serie per il certificato. Il numero deve essere un numero intero positivo
Tipo di algoritmo della firma	Algoritmo di firma da utilizzare Valori consentiti: sha256RSA, sha512RSA
Lunghezza della chiave pubblica	Valori consentiti, valore predefinito: 2048
Inizio della validità del certificato (GMT) Indicazione della data di inizio validità del certificato. La data viene intesa come ora di Greenwich (GMT).	
Giorno, Mese, Anno, Ora, Min, Sec.	Unità di tempo per il periodo di validità del certificato
Fine della validità del certificato (GMT) Indicazione della data di fine validità del certificato. La data viene intesa come ora di Greenwich (GMT)	
Giorno, Mese, Anno, Ora, Min, Sec.	Unità di tempo per il periodo di validità del certificato
Richiedente Dati del richiedente del certificato secondo le convenzioni previste dallo standard X.509 (ad esempio, campo Paese (C) DE per Germania). Tutti e quattro i campi sono obbligatori.	
Paese (C)	Codice paese a due cifre
Organizzazione (O)	Il nome legale completo dell'azienda

Parametri	Descrizione
Unità organizzativa (OU)	L'unità organizzativa è la succursale dell'azienda che sta ordinando il certificato
Nome generale (CN)	Nome di dominio completo (FQDN)
Richiedente alternativo Questa informazione opzionale effettua una distinzione tra il formato del nome DN (come i dati del richiedente) e qualsiasi altro formato (ad esempio un indirizzo IP). La maschera di immissione dipende dal formato selezionato. Se si seleziona un altro formato, è possibile configurare più di una voce SAN.	
Formato del nome di DN	Di solito viene fornito anche come Nome Generale RDN all'interno del campo Oggetto del certificato principale
Altro formato	Altri nomi, forniti come nomi generici
Estensione del nome alternativo del richiedente	(opzionale) Valori consentiti, valore predefinito: nome DNS, indirizzo IP, indirizzo di posta elettronica, Uniform Resource Indicator, altro
Nome alternativo del richiedente	
Tipo punto di distribuzione CRL	Valori consentiti: nome DNS, indirizzo IP, indirizzo di posta elettronica, Uniform Resource Indicator, altro
Punto di distribuzione del CRL	Qui è possibile indicare il punto (opzionale con un URL) da cui possono essere distribuiti gli elenchi di revoche dei certificati (CRL)

28.3.2.22 Sicurezza > SSL > Gestione certificati

Descrizione dei parametri della scheda:

- **Mostra certificato da file**

Parametri	Descrizione
Formato PKCS#12	Se il certificato è salvato in un file PKCS#12, questo campo deve essere attivato.
Password di decrittografia	Se è stato selezionato il campo Formato PKCS#12, è necessario inserire in questo campo la stessa password utilizzata per la creazione del file.
File con il certificato	Immissione del percorso e del nome file del certificato. Se necessario, fare clic su Sfoglia per definire la posizione di memorizzazione.

28.3.2.23 Sicurezza > SSL > Gestione certificati > Certificati server

Descrizione dei parametri delle schede:

- **Crea richiesta del certificato (CSR)**
- **Importa certificato server (PKCS#12)**
- **Mostra certificato**
- **Cancella certificato**
- **Esporta certificato (X.509)**
- **Importa certificato prorogato (X.509)**

- **Attiva certificato**

Parametri	Descrizione
Nome della richiesta del certificato	Nome del certificato da generare.
Tipo di algoritmo della firma	Algoritmo della firma da utilizzare per questo certificato Valori consentiti: sha256RSA, sha512RSA
Lunghezza della chiave pubblica	Valori consentiti: 2048
Richiedente Dati del richiedente del certificato secondo le convenzioni previste dallo standard X.509 (ad esempio, campo Paese (C) DE per Germania). Tutti e quattro i campi sono obbligatori.	
Paese (C)	Codice paese a due cifre
Organizzazione (O)	Il nome legale completo dell'azienda
Unità organizzativa (OU)	L'unità organizzativa è la succursale dell'azienda che sta ordinando il certificato
Nome generale (CN)	Nome di dominio completo (FQDN)
Richiedente alternativo Questa informazione opzionale effettua una distinzione tra il formato del nome DN (come i dati del richiedente) e qualsiasi altro formato (ad esempio un indirizzo IP). La maschera di immissione dipende dal formato selezionato. Se si seleziona un altro formato, è possibile configurare più di una voce SAN.	
Formato del nome di DN	Di solito viene fornito anche come Nome Generale RDN all'interno del campo Oggetto del certificato principale
Altro formato	Altri nomi, forniti come nomi generici
Estensione del nome alternativo del richiedente	(opzionale) Valori consentiti, valore predefinito: nome DNS, indirizzo IP, indirizzo di posta elettronica, Uniform Resource Indicator, altro
Nome alternativo del richiedente	(opzionale)
Nome del certificato	Nome del certificato da importare.
Password di decrittografia	Password utilizzata per la creazione di file. Valori consentiti: da 7 a 32 caratteri
File con il certificato	Nel campo **File con il certificato** il può essere inserito il certificato o è possibile selezionarlo tramite il campo Sfoglia. L'**Impronta digitale** del certificato deve essere visualizzata prima che questo possa essere importato.

28.3.2.24 Sicurezza > Sicurezza Web

Descrizione dei parametri della scheda:

- **Filtro accesso Web**

Parametri	Descrizione
Client Web	Solo in combinazione con UC Suite: attivazione e disattivazione dell'accesso Web tramite cellulari e applicazioni mobili (myPortal for Mobile/Tablet, myPortal to go, Application Launcher e applicazioni di terzi tramite Web Service) Info: uso di client Web unitamente a UC Smart tramite Modalità esperti > Applicazioni > UC Smart > Impostazioni di base
Accesso tramite HTTPS	Sono consentite solo connessioni crittografate.
Accesso tramite HTTP	Sono consentite connessioni non crittografate.
Salvare i dati di accesso nel terminale	Se la funzione è abilitata, non devono essere inseriti i dati di accesso all'avvio dell'applicazione

28.3.2.25 Sicurezza > Sicurezza SQL

Descrizione dei parametri della scheda:

- **Password di accesso SQL**

Parametri	Descrizione
Genera nuova	Viene generata una password SQL crittografata, non nota all’utente.
Attiva predefinita	La password SQL predefinita è attivata.

28.3.3 Interfacce di rete

In **Interfaccia di rete** sono riunite funzioni quali ad esempio la configurazione delle interfacce singole LAN. Le interfacce possono essere configurate in modo indipendente l'una dall'altra.

28.3.3.1 Interfacce di rete > Scheda madre > Nome host

Descrizione dei parametri delle schede:

- **Modifica nome host**

Parametri	Descrizione
Nome dell'host	Nome host del sistema di comunicazione - liberamente scelto. Esempio: `commsystem` Se il nome e l'indirizzo IP sistema di comunicazione sono memorizzati in un server DNS, i nomi possono essere risolti. Il nome del sistema di comunicazione è costituito dal nome host e dal nome di dominio. Esempio: `commsystem.mynet.home`

28.3.3.2 Interfacce di rete > Scheda madre > LAN 1 (WAN)

Descrizione dei parametri delle schede:

- **Mostra modalità LAN 1**
- **Modifica interfaccia LAN 1**
- **Modifica ACD**

Parametri	Descrizione
Selezione del provider di servizi Internet	Selezione che determina il modo in cui avviene l'accesso a un ISP (provider di servizi Internet) tramite l'interfaccia WAN.
Selezione del provider di servizi Internet: non configurata o disabilitata	L'interfaccia WAN non viene utilizzata.
Selezione del provider di servizi Internet: Tipo di connessione LAN TCP/IP	L'interfaccia WAN viene utilizzata per l'accesso a un ISP, che è già configurato in un router Internet esterno. Non è necessario che il sistema di comunicazione e il router Internet si trovino sullo stesso segmento LAN, ma l'interfaccia WAN deve essere collegata al segmento LAN del router Internet.
Selezione del provider di servizi Internet: T-Online, T-DSL Business, …	Il sistema di comunicazione funziona come un router Internet. L'interfaccia WAN è utilizzata per accedere a un ISP preconfigurato.
Selezione del provider di servizi Internet: PPPoE provider	Il sistema di comunicazione funziona come un router Internet. L'interfaccia WAN è utilizzata per l'accesso a un ISP tramite PPPoE. PPPoE è il protocollo più comunemente utilizzato dai modem DSL.
Selezione del provider di servizi Internet: PPTP provider	Il sistema di comunicazione funziona come un router Internet. L'interfaccia WAN è utilizzata per l'accesso a un ISP tramite PPTP. Questa variante è comune, ad esempio, in Austria.
Accesso a Internet tramite un router esterno	L'accesso a Internet avviene tramite un router esterno. Questo contrassegno è utilizzato internamente dalla procedura guidata **Configurazione di Internet** e non deve essere modificato.
Configurazione automatica dell'indirizzo (tramite DHCP)	Un server DHCP esterno (eventualmente il server DHCP del router Internet) assegna un indirizzo IP al sistema di comunicazione.
Accetta l'indirizzo IP del router predefinito	Il server DHCP esterno comunica l'indirizzo IP del router predefinito (ad esempio, il router Internet) al sistema di comunicazione.
Accetta indirizzo IP del server DNS	Il server DHCP esterno comunica l'indirizzo IP del server DNS al sistema di comunicazione.
Accetta indirizzo IP del server SNTP	Il server DHCP esterno comunica l'indirizzo IP del server SNTP al sistema di comunicazione.
Indirizzo IP	Indirizzo IP dell'interfaccia LAN.
Maschera di sottorete:	Netmask del segmento LAN.
Indirizzo MAC	Visualizza l'indirizzo MAC dell'interfaccia LAN.
Modalità di collegamento Ethernet	Modalità interfaccia WAN.

Parametri	Descrizione
Modalità di collegamento Ethernet: Auto	Commutazione automatica tra la modalità full duplex a 100 e 1000 Mbps.
Modalità di collegamento Ethernet: 100HDX	100 Mbps, full duplex.
Modalità di collegamento Ethernet: 100FDX	100 Mbps, full duplex.
Modalità di collegamento Ethernet: 1000FDX	1000 Mbps, full duplex.
NAT	Il NAT (Network Address Translation) è attivato. Di solito questa attività è già assunta dal router esterno.
Controllo della larghezza di banda per le connessioni vocali	Questo campo consente il controllo della larghezza di banda per le connessioni vocali.
Larghezza di banda per download	Valore della larghezza di banda complessiva in kbit/sec. per il download dall'ISP.
Larghezza di banda per upload	Valore della larghezza di banda complessiva in kbps per il caricamento fornito dall'ISP.
Larghezza di banda utilizzata per voce/fax (%)	Percentuale di larghezza di banda disponibile per le connessioni voce/fax. Intervallo di valori, valore predefinito: 0 - 100, 80
Tagging IEEE802.1p/q	Se questa casella di controllo è selezionata, nei pacchetti Ethernet (Layer 2) viene incluso un "tipo di servizio" ai fini della prioritizzazione L'opzione è disattivata per impostazione predefinita.
ID VLAN IEEE802.1p/q	Inserire il numero ID della VLAN se lo switch utilizzato ha problemi con il valore predefinito "0".
Classe QoS di livello 2	
Dati di segnalazione	Classe di priorità per la configurazione della connessione. 0 = priorità minima / 7 = priorità massima. Intervallo di valori, valore predefinito: 0 - 7, 3
Carico utile fax/modem	Classe di priorità per i dati fax e modem della connessione IP. 0 = priorità minima / 7 = priorità massima. Intervallo di valori, valore predefinito: 0 - 7, 5
Controllo della rete	Classe di priorità per i dati di controllo della rete (trasferimento di trap SNMP, ad esempio). 0 = priorità minima / 7 = priorità massima. Intervallo di valori, valore predefinito: 0 - 7, 0
Carico utile vocale	Classe di priorità per i dati vocali della connessione IP. 0 = priorità minima / 7 = priorità massima. Intervallo di valori, valore predefinito: 0 - 7, 5
Dati di accesso a Internet per ...	

Parametri	Descrizione
ID connessione / Nome utente / Numero T-Online / Numero utente secondario/ Suffisso/ Account di accesso a Internet / Accesso con DSL ...	Dati di accesso del provider di servizi Internet.
Password CHAP	Password per l'accesso al provider di servizi Internet.
Reinserisci la password	Password per l'accesso al provider di servizi Internet.
Parametri IP	
Indirizzo IP partner della connessione PPP	Indirizzo IP del server ISP, se l'ISP utilizza un indirizzo IP statico.
Indirizzo IP locale della connessione PPP	Indirizzo IP comunicato dall'ISP per l'accesso a Internet.
Negoziazione dell'indirizzo IP	Selezione per determinare il modo in cui i partner della connessione devono negoziare l'indirizzo IP durante la configurazione della connessione.
Negoziazione dell'indirizzo IP: indirizzo IP configurato	È possibile utilizzare solo l'indirizzo IP configurato.
Negoziazione dell'indirizzo IP: accetta qualsiasi indirizzo IP	È accettato qualsiasi indirizzo proposto dal partner.
Negoziazione dell'indirizzo IP: richiedi nuovo indirizzo IP	A ogni connessione viene richiesto un nuovo indirizzo IP.
Richiesta DNS	
Accesso a Internet con richiesta DNS	Il server DNS viene determinato automaticamente.
Indirizzo IP del server DNS primario	Viene selezionato un server DNS speciale.
Parametri PPP generali	
Router predefinito	La connessione PPP creata qui viene utilizzata come destinazione di routing.
Compressione intestazione IP	L'intestazione TCP è compressa. Le intestazioni UDP e RTP sono sempre compresse.
Invio di una richiesta di eco LCP	Viene inviata una richiesta di eco LCP. Questa funzione serve a verificare se la connessione è ancora attiva.
Riconnessione PPP automatica	La connessione PPP viene ristabilita automaticamente dopo una disconnessione (ad esempio, nel caso di un accesso ISP con tariffa fissa e disconnessione forzata dopo 24 ore).
Parametro PPTP	

Parametri	Descrizione
Indirizzo IP locale della connessione di controllo	Indirizzo IP per la connessione PPTP, assegnato dall'ISP.
Indirizzo IP remoto della connessione di controllo	Indirizzo IP del proprio server ISP per la connessione PPTP.
Maschera di sottorete remota per la connessione di controllo	Maschera di sottorete per la connessione PPTP, assegnata dall'ISP.
Mantenimento breve	
Mantenimento breve	Per la connessione PPP è attiva la modalità di funzionamento "mantenimento breve". La voce seguente è possibile solo quando è abilitata la modalità di mantenimento breve.
Tempo di mantenimento breve (sec)	Tempo di assenza di trasmissioni di dati dopo il quale la connessione PPP deve essere annullata. Il timer di mantenimento breve viene attivato solo dai pacchetti in uscita. Intervallo di valori, valore predefinito: 10 - 9999, 60
Autenticazione	
Autenticazione PPP	È abilitata l'autenticazione di base. L'impostazione deve essere effettuata in base alle specifiche dell'ISP.
Nome d'utente PPP	Nome utente liberamente selezionabile da utilizzare per l'autenticazione tramite PAP o CHAP.
Modalità di autenticazione PAP	Attivazione e tipo di autenticazione PAP per la connessione PPP: Non utilizzato, client PAP, host PAP.
Password PAP	Password per l'autenticazione PAP.
Modalità di autenticazione CHAP	Attivazione e tipo di autenticazione CHAP per la connessione PPP: Non utilizzato, client CHAP, host CHAP, client e host CHAP.
Password CHAP	Password per l'autenticazione CHAP.
Compressione dei dati	
Compressione dei dati DEFLATE	Per la compressione dei pacchetti di dati PPP con l'algoritmo di compressione DEFLATE.
Compressione dei dati COMPRESS	Per la compressione dei pacchetti di dati PPP con l'algoritmo di compressione COMPRESS.
Traduzione degli indirizzi	
NAT	Il NAT (Network Address Translation) è attivato. Sono supportati i seguenti protocolli: TCP, UDP e ICMP (solo in modalità passiva).
Mappatura degli indirizzi	verrà abbandonata.
Impostazioni degli instradamenti	

Parametri	Descrizione
Circuito Full-Time	A seconda del modello di tariffa, il circuito full-time (connessione permanente) all'ISP può essere abilitato o disabilitato. Il circuito full-time deve essere disabilitato per un modello di tariffa a tempo e abilitato per un modello di tariffa fisso.
Tempo di mantenimento breve (sec)	Se il Circuito Full-Time è disabilitato (modello di tariffa a tempo), immettere la durata dell'inattività trascorsa la quale viene interrotta la connessione Internet (ad es. 60 secondi). Intervallo di valori, valore predefinito: 10 - 9999, 60
Disconnessione forzata alle (ora:min)	Se il Circuito Full-Time è disabilitato (modello di tariffa fisso), inserire l'ora in cui la connessione a Internet deve essere disattivata (ad esempio, 04:59).
Tempo di connessione	Visualizza il tempo di connessione trascorso in giorni-ore-minuti-secondi.
Parametri QoS dell'interfaccia	
Larghezza di banda per download	Valore della larghezza di banda complessiva in kbit/sec. per il download dall'ISP.
Larghezza di banda per upload	Valore della larghezza di banda complessiva in kbps per il caricamento fornito dall'ISP.
Controllo della larghezza di banda per le connessioni vocali	Il controllo della larghezza di banda impedisce che le velocità di trasmissione disponibili siano sovraccaricate dalle connessioni vocali all'interno di una connessione multilink. In altre parole, quando la compressione dell'intestazione è attiva, su un canale B sono consentite al massimo 5 connessioni vocali. Questo campo consente il controllo della larghezza di banda per le connessioni vocali. Vengono prese in considerazione solo le connessioni vocali con percorsi configurati nel gateway vocale.
Larghezza di banda utilizzata per voce/fax (%)	Percentuale di larghezza di banda disponibile per le connessioni voce/fax. Intervallo di valori, valore predefinito: 0 - 100, 80

Descrizione dei parametri delle schede:

- **Modifica ACD**

Parametri	Descrizione
Tempo di connessione	Visualizza il tempo di connessione trascorso in giorni-ore-minuti-secondi.
Forza la riconnessione alle	Ora in cui la connessione deve essere cancellata e ristabilita.
Abilita ACD	Abilitare il cleardown automatico per evitare la disconnessione da parte dell'ISP in un momento inopportuno.

28.3.3.3 Interfacce di rete > Scheda madre > LAN 2

Descrizione dei parametri delle schede:

- **Modifica interfaccia LAN 2**

Parametri	Descrizione
Accesso a Internet tramite router esterno	L'accesso a Internet avviene tramite un router esterno.
Interfaccia attivata	L'interfaccia LAN è attivata.
indirizzo IP	Indirizzo IP del sistema di comunicazione.
Maschera di rete:	Maschera di rete del segmento LAN su cui si trova il sistema di comunicazione.
Indirizzo MAC	Visualizzazione dell'indirizzo MAC del sistema di comunicazione.
Modalità collegamento Ethernet	Modo dell'interfaccia LAN.
Modalità collegamento Ethernet: Auto	Commutazione automatica fra 100 e 1000 Mbit/sec., nonché fra funzionamento half-duplex e full-duplex. In questo Modo è possibile attivare la funzione Risparmio energia. Dopo la migrazione a V2R3 o versione successiva, premere Applica in primo piano per il collegamento ethernet desiderato nella pagina di interfaccia di rete in modo da impostare il valore su Auto. In alternativa, i sistemi devono essere impostati su Auto o 100 prima della migrazione.
Modalità collegamento Ethernet: 100HDX	100 MBit/sec., half-duplex. In questo Modo non è possibile attivare la funzione Risparmio energia.
Modalità collegamento Ethernet: 100FDX	100 Mbit/sec., full-duplex. In questo Modo non è possibile attivare la funzione Risparmio energia.
Modalità collegamento Ethernet: 1000FDX	1000 Mbit/sec., full-duplex. In questo Modo non è possibile attivare la funzione Risparmio energia.
IEEE802.1p/q-Tagging	Se questa casella di controllo è selezionata, nei pacchetti Ethernet (Layer 2) viene indicato un "Type of service" per la definizione della priorità. Per impostazione predefinita, questa opzione è disattivata.
IEEE802.1p/q-VLAN-ID	Occorre specificare il numero ID della VLAN solo se l'interruttore usato ha problemi con il valore predefinito "0".
Livello classe QoS 2	
Dati di segnalazione	Classe di priorità per stabilire una connessione. 0 = priorità inferiore / 7= priorità superiore. Valori consentiti, valore predefinito: 0-7, 3
Payload fax/modem	Classe di priorità per dati fax e modem della connessione IP. 0 = priorità inferiore / 7= priorità superiore. Valori consentiti, valore predefinito: 0-7, 5
Controllo della rete	Classe di priorità per i dati del controllo di rete (ad esempio, la trasmissione di trap SNMP). 0 = priorità inferiore / 7= priorità superiore. Valori consentiti, valore predefinito: 0-7, 0

Parametri	Descrizione
Payload voce	Classe di priorità per dati voce. 0 = priorità inferiore / 7= priorità superiore. Valori consentiti, valore predefinito: 0-7, 5

28.3.3.4 Interfacce di rete > Scheda madre > LAN 3 (Admin)

Descrizione dei parametri delle schede:

- **Modifica interfaccia LAN 3**

Parametri	Descrizione
Interfaccia attivata	L'interfaccia LAN è attivata.
Configurazione automatica indirizzo (via DHCP)	Un server DHCP esterno assegna al sistema di comunicazione un indirizzo IP.
Accetta indirizzo IP del router predefinito	Il server DHCP esterno trasmette al sistema di comunicazione l'indirizzo IP del router predefinito (ad esempio, il router Internet).
Accetta indirizzo IP dei server DNS	Il server DHCP esterno trasmette al sistema di comunicazione l'indirizzo IP del server DNS.
Accetta indirizzo IP dei server SNTP	Il server DHCP esterno trasmette al sistema di comunicazione l'indirizzo IP del server SNTP.
indirizzo IP	Indirizzo IP dell'interfaccia LAN.
Maschera di rete:	Maschera di rete del segmento LAN.
Indirizzo MAC	Visualizzazione dell'indirizzo MAC dell'interfaccia LAN.
Modalità collegamento Ethernet	Modo dell'interfaccia LAN.
Modalità collegamento Ethernet: Auto	Commutazione automatica fra 100 e 1000 Mbit/sec., nonché fra funzionamento half-duplex e full-duplex.
Modalità collegamento Ethernet: 100HDX	100 MBit/sec., half-duplex.
Modalità collegamento Ethernet: 100FDX	100 Mbit/sec., full-duplex.
Modalità collegamento Ethernet: 1000FDX	1000 Mbit/sec., full-duplex.

28.3.3.5 Interfacce di rete > Scheda madre > Server FTP

Descrizione dei parametri delle schede:

- **Modifica i parametri del server FTP**

Parametri	Descrizione
Attiva server FTP	Se questa casella di controllo è selezionata, il server FTP interno è abilitato.
Utente download "Phone"	
Servizio	Nome per l'accesso dei telefoni IP al server FTP per il download degli aggiornamenti software più recenti. Il nome non può essere modificato
Nuova password	Password per l'accesso dei telefoni IP al server FTP. Se viene modificata la password predefinita, occorre modificarla anche nei telefoni IP.
Conferma password	Password per l'accesso dei telefoni IP al server FTP.
Utente download "FTP_Admin"	
Servizio	Nome per l'accesso dell'amministratore al server FTP. Il nome non può essere modificato
Nuova password	Password per l'accesso dell'amministratore al server FTP.
Conferma password	Password per l'accesso dell'amministratore al server FTP.

28.3.3.6 Interfacce di rete > Scheda madre > Modo DHCP

Descrizione dei parametri delle schede:

- **Modifica modo DHCP**

Parametri	Descrizione
Nessun DHCP	Se il pulsante di opzione è selezionato, il server DHCP interno è disabilitato.
Server DHCP	Se il pulsante di opzione è selezionato, il server DHCP interno è abilitato.
Agente di inoltro DHCP	Se il pulsante di opzione è selezionato, il sistema di comunicazione funge da agente di inoltro DHCP. Le interrogazioni DHCP degli utenti IP vengono in seguito inoltrate dal sistema di comunicazione al server DHCP effettivo. Il server DHCP e gli utenti IP non devono risiedere nello stesso segmento di rete.

28.3.3.7 Interfacce di rete > Scheda madre > Modalità DHCP > Server DHCP > Parametri globali

I dati specifici della rete vengono trasmessi dal server DHCP alle stazioni IP.

Descrizione dei parametri delle schede:

- **Modifica parametri globali**

Parametri	Descrizione
Abilita server DHCP	Indica che il server DHCP interno è abilitato e che i suoi parametri globali possono essere configurati. Non può essere modificato.

Parametri	Descrizione
Solo dispositivi Mitel/Unify	Indica che il server DHCP interno accetta richieste solo da dispositivi telefonici Mitel e Unify. Se il client riceve più risposte, ad esempio dal server DHCP di OpenScape Business e da un altro server della rete, preferirà la risposta ricevuta da OpenScape Business, se utilizza dispositivi compatibili: • OpenScape DeskPhone CP x00 con versione software V1R8.4.0 (HFA) / V1R11.6.0 (SIP) o superiore • OpenScape DeskPhone CP x10 con versione software V2R0.18.0 (HFA o SIP) o superiore • Mitel MiVoice 69xx/68xx (SIP)
Maschera di sottorete:	La maschera di sottorete definisce la dimensione della sottorete. Esempio: `255.255.255.0`.
Indirizzo di trasmissione	Con l'indirizzo broadcast, tutte le stazioni IP di una rete o sottorete possono essere indirizzate dal server DHCP (opzionale). Esempio: `0.0.0.0`.
Gateway predefinito	
Gateway 1	Indirizzo IP al quale è possibile raggiungere il gateway predefinito. Se nella rete viene utilizzato un router Internet, il router Internet è il gateway predefinito. Esempio: `192.168.1.1`. Se il sistema di comunicazione è collegato direttamente a un modem Internet, il sistema di comunicazione è il gateway predefinito. Esempio: `192.168.1.2`.
Gateway 2	Indirizzo IP al quale è possibile raggiungere un secondo gateway predefinito (router) (opzionale).
Gateway 3	Indirizzo IP al quale è possibile raggiungere un terzo gateway predefinito (router) (opzionale).
Server DNS	
Nome del dominio	Nome di dominio della rete interna, max. 80 caratteri, ad esempio `mynet.home` (opzionale).
Server 1	Indirizzo IP al quale è possibile raggiungere il server DNS. Se il sistema di comunicazione è collegato direttamente a un modem Internet, il valore predefinito `0.0.0.0` non deve essere cambiato. Il sistema di comunicazione lo utilizza per collegarsi automaticamente a un server DNS da Internet. È possibile inserire anche un server DNS esterno. Esempio: il server DNS del router Internet (`192.168.1.1)` o un server DNS da Internet (`google-public-dns-a.google.com`).
Server 2	Indirizzo IP al quale è possibile raggiungere un secondo server DND (opzionale).
Server 3	Indirizzo IP al quale è possibile raggiungere un terzo server DND (opzionale).
Tempo del lease in ore (0 infinito)	Periodo massimo di validità in ore, 0 = durata infinita (valore predefinito: 1 ora).

Parametri	Descrizione
Abilita aggiornamento DNS dinamico	Se questa casella di controllo è attivata, il server DNS può essere aggiornato dinamicamente. Impostazione predefinita: non abilitata. **Nota:** Se l'opzione Aggiornamento DNS dinamico è abilitata, è obbligatorio configurare il **Nome di dominio** nel campo Nome di dominio del pool di indirizzi IP.
Usa DLI interno	Se questa casella di controllo è selezionata, viene utilizzato il DLI interno. Se la casella di controllo è deselezionata, vengono visualizzati i parametri di un server DLS esterno. Impostazione predefinita: abilitata.
Server DLS esterno	
Indirizzo IP	Indirizzo IP al quale è possibile raggiungere il server DLS esterno.
Porta	Porta attraverso la quale è possibile raggiungere il server DLS esterno.

28.3.3.8 Interfacce di rete > Scheda madre > Modalità DHCP > Server DHCP > Pool di indirizzi IP

Descrizione dei parametri delle schede:

- **Visualizza pool di indirizzi IP**
- **Aggiungi pool di indirizzi IP**
- **Modifica pool di indirizzi IP**
- **Elimina pool di indirizzi IP**

Parametri	Descrizione
Indirizzo di sottorete	L'indirizzo di sottorete definisce l'intervallo massimo di indirizzi IP. Esempio: `192.168.1.0`.
Maschera di sottorete:	La maschera di sottorete definisce la dimensione della sottorete. Valore standard: `255.255.255.0`.
intervallo indirizzi	
Intervallo indirizzi 1	Limiti inferiore e superiore dell'intervallo di indirizzi IP della sottorete. Esempio: da `192.168.1.50` a `192.168.1.254`.
Intervallo indirizzi 2	Limiti inferiore e superiore di un secondo intervallo di indirizzi IP all'interno della stessa sottorete (opzionale).
Intervallo indirizzi 3	Limiti inferiore e superiore di un terzo intervallo di indirizzi IP all'interno della stessa sottorete (opzionale).
Gateway predefinito	

Parametri	Descrizione
Gateway 1	Indirizzo IP al quale è possibile raggiungere il gateway predefinito. Se nella rete viene utilizzato un router Internet, il router Internet è il gateway predefinito. Esempio: `192.168.1.1`. Se il sistema di comunicazione è collegato direttamente a un modem Internet, il sistema di comunicazione è il gateway predefinito. Esempio: `192.168.1.2`.
Gateway 2	Indirizzo IP al quale è possibile raggiungere un secondo gateway predefinito (router) (opzionale).
Gateway 3	Indirizzo IP al quale è possibile raggiungere un terzo gateway predefinito (router) (opzionale).
Indirizzo di trasmissione	Con l'indirizzo broadcast, tutte le stazioni IP di una rete o sottorete possono essere indirizzate dal server DHCP (opzionale). Valore predefinito: `0.0.0.0`.
Nome del dominio	Nome di dominio della rete interna, max. 80 caratteri, ad esempio `mynet.home` (opzionale).
Server DNS	
Server 1	Indirizzo IP al quale è possibile raggiungere il server DNS. Se il sistema di comunicazione è collegato direttamente a un modem Internet, il valore predefinito `0.0.0.0` non deve essere cambiato. Il sistema di comunicazione lo utilizza per collegarsi automaticamente a un server DNS da Internet. È possibile inserire anche un server DNS esterno. Esempio: il server DNS del router Internet (`192.168.1.1)` o un server DNS da Internet (`google-public-dns-a.google.com`).
Server 2	Indirizzo IP al quale è possibile raggiungere un secondo server DND (opzionale).
Server 3	Indirizzo IP al quale è possibile raggiungere un terzo server DND (opzionale).
Sicurezza migliorata	
Opzione relè	Un numero esadecimale configurato dall'amministratore per una maggiore sicurezza. Il valore di questo campo è vuoto per impostazione predefinita e questa opzione non verrà presa in considerazione se non è configurata.
Tempo del lease in ore (0 infinito)	Periodo massimo di validità in ore, 0 = durata infinita (valore predefinito: 1 ora).

28.3.3.9 Interfacce di rete > Scheda madre > Modalità DHCP > Server DHCP > Indirizzi IP statici

Descrizione dei parametri delle schede:

- **Visualizza indirizzo IP statico**
- **Aggiungi indirizzo IP statico**
- **Modifica indirizzo IP statico**
- **Elimina indirizzo IP statico**

Parametri	Descrizione
Nome host	Nome o descrizione della stazione IP (ad esempio, PC o server) che deve ricevere un indirizzo IP fisso. Esempio: `Server di stampa`.
Indirizzo IP	Indirizzo IP fisso desiderato. Esempio: `192.168.1.10`.
Identificatore client	Indirizzo MAC della stazione IP ex. Dispositivo Mitel SIP-DECT RFP.
Maschera di sottorete:	Netmask della sottorete. Esempio: `255.255.255.0`.
Gateway predefinito	
Gateway 1	Indirizzo IP al quale è possibile raggiungere il gateway predefinito. Se nella rete viene utilizzato un router Internet, il router Internet è il gateway predefinito. Esempio: `192.168.1.1`. Se il sistema di comunicazione è collegato direttamente a un modem Internet, il sistema di comunicazione è il gateway predefinito. Esempio: `192.168.1.2`.
Gateway predefinito 1	Indirizzo IP al quale è possibile raggiungere un secondo gateway predefinito (router) (opzionale).
Gateway predefinito 1	Indirizzo IP al quale è possibile raggiungere un terzo gateway predefinito (router) (opzionale).
Indirizzo di trasmissione	Con l'indirizzo broadcast, tutte le stazioni IP di una rete o sottorete possono essere indirizzate dal server DHCP (opzionale). Esempio: `0.0.0.0`.
Nome del dominio	Nome di dominio della rete interna, max. 80 caratteri, ad esempio `mynet.home` (opzionale).
Server DNS	
Server 1	Indirizzo IP al quale è possibile raggiungere il server DNS. Se il sistema di comunicazione è collegato direttamente a un modem Internet, il valore predefinito `0.0.0.0` non deve essere cambiato. Il sistema di comunicazione lo utilizza per collegarsi automaticamente a un server DNS da Internet. È possibile inserire anche un server DNS esterno. Esempio: il server DNS del router Internet (`192.168.1.1)` o un server DNS da Internet (`google-public-dns-a.google.com`).
Server 2	Indirizzo IP al quale è possibile raggiungere un secondo server DND (opzionale).
Server 3	Indirizzo IP al quale è possibile raggiungere un terzo server DND (opzionale).
Sicurezza migliorata	
Opzione relè	Un numero esadecimale configurato dall'amministratore per una maggiore sicurezza.
Tempo del lease in ore (0 infinito)	Periodo massimo di validità in ore, 0 = durata infinita (valore predefinito: 1 ora).

28.3.3.10 Interfacce di rete > Scheda madre > Modalità DHCP > Server DHCP > Ultimi lease attivi

L'indirizzo IP assegnato da un server DHCP rimane valido per una stazione IP fino alla scadenza del "periodo del lease", anche se la stazione IP viene spenta durante questo periodo. Qui vengono visualizzate le ultime assegnazioni attive.

Descrizione dei parametri delle schede:

- **Visualizza lease**
- **Elimina lease**

Parametri	Descrizione
Indirizzo IP	Indirizzo IP assegnato alla stazione IP dal server DHCP.
Indirizzo MAC	Indirizzo MAC della stazione IP a cui è stato assegnato un indirizzo IP.
ID client	ID client della stazione IP. Se l'ID del client non è disponibile, viene visualizzato l'indirizzo MAC della stazione IP.
Nome host	Nome o numero di chiamata della stazione IP a cui è stato assegnato un indirizzo IP.
Avvio del lease	Ora di inizio dell'assegnazione. A questo punto alla stazione IP viene assegnato un indirizzo IP.
Fine del lease	Ora di fine dell'assegnazione. Dopo questo periodo, la stazione IP deve inviare una nuova richiesta di indirizzo IP.

28.3.3.11 Interfacce di rete > Scheda madre > Modo DHCP > Server DHCP > Tutti i lease

L'indirizzo IP assegnato da un server DHCP rimane valido per un utente IP finché non scade il "Lease Time", anche se l'utente IP viene disattivato durante tale periodo. In questo spazio vengono visualizzate tutte le assegnazioni.

Descrizione dei parametri delle schede:

- **Mostra Lease**
- **Cancella Lease**

Parametri	Descrizione
indirizzo IP	Indirizzo IP dell'utente IP assegnato dal server DHCP
Indirizzo MAC	Indirizzo MAC dell'utente IP a cui è assegnato un indirizzo IP.
ID client	ID Client dell'utente IP. Se l'ID client non è disponibile, viene visualizzato l'indirizzo MAC dell'utente IP.
Nome dell'host	Nome o numero di telefono dell'utente IP a cui è stato assegnato un indirizzo IP.
Avvio del Lease	Momento di inizio dell'assegnazione. A questo punto, all'utente IP è stato assegnato un indirizzo IP.

Parametri	Descrizione
Fine del Lease	Momento finale dell'assegnazione. Successivamente, l'utente procede a una nuova interrogazione per un indirizzo IP.

28.3.3.12 Interfacce di rete > Scheda applicazioni > Nome host

Descrizione dei parametri delle schede:

- **Modifica nome host**

Parametri	Descrizione
Nome dell'host	Nome host della scheda applicazioni - liberamente scelto. Esempio: `applboard` Se il nome e l'indirizzo IP della scheda applicazioni sono memorizzati in un server DNS, i nomi possono essere risolti. Il nome della scheda applicazioni è costituito dal nome host e dal nome di dominio. Esempio: `applboard.mynet.home`

28.3.3.13 Interfaccia di rete > Scheda applicazioni > LAN 1

Descrizione dei parametri delle schede:

- **Modifica interfaccia LAN 1**

Parametri	Descrizione
Interfaccia attivata	Se questa casella di controllo è selezionata, l'interfaccia LAN 1 della scheda applicazioni è attiva.
Configurazione automatica indirizzo (via DHCP)	Se questa casella di controllo è selezionata, vengono automaticamente assegnati l'indirizzo IP e la maschera di rete dal server DHCP all'interfaccia LAN 1. Inoltre, è possibile definire se dal server DHCP devono essere trasferiti altri parametri di rete.
Accetta indirizzo IP del router predefinito	Se questa casella di controllo è selezionata, il server DHCP recupera l'indirizzo IP del router predefinito.
Accetta indirizzo IP dei server DNS	Se questa casella di controllo è selezionata, il server DHCP recupera l'indirizzo IP del server DNS.
Accetta indirizzo IP dei server SNTP	Se questa casella di controllo è selezionata, il server DHCP recupera l'indirizzo IP del server SNTP.
indirizzo IP	Indirizzo IP al quale può essere raggiunta la scheda applicazioni.
Maschera di rete:	Maschera di rete alla quale può essere raggiunta la scheda applicazioni.
Indirizzo MAC	Indirizzo MAC della scheda applicazioni (non modificabile).
Modalità collegamento Ethernet	Modo dell'interfaccia LAN 1.

Parametri	Descrizione
Modalità collegamento Ethernet: Auto	Commutazione automatica fra 100 e 1000 Mbit/sec., nonché fra funzionamento half-duplex e full-duplex. In questo Modo è possibile attivare la funzione Risparmio energia.
Modalità collegamento Ethernet: 100HDX	100 MBit/sec., half-duplex. In questo Modo non è possibile attivare la funzione Risparmio energia.
Modalità collegamento Ethernet: 100FDX	100 Mbit/sec., full-duplex. In questo Modo non è possibile attivare la funzione Risparmio energia.
Modalità collegamento Ethernet: 1000FDX	1000 Mbit/sec., full-duplex. In questo Modo non è possibile attivare la funzione Risparmio energia.

28.3.3.14 Interfaccia di rete > Scheda applicazioni > LAN 2

Descrizione dei parametri delle schede:

- **Modifica interfaccia LAN 2**

Parametri	Descrizione
Interfaccia attivata	Se questa casella di controllo è selezionata, l'interfaccia LAN 2 della scheda applicazioni è attiva.
indirizzo IP	Indirizzo IP al quale può essere raggiunta la scheda applicazioni.
Maschera di rete:	Maschera di rete alla quale può essere raggiunta la scheda applicazioni.
Indirizzo MAC	Indirizzo MAC della scheda applicazioni (non modificabile).
Lunghezza max. pacchetto dati (byte)	Lunghezza massima del pacchetto dati in byte utilizzato per il protocollo IP. Sono ammessi valori da 576 a 1500.
Modalità collegamento Ethernet	Modo dell'interfaccia LAN 2.
Modalità collegamento Ethernet: Auto	Commutazione automatica fra funzionamento half-duplex e full-duplex. In questo Modo è possibile attivare la funzione Risparmio energia.
Modalità collegamento Ethernet: 100HDX	100 MBit/sec., half-duplex. In questo Modo non è possibile attivare la funzione Risparmio energia.
Modalità collegamento Ethernet: 100FDX	100 Mbit/sec., full-duplex. In questo Modo non è possibile attivare la funzione Risparmio energia.
Modalità collegamento Ethernet: 1000FDX	1000 Mbit/sec., full-duplex. In questo Modo non è possibile attivare la funzione Risparmio energia.
IEEE802.1p/q-Tagging	Se questa casella di controllo è selezionata, viene impostato il formato Ethernet utilizzato dalla scheda applicazioni. Per impostazione predefinita, questa opzione è disattivata.
IEEE802.1p/q-VLAN-ID	Inserire un numero ID per la VLAN diverso dal valore predefinito "0", se lo switch usato ha problemi con il valore predefinito "0".
Livello classe QoS 2	

Parametri	Descrizione
Dati di segnalazione	Classe di priorità per stabilire una connessione. 0 = priorità inferiore / 7= priorità superiore.
Payload fax/modem	Classe di priorità per dati fax e modem della connessione IP. 0 = priorità inferiore / 7= priorità superiore.
Controllo della rete	Classe di priorità per i dati del controllo di rete (ad esempio, la trasmissione di trap SNMP). 0 = priorità inferiore / 7= priorità superiore.
Payload voce	Classe di priorità per dati voce della connessione IP. 0 = priorità inferiore / 7= priorità superiore.

28.3.4 Routing

In **Routing** vengono gestite le tabelle di routing. Nelle reti di piccole dimensioni l'amministratore può gestire manualmente una tabella di routing per ciascun router. Nelle reti più grandi, questa attività viene automatizzata con il supporto di protocolli che distribuiscono in rete le informazioni di routing.

28.3.4.1 Routing > Routing IP > Scheda madre > Route statiche

Il sistema di comunicazione supporta solo rotte statiche. I percorsi statici collegano assieme due periferiche IP. Vengono creati manualmente.

A seconda dell'applicazione, può essere necessario impostare un istradamento diverso per il sistema (scheda madre) e la UC Booster Card (scheda applicazioni).

Descrizione dei parametri delle schede:

- **Mostra tabella delle rotte statiche**
- **Aggiungi rotta statica**
- **Modifica rotta statica**
- **Elimina rotta statica**

Parametri	Descrizione
Indice di route	L'indice di route viene assegnato automaticamente e visualizzato solo ai fini informativi. Non può essere modificato.
Nome delle route	Nome o descrizione del percorso statico, liberamente scelto.
Rete di destinazione/Host	Indirizzo IP della rete di destinazione.
Maschera di rete:	Maschera di sub-rete della rete di destinazione..
Gateway della route	Indirizzo IP del router successivo su questa rotta o indirizzo IP dell'interfaccia locale o remota di un peer PSTN.

28.3.4.2 Routing > Routing IP > Scheda madre > Router predefinito

A seconda dell'applicazione, può essere necessario impostare un istradamento predefinito diverso per il sistema (scheda madre) e la UC Booster Card (scheda applicazioni).

Descrizione dei parametri delle schede:

- **Modifica router predefinito**

Parametri	Descrizione
Routing predefinito tramite	Attivazione/disattivazione del routing IP tramite un router predefinito.
Nessuna interfaccia	Disattiva il routing IP tramite un router predefinito.
LAN	Attiva il routing IP tramite un router predefinito.
Indirizzo IP del router predefinito	Indirizzo IP del router predefinito, a condizione che nel campo **Routing predefinito** tramite sia selezionata come interfaccia l'opzione **LAN**. Esempio: indirizzo IP del router Internet, `192.168.1.1`.

28.3.4.3 Routing > Routing IP > Scheda madre > Server DNS

È possibile visualizzare ed eventualmente modificare l'indirizzo IP del server DNS. L'impostazione è necessaria per le linee con indirizzi IP dinamici.

Descrizione dei parametri delle schede:

- **Modifica impostazioni di DNS**

Parametri	Descrizione
Indirizzo IP del server DNS	Indirizzo IP al quale può essere raggiunto il server DNS. Se il sistema di comunicazione è collegato direttamente a un modem Internet, il valore predefinito `0.0.0.0` non deve essere modificato. Il sistema di comunicazione si connette automaticamente con un server DNS in Internet. È anche possibile inserire un server DNS esterno. Esempio: il server DNS del router Internet (`192.168.1.1)` o un server DNS di Internet (`google-public-dns-a.google.com`). In un sistema OpenScape Business S è necessario il riavvio per applicare le modifiche.

28.3.4.4 Routing > Routing IP > Scheda applicazioni > Rotte statiche

A seconda dell'applicazione, può essere necessario impostare un istradamento diverso per il sistema (scheda madre) e la UC Booster Card (scheda applicazioni).

Descrizione dei parametri delle schede:

- **Mostra tabella delle rotte statiche**
- **Aggiungi rotta statica**
- **Modifica rotta statica**
- **Elimina rotta statica**

Parametri	Descrizione
Indice di route	L'indice di route viene assegnato automaticamente e visualizzato solo ai fini informativi. Non può essere modificato.
Nome delle route	Nome o descrizione del percorso statico, liberamente scelto (opzionale) Valori consentiti: max. 35 caratteri
Rete di destinazione/Host	Indirizzo IP della rete di destinazione.
Maschera di rete:	Maschera di sub-rete della rete di destinazione..
Gateway della route	Indirizzo IP del router successivo su questa rotta o indirizzo IP dell'interfaccia locale o remota di un peer PSTN.

28.3.4.5 Routing > Routing IP > Scheda applicazioni > Router predefinito

A seconda dell'applicazione, può essere necessario impostare un istradamento predefinito diverso per il sistema (scheda madre) e la UC Booster Card (scheda applicazioni).

Descrizione dei parametri delle schede:

- **Modifica router predefinito**

Parametri	Descrizione
Routing predefinito tramite	Attivazione/disattivazione del routing IP tramite un router predefinito.
Nessuna interfaccia	Disattiva il routing IP tramite un router predefinito.
LAN	Attiva il routing IP tramite un router predefinito.
Indirizzo IP del router predefinito	Indirizzo IP del router predefinito, a condizione che nel campo Routing predefinito tramite sia selezionata come interfaccia l'opzione LAN.

28.3.4.6 Routing > NAT

È possibile visualizzare, aggiungere, modificare ed eliminare una regola NAT per la traduzione degli indirizzi di rete. L'editor di tabelle NAT fornisce pratiche funzioni per modificare tutte le voci NAT esistenti e nuove per la traduzione degli indirizzi sulla rete.

Descrizione dei parametri delle schede:

- **Aggiungi NAT**
- **Editor tabelle NAT**

Parametri	Descrizione
Regola NAT attiva	
Descrizione	
Indirizzo IP locale	Indirizzo di destinazione locale della LAN.
Porta locale	Numero di porta locale del protocollo configurato nella LAN

Parametri	Descrizione
Porta globale	Numero di porta del protocollo configurato
Protocollo	Protocollo di trasporto da utilizzare. Il protocollo di trasporto impostato si applica sia a indirizzi globali che locali.
Protocollo: **TCP**	TCP (Transmission Control Protocol) TCP è un protocollo affidabile, orientato alla connessione per la trasmissione dei pacchetti IP. Prima dell'inizio della connessione viene stabilito un canale virtuale fra i punti finali della connessione di rete. Su questo canale è possibile trasmettere i dati in entrambe le direzioni. TCP è presente principalmente negli ambienti WorldWideWeb, e-mail e Peer-to-Peer. Inoltre viene utilizzato per la segnalazione chiamate nella telefonia IP poiché è in grado di riconoscere la perdita di dati in una trasmissione e di ridurla automaticamente.
Protocollo: **UDP**	UDP, User Datagram Protocol UDP è un protocollo semplice, indipendente dalla connessione per la trasmissione dei pacchetti IP. All'inizio della connessione non viene attivato alcun canale virtuale sul lato opposto come per TCP, pertanto i PC possono iniziare prima a scambiarsi i dati. Per l'indirizzamento dei pacchetti voce, con UDP viene inviato il numero di porta del servizio che deve ricevere i dati. Viene utilizzato principalmente nel settore DNS e per la trasmissione dati nella telefonia IP. Poiché in un protocollo di questo tipo non viene controllato se la controparte ha ricevuto i dati correttamente, può verificarsi una perdita di trasmissione voce.

28.3.4.7 Routing > PSTN

Con questi parametri viene configurata una connessione IP remota (dial-up) tramite la rete telefonica tradizionale.

Descrizione dei parametri delle schede:

- **Modifica dati PSTN globali**

Parametri	Descrizione
Numero del router (numero interno)	Utilizzato per selezionare il numero DID del sistema. Tutte le applicazioni che utilizzano la funzione di router sono accessibili dall'esterno tramite questa selezione passante. Ogni partner di routing esterno che non trasmette alcun numero di telefono deve utilizzare altri numeri di telefono. Questi numeri sono configurati come MSN.
Ripetizione della selezione	
Numero di ripetizioni della selezione	Tentativi di stabilire una connessione effettuati dal sistema. Valori consentiti: da 0 a 255
Pausa di ripetizione della selezione (s)	Pausa tra tentativi di riselezione in secondi. Valori consentiti: 1-1, 000
Scripting	

Parametri	Descrizione
ID 1 per Scripting	Prima parte del codice per l'accesso al provider Internet. Il provider Internet richiede le voci host, identificativo utente e password, ad esempio: Host=ERT005, Utente=KJUMBERT, Password=123456. Le voci sono quindi come segue: ID 1 per Scripting: HOST:ERT005 - Host ID 2 per Scripting: USER:KJUMBERT - Nuova password per Scripting: PASSWORD:123456.
ID 2 per Scripting	Seconda parte del codice per l'accesso al provider Internet.
Nuova password per Scripting	Password per l'accesso al provider Internet.

28.3.4.8 Routing > PSTN > Protocollo PPP

Descrizione dei parametri delle schede:

- **Carica via HTTP**

Parametri	Descrizione
Carica	Il file di registro PPP può essere scaricato tramite HTTP. A seconda delle impostazioni del browser, viene indicato se il file di registro da scaricare deve essere salvato o aperto nell'editor predefinito.

28.3.4.9 Routing > PSTN > Partner PSTN

Descrizione dei parametri delle schede:

- **Aggiungi partner PSTN**
- **Mostra partner PSTN**
- **Modifica partner PSTN**

Parametri	Descrizione
Nome del partner	Nome del partner PSTN. Sono disponibili i seguenti partner PSTN: • PSTN predefinito - non configurabile • Partner PSTN 1: predefinito per CLA, funzione riconfigurabile • Partner PSTN 2: predefinito per ISDN, funzione riconfigurabile • Partner PSTN 3: nome e funzione liberamente configurabili • Partner PSTN 4: nome e funzione liberamente configurabili Valori consentiti: da 1 a 14 caratteri
Tipo di connessione di PSTN	Configurazione della connessione PSTN: (Selezione predefinita: Attivata).
Tipo di connessione di PSTN: Non configurato	Il partner PSTN può essere preconfigurato. Con questa impostazione, tuttavia, non è possibile stabilire connessioni tramite questo partner PSTN.
Tipo di connessione di PSTN: In funzione	Il partner PSTN è attivato. Con questa impostazione è possibile stabilire connessioni tramite questo partner PSTN.

Parametri	Descrizione
Tipo di connessione di PSTN: Fallback DSL	Uso dell'accesso DSL per la connessione PSTN (il router predefinito è l'accesso DSL)
Parametri IP	
Indirizzo IP del partner PSTN	Indirizzo IP del PC host del numero chiamato, col quale viene stabilita la connessione PSTN.
Indirizzo IP dell'interfaccia locale PSTN	Indirizzo IP del sistema di comunicazione locale che deve essere utilizzato per la connessione PSTN.
Negoziazione dell'indirizzo IP	Gestione dell'indirizzo IP tra i partner durante l'instaurazione della connessione.
Negoziazione dell'indirizzo IP: Utilizza indirizzo IP configurato	Viene accettato solo l'indirizzo IP configurato del partner PSTN.
Negoziazione dell'indirizzo IP: Accetta qualsiasi indirizzo IP	Nessuna negoziazione indirizzi IP
Negoziazione dell'indirizzo IP: Richiedi nuovo indirizzo IP	L'indirizzo IP viene negoziato
Parametri generali PPP	
Router predefinito	Qui il partner PSTN qui impostato non deve essere preconfigurato ma usato come destinazione di routing. Può essere presente solo un router predefinito. Qui è possibile l'accesso DSL o la configurazione del partner PSTN.
Accesso ad Internet con interrogazione DNS	L'accesso deve essere utilizzato come accesso a Internet. Può essere attivato solo un accesso a Internet per sistema (tramite partner PSTN o connessione DSL).
Voce Assistenza	Chiamando il numero MSN del partner PSTN, la funzione test numero di telefono deve essere disabilitata. La voce Assistenza può essere attivata solo se il partner PSTN dispone di un numero MSN ed è stata attivata un'autenticazione PAP o CHAP.
Numero MSN/Interno (numero interno)	Configurazione del numero MSN. Se il partner trasmette il proprio numero di telefono, questo deve essere configurato, in caso contrario la chiamata viene rifiutata. Se sono stati configurati i numeri di telefono del partner ma il partner non li trasferisce, la connessione viene comunque realizzata.
Canali B	Numeri di canali B utilizzati. Valori consentiti: 1 o 2

Parametri	Descrizione
Richiamata automatica	Una chiamata viene respinta, quindi il partner viene immediatamente richiamato. Ciò impedisce l'accesso di stazioni non autorizzate. La stazione chiamante deve utilizzare il canale D della connessione ISDN per trasferire il numero di telefono e consentire la composizione del numero tramite il sistema. Con il partner PSTN questo numero di telefono deve essere configurato per il fascio in uscita. Se è attivata la "richiamata", da questo partner sono accettate solo connessioni in uscita. Se il partner di comunicazione è anch'esso un gateway e se è attivata la funzione "Richiamata", non è possibile stabilire alcuna connessione in quanto nessuno dei partner accetta di stabilire una connessione in entrata. In caso di una tale configurazione errata in cui è attivato solo "Richiamata senza ripetizione della selezione", ciò viene rilevato e la connessione permanente viene soppressa. Se tuttavia è attivo il pulsante ripetizione, il problema non viene riconosciuto.
Lato opposto V.34	Accettare un terminale V.34 (ad esempio un modem).
Riconnetti PPP automaticamente	La connessione PPP viene automaticamente stabilita dopo una disconnessione (ad esempio, accedendo con un ISP che prevede una tariffa flat a disconnessione forzata dopo 24 ore).
Invia richiesta eco di LCP	È stata inviata una richiesta eco LCP. Questa funzione viene utilizzata per verificare se la connessione è ancora attiva.
Modalità Short Hold	
Modalità Short Hold	La modalità di funzionamento "Short Hold" per la connessione PPP è attivata. Le seguenti funzioni possono essere usate solo se è attivata la modalità Short Hold.
Tempo Short Hold (sec.)	Periodo di tempo senza trasferimento di dati, trascorso il quale la connessione PPP viene interrotta. Il Short Hold Timer viene attivato solo da pacchetti in uscita. Valori consentiti: da 10 a 9999
Analisi del clock degli addebiti Short Hold	Ottimizzazione della modalità Short Hold, in considerazione del clock addebiti. Per le chiamate su PPP viene eseguita una valutazione del clock addebiti (analisi dei messaggi facility con elementi informativi AOC). Se il proprio provider di servizi Internet non fornisce alcuna informazione sugli addebiti, viene utilizzato come valore di timeout predefinito 0 secondi.
Autenticazione	
Autenticazione PPP	L'autenticazione PPP viene attivata.
Nome d'utente PPP	Nome utente liberamente scelto da utilizzare per l'autenticazione tramite PAP o CHAP.
Modalità di autenticazione PAP	Attivazione e tipo di autenticazione PAP per la connessione PPP: non utilizzato, client PAP, host PAP.
Password PAP	Password per autenticazione PAP.
Modalità di autenticazione CHAP	Attivazione e tipo di autenticazione CHAP per la connessione PPP: non utilizzato, client CHAP, host CHAP, client e host CHAP.
Password CHAP	Password per autenticazione CHAP.

Parametri	Descrizione
Compressione dell'intestazione	
Compressione dell'intestazione IP	La compressione di IP/TCP o intestazione IP/UDP/RTP è attivata. La compressione dell'intestazione migliora la trasmissione dei dati negli scenari voice-over-PPP. Vengono compressi tutti i pacchetti voce i cui numeri di porta UDP rientrano nell'intervallo impostato.
Compressione dei dati	
Compressione di dati DEFLATE	Compressione con algoritmo DEFLATE
Compressione di dati COMPRESS	Compressione con algoritmo COMPRESS
Traduzione dell'indirizzo	
NAT	NAT (Network Adress Translation) è attivo. Sono supportati i seguenti protocolli: TCP, UDP e ICMP (solo in modo passivo).
Mapping indirizzi	La mappatura degli indirizzi è attivata.
Parametri QoS dell'interfaccia	
Controllo della larghezza di banda per connessioni voce	In una connessione multilink, il controllo della larghezza di banda impedisce l'eccesso di prenotazioni delle trasmissioni disponibili con connessioni vocali: ad esempio se si attiva la compressione dell'intestazione, sono disponibili un massimo di 5 connessioni vocali (G.729/60ms o G.723/60ms) su un canale B. Questo campo attiva il controllo della larghezza di banda per connessioni voce. Vengono considerate solo le connessioni voce le cui rotte sono configurate nel gateway voce.
Larghezza di banda per connessioni voce/fax (%)	Indicazione percentuale della larghezza di banda disponibile per connessioni voce/fax. Valori consentiti, valore predefinito: 0-95, 80

Descrizione dei parametri delle schede:

- **Ripristina le impostazioni iniziali**

Parametri	Descrizione
Applica	I valori per il partner PSTN selezionato vengono riportati ai valori di fabbrica.

Descrizione dei parametri delle schede:

- **Aggiungi numero di telefono**
- **Modifica numero di telefono**
- **Cancella numero di telefono**

Parametri	Descrizione
Numero di telefono	Numero di telefono mediante il quale è raggiungibile il partner PSTN. Questo numero deve essere univoco all'interno dell'intera configurazione e può contenere fino a 22 cifre a base decimale (0-9). È consentito l'uso di trattini. Per ogni partner PSTN possono essere configurati fino a cinque numeri telefonici. Alla trasmissione del numero di telefono, questo viene verificato e le chiamate vengono accettate solo se per il numero in arrivo è definito un partner PSTN provvisto dell'abilitazione necessaria.
Direzione della chiamata	Viene eseguita la connessione al numero telefonico sopra indicato.
Direzione della chiamata: Bloccato	Il numero non è utilizzabile.
Direzione della chiamata : in entrata	Il partner può effettuare chiamate ma non essere chiamato.
Direzione della chiamata: in uscita	Il partner può essere chiamato ma non può effettuare chiamate.
Direzione della chiamata : In entrata e in uscita	Il partner può essere chiamato e può effettuare chiamate.
Elimina	Il numero di telefono selezionato viene eliminato.

28.3.5 LCR

In **LCR** sono incluse le funzioni richieste per il Least Cost Routing, quali le abilitazioni, i piani di composizione e le regole di composizione.

28.3.5.1 LCR > Flag LCR

Descrizione dei parametri della scheda:

- **Modifica flag LCR**

Parametri	Descrizione
Flag LCR	
Activate LCR	LCR viene abilitato e quindi si attiva la ricerca automatica dei percorsi.
Reset dati LCR	
Eliminare i dati LCR configurati e inizializzare LCR con i dati predefiniti	Se si seleziona questa casella, le voci LCR configurate (piani di composizione, tabelle delle rotte e regole di composizione) vengono eliminate e sostituite da voci predefinite.

Suggerimento: Se si commette un errore nella configurazione di LCR, è possibile che le connessioni in uscita non funzionino o funzionino in modo inadeguato.

Concetti correlati

Dati dell'utente alla pagina 159

28.3.5.2 LCR > Classi di servizio

Descrizione dei parametri della scheda:

- **Modifica delle abilitazioni LCR**

Parametri	Descrizione
Indice	Elenco indice gerarchico
Numero di telefono	Numero di telefono dell'utente
Servizio	Nome dell'utente
Gruppo d'abilitazione	Ciascun utente viene assegnato a un gruppo di abilitazione LCR (Class Of Service, COS). Per impostazione predefinita, tutti gli utenti sono configurati con il massimo livello di abilitazione LCR (15) Valori consentiti: da 1 a 15

Suggerimento: Un utente può impegnare una rotta solo se il suo livello di abilitazione è superiore all'abilitazione LCR nella tabella delle rotte.

28.3.5.3 LCR > Piano di composizione

Descrizione dei parametri delle schede:

- **Modifica piano di composizione**
- **Visualizza piano di composizione**

Parametri	Descrizione
Piano di composizione	Nel Piano di composizione viene ricercato un modello che corrisponda alle cifre selezionate. Il risultato viene utilizzato come criterio per selezionare la tabella delle rotte. Viene inoltre verificato se l'abilitazione dell'utente è adeguata per il fascio. Per le connessioni esterne, ogni numero di telefono, compreso il numero di codice (fino a max. 24 caratteri tra cui il trattino di separazione di campo) nel piano di selezione viene verificato. Il piano di composizione determina quindi quale tabella delle rotte sarà assegnata a un utente per la realizzazione delle connessioni. Con la tabella delle rotte vengono create le rotte (percorsi). La tabella delle regole di selezione definisce come le cifre selezionate dagli utenti vengano convertite e composte dal sistema di comunicazione.
Servizio	Nella colonna Nome è possibile assegnare un nome a ogni profilo, ad es., Chiamate locali, Chiamate interurbane, Estero. La visualizzazione della colonna Nome dipende dalla versione del sistema di comunicazione. Per il nome, è opportuno scegliere un nome descrittivo. Un nome può essere utilizzato anche più volte. Tramite le procedure guidate numeri di telefono vengono assegnati automaticamente i corrispondenti nomi.

Parametri	Descrizione
Cifre selezionate	Con questo schema il numero di telefono viene valutato per poterlo destinare alla tabella delle rotte corrispondente. È possibile utilizzare i delimitatori di campo C nonché i segnaposto X, N e Z. Cifre fisse 0...9 - Trattino di separazione di campo (valutazione tramite la regola di selezione); segnaposto X per una cifra tra 0...9; segnaposto N per una cifra tra 2...9; segnaposto Z per una o più cifre fino al termine delle composizione del numero; C - tono di composizione simulato (può essere digitato un massimo di 3 volte)
Tabella delle rotte	Nella colonna Tabella delle rotte viene indicato quale tabella delle rotte deve essere utilizzata per il profilo. La freccia collega alla definizione della rispettiva tabella delle rotte. Valori consentiti: da 1 a 254, di cui da 1 a 15 preimpostati
Codice add.	La casella di controllo di questa colonna viene selezionata/deselezionata a seconda che il codice di addebito debba essere obbligatoriamente inserito dopo il codice di impegno della linea o meno (negli Stati Uniti: fine della selezione). Se la casella di controllo non è selezionata, il codice addebito viene richiesto solo dopo la selezione completa di piano di composizione, se configurato per il fascio.
Controllo della selezione	Se selezionata, le cifre composte sono soggette al controllo della selezione (abilitazione). Ciò vale sia per i sistemi di reti che per i sistemi di comunicazione indipendenti. Pertanto, i singoli numeri di telefono possono essere esclusi dalle abilitazioni. Se occorre implementare il controllo della selezione, si applicano le regole note tramite le Liste nr.permessi e le Liste nr.vietati.
Servizio d’emergenza	Se viene composto un numero configurato come numero di emergenza (colonna Servizio d'emergenza selezionata) e se non ci sono linee libere, una linea non usata per un numero di emergenza (colonna Servizio d'emergenza non selezionata) viene liberata e quindi automaticamente utilizzata per la chiamata d'emergenza.

28.3.5.4 LCR > Tabella delle rotte

Descrizione dei parametri delle schede:

- **Modifica tabella di routing**

Parametri	Descrizione
Tabelle rotte	Ai numeri di telefono definiti nel piano di composizione può essere assegnata, tramite le tabelle delle rotte, un'azione (composizione). Valori consentiti: 254 tabelle delle rotte
Indice	La ricerca nella Tabella delle rotte avviene dall'alto verso il basso, in sequenza gerarchica. Viene verificato se il fascio è libero o se l’utente dispone dell’abilitazione LCR richiesta. In caso affermativo, la selezione avviene secondo la regola riportata nella tabella delle rotte. Valori consentiti: da 1 a 16
Percorso dedicato	Viene utilizzato il fascio abbinato all'utente mediante assegnazione fissa (ad esempio assegnazione del fascio con Gestione multisito.

Parametri	Descrizione
Fascio	Per informazioni sul fascio da assegnare, vedere "Linee/Rete" Valore predefinito: Nome del fascio configurato nel sistema
Regola di selezione	Grazie alle regole di composizione LCR i numeri di telefono immessi possono essere trasformati in nuove sequenze di cifre, come desiderato. La conversione delle cifre consente di accedere a vari gestori di rete. Definizione in "Regola di composizione". Valori consentiti: 254 regole di composizione
Abil. min.	L'abilitazione min. indica il livello di abilitazione LCR minimo che l'utente deve possedere per utilizzare la rotta assegnata. Qui è possibile definire, ad esempio, che un utente può chiamare solo un determinato carrier o solo in determinati momenti, mentre gli altri utenti avranno la possibilità di utilizzare rotte alternative. Il valore dell'abilitazione massima è 15. Valori consentiti: da 1 a 15
Avvertenza	Se il percorso primario della tabella è occupato, LCR seleziona quello successivo (possibilmente in base alla convenienza). Ciò può essere segnalato all'utente tramite un segnale acustico e/o ottico. Valori consentiti: Nessuno, Tono, Display, Display + tono
Gateway dedicato	Questo parametro definisce il modo in cui viene identificato il nodo del destinatario in un sistema di reti con protocollo IP. Valori consentiti: No, Forzato, Più sedi
Gateway dedicato: **No**	Il nodo partner viene identificato tramite un numero di destinazione.
Gateway dedicato: **Forzato**	Viene obbligatoriamente instradato al gateway indicato nella colonna **ID Nodo GW** tramite il proprio ID nodo.
Gateway dedicato: **Più sedi**	descrizione del chiamante del nodo partner: viene istradato al gateway assegnato al rispettivo chiamante mediante la procedura guidata Multigateway o la maschera di immissione**Utenti** > **Modifica i dati del WorkPoint Client** > **ID del sistema secondario**. Il chiamante senza la relativa voce viene istradato al gateway indicato nella colonna **ID nodo GW** tramite il proprio ID nodo (predefinito).
ID nodo GW	Indica l'ID nodo gateway per la selezione **Forzato** o **Più sedi** nel parametro **Gateway dedicato**.
Pulsanti	
Freccia blu nella colonna **Regola di composizione**	Visualizza la pagina con i parametri **Regola di composizione**.

28.3.5.5 LCR > Regola di composizione

Descrizione dei parametri della scheda:

- **Modifica regola di composizione**

Parametri	Descrizione
	Grazie alle regole di composizione LCR i numeri di telefono immessi possono essere trasformati in nuove sequenze di cifre, come desiderato. La conversione delle cifre consente di accedere a vari gestori di rete. La regola di composizione utilizzata viene definita tramite la voce nella tabella delle rotte.
Nome della regola	Nome e regola di composizione liberamente definibile, alcune regole di composizione sono predefinite Valori consentiti: max. 16 caratteri
Formato della regola di selezione	Programma per le cifre da comporre. I singoli passi del programma vengono elaborati da sinistra a destra. I caratteri per il codice del programma sono riservati per le seguenti funzioni:
A	Ripetere i campi restanti (trasmettere). "A" trasmette tutti i campi di cifre successivi. Il punto di riferimento è l'ultimo delimitatore nel campo delle cifre composte nel piano di composizione. Se "A" è inserito senza riferimento esplicito, indica tutte le cifre dopo il codice di accesso, ovvero, "A" corrisponde a "E2A"
B	Viene utilizzato in un collegamento in rete multi-gateway quando un numero esterno chiamato di tipo (TON, type of number) "sconosciuto", deve essere istradato verso il nodo multi-gateway. Per assicurare che questo numero di telefono sia univoco, viene esteso in numero nazionale o internazionale secondo il TON nell'LCR. Questo è necessario se i numeri DID non sono univoci e devono essere configurati nel formato nazionale o internazionale.
D (n)	selezionare la stringa di cifre (da 1 a 25). Nella stringa di cifre, "D" può ricorrere più volte e può trovarsi in posizioni qualsiasi.
E (n)	Invio del contenuto del campo (da 1 a 10). "E" può ricorrere più volte e trovarsi in posizioni qualsiasi. La successione di "E" in relazione a (n) è a piacere. Un determinato campo può essere attivato più volte, anche in sequenza. "E", ad eccezione di "E1" (codice di accesso), può essere compreso fra altri parametri a piacere. Con la selezione a passi (contrapposta a quella a blocchi), l'ultimo elemento della regola di selezione non può essere E(n), bensì E(n)A.
M (n)	codice di autorizzazione (da 1 a 16). Questa lettera non deve trovarsi sull'ultima posizione.
P (n)	P (n) può verificarsi più di una volta nella stringa e può trovarsi in qualsiasi posizione. P (n) può essere circondato da altri parametri. (Da 1 a 60 volte l'unità di pausa a livello di sistema).
S	switch, commutazione del tipo di selezione da DC a DTMF (in CONNECT, PROGRESS o CALL PROC con PI). Nella stringa di cifre, "S" può ricorrere una sola volta e non deve essere sull'ultima posizione. Dopo "S" non può più essere utilizzato il parametro "C".
C	Nella stringa di cifre, il carrier "C" può essere inserito una sola volta. Le cifre successive vengono trasmesse senza pausa di selezione e utilizzate in "Single Stage", "Two Stage", "DICS" e "PRI" per l'accesso al carrier.
U	applicazione del tipo di selezione SUB-indirizzo. Nella stringa di cifre, "U" può ricorrere una sola volta e non deve essere sull'ultima posizione. Dopo "U", i parametri "S", "P" e "C" non possono essere più utilizzati.

Parametri	Descrizione
N (n) (Solo per USA!):	gruppo SFG della rete (da 1 a 5) o numero di banda (1)
L (solo per USA!)	"L" può trovarsi solo alla fine della stringa. "L" significa che la chiamata viene trattata come una chiamata di emergenza.
Metodo del gestore di rete	Selezione del rispettivo provider di rete
Sconosciuto	Nessuna informazione esplicita sul gestore di rete.
Fornitore rete principale	In caso di impegno di una linea del gestore di rete principale, la composizione dei numeri viene semplificata utilizzando la selezione in blocco o cifra per cifra nella rete pubblica.
MCL Single Stage	Con MCL Single Stage, si utilizza un prefisso per selezionare il gestore di rete desiderato, quindi si compone il numero di telefono. La composizione viene eseguita sul canale D nel caso di una linea ISDN e come composizione normale per linee urbane analogiche.
MCL Two Stage	Con MCL Two Stage, si utilizza un prefisso per selezionare il gestore di rete desiderato. Dopo una fase di sincronizzazione, viene inviato prima un codice di autorizzazione configurabile e successivamente il numero di telefono di destinazione sotto forma di caratteri DTMF. Per la sincronizzazione a tempo deve essere programmato un intervallo compreso tra 2 e 12 secondi.
Corporate Network	Una rete aziendale è collegata direttamente a OpenScape Business. La funzione LCR determina, sulla base del numero composto dall'utente, la linea e instrada la chiamata tramite il fascio di linee della rete pubblica o tramite quello della rete aziendale.
Server controllo accesso	Con questo tipo di LCR, è possibile selezionare il gestore di rete desiderato con un prefisso tramite Dial-In Control Server (DICS) e successivamente trasmettere il numero di telefono e un codice di autorizzazione configurabile nell'indirizzo SUB. La composizione avviene quindi nel canale D.
Primary Rate Interface (interfaccia multiplex primaria) (solo per USA)	Nel caso del collegamento primario multiplex, la scelta del gestore di rete o del Calling Service viene codificata nel messaggio SETUP tramite i seguenti elementi informativi: Network Specific Facility, Operator System Access e Transit Network Selection.
Tipo	Type of Number [TON]; qui è possibile selezionare dall'elenco a discesa, per ogni regola, i seguenti tipi di numeri per il "Called Party Number": numero di sistema, prefisso interurbano, prefisso nazionale. La voce predefinita è "Sconosciuto". Il tipo di numero è impostato solo in E.164. In una rete, i parametri sono impostati a “sconosciuto”.

28.3.5.6 LCR > Multisito

Descrizione dei parametri della scheda:

- **Modifica dell'intervallo**

Parametri	Descrizione
Indicativo località	Immissione del prefisso locale per una località (con zeri non significativi, ad esempio `02` per Milano e `06` per Roma). È possibile inserire codici località diversi o uguali.
Area	Inserire il nome di una località (ad esempio, le città corrispondenti ai codici località `Milano` e `Roma` o se il codice località è lo stesso, le descrizioni dei reparti `Assistenza` e `Vendite`).
Percorso dedicato	Selezione del fascio o della registrazione ITSP per questa località.
Elimina	Elimina le voci selezionate della località.
Pulsanti	
Salva	Salva le modifiche.

Descrizione dei parametri della scheda:

- **Modifica gli utenti/i gruppi**

Parametri	Descrizione
Area	Selezione della località per l'utente o il gruppo.
Percorso dedicato	Selezione del fascio o della registrazione ITSP per questo utente o per il gruppo.
Cerca	Ricercare utenti e gruppi inserendo il termine da cercare nei campi di ricerca **N° tel**, **DID** o **Nome** e quindi premendo il tasto Invio. Se si lasciano vuoti tutti i campi di ricerca e quindi si fa clic sul tasto Invio, vengono visualizzati tutti gli utenti e i gruppi. L'opzione **Tipo** consente di visualizzare tutti i tipi di utenti (ad esempio, **Client SIP** o **Client di sistema**).

28.3.6 Gateway voce

In **Gateway voce** sono riunite le funzioni relative alla telefonia IP.

28.3.6.1 Gateway voceParametri SIP

Descrizione dei parametri delle schede:

- **Modifica parametri SIP**

Parametri	Descrizione
Protocollo di trasporto SIP	
SIP tramite TCP	"Transmission Control Protocol". TCP è un protocollo di trasporto obbligatorio per SIP e qui non può essere disattivato.
SIP tramite UDP	"User Datagram Protocol". UDP è il protocollo di trasporto predefinito per SIP ma può essere disattivato se non è utilizzato da alcun endpoint, linea o ITSP. Si consiglia vivamente di tenere UDP attivato.

Parametri	Descrizione
SIP tramite TLS	"Transport Layer Security". TLS è il protocollo di trasporto di sicurezza per SIP e qui non può essere disattivato.
Registrar SIP	
Durata della registrazione (sec.)	Intervallo (in secondi) al quale la registrazione di un endpoint SIP deve essere ripetuta. Il valore dell'intervallo non deve essere troppo elevato perché la registrazione è utilizzata per determinare se l'endpoint è fuori servizio. (Il periodo di registrazione delle linee ITSP è configurato nei profili ITSP). Valori consentiti, valore predefinito: 10-86400, 120
RFC 3261 - Valori timer	
Tempo di timeout transazione (min)	Indica il tempo di attesa (in millisecondi) prima di una ritrasmissione della risposta di invito per il timer D secondo la specifica RFC 3261. Questa impostazione è rilevante per la transazione client invito. Valori consentiti, valore predefinito: 2000-64000, 32000
Timer sessione SIP	
Utilizza RFC 4028	RFC 4028 definisce una proroga dei Session Initiation Protocol (SIP). Questa espansione permette un refresh periodico delle sessioni SIP. Con il refresh, gli agenti utente e i proxy possono determinare se la sessione SIP è ancora attiva. La possibilità di configurazione qui è utilizzata per controllare il refresh della sessione sull'interfaccia di linea (per gli ITSP, vedere il profilo rispettivo).
Scadenza sessione (s)	Definisce la durata dell'intervallo per una sessione SIP. Il valore consigliato è "1800". Il valore configurato è usato per le interfacce di linea e ITSP. Valori consentiti, valore predefinito: 90-65535, 1800
Scadenza sessione minima (sec.)	Definisce la durata minima consentita per una sessione SIP. Il valore configurato è usato per le interfacce di linea e ITSP. Valori consentiti, valore predefinito: 90-65535, 90
Record DNS	
Tempo blocco per destinazione irraggiungibile (sec.)	Questo timer viene utilizzato per controllare la lista nera dello stack SIP. Se un server SIP risolto tramite DNS non è raggiungibile, verrà bloccato per il periodo di tempo configurato. Il valore predefinito è di 60 secondi. Nei casi in cui vengono utilizzati server ridondanti (ad es., risultati DNS in più server), si consiglia di impostare un valore più elevato (ad es. 900).
Chiamate tramite provider	
Chiamate possibili tramite provider	Qui viene visualizzato il numero di chiamate simultanee tramite tutti i provider attivi. Questo valore viene impostato durante la configurazione a seconda della larghezza di banda disponibile e della configurazione ITSP.

28.3.6.2 Gateway voce > Impostazioni ID Loc ITSP

Descrizione dei parametri delle schede:

- Aggiungi info posizione ITSP

  L'Info posizione ITSP è usata nel protocollo SIP per informare il destinatario di una chiamata di emergenza sull'origine geografica della chiamata. Nel protocollo SIP, il formato dell'ID posizione è definito RFC4119 & RFC5139 (oggetto posizione con codifica XML nel corpo MIME). L'ID Loc ITSP consente di definire tutti i campi definiti negli RFC rilevanti, mentre, in una distribuzione specifica, solo un sottogruppo di questi dati deve essere configurato. (ad es., in Svizzera viene usato solo il campo NAM per definire una posizione). I dati necessari a definire una posizione sono forniti dal proprio ITSP.

Parametri	Descrizione
Nome Loc-ID	Il nome dell'ID posizione.
Paese	Il paese è identificato dal codice ISO 3166 a due lettere
A1	Suddivisioni nazionali (stato, cantone, regione, provincia, prefettura)
A2	Contea, parrocchia, gun, distretto
A3	Città, comune, shi
A4	Divisione della città, quartiere, città, quartiere, reparto, chou
A5	Quartiere, isolato
A6	Via
PRD	Strada che porta in direzione di
POD	Suffisso di strada
STS	Suffisso di strada
HNO	Numero civico, solo parte numerica
HNS	Suffisso numero civico
LMK	Punto di riferimento o nome edificio
LOC	Informazioni supplementari posizione
FLR	Piano
NAM	Nome (residenza o ufficio occupante)
PC	Codice postale
SALA	Sala
PLC	Tipo di luogo
PCN	Postali nome di comunità
POBOX	Casella postale
ADDCODE	Codice aggiuntivo
SEAT	Sedile (scrivania, armadio, workstation)
RD	Strada principale nome
RDSEC	Strada sezione
RDBR	Ramo stradale nome

Parametri	Descrizione
RDSUBBR	Sub-ramo stradale nome
PRM	Nome della via pre-modificatore
POM	Nome della strada post-modificatore
Attivare le impostazioni avanzate	Quando sono attivati, i campi dei parametri avanzati possono essere configurati.
BLD	Edificio (struttura)
UNIT	Unità (appartamento, suite)

28.3.6.3 Gateway voce > Parametri Codec

Descrizione dei parametri delle schede:

- **Modifica parametri Codec**

Parametri	Descrizione
Codec	I parametri per i codec G.711 A-law, G.711 µ-law, G.729A e G.729AB possono essere elaborati.
Codec: G.711 A-law	G.711 (A-law e µ-law): codifica voce a 56 o 64 Kbit/sec. - qualità voce molto buona. G.711 viene impostato anche nelle reti fisse (ISDN). Il metodo A-law è una delle tecniche di digitalizzazione principali in Europa per i segnali audio analogici nel settore telecomunicazioni.
Codec: G.711 µ-law	G.711 (A-law e µ-law): codifica voce a 56 o 64 Kbit/sec. - qualità voce molto buona. G.711 viene impostato anche nelle reti fisse (ISDN). In Nord America e in Giappone, viene utilizzato il metodo "µ-law", simile alla "A-law", tuttavia non compatibile. Per la comunicazione, ad esempio nel caso di una conversazione telefonica tra Europa e Stati Uniti, i dati digitali devono essere tradotti mediante convertitori appropriati.
Codec: G.729A	Codifica voce a 8 kbit/s.
Codec: G.729AB	Codifica voce a 8 kbit/s. Padding delle pause vocali con rumore di comfort.
Priorità	Ai Codec audio è possibile assegnare priorità da 1 (alta) a 4 (bassa). Il sistema di comunicazione tenta automaticamente di utilizzare un codec audio a priorità elevata per ogni connessione. Se si utilizza un Codec audio a bassa compressione (buona qualità voce), il carico della rete risulta elevato. In caso di utilizzo intenso della telefonia IP, il trasferimento dati su una rete già sovraccarica può comportare un peggioramento della qualità voce.
Riconoscimento delle pause vocali (VAD)	Attivazione del riconoscimento delle pause vocali (VAD, Voice Activity Detection). In caso di pause prolungate il carico di rete può diminuire.

Parametri	Descrizione
Dimensione del frame	Per ciascun Codec è possibile definire la dimensione del frame (dimensioni dei pacchetti IP) con un valore da 10 a 90 millisecondi. In questo modo si definisce la frequenza di campionamento per il segnale voce nei pacchetti IP. I valori più alti (ad es. 90 ms) indicano da un lato un comportamento migliore dei dati nell'overhead dei pacchetti IP, dall'altro un maggiore ritardo nella trasmissione. I valori configurabili dipendono dal codec. Per i servizi di rete di OpenScape Business con OpenScape Voice tramite SIP-Q V2: Cordless IP e OpenScape Mobile Connect supportano soltanto una dimensione di frame di 20 ms per il codec G.711. Se nel sistema di reti è presente uno di questi due prodotti, la dimensione del frame deve essere impostato su 20 ms. Valori consentiti, valore predefinito: 10 - max. 90, 20
Canali DSP avanzati	
Usare solo G.711	Vengono utilizzati solo i protocolli G.711 A-law, G.711 µ-law. Con G.711 occorrono meno risorse DSP, quindi sono possibili più conversazioni simultanee.
Fax T.38	
Fax T.38	Determina se deve essere utilizzato il protocollo fax T.38. Per un sistema con scheda Booster e/o Booster Server: Se il flag è attivato, durante il trasferimento viene eseguita la correzione degli errori nel protocollo T.38. Viene visualizzata una finestra a comparsa per notificare all'utente che è necessario un riavvio manuale del sistema o di un server OCAB/Booster.
Usa FillBitRemoval	Determina se, quando si utilizza il protocollo fax T.38, occorre cancellare i bit di padding durante la trasmissione e ripristinarli durante la ricezione. In questo modo è possibile risparmiare banda.
Dimensione max. datagramma UDP per fax T.38 (byte)	Dimensione massima di datagrammi T.38 UDP in byte. Valori consentiti, valore predefinito: 1 - 1472, 1472
Correzione errori utilizzata per fax T.38 (UDP)	Specifica il metodo da utilizzare per la correzione degli errori. Valori consentiti: t38UDPFEC, t38UDPRedundancy Per un sistema con scheda Booster e/o Booster Server: Quando si seleziona un'opzione, viene visualizzata una finestra a comparsa per notificare all'utente che è necessario un riavvio manuale del sistema o di un server OCAB/Booster. Valore predefinito: t38UDPRedundancy
T.30 Fax	
Attiva ECM	Per un sistema con scheda Booster e/o Booster Server: Se il flag è attivato, durante il trasferimento viene eseguita la correzione degli errori nel protocollo T.30. Viene visualizzata una finestra a comparsa per notificare all'utente che è necessario un riavvio manuale del sistema o di un server OCAB/Booster. Valore predefinito: attivato

Parametri	Descrizione
Modalità di compatibilità con VoIP	Per un sistema con scheda Booster e/o Booster Server: Questo flag va attivato se si incontrano problemi con la trasmissione dei fax sulle reti VoIP. Viene visualizzata una finestra a comparsa per notificare all'utente che è necessario un riavvio manuale del sistema o di un server OCAB/Booster. Valore predefinito: disattivato
Altro	
ClearChannel	Un ClearChannel è un canale aperto in cui i terminali sono responsabili per il protocollo utilizzato nel canale. Il parametro determina se deve essere attivata la funzionalità di interfaccia ClearChannel.
Dimensione del frame	In questo campo è possibile determinare la frequenza di campionamento. Le opzioni possibili sono 10, 20, 30, 40, 50 e 60 millisecondi (ms). Valori consentiti, valore predefinito: 10 - 60, 20
RFC2833 RFC2833 definisce come devono essere trasmessi i segnali del tono di linea.	
Trasmissione di toni fax/ modem secondo RFC2833	Trasmissione outband (tramite segnalazione SIP), modalità consigliata per la trasmissione sicura di toni
Trasmissione di toni DTMF secondo RFC2833	Trasmissione outband (tramite segnalazione SIP), modalità consigliata per la trasmissione sicura di toni
Tipo payload per RFC2833	Può essere necessaria una modifica, in funzione dell'interlocutore Valori consentiti, valore predefinito: 96 - 126, 98
Trasmissione ridondante di toni RFC2833 secondo RFC2198	Utilizzato per migliorare la sicurezza durante la trasmissione

28.3.6.4 Gateway voce > Parametri codec di destinazione

Per certi partner di comunicazione è possibile definire priorità per l'uso dei codec audio.

Descrizione dei parametri delle schede:

- **Aggiungi parametri Codec di destinazione**

Parametri	Descrizione
Codec: G.711 A-law	G.711 (A-law e µ-law): codifica voce a 56 o 64 Kbit/sec. - qualità voce molto buona. G.711 viene impostato anche nelle reti fisse (ISDN). Il metodo A-law è una delle tecniche di digitalizzazione principali in Europa per i segnali audio analogici nel settore telecomunicazioni.

Parametri	Descrizione
Codec: G.711 µ-law	G.711 (A-law e µ-law): codifica voce a 56 o 64 Kbit/sec. - qualità voce molto buona. G.711 viene impostato anche nelle reti fisse (ISDN). In Nord America e in Giappone, viene utilizzato il metodo "µ-law", simile alla "A-law", tuttavia non compatibile. Per la comunicazione, ad esempio nel caso di una conversazione telefonica tra Europa e Stati Uniti, i dati digitali devono essere tradotti mediante convertitori appropriati.
Codec: G.729A	Codifica voce a 8 kbit/s.
Codec: G.729AB	Codifica voce a 8 kbit/s. Padding delle pause vocali con rumore di comfort.
Priorità	Ai Codec audio è possibile assegnare priorità da 1 (alta) a 4 (bassa). Il sistema di comunicazione tenta automaticamente di utilizzare un codec audio a priorità elevata per ogni connessione. Se si utilizza un Codec audio a bassa compressione (buona qualità voce), il carico della rete risulta elevato. In caso di utilizzo intenso della telefonia IP, il trasferimento dati su una rete già sovraccarica può comportare un peggioramento della qualità voce.
Destinazione	
Tipo di indirizzo di destinazione	Visualizza il tipo di destinazione a cui devono essere assegnate le priorità definite dei codec audio.
indirizzo IP	Indirizzo IP della destinazione alla quale si applicano le priorità dei codec audio impostate (ad esempio nodo di rete, server SIP)

28.3.6.5 Gateway voce > Provider di servizi di telefonia Internet

Descrizione dei parametri delle schede:

- **Aggiungi provider di servizi di telefonia Internet**
- **Modifica provider di servizi di telefonia Internet**
- **Elimina provider di servizi di telefonia Internet**

Parametri	Descrizione
Modello base	Selezione di un modello vuoto (predefinito) o di una configurazione campione predefinita per un particolare provider di servizi. Questo modello può essere adattato alle esigenze individuali e salvato come nuovo ITSP.
Nome provider	Nome desiderato per l'ITSP. L'ITSP configurato apparirà nell'elenco degli ITSP con questo nome.
Abilita provider	Viene attivato l'ITSP.
Identificatore del provider nel sistema	Assegnazione di una designazione unica nel sistema. Possono essere attivi contemporaneamente un massimo di 8 ITSP. Valori consentiti: Provider 1-8
Nome del dominio	Nome di dominio del gateway dell'ITSP, spesso non coincide con il nome di dominio web.
Protocollo di trasporto	Protocollo di trasporto desiderato. È possibile selezionare UDP o TCP.

Parametri	Descrizione
Sicurezza del trasporto	I valori possibili sono **tradizionale (upd o tcp)** per le chiamate tradizionali che utilizzano udp/tcp o **sicuro (tls)** per le chiamate sicure che utilizzano TLS. Valore predefinito: **tradizionale (udp o tcp)**
Sicurezza dei supporti multimediali	I valori possibili sono **Solo RTP** (è supportato solo il profilo AVP) o **Solo SDES** (è supportato solo il profilo SAVP). Valore predefinito: **Solo RTP**
Provider Registrar	
Usa Registrar	Deve essere selezionato se il trunk funziona con la registrazione (opzione predefinita = off).
Indirizzo IP/Nome host	Nome host o indirizzo IP del server Registrar esterno.
Porta	Numero di porta del server Registrar esterno, ad esempio, 5060. Inserire la porta 00 se l'ITSP utilizza il DNSSRV.
Intervallo di registrazione presso il provider (sec.)	Intervallo (in secondi) con cui viene ripetuta la registrazione ITSP. Il valore dell'intervallo non deve essere 0 e non deve essere impostato troppo alto perché, ripetendo la registrazione presso l'ITSP, può venire rilevata anche una caduta della connessione e, se necessario, può essere selezionato un percorso alternativo (via ISDN o un provider alternativo). Valore predefinito: 120 secondi
Proxy del provider	
Indirizzo IP/Nome host	Nome di dominio o indirizzo IP del server proxy (ad esempio, sip-voice.de). La voce è obbligatoria e di solito è identica a quella del registrar del provider.
Porta	Numero di porta del server proxy (ad esempio, 5060). Di regola, è identico al numero di porta del provider. Immettere la porta 0 se l'ITSP utilizza più server e DNSSRV.
Proxy in uscita del provider	
Usa proxy in uscita	Da abilitare solo se l'ITSP utilizza un proxy in uscita diverso da quello del provider. Disabilitato per impostazione predefinita.
Indirizzo IP/Nome host	Nome di dominio o indirizzo IP del proxy in uscita.
Porta	Numero della porta del proxy in uscita. Immettere la porta 0 se l'ITSP utilizza più server e DNSSRV.
Proxy in entrata del provider	
Usa proxy in entrata	Da impostare solo se l'ITSP invia facoltativamente le richieste da un secondo server. Disabilitato per impostazione predefinita.
Indirizzo IP/Nome host	Nome di dominio o indirizzo IP del secondo server ITSP
Porta	Numero di porta del secondo server ITSP. Inserire la porta 0 se l'ITSP utilizza il DNSSRV.

Parametri	Descrizione
STUN provider	
Usa STUN	Da impostare solo se l'ITSP utilizza un server STUN. L'impostazione a livello di sistema nella configurazione STUN vale come modalità STUN per tutti gli ITSP (impostazione predefinita = off).
Indirizzo IP/Nome host	Nome host o indirizzo IP del server STUN.
Porta	Numero di porta STUN del server STUN.
Dati provider SIP estesi	
Mostra dati provider SIP estesi	Abilitando questo flag, sono disponibili alcuni parametri di configurazione aggiuntivi per controllare lo stack SIP e adattare il contenuto dei campi dell'intestazione SIP.
CLIP / CLIR	Il sistema fornisce vari parametri per controllare il formato dei campi dell'intestazione SIP in base alle esigenze del trunk nativo È possibile controllare il contenuto dei seguenti campi di intestazione che descrivono l'origine di una chiamata: • Da: DisplayPart <sip:UserPart@HostPart • P-Asserted-Identity: DisplayPart <sip:UserPart@HostPart> • P-Preferred-Identity: DisplayPart <sip:UserPart@HostPart>
CLIP in uscita nell'intestazione From - parte visualizzata	Impostazioni possibili: • Omit: il campo viene omesso • Numero di chiamata: il numero configurato per una stazione. È possibile definire il numero da utilizzare nei "parametri del percorso" • Account: il nome utente assegnato al trunk nativo • nome visualizzato
CLIP in uscita nell'intestazione From - parte utente:	Impostazioni possibili: • Numero di telefono • Account
Intestazione From in uscita - parte dominio/host:	Modificare la parte dominio/host dell'URI con l'indirizzo IP del sistema. Questo parametro influisce sulla parte host di tutti e tre i file di intestazione Da:, PAI e PPI Impostazioni possibili: • nome di dominio • indirizzo IP locale • indirizzo IP pubblico
Diversion: Da contiene il numero chiamante originale:	Se viene stabilita una chiamata in uscita a causa dell'inoltro di chiamata, il sistema può fornire informazioni sull'interlocutore originale. Se abilitato, il sistema invia il chiamante originale (A-Ext) nel campo dell'intestazione From:, altrimenti invia il numero della stazione di inoltro.

Parametri	Descrizione
Diversion: PAI contiene il numero del chiamante originale	Se viene stabilita una chiamata in uscita a causa dell'inoltro di chiamata, il sistema può fornire informazioni sull'interlocutore originale. Se abilitato, il sistema invia il chiamante originale (A-Ext) nel campo dell'intestazione P-Asserted-Id, altrimenti invia il numero della stazione di inoltro. Impostando questo flag, il sistema invia il chiamante originale nel campo di intestazione P-Asserted_ID: e P-Preferred-ID:.
CLIP in uscita nell'intestazione P-Asserted-Id - parte visualizzata:	Impostazioni possibili: • Omit: il campo viene omesso • Numero di chiamata: il numero configurato per una stazione. È possibile definire il numero da utilizzare nei "parametri del percorso" • Account: il nome utente assegnato al trunk nativo • nome visualizzato
CLIP in uscita nell'intestazione P-Asserted-Id - parte utente:	Impostazioni possibili: • Omit: il campo viene omesso • Numero di telefono • Account
CLIP in uscita nell'intestazione P-Preferred-Id - parte visualizzata:	Impostazioni possibili: • Omit: il campo viene omesso • Numero di chiamata: il numero configurato per una stazione. È possibile definire il numero da utilizzare nei "parametri del percorso" • Account: il nome utente assegnato al trunk nativo • nome visualizzato
CLIP in uscita nell'intestazione P-Preferred-Id - parte utente:	Impostazioni possibili: • Omit: il campo viene omesso • Numero di telefono • Account
CLIP in uscita nell'intestazione Diversion - parte visualizzata:	Impostazioni possibili: • Omit: il campo viene omesso • Numero di chiamata: il numero configurato per una stazione. È possibile definire il numero da utilizzare nei "parametri del percorso" • Account: il nome utente assegnato al trunk nativo • nome visualizzato
CLIP in uscita nell'intestazione Diversion - parte utente:	Impostazioni possibili: • Omit: il campo viene omesso • Numero di telefono • Account
CLIP in uscita nell'intestazione History-Info - parte utente:	Impostazioni possibili: • omit • callnumber

Parametri	Descrizione
CLIR in uscita nell'intestazione From - parte visualizzata:	Impostazioni possibili: • Omit • Numero di telefono • Account • Anonimo **From: Anonymous <sip: ...@...>**
CLIR in uscita nell'intestazione From - parte utente:	Impostazioni possibili: • Numero di telefono • Account • Totalmente anonimo**From: ...<sip:anonymous@anonymous.invalid>** • Anonimo per l'utente **From: ... <sip:anonymous@...>**
Intestazione Privacy CLIR in uscita	Impostazioni possibili: • Omit • Id **Privacy: id** • Utente **Privacy: user** • Utente, id **Privacy: user;id**
COLP / TIP supportati per le chiamate in uscita:	In ISDN è stata introdotta la funzione COLP (Connect Line Identification Presentation). In SIP questa funzione viene talvolta definita TIP (Termination Identification Presentation). RFD3324 (sezione 5.) definisce un meccanismo per trasportare l'identità dell'accettante (C) nel campo di intestazione P-Asserted-Identity della risposta 200 OK: Impostazioni possibili: • COLP supportato • COLP non supportato
Formattazione numero di chiamata	
Chiamata in arrivo - Numero del destinatario:	Questo flag si riferisce all'indirizzo di destinazione di una chiamata. Per impostazione predefinita, viene recuperato dal campo **parte utente** del campo **TO: intestazione**. Impostazioni possibili: • Linea di richiesta **INVITE sip: +498970070@...** • Per la parte visualizzata dell'intestazione **To: +498970070 <sip:+** • Per la parte utente dell'intestazione **To: <sip: +498970070@...** • Parte visualizzata dell'intestazione P-Called-Party-Id **P-Called-Party-ID: +498970070 <sip:..** • Parte utente dell'intestazione P-Asserted-Id **P-Called-Party-ID: <sip: +498970070@..**

Parametri	Descrizione
Chiamata in arrivo - Numero del chiamante:	Questo flag si riferisce all'indirizzo di origine di una chiamata. Per impostazione predefinita, il sistema esclude il numero chiamante dalla parte utente dell'intestazione From. Impostazioni possibili: • automatico • Dalla parte visualizzata dell'intestazione **Da: +498970070 <sip:+** • Dalla parte utente dell'intestazione **From: <sip: +498970070@...** • Parte visualizzata dell'intestazione P-Asserted-Id **P-Asserted-ID: +498970070 <sip:..** • Parte utente dell'intestazione P-Called-Party-Id **P-Asserted-ID: <sip: +498970070@..** In modalità automatica, il sistema cerca innanzitutto nella parte utente della P-Asserted-Identity, se presente. Se non è presente la parte P-Asserted-Identity, viene presa la parte utente del campo di intestazione From:.
Chiamata in arrivo - Tipo di numero (chiamante):	Impostazioni possibili: • automatico • internazionale
Chiamata in arrivo - Tipo di numero (chiamato):	Impostazioni possibili: • automatico • internazionale • nazionale
Chiamata in uscita - Tipo di numero (chiamante):	Impostazioni possibili: • automatico • internazionale • nazionale
Chiamata in uscita - Tipo di numero (chiamato):	Impostazioni possibili: • automatico • internazionale • nazionale
Mappatura del numero del provider:	Impostazioni possibili: • in qualsiasi caso • Solo chiamate in entrata (se configurato) • off

Parametri	Descrizione
CLIP senza supporto screening:	Impostazioni possibili: • non supportato • CLIP in From / numero attendibile in PAI • Supportato - Nessun trattamento speciale • CLIP in Da / Numero DID in PAI
Numero di chiamata con prefisso internazionale/nazionale:	Impostazioni possibili: • no • sì
Numero di chiamata in formato E164:	Impostazioni possibili: • no • sì
Ottimizzazione del percorso:	Impostazioni possibili: • non consentito • consentito • consentito (IP locale in Contatto)
Supporto MEX:	Impostazioni possibili: • no • sì
L'URI di contatto contiene:	Questo parametro viene utilizzato per configurare il contenuto della parte utente dell'URL del contatto **Contact: sip:UserPart@HostPart:port** Impostazioni possibili: • Numero di chiamata: la parte utente dell'URI del contatto contiene il numero di chiamata • AOR di registrazione: l'URI di contatto contiene la parte account=utente della registrazione.
Porta TCP utilizzata nell'URI del contatto:	Questo parametro è utilizzato per configurare la porta tcp utilizzata nella parte host del contatto-URI **Contact: sip:UserPart@HostPart:port** Impostazioni possibili: • ephem.src-port: Per impostazione predefinita, viene utilizzata la porta effimera tcp src • Porta server SIP: La porta del server SIP viene utilizzata nell'URL del contatto
Registrazione	
Il contatto registrato contiene un indirizzo IP:	Impostazioni possibili: • localIPAddr • domainName
ContactUriWithProtocol:	attivazione/disattivazione

Parametri	Descrizione
Registrazione BNC (SIPconnect):	Impostazioni possibili: • registrazione normale • Registrazione BNC
Intervallo di riregistrazione dopo il fallimento (sec):	
Modalità di riregistrazione:	Impostazioni possibili: • continua • SIPConnect
Intervallo di riregistrazione dopo il fallimento:	Impostazioni possibili: • CallFailureIsNoRegFailure • CallFailureIsRegFailure
Sicurezza	
Modo UDP:	Impostazioni possibili: • UDP simmetrico • UDP asimmetrico
Selezione Peer approvata:	Impostazioni possibili: • considera affidabili solo i server configurati • considera affidabili i server ricevuti nelle risposte SIP
Varie	
Carico diretto:	Per una connessione ITSP diretta, questo parametro DEVE essere impostato su falso. Se si utilizza un SBC esterno davanti a OpenScape Business, questo parametro è impostato su vero.
Evitare la rinegoziazione dei media:	Per una connessione ITSP diretta, questo parametro DEVE essere impostato su vero. Se il carico diretto del parametro di gestione dei supporti è impostato su vero, questo parametro non ha alcun effetto. (ad esempio, nei casi in cui si utilizza un SBC esterno davanti al sistema OpenScape Business)
Cambiamento dell'attributo di direzione:	Impostazioni possibili: • mantieni attributo • cambia in sendrecv
Attributo di soppressione del silenzio:	Impostazioni possibili: • supportato • non supportato
Estensione Mediasec:	Impostazioni possibili: • supportato • non supportato

Parametri	Descrizione
Filtro SDP:	Impostazioni possibili: • predefinito • profilo di compatibilità • Apri
UseRouteURIAuthentication:	Vero imposta il comportamento per l'uso dell'URI del percorso invece dell'URI della richiesta nell'intestazione (Proxy-) Autorizzazione per INVITE o INFO (non per REGISTER). L'URI di richiesta sarà usato quando non è presente un URI del percorso. Per gli ITSP questo parametro DEVE essere impostato su vero.
Ignora 100 Rel:	Ignora un campo di intestazione "Supportato": "100rel" se ricevuto in INVITE. Poiché 100rel può interferire con l'interworking per gli abbonati non-SIP, questo parametro DEVE essere impostato su vero
Supporta 100rel	Se si imposta questo flag, il sistema aggiunge un'intestazione 100rel supportato nell'invito in uscita. Ciò consentirà all'ITSP di inviare risposte provvisorie affidabili seguite da messaggi UPDATE. Questo parametro è utilizzabile senza limitazioni per la famiglia di schede madri e server OpenScape Business V3.
UseViaRPort:	Se impostato su vero, il parametro rport viene aggiunto a Via-Header. *Tramite: SIP/2.0/UDP 192.168.138.1:5060;rport;* Se impostato su falso, non viene aggiunto alcun parametro rport a Via-Header. *Tramite: SIP/2.0/UDP 192.168.138.1:5060;*
UPDATE supportato:	Se impostato su vero, UPDATE viene utilizzato in base al contenuto del campo di intestazione Consenti. Se UPDATE non è impostato nel campo di intestazione Consenti ricevuto, lo stack SIP non invia mai un UPDATE. Se impostato su falso, il metodo UPDATE non verrà mai utilizzato (al suo posto verrà utilizzato un re-INVITE) Per ITSP questo parametro DEVE essere impostato su vero (valore predefinito)
Supporto intestazione P-Early-Media:	Impostazioni possibili: • non supportato • supportato
Supporto timer sessione:	Impostazioni possibili: • non attivato • aggiornamento criterio remoto

Parametri	Descrizione
Invio automatico timer di risposta 183 (sec):	Con questo timer viene attivata una risposta provvisoria (183) dopo il timeout se non sono disponibili informazioni sull'avanzamento dal sistema. Questo è necessario perché alcune piattaforme non interrompono i timer di supervisione quando ricevono un tentativo di 100 (ad esempio, Broadsoft) 0 non viene inviata alcuna risposta automatica; tutte le risposte sono attivate dal sistema 1-10 timeout in secondi, il timer viene avviato alla ricezione di una richiesta INVITE dall'ITSP. Alla scadenza del timer, lo stack SIP invia un 183 0 (valore predefinito)
Mantenimento UDP:	Impostazioni possibili: • UdpKeepAliveON • UdpKeepAliveOFF • SendAliveOptions
Intervallo di mantenimento per OPTIONS (sec):	Con questo parametro si definisce l'intervallo per l'invio di SIP OPTIONS 60 (valore predefinito)
Registrazione su errore OPTIONS:	Impostazioni possibili: • NoRegisterOnFailure • RegisterOnFailure
Risposta a OPTIONS:	Impostazioni possibili: • Risposta completa • Senza corpo
Pulsanti	
Riavvia ITSP	Avvia una nuova registrazione con l'ITSP (possibile solo con un ITSP attivato).

Descrizione dei parametri delle schede:

- **Modifica configurazione STUN**

Parametri	Descrizione
Modalità STUN	Questa impostazione si applica globalmente a tutti gli ITSP, purché STUN sia abilitato per loro. La necessità o meno di STUN dipende dall'infrastruttura ITSP e dal router Internet utilizzato. STUN non è necessario se l'ITSP risolve l'attraversamento del NAT sulla propria rete. STUN garantisce che nei messaggi SIP venga utilizzato l'indirizzo IP accessibile al pubblico anziché l'indirizzo IP interno.
Modalità STUN: Sempre	STUN è sempre attivo.
Modalità STUN: Automatico	Il tipo di NAT del router verso Internet viene controllato automaticamente. Se STUN è richiesto, viene abilitato. Se non è richiesto o possibile nessun STUN, quest'ultimo è disabilitato. Questa è l'impostazione predefinita consigliata.

Parametri	Descrizione
Modalità STUN: Usa IP statico	Se l'ITSP richiede l'autenticazione IP statica, è necessario un indirizzo IP statico (indirizzo IP pubblico) nel modem DSL o nel router Internet. È necessario specificare anche l'indirizzo IP statico e la porta.
Modalità STUN: Usa IP statico, indirizzo IP pubblico	Indirizzo IP statico del modem DSL o del router Internet.
Modalità STUN: Usa IP statico, porta SIP pubblica	Porta del modem DSL o del router Internet.
Modalità STUN: Router con conservazione delle porte	Se nessuna delle modalità STUN menzionate in precedenza funziona, è opportuno provare questa modalità. Alcuni modem e router Internet non modificano la porta RTP per NAT e necessitano di questa modalità per il corretto funzionamento.
Tipo Nat rilevato	Se è attivo un ITSP, il tipo di NAT viene visualizzato qui.
Porta server STUN predefinita	
Indirizzo IP/Nome host	Indirizzo IP o nome host del server STUN (ad es. `stun.serviceprovider.com`). Questo server STUN viene utilizzato per SIP@Home quando non viene utilizzato alcun ITSP o se l'ITSP utilizzato non offre alcun server STUN.
Porta	Numero di porta del server STUN (ad es. `3478`)

Descrizione dei parametri delle schede:

- **Rilevamento del tipo NAT**

Parametri	Descrizione
Attivazione automatica	Abilita il rilevamento automatico del tipo di NAT.
Avvia rilevamento tipo di NAT	Avvia il rilevamento manuale del tipo NAT.

Descrizione dei parametri delle schede:

- **Aggiungi stazione di telefonia Internet**
- **Modifica stazione di telefonia Internet**
- **Elimina stazione di telefonia Internet**

Parametri	Descrizione
Stazione di telefonia Internet	Dati di accesso dell'account assegnato dall'ITSP. In base all'ITSP, possono venire utilizzati termini diversi, ad esempio: Utente SIP, ID SIP, ecc. Potrebbe essere necessario inserire qui anche il numero di cliente ITSP. Se si utilizza l'autenticazione IP statica, il numero del PABX deve essere inserito qui.
Nome autorizzazione	Nome dell'autorizzazione assegnato dall'ITSP. Spesso è identico all'abbonato alla telefonia via Internet.
Password	Password assegnata dall'ITSP. In base all'ITSP, possono venire utilizzati termini diversi, ad esempio: Password, Password SIP, ecc.
Conferma password	Password assegnata dall'ITSP. In base all'ITSP, possono venire utilizzati termini diversi, ad esempio: Password, Password SIP, ecc.

Descrizione dei parametri delle schede:

- **Aggiungi voce MSN**
- **Modifica voce MSN**
- **Elimina voce MSN**
- **Elimina tutte le voci MSN**

Parametri	Descrizione
Numero di telefono della telefonia Internet / **Numero di telefono della telefonia Internet** / **Numero di telefono della telefonia Internet**	(Singolo) Numero di chiamata assegnato dall'ITSP.
DID / **Numero di chiamata interno**	Numero di chiamata interno assegnato.
Voce predefinita	L'attivazione come voce predefinita consente agli utenti che non dispongono di un proprio numero telefonico di telefonia via Internet di effettuare chiamate tramite questo numero. L'opzione può essere selezionata solo per un MSN. (solo per il supporto alle chiamate vocali, non per il fax)
Stazione di telefonia Internet / **Stazione di telefonia Internet**	Visualizza la stazione di telefonia Internet

Descrizione dei parametri delle schede:

- **Aggiungi intervallo DID**
- **Modifica intervallo DID**
- **Elimina intervallo DID**

Parametri	Descrizione
Numero PABX	Numero di testa assegnato dall'ITSP (senza numero DID)
Banda telefonica diretta da ... a	Gamma di numeri DID assegnati dall'ITSP
Inizio dell'intervallo del numero di chiamata interno	Primo numero interno per il quale si desidera l'assegnazione automatica dei numeri di chiamata.
Assegna automaticamente la banda di selezione diretta alle stazioni	Se selezionato, i numeri DID vengono assegnati automaticamente in ordine crescente ai numeri di chiamata interni e vengono generate le voci MSN corrispondenti.

28.3.6.6 Gateway voce > Servizi di rete > Nodi

Descrizione dei parametri delle schede:

- **Aggiungi nodo di rete**
- **Modifica nodo di rete**
- **Elimina nodo di rete**

Parametri	Descrizione
ID nodo	Solo per la configurazione manuale senza procedura guidata, ad esempio con numerazione aperta: indicazione di un numero di nodo univoco sul sistema di reti.

Parametri	Descrizione
indirizzo IP	Solo per la configurazione manuale senza procedura guidata, ad esempio con numerazione aperta: indirizzo IP del nodo
Monitoraggio del nodo	Selezionando il monitoraggio dei nodi viene effettuato un controllo periodico della comunicazione con il nodo. A tal fine è necessario che il monitoraggio del nodo sia attivato anche nell'altro nodo.
Livello di sicurezza della crittografia dei nodi	Selezionando l'opzione "sicuro" viene attivata la crittografia per la comunicazione vocale con il nodo. A questo scopo, nel sistema occorre configurare la "Crittografia segnalazione e payload (SPE)". Valori consentiti: tradizionale, sicuro

28.3.6.7 Gateway voce > Servizi di rete > Routing

Descrizione dei parametri delle schede:

- **Aggiungi numero di telefono**
- **Cancella tutti i numeri di telefono**

Parametri	Descrizione
ID nodo	Scelta del numero del nodo
Numero di telefono	Solo per la configurazione manuale senza procedura guidata, ad esempio con numerazione aperta: indicazione del codice tramite il quale il nodo è raggiungibile.

28.3.6.8 Gateway voce > Interconnessione SIPQ

Con una connessione SIP-Q vengono definiti i parametri per due possibili fasci SIP-Q esterni. Tramite questi percorsi è possibile collegare qualsiasi server SIP esterno, ad esempio OpenScape 4000 o OpenScape Voice. Esempi corrispondenti sono riportati nei modelli disponibili.

Descrizione dei parametri delle schede:

- **Aggiungi interconnessione SIPQ**
- **Modifica interconnessione SIPQ**
- **Elimina interconnessione SIPQ**

Parametri	Descrizione
Modello base	Modelli che devono essere utilizzati come base.
Servizio	Nome del server SIP esterno (nome modello).
Abilita linea	La connessione al server SIP esterno è stata attivata. Valore predefinito: disattivato
Identificativo linea nel sistema	Selezione tra due connessioni SIP-Q esterne. Se presente, una delle seguenti connessioni SIPQ è sempre occupata dalla UC Booster Card o dall'UC Booster Server.

Parametri	Descrizione
Nome dominio remoto	Nome dell'host o indirizzo IP del server SIP esterno. Il valore è normalmente identico a quello inserito in **Indirizzo IP/Nome dell'host**.
Server SIP	
Indirizzo IP/nome dell'host	Nome dell'host o indirizzo IP del server SIP esterno.
Porta	Porta SIP del server SIP esterno. Valori consentiti: 0 o 1024-65535, valore predefinito: 5060
Trasporto sicuro	In caso di collegamento a OpenScape 4000 e OpenScape Voice, è possibile attivare la segnalazione SIP crittografata (funzione Crittografia segnalazione e payload, SPE). Valore predefinito: disattivato
Registrar SIP	
Utilizza registrar del provider	Il server SIP esterno richiede una registrazione. Valore predefinito: disattivato
Indirizzo IP/nome dell'host	Nome host o indirizzo IP del server Registrar.
Porta	Numero di porta del server Registrar. Valori consentiti: 0 o 1024-65535, valore predefinito: 5060
Intervallo di riregistrazione (sec.)	Intervallo (in secondi) entro il quale viene ripetuta la registrazione. Valori consentiti: da 30 a 86400, valore predefinito: 300
Outbound Proxy/Inbound Proxy	
Usa Outbound/Inbound Proxy del provider	Attivazione del proxy in uscita: alcuni scenari di ridondanza (ad esempio con OpenScape Branch Proxy) richiedono l'elaborazione della segnalazione SIP tramite un proxy in uscita. Attivazione del proxy in entrata: in scenari di ridondanza specifici (ad esempio con OpenScape Voice), la segnalazione proviene da un server SIP separato (proxy in entrata). Valore predefinito: sempre disattivato
Indirizzo IP/nome dell'host	Nome host o indirizzo IP del proxy outbound o inbound.
Porta	Numero di porta del proxy outbound o inbound. Valori consentiti: 0 o 1024-65535

Descrizione dei parametri delle schede:

- **Aggiungi utente interconnessione SIPQ**
- **Modifica utente interconnessione SIPQ**
- **Elimina utente interconnessione SIPQ**

Parametri	Descrizione
UserId	Immissione dell'ID utente per l'accesso al server SIP.

Parametri	Descrizione
Nome di autorizzazione/Realm	Immissione del nome di autorizzazione o del Realm per l'accesso al server SIP.
Password	Immissione della password per l'accesso al server SIP.
Conferma password	Ripetizione della password per l'accesso al server SIP.

28.3.6.9 Gateway Voce > Linea server SIP nativo

Qui vengono definiti i parametri per le 10 potenziali linee SIP native. Tramite queste linee è possibile connettere qualsiasi server SIP esterno.

Descrizione dei parametri delle schede:

- **Aggiungi linea server SIP nativo**
- **Modifica trunk server SIP nativo**
- **Elimina trunk server SIP nativo**

Parametri	Descrizione
Modello base	Modello da usare come base.
Nome trunk	Nome del server SIP esterno (nome modello).
Trunk abilitato	La connessione con il server SIP esterno è attivata. Valore predefinito: disattivato
Identificatore trunk nel sistema	Possibilità di scegliere tra 10 connessioni SIP native esterne. Gli elementi disattivati sono occupati dagli ITSP già configurati (max 8 ITSP possibili, in questo caso rimangono 2 connessioni SIP native).
Nome del dominio remoto	Nome host o indirizzo IP del server SIP esterno. Questo valore è, in genere, identico al valore **Indirizzo IP/Nome host**. Esempio: Il **Nome del dominio remoto** viene usato nella parte host dei campi Da e PPI/PAI-Header (vedere di seguito): Da: sip: +49...@NomeDominio P-Asserted-Identity: sip: +49...@NomeDominio
Protocollo di trasporto	Selezione del protocollo UDP o TCP.
Sicurezza del trasporto	Selezionare tra UDP o TCP tradizione e TLS sicuro.

Parametri	Descrizione
Sicurezza media	Selezionare tra Solo RTP, Solo SDES e DTLS-SRTP. DTLS-SRTP è un protocollo che combina Datagram Transport Layer Security (DTLS) con Secure Real-time Transport Protocol (SRTP) per fornire streaming media crittografati e autenticati su Internet. **Nota:** Nelle nuove implementazione (dalla V3R4 in poi), l'opzione predefinita è DTLS-SRTP. Se su cambia da Solo RT o Solo SDES DTLS-SRTP, è necessario riavviare il trunk affinché la modifica abbia effetto. **Nota:** Le impostazioni restrittive dei firewall potrebbero provocare problemi di payload vocale sporadici o permanenti. In questo caso, disabilitare l'opzione DTLS-SRTP.
Server SIP	
Indirizzo IP/Nome host	Nome host o indirizzo IP del server SIP esterno.
Porta	Porta SIP del server SIP esterno. Valore predefinito: 5060, inserire la porta 0 se l'ITSP utilizza DNSSRV
Registrar SIP	
Usa Registrar	Deve essere selezionato se il trunk funziona con la registrazione (valore predefinito = off)
Indirizzo IP/Nome host	Nome host o indirizzo IP del server registrar esterno
Porta	Porta del server registrar esterno valore predefinito: 5060, inserire la porta 0 se si utilizza DNSSRV
Intervallo nuova registrazione	L'intervallo con cui viene ripetuta una registrazione (valore predefinito = 600)
Server STUN	
Usa STUN	Deve essere selezionato se il trunk funziona con STUN (valore predefinito = off)
Indirizzo IP/Nome host	Nome host o indirizzo IP del server STUN
Porta	Porta del server STUN
Dati SIP estesi	
Mostra dati SIP estesi	Abilitando questo flag, diventano disponibili parametri di configurazione aggiuntivi per controllare lo stack SIP e adattare il contenuto dei campi di intestazione SIP

Parametri	Descrizione
CLIP/CLIR	Il sistema offre vari parametri per controllare il formato dei campi di intestazione SIP, a seconda delle necessità del trunk nativo È possibile controllare il contenuto dei seguenti campi di intestazione, che descrivono l'origine di una chiamata: • Da: DisplayPart <sip:UserPart@HostPart • P-Asserted-Identity: DisplayPart <sip:UserPart@HostPart> • P-Preferred-Identity: DisplayPart <sip:UserPart@HostPart>
CLIP in uscita nell'intestazione Da - parte visualizzata	Impostazioni possibili: • Ometti: il campo viene omesso • Numero di chiamata: il numero configurato per una stazione. È possibile definire quale numero usare nei "parametri di instradamento" • Account: il nome utente assegnato al trunk nativo • nome visualizzato
CLIP in uscita nell'intestazione Da - parte utente:	Impostazioni possibili: • Numero di telefono • Account
In uscita dall'intestazione - parte dominio/host:	Cambiare la parte dominio/host dell'URI da compilare con l'indirizzo IP del sistema. Il parametro influisce sulla parte host di tutti e tre i campi di intestazione Da:, PAI e PPI Impostazioni possibili: • nome del dominio • indirizzo IP locale • indirizzo IP pubblico
Deviazione: Da contiene il numero del chiamante originale:	Se viene stabilita una chiamata in uscita a causa dei un inoltro di chiamata, il sistema può fornire informazioni sul chiamante. Se è impostato su Vero, il sistema invia il chiamate originale (A-Ext) nel campo intestazione Da:, altrimenti invia il numero della stazione di inoltro.
Deviazione: PAI contiene il numero del chiamante originale	Se viene stabilita una chiamata in uscita a causa dei un inoltro di chiamata, il sistema può fornire informazioni sul chiamante. Se è impostato su Vero, il sistema invia il chiamate originale (A-Ext) nel File intestazione P-Asserted-Id, altrimenti invia il numero della stazione di inoltro. Impostando questo flag, il sistema invia il chiamante originale nei campi intestazione P-Asserted_ID: e P-Preferred-ID:.
CLIP in uscita nell'intestazione P-Asserted-Id - parte visualizzata:	Impostazioni possibili: • Ometti: il campo viene omesso • Numero di chiamata: il numero configurato per una stazione. È possibile definire quale numero usare nei "parametri di instradamento" • Account: il nome utente assegnato al trunk nativo • nome visualizzato

Parametri	Descrizione
CLIP in uscita nell'intestazione P-Asserted-Id - parte utente:	Impostazioni possibili: • Ometti: il campo viene omesso • Numero di telefono • Account
CLIP in uscita nell'intestazione P-Preferred-Id - parte visualizzata:	Impostazioni possibili: • Ometti: il campo viene omesso • Numero di chiamata: il numero configurato per una stazione. È possibile definire quale numero usare nei "parametri di instradamento" • Account: il nome utente assegnato al trunk nativo • nome visualizzato
CLIP in uscita nell'intestazione P-Preferred-Id - parte utente:	Impostazioni possibili: • Ometti: il campo viene omesso • Numero di telefono • Account
CLIP in uscita nell'intestazione Deviazione - parte visualizzata:	Impostazioni possibili: • Ometti: il campo viene omesso • Numero di chiamata: il numero configurato per una stazione. È possibile definire quale numero usare nei "parametri di instradamento" • Account: il nome utente assegnato al trunk nativo • nome visualizzato
CLIP in uscita nell'intestazione Deviazione - parte utente:	Impostazioni possibili: • Ometti: il campo viene omesso • Numero di telefono • Account
CLIP in uscita nell'intestazione History-Info - parte utente:	Impostazioni possibili: • ometti • numero chiamata
CLIR in uscita nell'intestazione Da - parte visualizzata:	Impostazioni possibili: • Ometti • Numero di telefono • Account • Anonimo **From: Anonimo <sip: ...@...>**
CLIR in uscita nell'intestazione Da - parte utente:	Impostazioni possibili: • Numero di telefono • Account • Totalmente anonimo**From: ...<sip:anonymous@anonymous.invalid>** • Anonimo per l'utente **Da: ... <sip:anonymous@...>**
CLIR in uscita intestazione Privacy	Impostazioni possibili: • Ometti • Id **Privacy: id** • Utente **Privacy: user** • Utente, id **Privacy: user;id**

Parametri	Descrizione
COLP/TIP supportati per le chiamate in uscita:	In ISDN è stata introdotta la funzione COLP (Connect Line Identification Presentation). In SIP questa funzione viene indicata, a volte, come TIP (Termination Identification Presentation). RFD3324 (sezione 5.) definisce un meccanismo per trasportare l'identità della parte che accetta (C) nel campo dell'intestazione P-Asserted-Identity della risposta 200 OK: Impostazioni possibili: • COLP supportato • COLP non supportato
Formattazione dei numeri di telefono	
Chiamata in entrata - Numero dell'utente chiamato:	Questo flag si riferisce all'indirizzo di destinazione di una chiamata. Per impostazione predefinita, viene recuperato dalla **parte utente** del campo **A: intestazione**. Impostazioni possibili: • Linea richiesta **INVITE sip: +498970070@...** • Per la parte visualizzata dell'intestazione **To: +498970070 <sip:+** • Per la parte utente dell'intestazione **To: <sip: +498970070@...** • Parte visualizzata dell'intestazione P-Called-Party-Id **P-Called-Party-ID: +498970070 <sip:..** • Parte utente dell'intestazione P-Called-Party-Id **P-Called-Party-ID: <sip: +498970070@..**
Chiamata in entrata - Numero del chiamante:	Questo flag si riferisce all'indirizzo di origine di una chiamata. Per impostazione predefinita, il sistema estrae il chiamante dalla parte utente dell'intestazione Da. Impostazioni possibili: • automatico • Parte visualizzata dell'intestazione Da **Da: +498970070 <sip:+** • Parte utente dell'intestazione Da **Da: <sip: +498970070@...** • Parte visualizzata dell'intestazione P-Asserted-Id **P-Asserted-ID: +498970070 <sip:..** • Parte utente dell'intestazione P-Asserted-Id **P-Asserted-ID: <sip: +498970070@..** Il modalità automatica, il sistema cerca prima nella parte utente di P-Asserted-Id entity, se presente. Se P-Asserted-Identity non è presente, viene usata la parte utente del campo di intestazione Da:.

Parametri	Descrizione
URI contatto contiene:	Questo parametro viene usato per configurare il contenuto della parte utente dell'URI del contatto **Contact: sip:UserPart@HostPart:port** Impostazioni possibili: • Numero di chiamata: la parte utente dell'URI del contatto contiene il numero di chiamata • AOR registrazione: l'URI del contatto contiene la parte account=utente della registrazione.
Porta TCP usata nell'URI del contatto:	questo parametri viene usato per configurare la porta-tcp usata nella parte host dell'URI del contatto **Contact: sip:UserPart@HostPart:port** Impostazioni possibili: • ephem.src-port: Per impostazione predefinita, viene usata la porta tcp src effimera • Porta server SIP: La porta del server SIP viene usata nell'URI del contatto

Descrizione dei parametri delle schede:

- **Aggiungi utente trunk server SIP nativo**
- **Modifica utente trunk server SIP nativo**
- **Elimina utente trunk server SIP nativo**

Parametri	Descrizione
UserId	Inserimento dell'ID utente per l'accesso al server SIP.
Nome autorizzazione	Inserimento del nome dell'autorizzazione per l'accesso al server SIP.
Password	Inserimento della password per l'accesso al server SIP.
Conferma password	Ripetizione della password per l'accesso al server SIP.

28.3.7 Utenti

In **Utente** sono riunite le funzioni relative agli utenti. Fra queste, Nome e Numero di telefono dell'utente e la programmazione tasti.

28.3.7.1 Utente > Utente > Utenti UP0

Descrizione dei parametri delle schede:

- **Modifica utente**

Parametri	Descrizione
N. chiamata	Numero di telefono interno dell'utente.
DID	MSN (Interno) dell'utente.

Parametri	Descrizione
Nome	Nome proprio dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Cognome	Cognome dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Visualizza	Nome dell'utente liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri
Servizio	Nome dell'utente liberamente scelto. Valori consentiti: max. 16 caratteri
Clip/Lin	Sequenza di cifre che viene mostrata per le chiamate esterne in uscita alla destinazione chiamata al posto del numero di telefono effettivo (ad esempio, per i servizi di emergenza E911 negli USA) Valori consentiti: max. 16 cifre
In funzione	Indica se l'utente è operativo.
Tipo di dispositivo	Consente di visualizzare il terminale associato all'utente.
Numero di telefono fax	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'interno.
Selezione passante fax	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'esterno.
Accesso	Visualizzazione della porta fisica a cui è collegato il terminale.
ID Loc ITSP	L'ID posizione ITSP per un utente.
Cerca	È anche possibile visualizzare gli utenti selezionati inserendo nei campi **Cerca** il testo da cercare e confermando con il tasto Invio. Vengono visualizzati gli utenti che corrispondono al termine ricercato. Se tutti i campi **Cerca** vengono lasciati vuoti e si preme il tasto Invio, verranno elencati tutti gli utenti.
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.
Pulsanti	
Freccia blu nella colonna **N. chiamata**	Richiama la pagina con la scheda **Modifica i parametri dell'utente**, **Modifica i flag dell'utente**, **Modifica i dati del WorkPoint Client** e **Modifica Gruppi/ Inoltro**.
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

Descrizione dei parametri delle schede:

- **Master/slave UP0**

  Questa scheda è presente solo in OpenScape Business X8, poiché con questo sistema le porte slave vengono gestite in modo dinamico. OpenScape Business X1/X3/X5 sono assegnati in modo fisso alle porte slave.

Parametri	Descrizione
N. chiamata	Numero di telefono interno dell'utente.
DID	MSN (Interno) dell'utente.
Servizio	Nome dell'utente liberamente scelto. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Accesso	Visualizzazione della porta fisica a cui è collegato il terminale.
Aggiungi slave	Se si seleziona questa casella di controllo, alla porta master selezionata viene assegnata in via preliminare una porta slave. Dopo aver salvato la selezione con **Applica** è possibile configurare anticipatamente l'interno e il nome del telefono di sistema slave. Se successivamente all'adattatore slave del telefono di sistema master viene collegato il telefono di sistema slave, questo viene assegnato alla porta slave precedentemente selezionata. Se il telefono di sistema slave viene collegato senza porta slave predefinita, si utilizza automaticamente la porta libera successiva (a partire dalla porta 384).
Cancella slave	Se si seleziona questa casella di controllo, la preconfigurazione del telefono di sistema slave viene eliminata. Se un telefono di sistema slave è collegato all'adattatore slave del telefono di sistema master, la casella di controllo diventa ombreggiata. La preconfigurazione non può essere eliminata.
Cerca	È anche possibile visualizzare gli utenti selezionati inserendo nei campi **Cerca** il testo da cercare e confermando con il tasto Invio. Vengono visualizzati gli utenti che corrispondono al termine ricercato. Se tutti i campi **Cerca** vengono lasciati vuoti e si preme il tasto Invio, verranno elencati tutti gli utenti.
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.
Pulsanti	
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

Descrizione dei parametri delle schede:

- **Info terminale**

Parametri	Descrizione
N. chiamata	Numero di telefono interno dell'utente.
Servizio	Nome dell'utente.

Parametri	Descrizione
Tipo di dispositivo	Visualizzazione del terminale associato all'utente.
Versione software corrente	Versione Software del terminale assegnato (se disponibile).
Versione HW	Versione hardware del terminale assegnato (se disponibile).
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.
Pulsanti	
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

28.3.7.2 Stazione > Stazione > Client IP

Descrizione dei parametri delle schede:

- **Modifica abbonato**

Parametri	Descrizione
N. di chiamata	Numero di telefono interno dell'utente.
DID	MSN (Interno) dell'utente.
Nome	Nome proprio dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Cognome	Cognome dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Visualizzazione	Nome dell'utente liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Tipo	Tipo di utente.
Tipo: **Nessuna porta**	Questo numero di chiamata non è ancora stato assegnato a nessuna stazione.
Tipo: **Client di sistema**	Un client di sistema è una stazione IP in grado di utilizzare tutte le funzionalità del sistema di comunicazione tramite CorNet-IP (precedentemente denominato client di sistema HFA)
Tipo: **Utente RAS**	A un utente RAS (utente del servizio di accesso remoto) viene concesso l'accesso Internet alla rete IP tramite la connessione ISDN. Ciò consente di effettuare la manutenzione e la licenza del sistema di comunicazione da remoto.

Parametri	Descrizione
Tipo: **Client SIP**	Un client SIP è una stazione IP che utilizza il protocollo SIP. Può accedere solo a funzionalità limitate del sistema di comunicazione tramite SIP.
Tipo: **Utente Deskshare**	Un utente Deskshare è un utente IP che può effettuare l'accesso a un altro telefono del sistema IP (accesso mobile) e quindi utilizzare questo telefono come se fosse il proprio (compreso il numero di telefono).
Clip/Lin	Sequenza di cifre che viene mostrata per le chiamate esterne in uscita alla destinazione chiamata al posto del numero di telefono effettivo (ad esempio, per i servizi di emergenza E911 negli USA)
Attivo	Indica se la stazione è operativa.
Numero fax	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'interno.
DID fax	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'esterno.
ITSP Loc-ID	L'ID della posizione ITSP di una stazione.
Cerca	È anche possibile visualizzare gli abbonati selezionati inserendo un termine di ricerca nei campi di **ricerca** e premendo il tasto Invio. Vengono visualizzati gli abbonati che corrispondono al termine di ricerca. Se si lasciano vuoti tutti i campi di **ricerca** si preme il tasto Invio, verranno nuovamente elencati tutti gli abbonati.
Elementi per pagina	Selezione per determinare se visualizzare 10, 25, 50 o 100 elementi per pagina.
Pulsanti	
Freccia blu nella colonna **N. di chiamata**	Apre la pagina con le schede **Modifica i parametri della stazione**, **Modifica i flag della stazione**, **Modifica i dati del WorkPoint Client** e **Modifica Gruppo/Inoltro di chiamata**.
>	Permette di passare alla pagina successiva.
<	Permette di tornare indietro di una pagina.
>|	Permette di spostarsi alla fine dell'elenco.
|<	Permette di spostarsi all'inizio dell'elenco.

Descrizione dei parametri delle schede:

- **Info terminale**

Tenere presente che l'ordinamento è rigorosamente alfabetico per tutte le colonne. Non esiste un ordinamento numerico specifico per colonna, per tipi di dati specifici come **Indirizzo IP** o **Versione SW attuale**.

Parametri	Descrizione
N. di chiamata	Numero di telefono interno dell'utente.
Visualizzazione	Nome della stazione.
Tipo di dispositivo	Consente di visualizzare il tipo di dispositivo associato alla stazione.

Parametri	Descrizione
Indirizzo IP	Indirizzo IP del dispositivo associato; collegamento diretto al WBM del telefono IP
Indirizzo MAC	Indirizzo MAC del telefono associato
Versione SW attuale	Versione software del dispositivo associato (se disponibile).
Versione HW	Versione hardware del dispositivo associato (se disponibile).
Porta PC	Se questo flag è attivato, la porta Ethernet del PC di tutti i telefoni di sistema attivi è attivata. Impostazione predefinita: funzione disattivata
Impostazioni codec	Se questo flag è attivato, per tutti i telefoni di sistema si applica la seguente priorità codec: G.729 - G.711 - G.722 Se questo flag è disattivato, si applica la seguente priorità codec: G.722 - G.711 - G.729 **Nota:** CP100 non supporta G.722 Impostazione predefinita: funzione disattivata
Elementi per pagina	Selezione per determinare se visualizzare 10, 25, 50 o 100 elementi per pagina.
Pulsanti	
>	Permette di passare alla pagina successiva.
<	Permette di tornare indietro di una pagina.
>|	Permette di spostarsi alla fine dell'elenco.
|<	Permette di spostarsi all'inizio dell'elenco.

Descrizione dei parametri delle schede:

- **Gateway secondario**

Parametri	Descrizione
Numero di telefono	Numero di telefono interno dell'utente.
Nome	Nome della stazione.
ID nodo	A ogni nodo di un sistema in rete deve essere assegnato un ID nodo univoco. Ciò consente di identificare in modo univoco i singoli nodi in un sistema collegato in rete.
Telefonia di fallback	Indica se la funzione è attivata.
Chiamata di fallback	Il numero di chiamata della stazione che verrà utilizzato in caso di errore.
Chiamata di fallback senza DID	Il numero di chiamata interno della stazione che verrà utilizzato in caso di errore.

Descrizione dei parametri delle schede:

- **Hosting di fallback**

Parametri	Descrizione
Numero di telefono	Numero di telefono interno dell'utente.
Nome	Nome della stazione.
ID nodo primario	L'ID nodo univoco sul quale la stazione è originariamente configurata.
Chiamata di fallback	Il numero di chiamata della stazione che verrà utilizzato in caso di errore.
Chiamata di fallback senza DID	Il numero di chiamata interno della stazione che verrà utilizzato in caso di errore

28.3.7.3 Utente > Utente > Utenti analogici

Descrizione dei parametri delle schede:

- **Modifica utente**

Parametri	Descrizione
N. chiamata	Numero di telefono interno dell'utente. **Nota:** I numeri di chiamata che iniziano con un asterisco (*) non possono essere utilizzati come destinazioni di fax.
DID	MSN (Interno) dell'utente.
Nome	Nome proprio dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Cognome	Cognome dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Visualizza	Nome dell'utente liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Clip/Lin	Sequenza di cifre che viene mostrata per le chiamate esterne in uscita alla destinazione chiamata al posto del numero di telefono effettivo (ad esempio, per i servizi di emergenza E911 negli USA) Valori consentiti: max. 16 cifre
In funzione	Indica se l'utente è operativo.
Tipo di dispositivo	Consente di visualizzare il terminale associato all'utente.

Parametri	Descrizione
Numero di telefono fax	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'interno.
Selezione passante fax	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'esterno.
Accesso	Visualizzazione della porta fisica a cui è collegato il terminale.
ID Loc ITSP	L'ID posizione ITSP per un utente.
Cerca	È anche possibile visualizzare gli utenti selezionati inserendo nei campi **Cerca** il testo da cercare e confermando con il tasto Invio. Vengono visualizzati gli utenti che corrispondono al termine ricercato. Se tutti i campi **Cerca** vengono lasciati vuoti e si preme il tasto Invio, verranno elencati tutti gli utenti.
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.
Pulsanti	
Freccia blu nella colonna **N. chiamata**	Richiama la pagina con la scheda **Modifica i parametri dell'utente**, **Modifica i flag dell'utente**, **Modifica i dati del WorkPoint Client** e **Modifica Gruppi/ Inoltro**.
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

28.3.7.4 Utente > Utente > Utenti ISDN

Descrizione dei parametri delle schede:

- **Modifica utente**

Parametri	Descrizione
N. chiamata	Numero di telefono interno dell'utente.
DID	MSN (Interno) dell'utente.
Nome	Nome proprio dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Cognome	Cognome dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Visualizza	Nome dell'utente liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali

Parametri	Descrizione
Clip/Lin	Sequenza di cifre che viene mostrata per le chiamate esterne in uscita alla destinazione chiamata al posto del numero di telefono effettivo (ad esempio, per i servizi di emergenza E911 negli USA) Valori consentiti: max. 16 cifre
In funzione	Indica se l'utente è operativo.
Tipo di dispositivo	Consente di visualizzare il terminale associato all'utente.
Numero di telefono fax	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'interno.
Selezione passante fax	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'esterno.
Accesso	Visualizzazione della porta fisica a cui è collegato il terminale.
ID Loc ITSP	L'ID posizione ITSP per un utente.
Cerca	È anche possibile visualizzare gli utenti selezionati inserendo nei campi **Cerca** il testo da cercare e confermando con il tasto Invio. Vengono visualizzati gli utenti che corrispondono al termine ricercato. Se tutti i campi **Cerca** vengono lasciati vuoti e si preme il tasto Invio, verranno elencati tutti gli utenti.
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.
Pulsanti	
Freccia blu nella colonna **N. chiamata**	Richiama la pagina con la scheda **Modifica i parametri dell'utente**, **Modifica i flag dell'utente**, **Modifica i dati del WorkPoint Client** e **Modifica Gruppi/ Inoltro**.
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

28.3.7.5 Utente > Utente > Utenti DECT > SLC Num. telefono

Descrizione dei parametri delle schede:

- **Modifica utente**

Parametri	Descrizione
N. chiamata	Numero di telefono interno dell'utente.
DID	MSN (Interno) dell'utente.
Nome	Nome proprio dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri

Parametri	Descrizione
Cognome	Cognome dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Visualizza	Nome dell'utente liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Clip/Lin	Sequenza di cifre che viene mostrata per le chiamate esterne in uscita alla destinazione chiamata al posto del numero di telefono effettivo (ad esempio, per i servizi di emergenza E911 negli USA) Valori consentiti: max. 16 cifre
In funzione	Indica se l'utente è operativo.
Tipo di dispositivo	Consente di visualizzare il terminale associato all'utente. Gli utenti base vengono mostrati come S0.
Accesso	Visualizzazione della porta fisica a cui è collegato il terminale.
ID Loc ITSP	L'ID posizione ITSP per un utente.
Parametri	Vista predefinita per tutti gli utenti: non modificare le impostazioni
Cerca	È anche possibile visualizzare gli utenti selezionati inserendo nei campi **Cerca** il testo da cercare e confermando con il tasto Invio. Vengono visualizzati gli utenti che corrispondono al termine ricercato. Se tutti i campi **Cerca** vengono lasciati vuoti e si preme il tasto Invio, verranno elencati tutti gli utenti.
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.
Pulsanti	
Freccia blu nella colonna **N. chiamata**	Richiama la pagina con la scheda **Modifica i parametri dell'utente**, **Modifica i flag dell'utente**, **Modifica i dati del WorkPoint Client** e **Modifica Gruppi/ Inoltro**.
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

28.3.7.6 Utente > Utente > Utenti DECT > Utenti DECT

Descrizione dei parametri delle schede:

- **Modifica utente**

Parametri	Descrizione
N. chiamata	Numero di telefono interno dell'utente.
DID	MSN (Interno) dell'utente.

Parametri	Descrizione
Nome	Nome proprio dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Cognome	Cognome dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Visualizza	Nome dell'utente liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Clip/Lin	Sequenza di cifre che viene mostrata per le chiamate esterne in uscita alla destinazione chiamata al posto del numero di telefono effettivo (ad esempio, per i servizi di emergenza E911 negli USA) Valori consentiti: max. 16 cifre
In funzione	Indica se l'utente è operativo.
Tipo di dispositivo	Visualizzazione del terminale assegnato all'utente. Gli utenti DECT vengono mostrati come Comfort PP.
Numero di telefono fax	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'interno.
Selezione passante fax	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'esterno.
Accesso	Visualizzazione della porta fisica a cui è collegato il terminale.
ID Loc ITSP	L'ID posizione ITSP per un utente.
Cerca	È anche possibile visualizzare gli utenti selezionati inserendo nei campi **Cerca** il testo da cercare e confermando con il tasto Invio. Vengono visualizzati gli utenti che corrispondono al termine ricercato. Se tutti i campi **Cerca** vengono lasciati vuoti e si preme il tasto Invio, verranno elencati tutti gli utenti.
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.
Pulsanti	
Freccia blu nella colonna **N. chiamata**	Richiama la pagina con la scheda **Modifica i parametri dell'utente**, **Modifica i flag dell'utente**, **Modifica i dati del WorkPoint Client** e **Modifica Gruppi/ Inoltro**.
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

28.3.7.7 Utente > Utente > Porte IVM/EVM > EVM

Descrizione dei parametri delle schede:

- **Modifica utente**

Parametri	Descrizione
N. chiamata	Numero di telefono interno della porta casella vocale.
DID	MSN (interno) delle porte casella vocale, se disponibili.
Nome	Nome proprio delle porte casella vocale liberamente scelto. Valori consentiti: max. 32 caratteri
Cognome	Cognome delle porte casella vocale liberamente scelto. Valori consentiti: max. 32 caratteri
Visualizza	Nome delle porte casella vocale liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Clip/Lin	Sequenza di cifre che viene mostrata per le chiamate esterne in uscita alla destinazione chiamata al posto del numero di telefono effettivo (ad esempio, per i servizi di emergenza E911 negli USA).
In funzione	Indica se la porta casella vocale è operativa.
Tipo di dispositivo	Per EVM, vengono visualizzati gli utenti S0.
Accesso	Visualizzazione della porta interna per la casella vocale.
ID Loc ITSP	L'ID posizione ITSP per un utente.
Tipo d'utente	Per EVM selezionare "Phonemail"; per Company AutoAttendant impostare su "Predefinito".
Parametri	Vista predefinita per tutte le porte casella vocale: non modificare le impostazioni (ad esempio, "Lingua", non è la lingua degli annunci della casella vocale).
Cerca	È anche possibile visualizzare le porte per le caselle vocali selezionate inserendo nei campi **Cerca** il testo da cercare e confermando con il tasto Invio. Vengono visualizzate le porte delle caselle vocali che corrispondono al termine ricercato. Se tutti i campi **Cerca** vengono lasciati vuoti e si preme il tasto Invio, verranno elencate tutte le porte per le caselle vocali.
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.
Pulsanti	
Freccia blu nella colonna **N. chiamata**	Richiama la pagina con la scheda **Modifica i parametri dell'utente**, **Modifica i flag dell'utente**, **Modifica i dati del WorkPoint Client** e **Modifica Gruppi/ Inoltro**.
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.

Parametri	Descrizione
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

28.3.7.8 Utente > Utente > Utenti virtuali

Descrizione dei parametri delle schede:

- **Modifica utente**

Parametri	Descrizione
N. chiamata	Numero di telefono interno dell'utente virtuale.
DID	MSN (Interno) dell'utente virtuale.
Nome	Nome proprio dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Cognome	Cognome dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Visualizza	Nome dell'utente liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Tipo	Libero o utente virtuale (visualizzazione fissa per Mobility Entry)
Clip/Lin	Sequenza di cifre che viene mostrata per le chiamate esterne in uscita alla destinazione chiamata al posto del numero di telefono effettivo (ad esempio, per i servizi di emergenza E911 negli USA)
In funzione	Indica se l'utente virtuale è operativo.
ID Loc ITSP	L'ID posizione ITSP per un utente.
Cerca	È anche possibile visualizzare gli utenti selezionati inserendo nei campi **Cerca** il testo da cercare e confermando con il tasto Invio. Vengono visualizzati gli utenti che corrispondono al termine ricercato. Se tutti i campi **Cerca** vengono lasciati vuoti e si preme il tasto Invio, verranno elencati tutti gli utenti.
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.
Pulsanti	
Freccia blu nella colonna **N. chiamata**	Richiama la pagina con la scheda **Modifica i parametri dell'utente**, **Modifica i flag dell'utente**, **Modifica i dati del WorkPoint Client** e **Modifica Gruppi/ Inoltro**.
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

28.3.7.9 Utente > Utente > Parametri utente

Descrizione dei parametri delle schede:

- **Modifica i parametri dell'utente**

Parametri	Descrizione
Utenti - ...	
Tipo	Tipo di utente.
Numero di telefono	Numero di telefono interno dell'utente.
Nome	Nome proprio dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Cognome	Cognome dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Visualizzazione	Nome dell'utente liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Selezione passante	MSN (Interno) dell'utente.
Tipo di dispositivo	Consente di visualizzare il terminale associato all'utente.
Clip/Lin	Sequenza di cifre che viene mostrata per le chiamate esterne in uscita alla destinazione chiamata al posto del numero di telefono effettivo (ad esempio, per i servizi di emergenza E911 negli USA) Valori consentiti: max. 16 cifre
Accesso	Visualizzazione della porta fisica a cui è collegato il terminale.
Provisioning dei dispositivi	Questo menu è visibile solo alle stazioni SIP e sono disponibili i seguenti valori: • **Standard** (valore predefinito) • **Dispositivo Mitel SIP DECT** (il dispositivo SIP specifico utilizzato per il Mitel SIP DECT). **Nota:** L'opzione **Dispositivo Mitel SIP DECT** è supportata solo su hardware V3 e sistemi OSBiz S.
Configurazione di Mitel SIP DECT: Questo menu diventa visibile solo quando in **Provisioning dei dispositivi** è selezionato **Dispositivo Mitel SIP DECT**.	
PIN	Il codice PIN del dispositivo.
Blocco tasti abilitato	Abilita (Sì) o disabilita (No) il blocco dei tasti del dispositivo.
PIN blocco tasti	Il PIN del blocco tasti.
Ora blocco tasti	Ora in cui il blococ tasto avrà effetto.

Parametri	Descrizione
Mostra directory personale	Scegliere se la directory personale è visibile (Sì) o meno (No).
Fax	
Numero di telefono	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'interno.
Selezione passante	Se è configurata una casella fax (ad esempio con il client UC myPortal for Desktop o myPortal for Outlook), inserire qui il numero di fax al quale l'utente può ricevere fax dall'esterno.
Mobility	
Tipo	Tipo di utente: • Utente Mobility • Stazione virtuale • Utente SFB • Stazione esterna attendibile: tipo di stazione virtuale da utilizzare per creare un utente esterno affidabile
Numero di telefono stazione esterna Mobile/Sfb/ Attendibile	Solo per client SIP e utenti mobili: Per il servizio One Number, si usa questo numero di telefono per l'autenticazione dell'accesso DISA via rete mobile. Inserire qui il relativo numero di telefono mobile dell'utente con il codice di linea esterna (ad esempio 0017312345678). **Nota:** Il campo **Numero di telefono stazione esterna attendibile** è obbligatorio. Se si procede all'applicazione della configurazione con il campo **Numero di chiamata stazione esterna attendibile** vuoto, apparirà un avviso che informa che "*Il numero di chiamata della stazione esterna attendibile non può essere vuoto!*". Inoltre, dopo aver fatto clic su **OK** sul primo avviso, apparirà un secondo popup, che informerà che "*Non è stato possibile gestire l'input, controllare*".
Web Feature ID	L'ID della funzione Web definisce come l'utente deve accedere al client Web mobile (nome utente). Scelta tra "nessuno" (solo Mobility Entry) e "automatico" (numero di telefono interno dell'utente) o scelta del numero del cliente o del telefono dall'elenco a discesa.
Parametri	
Tipo d'utente	Tipo di terminale collegato (menu a discesa)
Tipo d'utente: **Standard**	Telefoni di sistema o telefoni analogici
Tipo d'utente: **Fax**	Fax, ad esempio, nessuna inclusione possibile
Tipo d'utente: **Altoparlante**	Per la configurazione del paging tramite porta a/b

Parametri	Descrizione
Tipo d'utente: **Segreteria telefonica**	solo se analogico: se a questa interfaccia viene collegata una segreteria telefonica, questa impostazione consente di riprendere una chiamata alla segreteria telefonica mediante qualsiasi dispositivo, anche se la segreteria telefonica ha già risposto alla chiamata. A tal fine, nel terminale deve essere impostato un tasto con il numero di telefono interno dell'utente analogico. Questa voce dovrebbe essere selezionata non solo per le segreterie telefoniche, ma anche per le porte virtuali a cui non è stato assegnato alcun hardware. In questo modo il sistema di comunicazione non effettua il controllo per stabilire se la porta è attivata. Solo per porte virtuali: se come tipo segreteria telefonica viene configurato un utente senza accesso a Manager E, la porta deve inoltre essere configurata come una porta virtuale. In caso contrario questa non sarebbe visibile come utente nel WBM.
Tipo d'utente: **Utente AB MW LED**	Per i telefoni analogici (NoFe = telefono normale) con LED messaggio in attesa non per gli USA
Tipo d'utente: **Utente con ciclo di impulso**	Quando si utilizza un terminale a loop di impulsi con funzione apriporta
Tipo d'utente: **Modem**	Per questa impostazione non è possibile alcuna inclusione. Essa è infatti prevista per i modem.
	Se viene cancellato un utente fax o modem (Nr. di tel. e DISA vengono cancellati) è necessario eseguire un reset del tipo di telefono.
Lingua	Lingua per il controllo a menu del terminale (sistema telefonico).
Segnalazione di chiamate interne	Consente di assegnare a ciascun utente una delle otto segnalazioni di chiamate interne disponibili. Oltre alla suoneria per chiamate esterne, ne viene assegnata una destinata a segnalare le chiamate in arrivo dalla linea interna. Valore predefinito: Suoneria 1
Segnalazione di chiamate esterne	Qui possono essere impostati tre diversi tipi di segnalazione delle chiamate esterne: – Telefoni di sistema Tipo chiam. 1 = chiamata esterna (es. doppio squillo); Tipo chiam. 2 = chiamata esterna CO 2 (es. triplo squillo); Tipo chiam. 3 = chiamata esterna CO 3 (es. corto/lungo/corto) – Dispositivi analogici, Germania: Tipo chiam. 1 = Chiamata esterna; Tipo chiam. 2 = Richiamata; Tipo chiam. 3 = Campanello porta – Dispositivi analogici, altri paesi: Tipo chiam. 1 = Chiamata esterna; Tipo chiam. 2 = Chiamata esterna; Tipo chiam. 3 = Chiamata esterna Valore predefinito: Suoneria 1
Abilitazione (LCR)	Un utente può impegnare una rotta se la sua abilitazione LCR è di livello superiore o uguale a quella della tabella delle rotte; un utente con abilitazione 7 non può cioè impegnare una rotta che richiede l'abilitazione 8. Per impostazione predefinita, tutti gli utenti sono configurati con il massimo livello di abilitazione LCR (15). Valore predefinito: 15
Modo hotline	Scelta delle opzioni Hotline

Parametri	Descrizione
Modo hotline: **off**	Disattiva la funzione hotline.
Modo hotline: **A tempo**	La chiamata alla hotline viene eseguita dopo un tempo di attesa preimpostato (tempo di ritardo), vedere Telefonia/Impostazioni di base/Sistema/Rinvio-PO-Hotline
Modo hotline: **Hotline**	Attiva la funzione hotline. Quando si solleva il ricevitore, la connessione con la destinazione hotline viene stabilita immediatamente, vedere telefonia/ preferenze/sistema/rinvio-VPL-Hotline
Hotline	Per la scelta della destinazione Hotline, vedere Telefonia/Impostazioni di base/ Sistema Rinvio-PO-Hotline
Hotline: **nessuna**	Nessuna destinazione definita
Hotline: **Cifre 1-6**	Per la destinazione hotline, vedere Telefonia/Impostazioni di base/Sistema/ Rinvio-PO-Hotline
Sicurezza payload (per client di sistema IP)	Attivare o disattivare la crittografia delle conversazioni telefoniche (SPE). A tal fine, tutti gli utenti coinvolti devono aver attivato SPE. Valore predefinito: attiva
Sicurezza payload (per telefoni TDM/analogici)	Indica se il punto terminale specifico è protetto o meno dal punto di vista dell'infrastruttura in quanto la sicurezza payload funziona solo per i telefoni IP. Se questo parametro attivato e il flag del sistema di supporto SPE è attivato, l'informazione viene visualizzata indipendentemente dal fatto che il percorso di connessione tra questa stazione e una stazione IP sia crittografato. Se il parametro è disattivato, non viene visualizzata alcuna informazione. Valore predefinito: Off
Protocollo MWI	Selezione del protocollo MWI per gli utenti analogici. Disponibile solo per SLMAVx (OpenScape Business X8), 4SLAV integrato e SLAVx OpenScape Business X3, X5.
Protocollo MWI: Comtel3	Protocollo Comtel 3 selezionato. Valore predefinito.
Protocollo MWI: Alta tensione	Protocollo alta tensione selezionato. Disponibile solo per SLMAVx (OpenScape Business X8).
Pulsanti	
>	Passare all'utente successivo. Se in precedenza era stato applicato il filtro sugli utenti tramite l'immissione del testo desiderato nel campo **Cerca**, si può passare solo a questi utenti.
<	Passa all'utente precedente.

Descrizione dei parametri delle schede:

- **Modifica i flag dell'utente**

Parametri	Descrizione
Utenti - ...	
Tipo	Tipo di utente.
Numero di telefono	Numero di telefono interno dell'utente.

Parametri	Descrizione
Nome	Nome della stazione.
Flag utente	
Autorizzazione ad includersi On	Se il flag è attivato: l'utente può inserirsi nella connessione esistente di un utente interno. Gli utenti interessati vengono informati dell'inclusione tramite un tono di avviso e tramite un messaggio sul display. Valore predefinito: Disattivato
Interrompi non disturbare	Se il flag è attivato: se l'utente ha necessità di contattare un utente interno che ha attivato la funzione Non disturbare, può interrompere tale funzione. Dopo cinque secondi la chiamata viene segnalata all'utente chiamato. Se il flag è disattivato: la funzione non disturbare non può essere disattivata. Se l'utente si imbatte in un utente interno che ha attivato Non disturbare, viene emesso il tono di occupato. Valore predefinito: Disattivato
Consenti trasf. esterno	Se il flag è attivato: l'utente è autorizzato ad attivare una deviazione di chiamata verso una destinazione esterna. I costi generati dall'esecuzione di una deviazione di chiamata esterna vengono addebitati all'utente che ha attivato la deviazione di chiamata. Valore predefinito: Abilitato
Rifiuto chiamata su altoparlante Off	Se il flag è attivato: l'utente può essere contattato direttamente. Ciò consente di effettuare una chiamata interna senza che l'utente sollevi il ricevitore. L'altoparlante dell'utente viene quindi attivato automaticamente. Valore predefinito: Abilitato
Abilitazione DISA	Se il flag è attivato: l'utente può attivare o disattivare dall'esterno – come per gli utenti interni – tramite DISA (Direct Inward System Access) funzioni del sistema di comunicazione ed eseguire chiamate esterne in uscita. Un esempio sono l'attivazione e la disattivazione di: Deviazione di chiamata, Non disturbare e Chiave elettronica. Valore predefinito: Disattivato
Trasferta su fine chiamata	Se il flag è attivato: l'utente può trasferire una chiamata esterna a un altro utente esterno riagganciando. Esempio: L'utente è supervisore conferenza e si disconnette: se in conferenza rimangono degli utenti interni, il partecipante interno che è stato più a lungo connesso alla conferenza diventa automaticamente il supervisore conferenza. Se in conferenza rimangono solo utenti esterni, la conferenza viene conclusa e tutte le connessioni vengono disconnesse. Valore predefinito: Disattivato
Reimposta PIN	Se il flag è attivato: l'utente può resettare la chiave elettronica individuale di altri utenti interni riportandola al valore predefinito. Valore predefinito: Disattivato

Parametri	Descrizione
CLIP in entrata per linea analogica (solo per utenti analogici)	Se il flag è attivato: sul display del telefono dell'utente analogico viene visualizzato il numero di telefono del chiamante. A tal fine è necessario che il telefono analogico dell'utente supporti CLIP (Calling Line Identification Presentation). Valore predefinito: Abilitato
Identificazione chiamata di disturbo	Se il flag è attivato: l'utente può identificare i chiamanti esterni inopportuni sulla linea ISDN. A tal fine, è necessario che sia stata richiesta all'operatore di rete e ottenuta l'abilitazione del servizio "Identificazione chiamate di disturbo" (Malicious Call Identification MCID). Dopo l'abilitazione del servizio "Identificazione chiamate di disturbo" da parte dell'operatore di rete, si osservi quanto segue: per ogni connessione in entrata dalla linea ISDN, dopo il riaggancio da parte del chiamante, il rilascio della connessione all'utente chiamato viene ritardato per un certo lasso di tempo, per consentirgli di attivare il servizio "Identificazione chiamate di disturbo". La disponibilità delle linee ISDN risulterà diminuita. Valore predefinito: Disattivato
Registrazione in elenco telef.	Se il flag è attivato: nome e numero di telefono dell'utente vengono visualizzati nella rubrica del sistema (incluso ODS). Valore predefinito: Abilitato
Modifica d.selez.	Se il flag è attivato: prima della trasmissione della selezione, l'utente può modificare le cifre del numero di telefono immesse da tastiera. A tale scopo è necessario un telefono di sistema con display. Valore predefinito: Disattivato
No segnalaz. chiamata su occupato	Se questo flag è attivato, si applica quanto segue: lo stato dell'utente con chiamata di gruppo programmata (ad es., l'utente) predetermina l'esecuzione o meno di una segnalazione. L'utente è libero: tutti gli utenti a cui è applicabile la segnalazione delle chiamate vengono chiamati immediatamente. L'utente ha attivato la funzione avviso di chiamata: tutti gli utenti a cui è applicabile la segnalazione delle chiamate vengono chiamati dopo 5 secondi. L'utente non ha attivato la funzione avviso di chiamata o non può essere chiamato: non avviene alcuna segnalazione delle chiamate. Valore predefinito: Disattivato
Selezione associata / servizi	Selezione associata: se il flag è attivato, l'utente può comporre il numero di telefono per un altro utente interno come se fosse l'altro utente stesso a comporre. Servizi associati: se il flag è attivato, l'utente può gestire i servizi per un altro utente interno come se fosse l'altro utente stesso a gestire i servizi. Un esempio sono l'attivazione e la disattivazione di: Deviazione di chiamata, Segnalazione di chiamata e Chiave elettronica. Valore predefinito: Disattivato
Rifiuto dell'avviso di chiamata in attesa	Se il flag è attivato: se l'utente è occupato in una conversazione, non viene informato di altre chiamate in entrata tramite tono di avviso di chiamata e messaggio sul display. Valore predefinito: Abilitato

Parametri	Descrizione
Chiamata discreta	Se il flag è attivato: l'utente può inserirsi nella connessione voce esistente di un utente interno. Può ascoltare una chiamata in modo inosservato e parlare con l'utente interno senza che gli altri utenti sentano. A tal fine è necessario un collegamento duplex. Per le chiamate di consultazione e le conferenze, l'inclusione discreta non è possibile. Valore predefinito: Disattivato
Protez. ch.altoparlante discreta	Se il flag è attivato: l'utente non può essere contattato in modo discreto. Valore predefinito: Disattivato
Funzione di attivazione basata su DTMF	Rilevante solo per gli utenti Mobility Entry: per poter attivare i servizi durante una chiamata, è necessario attivare questo flag (ad es., in stato di conversazione). (il ricevitore codice rimane attivo; attenzione: risorse limitate) Valore predefinito: Disattivato
Cuffia	Se il flag è attivato, permette all'utente di disporre di una cuffia telefonica da collegare all'attacco del portatile. Il flag indica che è possibile rispondere alle chiamate senza sollevare il ricevitore ma semplicemente premendo il pulsante dell'auricolare nel telefono di sistema. Quando si collega una cuffia alla presa di un telefono di sistema, viene riconosciuta automaticamente dal sistema di comunicazione; in questo caso non è richiesta alcuna abilitazione. Se questo flag è attivato, non è possibile rilasciare una chiamata premendo il tasto Altoparlante, deve essere previsto un tasto di disconnessione per il rilascio delle chiamate. Valore predefinito: Disattivato
Ultima mailbox di destinazione attiva	Se il flag è attivato e la persona chiamata non è raggiungibile, le chiamate vengono inoltrate verso la mailbox del sostituto sul cui display del terminale viene visualizzato il numero del chiamante. Valore predefinito: Disattivato
Prio.ch./tono lib.avv.chiamata	Se il flag è attivo (Priorità di chiamata/Tono libero avviso di chiamata), le chiamate effettuate dall'utente vengono segnalate all'apparecchio chiamato con maggiore priorità. Il livello di priorità è analogo a quello delle chiamate esterne. La chiamate con priorità vengono inserite prima delle chiamate interne, ma dopo quelle esterne. Notare che, in generale, le prime chiamate esistenti (non quelle in attesa) non vengono visualizzate, indipendentemente dal tipo di chiamata. Se deve essere impostata la stessa priorità per una chiamata interna in un altro nodo, deve essere impostato il flag utente “Prio.ch./tono lib.avv.chiamata” (Area: Flag circuito, Prio.ch./tono lib.avv.chiamata) per la linea rispettiva. Se il flag è attivato, i chiamanti in attesa ricevono subito il segnale di libero. La funzione non va ad influire sulla segnalazione acustica. Le chiamate prioritarie vengono inoltre segnalate come chiamate interne. Questo servizio è ad esempio importante in connessioni Phonemail. Valore predefinito: Disattivato

Parametri	Descrizione
Registrazione vocale	Se il flag è attivato, l'utente può attivare la registrazione vocale durante la conversazione. Tramite Flags, l'interruttore **Tono di segnalazione con registrazione vocale** può essere inoltre indicato se debba essere emesso un tono di segnalazione durante la registrazione vocale. In PhoneMail deve essere configurato un registratore Live Recording adeguato. Valore predefinito: Disattivato
Comprimere gli output del display	Se il flag è attivato, le uscite video sono compresse per migliorare le prestazioni. Se i dati visualizzati sul display di un terminale UP0/E cambiano, il sistema di comunicazione aggiorna soltanto i dati modificati rispetto alla visualizzazione precedente. Se viene collegata un'applicazione (ad esempio Smartset / TAPI) attraverso l'adattatore RS 232 (adattatore dati o controllo), questa funzione deve essere disattivata. Questo flag deve essere disattivato nelle applicazioni che acquisiscono l'informazione del numero di telefono dal display del terminale (ciò significa: output non compresso con numero di telefono anziché output compresso con nome). I nomi vengono visualizzati solo se in "Visualizzare il nome/nr. di tel." il flag "Solo numero di telefono" è disattivato. Valore predefinito: Abilitato
Rilascio porta, DTMF	Se il flag è attivo, l'utente può utilizzare il codice DTMF/MFV per aprire una porta collegata a un apposito dispositivo. Valore predefinito: Disattivato
Risposta automatica, CSTA (solo per telefoni SIP OpenStage)	Se il flag è attivato: quando si compone un numero o si risponde tramite myPortal o myAttendant, nel relativo telefono SIP viene attivata la funzione vivavoce. Occorre rispettare le informazioni contenute nella documentazione del telefono SIP, in quanto per l'uso corretto delle funzioni possono essere necessarie ulteriori impostazioni sul telefono SIP. Se il flag è disattivato, la connessione viene realizzata immediatamente dopo aver sollevato il ricevitore. Valore predefinito: Abilitato
Disattivare Microfono handsfree	Se il flag è attivato, non è possibile utilizzare il microfono della funzione viva voce. Il flag è disponibile per i soli telefoni OpenStage. Valore predefinito: Disattivato
Presentazione numeri forzata	Se il flag è attivato, sul display dell'utente chiamato viene visualizzato il numero anziché il nome del chiamante. Valore predefinito: Disattivato
Uso (solo per alcuni paesi)	Con questo elenco a discesa, è possibile configurare la corrente in uscita delle interfacce di un modulo analogico (in mA, ad esempio 27 mA per la Cina).
Stato operativo generico	Da questo elenco è possibile definire il tipo di servizio della linea d'utente.
Output della lista delle chiamate	Se il flag è attivato, la lista delle chiamate è attiva sul telefono dell'utente (solo per dispositivi con display). Le chiamate alle quali l'utente non ha risposto sono dotate di un timbro orario (ora e data) e registrate in una lista in ordine cronologico. Vengono registrate solamente le chiamate con un numero di telefono o un nome. Se il chiamante effettua diverse chiamate, l'ora viene aggiornata e la numerazione del contatore del chiamante incrementata.

Parametri	Descrizione
Segnalazione centrale di occupato	Per utenti che dispongono di segnalazione di occupato su un sistema di comunicazione centrale, questo flag deve essere attivato (vedere anche Servizi QSIG). Non valido per gli USA. L'implementazione della segnalazione centrale di occupato prevede un numero massimo di 100 utenti per nodo.
Visualizzazione messaggio di emergenza	Se questo flag è attivato, viene visualizzato un testo di emergenza configurabile sullo schermo del telefono nella modalità di emergenza.
Ascolto di una chiamata	Se il flag è attivato: l'utente può ascoltare la chiamata di un utente interno qualsiasi. Al microfono dell'utente in ascolto viene tolto l'audio automaticamente. Gli utenti monitorati non vengono informati mediante tono di avviso o indicazione sul display. All'inizio e alla fine dell'ascolto della chiamata possono verificarsi salti nelle conversazioni, di durata fino a due secondi. Valore predefinito: Disattivato
Pulsanti	
>	Passare all'utente successivo. Se in precedenza era stato applicato il filtro sugli utenti tramite l'immissione del testo desiderato nel campo **Cerca**, si può passare solo a questi utenti.
<	Passa all'utente precedente.

Descrizione dei parametri delle schede:

- **Modifica i dati del WorkPoint Client**

Parametri	Descrizione
Utenti - ...	
Tipo	Tipo di utente.
Numero di telefono	Numero di telefono interno dell'utente.
Nome	Nome della stazione.
Parametri	
Messaggio di stato	Solo per client di sistema: questo flag attiva il meccanismo "keep alive" per i telefoni di sistema. Se un telefono di sistema si guasta, dopo 4 minuti viene segnalato come inattivo. Il flag deve essere disattivato se il telefono viene configurato come postazione home e si utilizza il servizio "Short Hold". Se questo flag non è attivato, il traffico messaggi tra il sistema di comunicazione e i telefoni di sistema viene ridotto.
Autenticazione attiva	Se il client IP deve identificarsi sul sistema di comunicazione con una password, è necessario attivare l'autenticazione e immettere la password. Per i client che non si trovano nella LAN interna ma accedono dall'esterno si tratta di un vantaggio. Solo per i client SIP: è necessario immettere la password. La stessa password deve essere utilizzata nel dispositivo.
Nuova password	Password per l'autenticazione. Solo per i client SIP: Se la password del dispositivo è già stata impostata, la stessa password deve essere utilizzata con Applica per mantenere il dispositivo registrato.

Parametri	Descrizione
Confermare la password	Ripetere la password per l'autenticazione.
SIP ID d'utente / Nome d'utente	Solo per client SIP: numero utente liberamente scelto per l'autenticazione dell'utente SIP, ad esempio, "SIP 120". Il valore definito qui deve essere inserito anche nel telefono SIP.
Realm	Solo per client SIP: nome liberamente scelto per la zona corrispondente, ad esempio, "OSBIZ-SIP". Questo valore deve essere uguale tutti i client SIP. Il valore definito qui deve essere inserito anche nel telefono SIP.
Usa indirizzo IP fisso	Solo per client SIP: l'immissione di un indirizzo IP statico garantisce che con esso possa registrarsi nel sistema un solo client SIP. Se il flag è attivato, vengono controllati l'indirizzo IP ed il numero di telefono. Se il flag non è attivato, viene controllato il solo numero di telefono.
Indirizzo IP	Solo per i client SIP: indirizzo IP del client SIP (ad esempio l'indirizzo IP del telefono SIP)
Tipo	Solo per i client di sistema: a un client mobile IP (opzione cellulare) non viene assegnato permanentemente alcun telefono IP. Con il numero di telefono di un client IP mobile, tramite procedura di accesso (*9419), l'utente può registrarsi in tutti i terminali IP che lo consentono (opzione Portatile bloccato non attivata).
Tipo: **Cellulare**	Solo per i client di sistema: all'utente non viene assegnato permanentemente alcun terminale IP. La funzione è supportata a partire dalla terza porta utente.
Tipo: **Non mobile**	Solo per i client di sistema: al terminale IP dell'utente viene assegnato permanentemente il numero di telefono. Quando si utilizza un telefono WLX, l'opzione Non mobile deve essere impostata prima che il telefono WLX venga registrato sul sistema di comunicazione.
Tipo: **Non mobile e bloccato**	Solo per i client di sistema: un utente non può accedere a questo terminale IP con un client di sistema mobile.
Bloccato per l'utente Deskshare	Solo per i client di sistema: questo telefono di sistema può essere condiviso da più utenti (Desksharing).
ID del sistema secondario	Questo parametro presenta due diverse funzioni: 1. Per tutti gli utenti: definisce il gateway multi-posizione assegnato all'utente. 2. Solo per i client di sistema: se nel sistema collegato in rete è impostato il flag "Emergenza" (in "Utente/Client IP/Gateway secondario"), è possibile inserire qui l'ID del nodo del sistema di backup per i client di sistema.
Registrazione Internet con SBC interna	Attiva la funzione SIP@Home. In questo modo un telefono SIP esterno che supporta STUN può registrarsi nel sistema OpenScape Business tramite Internet ed essere utilizzato come telefono interno.
Pulsanti	
>	Passare all'utente successivo. Se in precedenza era stato applicato il filtro sugli utenti tramite l'immissione del testo desiderato nel campo **Cerca**, si può passare solo a questi utenti.
<	Passa all'utente precedente.

Descrizione dei parametri delle schede:

- **Modifica Gruppi/Inoltro**

Parametri	Descrizione
Utenti - ...	
Tipo	Tipo di utente.
Numero di telefono	Numero di telefono interno dell'utente.
Nome	Nome della stazione.
Inoltro di chiamata	
Destinazione Giorno	Visualizzazione delle destinazioni di inoltro chiamata per le chiamate esterne in entrata di giorno (vedere la procedura guidata Telefonia utenti/Inoltro di chiamata)
Destinazione Notte	Visualizzazione delle destinazioni di inoltro chiamata per le chiamate esterne in entrata durante la notte (vedere la procedura guidata Telefonia utenti/Inoltro di chiamata).
Destinazione Interna	Visualizzazione delle destinazioni di inoltro chiamata per le chiamate interne in entrata di giorno (vedere la procedura guidata Telefonia utenti/Inoltro di chiamata).
Abilitazione	
Giorno	A ogni utente può essere assegnata una classe di abilitazioni per il servizio giorno. È possibile scegliere fra 15 classi di abilitazione diverse (vedere Telefonia/Abilitazioni).
Notte	A ogni utente può essere assegnata una classe di abilitazioni per il servizio notte. È possibile scegliere fra 15 classi di abilitazione diverse (vedere Telefonia/Abilitazioni).
Risposta per assente	
Gruppo	Ciascun utente può essere assegnato a un gruppo di risposta. È possibile scegliere tra 32 gruppi di risposta (120 con OpenScape Business S; vedere anche Chiamate in entrata/Risposta per assente).
Pulsanti	
>	Passare all'utente successivo. Se in precedenza era stato applicato il filtro sugli utenti tramite l'immissione del testo desiderato nel campo **Cerca**, si può passare solo a questi utenti.
<	Passa all'utente precedente.

28.3.7.10 Utente > Utente > Applicazioni UC

Qui vengono visualizzate le funzioni delle soluzioni di comunicazione unificata UC Smart e UC Suite. Si consiglia di effettuare le impostazioni di base selezionando "Configurazione > Installazione di base > Installazione di base > Modifica numeri di telefono e funzionali pre-configurati".

A seconda della soluzione UC utilizzata, vengono visualizzate funzioni diverse.

Descrizione dei parametri delle schede:

- **Modifica utente**

Parametri	Descrizione
N. chiamata	Numero di telefono del servizio
DID	MSN (Interno) del servizio
Nome	Nome proprio del servizio liberamente scelto. Valori consentiti: max. 32 caratteri
Cognome	Cognome del servizio liberamente scelto. Valori consentiti: max. 32 caratteri
Visualizza	Nome del servizio liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Tipo	A seconda della soluzione UC: UC Smart: MeetMe/Conferenza UC Suite: AutoAttendant/Fax/Contact Center Fax/Parcheggio/MeetMe/ Conferenza/Gruppo fax
Clip/Lin	Sequenza di cifre che viene mostrata per le chiamate esterne in uscita alla destinazione chiamata al posto del numero di telefono effettivo (ad esempio, per i servizi di emergenza E911 negli USA) **Nota:** CLIP non è supportato per il fax UC, ma solo per il fax analogico.
In funzione	Indica se il servizio è operativo.
ID Loc ITSP	L'ID posizione ITSP per un utente.
Cerca	È anche possibile visualizzare i servizi selezionati inserendo nei campi **Cerca** il testo da cercare e confermando con il tasto Invio. Vengono visualizzati i servizi che corrispondono al termine ricercato. Se tutti i campi **Cerca** vengono lasciati vuoti e si preme il tasto Invio, verranno elencati tutti i servizi.
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.
Pulsanti	
Freccia blu nella colonna **N. chiamata**	Richiama la pagina con la scheda **Modifica i parametri dell'utente**, **Modifica i flag dell'utente**, **Modifica i dati del WorkPoint Client** e **Modifica Gruppi/ Inoltro**.
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

28.3.7.11 Utente > Utente > Profili/Modelli

Qui è possibile configurare i profili utente (parametro utente, flag utente, gruppi/rinvio), in modo da consentire l'esecuzione delle impostazioni di base per diversi utenti contemporaneamente.

Descrizione dei parametri delle schede:

- **Modifica tutti i profili**

Parametri	Descrizione
Profili	Visualizzazione del numero profilo.
Servizio	Immissione di un nome profilo a scelta.

Descrizione dei parametri delle schede:

- **Visualizza tutti gli utenti del profilo**

Parametri	Descrizione
Profili	Visualizzazione del numero profilo.
Servizio	Visualizzazione del nome profilo.
N° tel membro	Visualizzazione del numero interno del profilo del membro.
Nome membro	Visualizzazione del numero interno del membro profilo.

Descrizione dei parametri delle schede:

- **Aggiungi/elimina membro profilo**

Parametri	Descrizione
Profilo - ...	Visualizzazione del numero profilo.
Servizio	Visualizzazione del nome profilo assegnato.
Membri profilo	
Scelta	Elenco degli utenti disponibili nel sistema.
Membri	Elenco degli utenti assegnati al profilo.
Pulsanti	
Aggiungi	Aggiungere gli utenti selezionati nell'elenco membri profilo.
Elimina	Eliminare l'utente selezionato dall'elenco dei membri profilo.

Descrizione dei parametri delle schede:

- **Importa/esporta profilo**

Parametri	Descrizione
Carica il profilo tramite HTTP	
Nome del file remoto (sistema di file del PC)	Caricamento di un file profilo esistente in formato XML

Parametri	Descrizione
Esporta il profilo tramite HTTP	
Nome file	Visualizzazione del nome file con il quale viene esportato il profilo (formato XML)
Azione	Download del profilo
Pulsanti	
Reimposta valori predefiniti	I valori di profilo per tutti gli utenti assegnati a questo profilo vengono riportati ai valori predefiniti.

Descrizione dei parametri delle schede:

- **Importa/Esporta tutti i profili**

Parametri	Descrizione
Carica tutti i profili tramite HTTP	
Nome del file remoto (sistema di file del PC)	Caricamento di un file profilo esistente. In questo file possono essere salvati anche più profili.
Esporta tutti i profili tramite HTTP	
Nome file	Visualizzazione del nome file con il quale viene salvato il profilo.
Azione	Download dei profili in un file profilo.
Pulsanti	
Reimposta valori predefiniti	I valori di profilo per tutti i profili e gli utenti assegnati vengono riportati ai valori predefiniti.

Descrizione dei parametri delle schede:

- **Modifica parametri utente: vedere Utenti > Utenti > Parametri utente**
- **Modifica flag utenti: vedere Utenti > Utenti > Parametri utente**
- **Modifica Gruppi/Inoltro: vedere Utenti > Utenti > Parametri utente**

28.3.7.12 Utente > Utente > Estensioni selezione passante

Qui viene visualizzata una panoramica dei numeri interni configurati con il relativo utente.

Descrizione dei parametri delle schede:

- **Visualizza estensioni selezione passante**

Parametri	Descrizione
N. chiamata	Visualizzazione del numero di telefono dell'utente.
Servizio	Visualizzazione del nome dell'utente.
DID	Visualizzazione MSN dell'utente.

Parametri	Descrizione
(possono essere visualizzati altri campi)	

28.3.7.13 Utente > Utente > Mobility Entry

Si raccomanda di configurare gli utenti mobili tramite la procedura guidata "Telefonia utenti > Integrazione con il numero di cellulare".

Descrizione dei parametri delle schede:

- **Modifica utente**

Parametri	Descrizione
N. chiamata	Immissione del numero interno dell'utente Mobility (ad esempio 777). Questo numero interno non deve essere già stato assegnato.
DID	Immissione del numero DID dell'utente Mobility. Questo numero interno non deve essere già stato assegnato.
Nome	Nome proprio dell''utente Mobility liberamente scelto. Valori consentiti: max. 32 caratteri
Cognome	Cognome dell''utente Mobility liberamente scelto. Valori consentiti: max. 32 caratteri
Visualizza	Nome dell''utente Mobility liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Tipo	Visualizzazione del tipo di utente Mobility.
Tipo di dispositivo	Visualizzazione del tipo di carattere del telefono di sistema a cui appartiene il file immagine.
Clip/Lin	Sequenza di cifre che viene mostrata per le chiamate esterne in uscita alla destinazione chiamata al posto del numero di telefono effettivo (ad esempio, per i servizi di emergenza E911 negli USA. Valori consentiti: max. 16 cifre
Accesso	Visualizzazione della porta fisica a cui è collegato il terminale.
Numero di cellulare	Immissione del numero di telefono mobile. Immissione del codice di linea urbana iniziale, ad esempio 0016012345678.
Web Feature ID	L'ID della funzione Web definisce come l'utente deve accedere al client Web mobile (nome utente). Scelta tra "nessuno" (utente Mobility Entry senza myPortal to go) e "automatico" (numero di telefono interno dell'utente o do MULAP) o scelta del numero del cliente o del telefono dall'elenco a discesa.
Cerca	È anche possibile visualizzare gli utenti selezionati inserendo nei campi **Cerca** il testo da cercare e confermando con il tasto Invio. Vengono visualizzati gli utenti che corrispondono al termine ricercato. Se tutti i campi **Cerca** vengono lasciati vuoti e si preme il tasto Invio, verranno elencati tutti gli utenti.
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.

Parametri	Descrizione
Pulsanti	
Freccia blu nella colonna **N. chiamata**	Richiama la pagina con la scheda **Modifica i parametri dell'utente**, **Modifica i flag dell'utente**, **Modifica i dati del WorkPoint Client** e **Modifica Gruppi/ Inoltro**.
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

Descrizione dei parametri delle schede:

- **Gateway secondario**

  Solo per sistemi in rete (multi location)

Parametri	Descrizione
Numero di telefono	Numero di telefono interno dell'utente Mobility.
Servizio	Nome dell’utente Mobility.
ID nodo	Immissione del nodo ID tramite il quale l'utente mobile è raggiungibile esternamente.

28.3.7.14 Utente > Utente > Utente SfB

Descrizione dei parametri delle schede:

- **Editor di tabelle di utenti**

Parametri	Descrizione
N° tel.	Immissione del numero interno dell'utente Mobility del client Skype for Business (ad es. 777). Questo numero interno non deve essere già stato assegnato.
DID	Numero di selezione passante per il client Skype for Business.
Nome proprio	Nome proprio dell'utente liberamente scelto. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali.
Cognome	Cognome dell'utente liberamente scelto. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali.
Visualizzazione	Nome dell'utente liberamente scelto. Per impostazione predefinita, vengono creati i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali.
Tipo	Visualizzazione del tipo di utente Mobility, in questo caso sempre Utente SfB.
Numero di telefono SfB	Il numero di telefono del client Skype for Business.

Parametri	Descrizione
Trova	È anche possibile visualizzare gli utenti selezionati inserendo nei campi **Cerca** il testo da cercare e confermando con il tasto Invio. Vengono visualizzati gli utenti che corrispondono al termine ricercato. Se tutti i campi **Cerca** vengono lasciati vuoti e si preme il tasto Invio, verranno elencati tutti gli utenti.
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.
Pulsanti	
Freccia blu nella colonna **N° tel.**	Richiama la pagina con la scheda **Modifica i parametri dell'utente**, **Modifica i flag dell'utente**, **Modifica i dati del WorkPoint Client** e **Modifica Gruppi/ Inoltro**.
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

28.3.7.15 Utenti > Utenti > Panoramica utenti

Elenca tutti gli utenti del sistema di comunicazione ordinati per numero di telefono (opzione predefinita). Facendo clic su un'altra intestazione di colonna, si ordinerà l'elenco secondo la colonna scelta, in ordine crescente; con un altro clic sulla stessa intestazione di colonna questa verrà ordinata in ordine decrescente.

Descrizione dei parametri delle schede:

- **Modifica utente**

Parametri	Descrizione
N. chiamata	Numero di telefono interno dell'utente.
DID	MSN (Interno) dell'utente.
Nome	Nome proprio dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Cognome	Cognome dell'utente liberamente scelto. Valori consentiti: max. 32 caratteri
Visualizza	Nome dell'utente liberamente scelto. Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Tipo di dispositivo	Visualizzazione del tipo di utente.
In funzione	Indica se l'utente è operativo.
Accesso	Visualizzazione della porta fisica a cui è collegato il terminale.

Parametri	Descrizione
Cerca	È anche possibile visualizzare gli utenti selezionati inserendo nei campi **Cerca** il testo da cercare e confermando con il tasto Invio. Vengono visualizzati gli utenti che corrispondono al termine ricercato. Se tutti i campi **Cerca** vengono lasciati vuoti e si preme il tasto Invio, verranno elencati tutti gli utenti.
Elementi per pagina	Definire se per ogni pagina verranno visualizzati 10, 25, 50 o 100 elementi.
Pulsanti	
Freccia blu nella colonna **N. chiamata**	Richiama la pagina con la scheda **Modifica i parametri dell'utente**, **Modifica i flag dell'utente**, **Modifica i dati del WorkPoint Client** e **Modifica Gruppi/ Inoltro**.
>	Salta alla pagina successiva.
<	Salta alla pagina precedente.
>|	Salta alla fine dell'elenco.
|<	Salta all'inizio dell'elenco.

28.3.7.16 Utenti > Programmazione dei tasti

Descrizione dei parametri delle schede:

- **Programmazione dei tasti**

  La programmazione dei tasti è supportata solo per i telefoni UP0 e i client HFA. È disponibile una funzione di ricerca (usando i campi n° tel., DID, nome, cognome, nome visualizzato e tipo di dispositivo).

Parametri	Descrizione
Elenco	Selezione del telefono dell'utente.
Commuta livello	Se è stato configurato un tasto con la funzione commuta livello, qui viene programmato il secondo livello
Utente	Facendo clic sull'area tasti del telefono si apre la mappatura tasti corrente.
Campo tasti	Visualizzazione della funzione tasti (Assegnazione di etichette ai tasti)
Tasto	Scelta della funzione desiderata

Descrizione dei parametri delle schede:

- **Applica layout tasti**

Parametri	Descrizione
Copia layout tasti da utente	Scelta dell'utente i cui tasti configurati devono essere importati per l'utente selezionato.
Tutti gli utenti	Copia della configurazione dei tasti per tutti gli utenti.
Casella di riepilogo	Copia del layout tastiera solo per l'utente selezionato
Utente	Visualizzazione del numero di telefono interno e del nome dell'utente.

Parametri	Descrizione
Tipo di dispositivo	Visualizzazione del tipo di telefono dell'utente. Il tipo di dispositivo non può essere modificato per gli utenti già attivi.
Copia il tipo di dispositivo dal terminale	Scelta dell'utente il cui tipo di dispositivo deve essere importato per l'utente selezionato
ai seguenti utenti	Selezione dei terminali nei quali deve essere importato il tipo di dispositivo. È possibile filtrare per tipo di dispositivo dei terminali.

28.3.8 Cordless

In **Cordless** sono incluse le funzioni per la soluzione cordless integrata per l'uso dei telefoni cordless (telefoni DECT) tramite il sistema di comunicazione. Qui vengono configurate le stazioni base e i telefoni DECT (utenti interni con servizi HFA).

28.3.8.1 Cordless > Per tutto il sistema

Descrizione dei parametri delle schede:

- **Modifica i dati globali del sistema**

Parametri	Descrizione
Dati CMI	
EIC	Immissione dell'identificativo DECT esadecimale a 8 cifre del sistema. Tale numero viene fornito al momento dell'acquisto del sistema DECT. Per la reimpostazione procedere come segue: 1° cifra: E/ARC (Classe diritti di accesso) 2°-5° cifra: EIC (Codice installazione attrezzatura) 6°-7° cifra: FPN (Fixed Part Number) 8° cifra: FPS (Fixed Part Subscriber)
Banda freq.	Selezione della banda di frequenza specifica del paese. Per impostazione predefinita viene visualizzata la banda di frequenza assegnata alla sigla internazionale del paese.
Codif. vocale	Visualizzazione dei codec vocali a livello di sistema (a-law, µ-law).
Crittografia	La cifratura è la crittografia dei dati sull'interfaccia aerea e può essere attivata o disattivata. Impostazione predefinita: attiva
Finestra reg.	Tempo di apertura della finestra per l'accesso ai telefoni DECT. La finestra di accesso viene aperta inserendo in uno telefono di sistema il codice *94 2 19970707 e la password. Immettere quindi il numero di telefono del telefono DECT da connettere nella finestra di accesso. Predefinito: 10 minuti

Parametri	Descrizione
Gestione eco	
Questi parametri possono essere utilizzati per disattivare, in **LineeParametri/Flag generali**, la soppressione dell'eco per gli utenti mobili a livello di nodo. L'impostazione viene eseguita dopo le impostazioni di linea per le chiamate. È possibile che una disattivazione generale o l'attivazione di linee specifiche porti a miglioramenti, tuttavia è necessario testare il risultato nei singoli casi.	
Eliminazione eco	A seconda del livello di emissione del telefono DECT, la funzione di eliminazione eco attiva lo smorzamento nella direzione di ricezione del telefono DECT. Se la funzione eliminazione eco è attivata, può verificarsi che in caso di forti rumori parassiti, anche il segnale di ricezione venga attenuato. Ciò può causare ulteriori difficoltà di comprensione. In modalità **Disattivo** la direzione di ricezione del telefono DECT non viene smorzata in caso di forti livelli di emissione. In caso di uso della linea analogica e in ambienti rumorosi, questa impostazione può garantire una migliore comprensione dell'utente sulla linea urbana nel telefono DECT. Predefinito: Automaticamente
Riduzione eco	La funzione di riduzione eco (EC) elimina i ritorni di segnale indesiderati introdotti nella rete fissa da circuiti a 4/2 fili (connessione a forca). In caso di attivazione della funzione di riduzione eco in assenza di echi, possono prodursi errori in quanto tale funzione cercherà di adattarsi a un eco inesistente. In modalità **Disattivo** è impossibile attivare questo parametro, pertanto la funzione di riduzione eco è sempre Off. Predefinito: Automaticamente
Eco artificiale	Tramite un percorso eco artificiale (AE), un segnale vocale della rete fissa viene restituito a un utente remoto attenuato di 24 dB. Ciò può essere necessario (ad esempio nelle connessioni internazionali) per assicurare un certo carico alla funzione di riduzione eco aggiunta. In modalità **Disattivo** è impossibile attivare questo parametro, pertanto la funzione eco artificiale è sempre Off. Predefinito: Automaticamente
PP Deviation Control	Con le connessioni VoIP tramite telefoni DECT si verificano spesso echi. Per eliminare/ridurre al minimo questi fenomeni è possibile attivare la funzione "PP Deviation Control". Questa funzione agisce su tutti i telefoni portatili DECT collegati al sistema di comunicazione. L'attivazione o la disattivazione della funzione è efficace solo se il portatile viene spento e riacceso. Nella modalità **Disattivo** la funzione di soppressione dell'eco non è attiva, quindi possono verificarsi echi nei portatili DECT durante le connessioni VoIP. Predefinita: Disattivo
Modalità ECO	
Modalità ECO	La modalità ECO può essere attivata a livello di sistema per tutti i telefoni DECT. La potenza di trasmissione dei telefoni DECT può essere ridotta di un valore fisso (statico) oppure ogni telefono DECT regola la sua potenza di trasmissione indipendentemente in base all'intensità del segnale ricevuto (adattivo). Predefinita: Disattivo
Modalità ECO: **Off**	La modalità ECO è disattivata a livello di sistema.

Parametri	Descrizione
Modalità ECO: **On**	La modalità ECO (statico) è attivata a livello di sistema. La potenza di trasmissione delle telefoni DECT viene ridotta di un valore fisso.
Modalità ECO: **Adattivo**	La modalità ECO (adattivo) è attivata a livello di sistema. Ogni singolo telefono DECT regola la sua potenza di trasmissione in modo indipendente in base alla potenza del segnale ricevuto. Al momento dell'handover, il telefono passa prima alla potenza di trasmissione elevata, quindi successivamente tale potenza può venire ridotta in base alla potenza del segnale.

28.3.8.2 Cordless > SLC

Descrizione dei parametri delle schede:

- **Modifica telefoni DECT**

Parametri	Descrizione
N. chiamata	Numero di telefono del telefono DECT.
DID	MSN del telefono DECT.
Servizio	Nome del telefono DECT.
In funzione	Dati di accesso del telefono DECT: Verde: il telefono DECT è attivo. Rosso: è stato impostato l'interruttore di blocco del modulo per un telefono DECT registrato. Giallo: il telefono DECT è stato automaticamente disconnesso a causa della modifica del PIN. Grigio: su questa porta non sono ancora stati registrati telefoni DECT.
Codice mobile	Codice PIN per la registrazione del telefono DECT. Il codice mobile deve essere univoco all'interno del sistema.
Accesso	Nome, numero e slot del cavo di prolunga S_0.
Slot	Visualizzazione dello slot del modulo SLC inserito.
Pulsanti	
Elimina	Il telefono DECT è stato rimosso dal sistema. Ciò determina la cancellazione del numero di telefono, della selezione passante e del nome e il rilascio della licenza utente TDM associata.

Descrizione dei parametri delle schede:

- **Aggiungi telefoni DECT**

Parametri	Descrizione
EIC	Se il sistema di comunicazione non appartiene a un sistema di reti (ID nodo = 0), all'identificativo di sistema viene assegnato il valore 1. Se il sistema di comunicazione appartiene a un sistema di reti (ID nodo > 0), l'identificativo di sistema deve corrispondere all'ID del nodo (**Cordless** > **Multi SLC** > **Identificativo sistema**).

Parametri	Descrizione
Slot	Slot del modulo SLC inserito.
N. SLC	Codice ID univoco a livello di sistema del modulo SLC. Intervallo di valori: 1-15,17-31,33-47,...,127. I multipli di 16 non sono consentiti.
Numero di telefoni	Numero di telefoni DECT già configurati di questo modulo SLC.
SLC Num. telefono	Numero di telefono univoco a livello di sistema del cavo di prolunga S_0.
Accesso	Nome, numero e slot del cavo di prolunga S_0.
Aggiungi telefoni DECT	
Numero di telefoni	Se il numero di telefoni DECT è minore della capacità consentita dal sistema (variabile in base alla versione), è qui possibile aggiungere un ulteriore numero di telefoni DECT per questo modulo SLC. I telefoni DECT appena aggiunti vengono visualizzati nella scheda **Modifica utente DECT**.

28.3.8.3 Cordless > Multi-SLC

Descrizione dei parametri delle schede:

- **Modifica multi-SLC**

Parametri	Descrizione
N. SLC	Codice ID univoco a livello di sistema del modulo SLC. Intervallo di valori: 1-15,17-31,33-47,...,127. I multipli di 16 non sono consentiti.
ID nodo	Visualizzazione dell'ID del nodo (se configurato). Se il sistema di comunicazione appartiene a un sistema di reti, qui vengono visualizzati tutti i moduli SLC configurati del sistema di reti.
SLC Num. telefono	Numero di telefono univoco a livello di sistema del cavo di prolunga S_0 del modulo SLC.

28.3.8.4 Cordless > Utenti base

Descrizione dei parametri delle schede:

- **Modifica utenti base**

Parametri	Descrizione
Slot	Visualizzazione dello slot in cui è inserito il modulo SLC della stazione base. Per la scheda madre (SLUC) viene visualizzato lo slot 2.

Parametri	Descrizione
Tipo	Tipo di stazione base. In un modulo SLC il tipo viene solo visualizzato, con la SLUC il tipo può essere anche selezionato. Se si modifica il tipo **Senza porta** in **Utente base**, i 16 telefoni DECT vengono automaticamente preconfigurati e viene impostato un collegamento di rete SLC.
Tipo: **Utente base**	Stazione base collegata.
Tipo: **Senza porta**	Nessuna stazione base collegata.
Servizio	Nome della stazione base.
Livello	Livello della stazione base. Intervallo di valori: 50% e 100%; valore predefinito: 100%
Stato	Stato della stazione base.
Master	Con un modulo SLC vengono visualizzate le porte a cui la stazione base è collegata. Con la SLUC vengono visualizzate tutte le porte del terminale collegato.

28.3.9 Chiamate in entrata

In **Chiamate in entrata** sono riunite le funzioni che vengono utilizzate per la cosiddetta gestione chiamate (Call Management, CM). Fra queste, le impostazioni per i gruppi e l'inoltro chiamate.

28.3.9.1 Chiamata in entrata > Gruppi/Gruppi di ricerca

Per la configurazione iniziale delle chiamate di gruppo e dei gruppi di ricerca, si consiglia di utilizzare la procedura guidata **Chiamata di gruppo/Gruppo di ricerca**.

Descrizione dei parametri delle schede:

- **Modifica numeri di chiamata di gruppo**
- **Visualizza gruppi utilizzati**
- **Visualizza tutti i membri del gruppo**
- **Aggiungi gruppo**
- **Elimina gruppo**
- **Modifica i parametri del gruppo**
- **Visualizza i numeri**
- **Aggiungi membro**
- **Modifica ordine dei membri**
- **Verifica MULAP di base**
- **Verifica preferenze MULAP**

Parametri	Descrizione
Indice	Numero consecutivo assegnato dal sistema di comunicazione.

Parametri	Descrizione
N. di chiamata	Numero di telefono della chiamata di gruppo, gruppo di ricerca, MULAP di base, MULAP esecutivo o gruppo di casella vocale
DID	Numero DID della chiamata di gruppo, gruppo di ricerca, MULAP di base, MULAP esecutivo o gruppo di casella vocale
Nome	Nome liberamente selezionabile per la chiamata di gruppo, gruppo di ricerca, MULAP di base, MULAP esecutivo o gruppo di casella vocale. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Cognome	Cognome liberamente selezionabile per la chiamata di gruppo, gruppo di ricerca, MULAP di base, MULAP esecutivo o gruppo di casella vocale. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Visualizzazione	Nome della chiamata di gruppo, gruppo di ricerca, MULAP di base, MULAP esecutivo o gruppo di casella vocale Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome.
Tipo	Definizione del tipo di gruppo Valore predefinito: Gruppo Per ulteriori informazioni, vedere: Tabella: Opzioni di tipo
Tipo chiam.	Definisce la segnalazione acustica delle chiamate esterne in entrata al gruppo Valore predefinito: 1 Nei telefoni analogici è disponibile solamente l'impostazione predefinita. Le modifiche non hanno alcun effetto.
Tipo di squillo: 1	Due squilli
Tipo di squillo: 2	Tono di chiamata triplo
Tipo di squillo 3	Tono di chiamata breve/lungo/breve
Rubrica telefonica	Quando questo flag è attivato (visualizza Sì), il numero di chiamata del gruppo appare nella rubrica interna. Valore predefinito: Abilitato
Mulap come membro del gruppo	Quando questo flag è attivato, il gruppo MULAP può essere aggiunto come membro in Gruppi.
Membro del gruppo	
Gruppo	Numero (indice) del gruppo
Membro	Numero (indice) del membro all'interno del gruppo
Numero di telefono	Numero di chiamata del membro del gruppo
Nome	Nome del membro del gruppo
Parametri	Parametri abilitati del membro del gruppo

Parametri	Descrizione
Parametro: M	Esperto (M): MULAP di base: Il membro è esperto del MULAP di base. MULAP esecutivo: Il membro ha funzioni Esecutive.
Parametro: R	Chiamata acustica (R): MULAP di base e MULAP esecutivo: Le chiamate in arrivo vengono segnalate acusticamente.
Parametro: A	Impegno automatico in uscita (A): MULAP di base: Il trunk MULAP di base viene selezionato automaticamente per una chiamata quando si solleva il ricevitore. MULAP esecutivo: Il trunk MULAP esecutivo viene selezionato automaticamente per una chiamata quando si solleva il ricevitore.
Parametro: K	Nessuna risposta automatica in entrata (K): MULAP di base e MULAP esecutivo: È infatti necessario premere anche il tasto MULAP.
Parametro: P	Rilascio automatico della privacy (P): MULAP di base e MULAP esecutivo: Premendo il tasto MULAP, è possibile rilasciare la linea MULAP impegnata per una conferenza.
Tasto MULAP configurato	Indica se è stato configurato un tasto MULAP per il membro del gruppo.
Instradamento	Viene visualizzato il percorso per un membro esterno al gruppo.
Gruppo	
Controllo di coerenza	Vengono visualizzate le possibili collisioni dovute alla sovrapposizione degli esperti dei MULAP di base o all’impegno automatico in uscita dei MULAP di base.

Tabella 63: Opzioni di tipo

Parametri	Descrizione
Sono consentite tutte le conversioni di tipo di gruppo senza eliminare i membri del gruppo, ad eccezione dei tipi di gruppo MULAP. **Nota:** Se un gruppo di tipo *Gruppo*, *Gruppo di ricerca lineare*, *Gruppo di ricerca ciclico* o *Casella vocale* ha come membro un gruppo MULAP, la conversione al tipo *Gruppo RNA* o *Gruppo di attesa di chiamata* non è consentita. **Nota:** Se un membro del gruppo imposta l'inoltro di chiamata (*1) su un altro *Gruppo di ricerca*, *Gruppo di attesa di chiamata* e *Gruppo RNA*, la chiamata non viene instradata. L'operazione non è consentita per evitare loop di chiamate. Per le chiamate dirette alla stazione l'inoltro è valido. Per i membri di un *Gruppo ciclico* o *Gruppo lineare (gruppo di ricerca)* l'operazione è consentita, *1 per ogni destinazione funziona, ad eccezione della casella vocale.	
Tipo: Gruppo di ricerca lineare	Una chiamata in entrata viene sempre segnalata per prima al primo membro di un gruppo di ricerca. L'ulteriore segnalazione viene effettuata in base alla sequenza di inserimento dei membri nella tabella dei gruppi.
Tipo: Gruppo di ricerca ciclico	Una chiamata in entrata viene sempre segnalata per prima al membro che segue l'abbonato che ha risposto all'ultima chiamata. L'ulteriore segnalazione viene effettuata in base alla sequenza di inserimento dei membri nella tabella dei gruppi.
Tipo: Gruppo	Chiamata di gruppo di tipo Gruppo: Le chiamate in arrivo vengono segnalate contemporaneamente a tutti i membri del gruppo disponibili. I membri del gruppo disponibili sono gli abbonati che non sono occupati. Se tutti i membri del gruppo sono occupati, la chiamata viene segnalata dal tono di avviso di chiamata. La segnalazione della chiamata continua per tutti i membri del gruppo (tono di avviso di chiamata per i membri del gruppo occupati) anche se l'abbonato riaggancia.
Tipo: RNA	Chiamata di gruppo di tipo RNA: Le chiamate in arrivo vengono segnalate contemporaneamente a tutti i membri del gruppo. Se un membro del gruppo è occupato, l'intera chiamata di gruppo viene contrassegnata come occupata (solo i membri occupati ricevono la segnalazione della chiamata in arrivo). Chi chiama il gruppo riceve il segnale di occupato.
Tipo: MULAP di base	Le chiamate in entrata vengono segnalate visivamente su tutti i telefoni associati al MULAP (Multiple Line Appearance) di base. L'abbonato può anche impostare se le chiamate in arrivo devono essere segnalate acusticamente per ogni singolo membro o no. Lo stato del MULAP di base cambia in occupato e gli altri chiamanti sentono il segnale di occupato quando rispondono a una chiamata. Il numero di telefono del MULAP di base viene visualizzato sul display dell'utente chiamato per le chiamate in uscita tramite il trunk del MULAP di base.

Parametri	Descrizione
Tipo: MULAP esecutivo	È possibile configurare i MULAP esecutivi se si desidera utilizzare funzioni esecutive e di segreteria limitate. Se un chiamante fa squillare il numero di telefono del MULAP esecutivo, la chiamata viene segnalata visivamente a tutti i telefoni appartenenti al MULAP esecutivo. Le chiamate in entrata vengono segnalate anche acusticamente ai membri con funzioni di segreteria.
Tipo: Chiamata in attesa	Chiamata di gruppo di tipo Chiamata in attesa: Le chiamate in arrivo vengono segnalate contemporaneamente a tutti i membri del gruppo disponibili. I membri del gruppo disponibili sono gli abbonati che non sono occupati. Una chiamata è segnalata da un tono di avviso di chiamata per i membri del gruppo occupati.
Tipo: Casella vocale	Messaggio vocale a un gruppo: Un gruppo di casella vocale consente a un gruppo specifico di abbonati di accedere ai messaggi vocali. Quando viene effettuata una chiamata al numero di un gruppo di casella vocale, la chiamata viene inviata direttamente alla casella vocale (ovvero alla segreteria telefonica) del gruppo e non ai membri del gruppo. Dopo che un messaggio vocale è stato lasciato nella casella vocale del gruppo, viene inoltrato alle caselle vocali di tutti i membri. Tutti i membri ricevono contemporaneamente il messaggio vocale. Ogni volta che un membro elimina un messaggio vocale, tale messaggio viene eliminato anche dalle caselle vocali di tutti gli altri membri e dalla casella vocale del gruppo. I messaggi vocali personali di tutti i membri non sono interessati da questa modifica.

28.3.9.2 Chiamate in entrata > Membri del gruppo

Descrizione dei parametri delle schede:

- **Modifica membro**
- **Cancella membro**

Parametri	Descrizione
Gruppo	Numero (indice) del gruppo
Membro gruppo	Numero (indice) del membro del gruppo
Numero di telefono	Numero di telefono del membro gruppo
Nome	Nome proprio del membro del gruppo liberamente scelto. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Cognome	Cognome del membro del gruppo liberamente scelto. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Servizio	Nome del membro del gruppo Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome.
Nome MULAP	Nome del gruppo MULAP (Multiple Line Appearance). Questo è il nome MULAP che viene visualizzato sul display del telefono quando viene chiamato questo gruppo Team. Il nome MULAP è uguale per tutti i membri del gruppo Team con lo stesso tipo.

Parametri	Descrizione
Nr. di tel. MULAP	Numero di telefono del gruppo MULAP
Master (M)	Basic MULAP: l'attivazione di questo flag trasforma un membro nel master del Basic MULAP. Se il master attiva una linea, questa vale per tutti i membri (telefoni) del Basic MULAP. Direttore MULAP: con l'attivazione di questo flag, un membro diventa il direttore. Sollevando il ricevitore le chiamate vengono indirizzate automaticamente tramite il numero Direttore MULAP. Le chiamate in arrivo sul numero Direttore MULAP vengono segnalate solo visivamente.
Segnalazione acustica (S)	Basic MULAP e Direttore MULAP: quando questo flag è attivato, le chiamate in arrivo vengono segnalate acusticamente. Valore predefinito: attivato per tutti i master di un Basic MULAP. Attivato per tutti i membri con funzione Segretario(a) di un gruppo Direttore MULAP.
Impegno automatico in uscita (I)	Basic MULAP: se questo flag è attivato, sollevando il ricevitore la chiamata viene automaticamente connessa tramite la linea MULAP. Direttore MULAP: se questo flag è attivato, sollevando il ricevitore la chiamata avviene automaticamente tramite il Direttore MULAP. Valore predefinito: attivato per tutti i master di un Basic MULAP. Attivato per tutti i membri con funzione Segretario(a) di un gruppo Direttore MULAP.
Nessuna risposta automatica in entrata (N)	Basic MULAP e Direttore MULAP: quando questo flag è attivato, non è possibile rispondere a una chiamata in arrivo semplicemente sollevando il ricevitore. È possibile rispondere a una chiamata in entrata solo premendo il tasto MULAP. Valore predefinito: Disattivato
Abilitazione conferenza automatica (P)	Basic MULAP e Direttore MULAP: quando questo flag è attivato, premendo il tasto MULAP la linea MULAP viene rilasciata per una conferenza. Questo stato viene segnalato a tutti gli altri membri dal lampeggiare del tasto MULAP. Premendo il tasto MULAP è possibile accedere alla conferenza. Valore predefinito: Disattivato
Tasto MULAP configurato	Basic MULAP: quando questo flag è attivato, sul rispettivo telefono viene configurato un tasto MULAP. Premendo il tasto l'impegno in uscita avviene sulla linea MULAP base. Il numero di telefono del MULAP base viene visualizzato sul display dei chiamati. Direttore MULAP: quando questo flag è attivato, sul rispettivo telefono viene configurato un tasto MULAP. Premendo il tasto l'impegno in uscita avviene sulla linea Direttore MULAP. Il numero di telefono del Direttore MULAP viene visualizzato sul display dei chiamati. Valore predefinito: Attivato
Fascio	Per un membro del gruppo esterno, viene visualizzato il fascio.
Tipo	Definizione del tipo di gruppi

28.3.9.3 Chiamate in entrata > Team/top

Per la configurazione iniziale dei gruppi Team e Top è consigliabile utilizzare la procedura guidata **Configurazione team** e **Direttore/Segretaria**.

Descrizione dei parametri delle schede:

- **Mostra tutti i gruppi Team/Top**
- **Mostra i gruppi Team/Top utilizzati**
- **Aggiungi gruppo Team/Top**
- **Modifica gruppo Team/Top**
- **Cancella gruppo Team/Top**
- **Modifica gruppo Team/Top**
- **Mostra tutti i membri del gruppo Team/Top**
- **Aggiungi membro Team/Top**
- **Modifica membro Team/Top**
- **Cancella membro Team/Top**
- **Visualizza caselle fax**
- **Aggiungi casella fax**

Parametri	Descrizione
Indice	Numero progressivo assegnato dal sistema di comunicazione.
Nome	Nome proprio del gruppo Team/Top liberamente scelto. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Cognome	Cognome del gruppo Team/Top liberamente scelto. Valori consentiti: max. 16 caratteri, senza dieresi o caratteri speciali
Servizio	Nome gruppo Team/Top Per impostazione predefinita, viene creato utilizzando i parametri Nome e Cognome in base all'algoritmo di visualizzazione del nome.
Tipo	Definizione del tipo di gruppi
Tipo: Team	Un gruppo Team offre pratiche funzioni pensate per i team. I numeri di telefono di tutti i membri del team vengono impostati tramite tasti MULAP (tasti di linea). In questo modo, ogni membro del team ha accesso a tutte le linee (ad esempio per la funzione risposta per assente) e può telefonare contemporaneamente su più linee.
Tipo: Top	Un gruppo Top offre pratiche funzioni per le funzioni di direttore e segretaria (funzioni Top) per un massimo di tre direttori e tre segretarie.
Team come membro del gruppo	Questo flag è configurabile solo quando il gruppo Team conta membri con lo stesso tipo di periferica, comportando la presenza di un singolo gruppo MULAP in questo gruppo Team. Se il flag è attivato, il gruppo MULAP può essere aggiunto come membro in Gruppi.
Assegnazione tasti a team	Definizione per la creazione dei tasti MULAP dei membri del gruppo Team
Assegnazione tasti a team: sulla prima/seconda console	Se il flag è attivato, i tasti MULAP vengono automaticamente configurati sulla prima o seconda console aggiuntiva (modulo chiave o BLF) del telefono Team.

Parametri	Descrizione
Assegnazione tasti a team: sui primi tasti liberi	Se il flag è attivato, i tasti MULAP vengono automaticamente configurati sul primo tasto libero del telefono Team.
Assegnazione tasti a top	Definizione per la creazione dei tasti MULAP dei membri del gruppo Top
Assegnazione tasti a top: sulla prima/seconda console	Se il flag è attivato, i tasti MULAP vengono automaticamente configurati sulla prima o seconda console aggiuntiva (modulo chiave o BLF) del telefono Top.
Assegnazione tasti a top: sui primi tasti liberi	Se il flag è attivato, i tasti MULAP vengono automaticamente configurati sul primo tasto libero del telefono Top.
Membro gruppo	
Gruppo	Numero (indice) del gruppo
Membri	Numero (indice) del membro all'interno del gruppo
Tipo	Definizione del tipo di membro
N° tel.	Numero del membro del gruppo (diventa un gruppo MULAP con un **Nr. di tel ed accessibile internamente con questo **Nr. di tel)
Servizio	Nome del membro del gruppo
Nr. di tel. MULAP	Numero di telefono del gruppo MULAP
Sel. Pass. MULAP	MSN (Interno) del gruppo MULAP
Nome MULAP	Nome gruppo MULAP. Questo è il nome MULAP che viene visualizzato sul display del telefono quando viene chiamato questo gruppo Team. Il nome MULAP è uguale per tutti i membri del gruppo Team con lo stesso tipo.
Tipo chiam.	Definisce la segnalazione acustica per le chiamate esterne in arrivo per il gruppo Valore predefinito: 1 Nei telefoni analogici è disponibile solamente l'impostazione predefinita. Le modifiche non hanno alcun effetto.
Tipo chiam.: 1	Doppio tono di chiamata
Tipo chiam.: 2	Tono di chiamata triplo
Tipo chiam.: 3	Tono di chiamata breve/lungo/breve
El. telef.	Se il flag è attivato (visualizzazione Sì) viene visualizzato il numero del gruppo nella rubrica interna. Valore predefinito: Attivato
Master (M)	Gruppo Team: l'attivazione di questo parametro trasforma un membro del gruppo Team in un master del gruppo. Se il master attiva una linea questa vale per tutti i membri (telefoni) del gruppo Team. Gruppo Top: con l'attivazione di questo flag, un membro diventa il direttore. Sollevando il ricevitore le chiamate vengono indirizzate automaticamente tramite la linea MULAP di questo membro. Di norma le chiamate in arrivo sul numero Direttore MULAP corrispondente vengono segnalate solo visivamente.

Parametri	Descrizione
Segnalazione acustica (S)	Gruppo Team e gruppo Top: quando questo flag è attivato, le chiamate in arrivo vengono segnalate acusticamente. Valore predefinito: attivato per tutti i membri di un gruppo Top. Attivato per tutti i membri con funzione Segretario/a di un gruppo Top.
Impegno automatico in uscita (I)	Gruppo Team e gruppo Top: Se questo parametro è attivato, sollevando il ricevitore la chiamata avviene automaticamente tramite la linea MULAP del membro. Valore predefinito: Attivato
Nessuna risposta automatica in entrata (N)	Gruppo Team e gruppo Top: quando questo flag è attivato, non è possibile rispondere a una chiamata in arrivo semplicemente sollevando il ricevitore. È possibile rispondere a una chiamata in entrata solo premendo il tasto MULAP. Valore predefinito: Disattivato
Abilitazione conferenza automatica (P)	Gruppo Team e gruppo Top: quando questo flag è attivato, premendo il tasto MULAP la linea MULAP viene rilasciata per una conferenza. Questo stato viene segnalato a tutti gli altri membri dal lampeggiare del tasto MULAP. Premendo il tasto MULAP è possibile accedere alla conferenza. Valore predefinito: Disattivato
Tasto MULAP configurato	Gruppo Team: quando questo flag è attivato, sul rispettivo telefono viene configurato un tasto MULAP. Premendo il tasto l'impegno in uscita avviene sulla linea MULAP del master. L'utente chiamato visualizza il numero di telefono MULAP del master sul display. Gruppo Top: quando questo flag è attivato, sul rispettivo telefono viene configurato un tasto MULAP. Premendo il tasto l'impegno in uscita avviene sulla linea Direttore MULAP. Il numero di telefono del Direttore MULAP viene visualizzato sul display dei chiamati. Valore predefinito: disattivato per tutti i membri di un gruppo Team. Attivato per tutti i membri di un gruppo Top.
Tipo MULAP	Definizione del tipo MULAP
Tipo MULAP: Basic MULAP	Le chiamate in arrivo vengono segnalate visivamente su tutti i telefoni appartenenti al Basic MULAP. Per ciascun membro inoltre viene indicato se le chiamate in entrata devono essere segnalate anche acusticamente. Dopo aver risposto alla chiamata il MULAP base risulta occupato e i chiamanti successivi sentono il tono di occupato. Il numero del Basic MULAP viene visualizzato sul display dell'utente chiamato per le chiamate in uscita tramite la linea Basic MULAP.
Tipo MULAP: Direttore MULAP	Tutti i membri di un Direttore MULAP sono raggiungibili al numero Direttore MULAP e ai propri numeri di telefono.
Numero di telefono fax	Numero di telefono della casella fax dei membri del gruppo
Selezione passante fax	MSN (Interno) della casella fax dei membri del gruppo

28.3.9.4 Chiamate in entrata > Risposta per assente

Descrizione dei parametri delle schede:

- **Assegna nome gruppi di risposta**
- **Mostra utenti del gruppo**
- **Assegna utenti del gruppo**

Parametri	Descrizione
Gruppo	
Gruppo	Numero (indice) del gruppo di risposta per assente Valori consentiti: da 1 a 32 (120 per OpenScape Business S)
Servizio	Nome del gruppo di risposta per assente
Utente	
N° tel.	Numero di telefono dell'utente interno
Servizio	Nome dell’utente interno
Assegnazione gruppo X	Se il flag è attivato: l'utente è assegnato al gruppo di risposta per assente X.
Gruppo	Gruppo di risposta per assente a cui è assegnato questo utente.

28.3.9.5 Chiamate in entrata > UCD

Descrizione dei parametri della scheda:

- **Modifica parametri UCD**

Parametri	Descrizione
Flags UCD	
UCD - rilasciare l'applicazione	Se il flag è attivato: il servizio di distribuzione delle chiamate (UCD) è abilitato a livello di sistema. Valore predefinito: Attivato
Agente sempre disponibile	Se il flag è attivato: tutti gli agenti UCD sono disponibili in modo permanente. Un agente sempre disponibile rimane disponibile per chiamate, fax e e-mail, anche se non ha risposto a una chiamata, fax o e-mail. Valore predefinito: Disattivato
Tempo di elaborazione automatica	
Tempo di elaborazione (cicli)	Definizione a livello di sistema del tempo di elaborazione automatico per gli agenti UCD in un ciclo chiamata, ovvero a intervalli di 5 secondi. Durante il periodo di elaborazione, l'agente abbandona per qualche momento la distribuzione delle chiamate per procedere all'elaborazione della chiamata appena conclusa. Valore predefinito: 0
Priorità nelle chiamate interne	

Parametri	Descrizione
Priorità interna	Definizione a livello di sistema della priorità per le chiamate interne mediante 10 livelli di priorità (1 = alta, 10 = bassa). Valore predefinito: 10
Priorità in caso di chiam.esterne	
Slot / Linea	Visualizzazione dei moduli, degli slot e del numero di linee (del canale B). Per le chiamate esterne la priorità viene determinata in base alla linea (per Canale B), indipendentemente che si tratti di linee IP o TDM.
Priorità	Definizione delle priorità per le chiamate esterne ricevute sulla linea in questione (canale B). La definizione si basa su 10 livelli di priorità (1 = alta, 10 = bassa). Valore predefinito: 1

Descrizione dei parametri delle schede:

- **Visualizza gruppi UCD**
- **Modifica gruppo UCD**

Parametri	Descrizione
Numero di telefono	Numero di telefono del gruppo UCD
MSN	MSN (Interno) del gruppo UCD
Servizio	Nome gruppo UCD
Ciclo prim. chiam.	Definizione del ciclo chiamate primario: La definizione si basa su cicli chiamata, ovvero intervalli di 5 secondi. Viene impostato il tempo di permanenza della chiamata in coda se non viene accettata dall'agente che risulta disponibile da più tempo. Infine la chiamata viene inoltrata al successivo agente disponibile. Valore predefinito: 3 cicli
Ciclo sec. chiam.	Definizione del ciclo chiamate secondario: La definizione si basa su cicli chiamata, ovvero intervalli di 5 secondi. Viene impostato il tempo di permanenza della chiamata in coda se non viene accettata dal successivo agente disponibile. Valore predefinito: 3 cicli
Chiam. in coda	Definizione del numero massimo di chiamate in coda: Se tale valore viene superato, le chiamate successivo possono essere inoltrate ad una destinazione di overflow (destinazione esterna, altro gruppo UCD, utente o gruppo interno). Valore predefinito: 10 (valore predefinito dell'ultimo gruppo UCD: 72)
AICC	Definizione AICC (Automatic Incoming Call Connection). L'impostazione si applica a tutti gli agenti di un gruppo UCD, indipendentemente dal fatto che siano dotati di telefono con cuffia. Valore predefinito: No

Parametri	Descrizione
AICC: sì	Gli agenti di questo gruppo UCD possono rispondere alle chiamate senza effettuare ulteriori operazioni. L'agente viene avvertito tramite un tono specifico dell'arrivo di una chiamata, che viene connessa automaticamente.
AICC: no	Gli agenti di questo gruppo UCD possono rispondere alle chiamate solo effettuando le normali operazioni (ad es. sollevando il ricevitore).
Cambio di annuncio	Definizione del possibile scambio di messaggi Valore predefinito: una sola volta
Cambio di annuncio: singolo	Per i chiamanti in coda d'attesa viene riprodotto un annuncio una sola volta.
Cambio di annuncio: ciclico	L'ultimo e il penultimo annuncio della configurazione vengono ripetuti ciclicamente.
Tempo superam.	Definizione del tempo superamento in secondi: Se non si risponde alla chiamata mediante l'applicazione UCD entro il periodo impostato, la chiamata viene rielaborata in base alle indicazioni di Call Management nel sistema di comunicazione. Questa impostazione è rilevante solo se è collegata un'applicazione UCD esterna. Valore predefinito: 600
Ritardo annuncio	Definizione del ritardo dell'annuncio in secondi: trascorso questo tempo, il chiamante in coda d'attesa riceve un messaggio. Valore predefinito: 0

Descrizione dei parametri della scheda:

- **Modifica parametri gruppo UCD**

Parametri	Descrizione
Indice destinazione	Per ogni gruppo UCD possono essere definite fino a sette destinazioni (indice 1-7) per gli annunci. Gli annunci delle destinazioni vengono riprodotti per l'utente nella coda d'attesa uno dopo l'altro.
Annuncio	Annuncio per l'indice destinazione corrispondente.
Destinazione d'attesa	L'annuncio può essere riprodotto ciclicamente (max 9 cicli di 5 secondi = 45 secondi) o continuamente. Una volta trascorso questo tempo, per il chiamante in coda d'attesa viene riprodotto l'annuncio dell'indice successivo (nessun annuncio se si è scelta l'opzione **continuo**). Opzione predefinita: Continuo

Descrizione dei parametri della scheda:

- **Aggiungi/Cancella membri gruppo UCD**

Parametri	Descrizione
Scelta	Elenco di tutti gli ID UCD degli agenti. Gli ID agente UCD non corrispondono ai numeri nel sistema di comunicazione.
Membri	Elenco degli agenti UCD del gruppo UCD selezionato
Pulsanti	
Aggiungi	Aggiunge gli ID UCD agente selezionati del gruppo UCD.
Elimina	Elimina gli ID UCD agente selezionati dal gruppo UCD.

Descrizione dei parametri della scheda:

- **Assegna a utente**

Parametri	Descrizione
IDAgente	Elenco degli agenti UCD del gruppo UCD selezionato.
Utenti	Elenco degli utenti del gruppo UCD a cui è possibile assegnare gli ID UCD agente.

28.3.9.6 Chiamate in entrata > Inoltri

Descrizione dei parametri delle schede:

- **Elenchi destinazioni chiamata - Definizione**

Parametri	Descrizione
Lista destinazioni chiamata	Selezione della lista destinazioni chiamata da elaborare. Valori consentiti: da 1 a 740
Modifica inoltro Per trovare una destinazione di chiamata più velocemente, è anche possibile inserire nei campi **Destinazione 1 - 4** una o più cifre. Successivamente si passa direttamente alla voce del menu che inizia con la serie di cifre inserita. È anche possibile immettere una sequenza di lettere.	
Destinazione 1-4: **Nessuna voce**	La destinazione di chiamata viene saltata.
Destinazione 1-4: **Destinazione esterna**	Fascio e numero di telefono esterno con il codice di accesso linea urbana.
Destinazione 1-4: ***Utente chiamato**	Utente chiamato.
Destinazione 1-4: ****Definito dall'utente**	Destinazione del trasferimento di chiamata a tempo (se configurato).
Destinazione 1-4: **#9 Ricerca sistema**	Utente disponibile successivo (eccetto interno del direttore).

Parametri	Descrizione
Destinazione 1-4: **#201 - #260**	Distribuzione delle chiamate (gruppo UCD).
Destinazione 1-4: **#801 - #817**	Risponditore.
Destinazione 1-4: 100, 101, ...	Numero di telefono di un utente o di un gruppo (ad esempio casella vocale)
L'inoltro chiamate inizia dopo	Tempo trascorso il quale una chiamata viene inoltrata alla destinazione di chiamata successiva. Nei gruppi UCD, l'inoltro segue i meccanismi dei cicli di chiamate primario e secondario (vedere gruppi UCD). Intervallo di valori: 5/10/15/...75 s, predefinito: 15 s
Inoltro di chiamata	Se occupato, la chiamata viene immediatamente inoltrata alla destinazione successiva. Valore predefinito: attivato
2ª suoneria	
Seconda suoneria destinazione	Gli utenti interni aggiuntivi presso i quali la chiamata viene segnalata o un attuatore (relè) di un modulo attuatore/sensore per una suoneria centrale.
Tipo seconda suoneria	La chiamata può essere segnalata immediatamente all'utente o una volta trascorso l'intero tempo di inoltro. Valore predefinito: Adesso

Descrizione dei parametri delle schede:

- **Elenchi destinazioni chiamata - Assegnazione**

Parametri	Descrizione
N. chiamata	Numero di telefono dell'utente o del gruppo.
Servizio	Nome dell'utente o del gruppo.
Tipo	Tipo di utente, ad esempio U_{P0}, client di sistema, AB, ISDN, SIP.
giorno	Numero della lista destinazioni chiamata per le chiamate esterne in entrata durante l'orario d'ufficio (servizio giorno) Valore predefinito: 14
Notte	Numero della lista destinazioni chiamata per le chiamate esterne in entrata con servizio notte attivato Valore predefinito: 15
Interna	Numero della lista destinazioni chiamata per chiamate interne in entrata Valore predefinito: 16

Parametri	Descrizione
Cerca	Se nei campi di ricerca **N° tel** o **Nome** viene inserito un termine di ricerca e successivamente si preme il tasto Invio, vengono visualizzati tutti i risultati che contengono il termine di ricerca. Immettendo `521` come numero di telefono verranno ad esempio trovati i numeri `+495213535` e `+498967521` oppure con `co` inserito come nome, verranno trovate le voci `Collins`, `Mcoin` e `Branco`. Se non si inserisce nulla in nessun campo di ricerca e si preme il tasto Invio, vengono visualizzate tutte le voci.

Descrizione dei parametri delle schede:

- **Membri dell'elenco dest.**

Parametri	Descrizione
Mostra tutti i membri con l'elenco destinazioni di chiamata	Per la lista destinazioni chiamata selezionata vengono visualizzati tutti gli utenti e gruppi che utilizzano tale lista.

Descrizione dei parametri delle schede:

- **Copia elenchi destinazioni di chiamata**

Parametri	Descrizione
Lista destinazioni chiamata	Selezione della lista destinazioni chiamata a cui l'utente deve essere assegnato. Valori consentiti: da 1 a 740
giorno	Lista destinazioni chiamata per le chiamate esterne in entrata durante l'orario d'ufficio (servizio giorno)
Notte	Lista destinazioni chiamata per le chiamate esterne in entrata con servizio notte attivato
Interna	La lista destinazioni chiamata è per chiamate interne in entrata
Elenchi destinazioni chiamata	
Scelta	Lista di tutti gli utenti.
Membri	Lista degli utenti a cui è assegnata la lista destinazioni chiamata.
Pulsanti	
Aggiungi	Gli utenti selezionati vengono trasferiti dalla finestra di selezione alla finestra dei membri.
Elimina	Gli utenti selezionati vengono cancellati dalla finestra dei membri.

28.3.10 Linee/Rete

In **Linee/Rete** sono riunite le funzioni relative a linee e fasci.

28.3.10.1 Linee/Rete > Linee

Descrizione dei parametri delle schede:

- **Mostra tutte le linee**
- **Cambia gruppo di linee**

Parametri	Descrizione
Linea	Visualizzazione della linea esterna fisica collegata al sistema di comunicazione.
Box-SI-Pt-Li o Box/Slot/ Porta/Linea	Visualizzazione del tipo di modulo, dello slot e del numero di porta (porta fisica) per collegare la linea al sistema di comunicazione.
Codice	Visualizzazione o configurazione del codice del fascio. Inserendo questo numero, la linea assegnata viene impegnata dal sistema di comunicazione. Viene usato per provare la linea o per programmare un tasto linea. Se vengono utilizzate applicazioni CSTA, impostare il valore per questo parametro.
Fascio	Visualizzazione o scelta del fascio a cui è assegnata la linea (nessuno o da fascio 1 a fascio 12). Se per una linea attiva viene inserito "nessuna", il sistema si comporta in modo instabile. Il sistema inoltre può ricevere chiamate su questa linea ma non può inoltrarle.
Stato	Visualizzazione dello stato della linea. Una linea non attiva è contrassegnata da una stella.
Tipo	Visualizzazione del tipo di linea. Le linee non attive sono contrassegnate con "No Port".

Descrizione dei parametri delle schede:

- **Tutte le linee di assegnaz.chiam.**

Parametri	Descrizione
Linea	Visualizzazione della linea esterna fisica collegata al sistema di comunicazione.
Box-SI-Pt-Li o Box/Slot/ Porta/Linea	Visualizzazione del tipo di modulo, dello slot e del numero di porta (porta fisica) per collegare la linea al sistema di comunicazione.
Nr. tel. Giorno	Visualizzazione del numero di telefono assegnato per il servizio giorno
Nome Giorno	Visualizzazione del nome del numero di telefono assegnato al servizio giorno
Nr. tel. Notte	Visualizzazione del numero di telefono assegnato per il servizio notte
Nome Notte	Visualizzazione del nome del numero di telefono assegnato al servizio notte

Descrizione dei parametri delle schede:

- **Aggiungi linea**

Parametri	Descrizione
Numero	Numero di linee da aggiungere.

Descrizione dei parametri delle schede:

- **Cambia direzione**

Parametri	Descrizione
Linea	Visualizza il numero della linea.
in uscita	Sulla linea è possibile effettuare chiamate in uscita. **Nota:** È possibile effettuare chiamate di emergenza anche se il flag è disattivato.
in entrata	Sulla linea è possibile ricevere chiamate.

Descrizione dei parametri delle schede:

- **Cambia linea**
- **Cancella linea**

Parametri	Descrizione
Linea	Visualizzazione dei numeri di linea.
Box/Slot/Porta/Linea	Visualizzazione della porta fisica della linea (box/slot/porta/linea).
Codice	Visualizzazione o immissione del codice del fascio.
Fascio	Visualizzazione o scelta del fascio a cui è assegnata la linea (nessuno o da fascio 1 a fascio 12).
Linea di assegnaz.chiam.	
Nr. tel. Giorno	Numero di telefono per connessione in entrata che non supporta connessioni passanti, servizio giorno.
Nr. tel. Notte	Numero di telefono per connessione in entrata che non supporta connessioni passanti, servizio notte.

Descrizione dei parametri delle schede:

- **Cambia flag ISDN**

Parametri	Descrizione
Protocollo: Descrizione	Ogni voce di modello di protocollo comprende gli elementi interfaccia, protocollo e informazioni aggiuntive: connessione base S0 2B+D tramite interfaccia S0, connessione base BRI 2B+D tramite interfaccia U2B1Q (USA), connessione primaria multiplex S2 30B+D, connessione primaria multiplex T1 23B+D (USA)
Logico/Fisico	Conteggio logico o fisico dei canali
Canale B slave neg: Master	Impostazione master/slave nell'ambito del layer 3. Per le connessioni, un lato deve essere configurato come slave e l'altro come master.
Su canale B alloc: Giù	Determinazione della numerazione dei canali B (deve essere la stessa in entrambi i sistemi)

Parametri	Descrizione
Formato S0 CHI: S2M	Formato protocollo CHI, impostare come S0 (formato breve) o S2M (formato lungo)
Simmetrico/asimmetrico	Uso simmetrico o non simmetrico degli elementi protocollo L3
Automatico/fisso	Negoziazione automatica o assegnazione fissa della simmetria
1 lunghezza CR: 2	Formato protocollo - lunghezza di riferimento chiamata
Segnalazione allarme	Utilizzo di segnalazioni di allarme nel protocollo layer 3
Timer protocollo attivato	Utilizzo del timer layer 3
Avvio veloce PRI	Utilizzo della procedura PRI QuickStart
IE_TNS	Utilizzo di elementi informativi Transit Network Selection
IE_OSA	Utilizzo di elementi informativi Open Access Service
CIDL	Utilizzo di segnalazione di chiamata e segnalazione ID collegamento nella connessione di rete
Lato utente/Lato rete	Definizione del protocollo Layer 2. Sul lato opposto è richiesta un'impostazione corrispondente
Rete/Utente	Definizione del protocollo Layer 2. Sul lato opposto è richiesta un'impostazione corrispondente
PP/PMP	Configurazione punto-punto o punto-multipunto, importante solo per S0
Costantemente attivo	Layer 2 permanentemente attivo
Verifica TEI attiva	Attivazione controllo TEI
Lato utente/Lato rete	Definizione del protocollo Layer 1. Sul lato opposto è richiesta un'impostazione corrispondente
PP/PMP	Definizione del protocollo Layer 1. La stessa impostazione è richiesta su entrambi i lati necessari
Tipo bus S: L	bus corto/lungo (range)
Costantemente attivo	Definizione del protocollo Layer 1. La stessa impostazione è richiesta su entrambi i lati necessari
Controllo CRC4	Definizione del protocollo Layer 1, rilevante solo per S2M, entrambi i lati richiedono la stessa impostazione
Report CRC4	Definizione del protocollo Layer 1, rilevante solo per S2M, entrambi i lati richiedono la stessa impostazione

Descrizione dei parametri delle schede:

- **Cambia canale B**

Parametri	Descrizione
Canale B	Visualizzazione del numero di canali B.

Parametri	Descrizione
In uscita	Sul canale B è possibile effettuare chiamate in uscita.
In entrata	Sul canale B è possibile ricevere chiamate.

Descrizione dei parametri delle schede:

- **Cambia direzione**

Parametri	Descrizione
Linea	Visualizzazione dei numeri di linea.
In uscita	Sulla linea è possibile effettuare chiamate in uscita.
In entrata	Sulla linea è possibile ricevere chiamate.

28.3.10.2 Trunk/Instradamento > Gruppo di trunk

Descrizione dei parametri delle schede:

- **Cambia percorso**

Parametri	Descrizione
Nome percorso	Nome del percorso. Il nome inserito sostituisce il numero di percorso predefinito nell'elenco Percorsi.
Codici di impegno	Qui vengono inseriti i codici di assegnazione per ciascun percorso. I codici di instradamento inseriti devono essere privi di collisioni, sia tra loro che all'interno dell'intero piano di numerazione del sistema di comunicazione. Utilizzare il pulsante Verificare per verificare la presenza di collisioni. Il codice di impegno è il codice che induce il sistema di commutazione a fornire una linea alla stazione che ha composto il codice. I codici di impegno funzionano solo se LCR non è stato attivato.
Codice CO (2° codice trunk)	Un secondo codice trunk (codice CO) viene definito se il sistema di comunicazione è un sottosistema di un altro sistema di comunicazione o è collegato in rete con diversi altri sistemi di comunicazione. È rilevante solo per i percorsi di rete (tipo di percorso = PABX). In questo caso, il secondo codice trunk è il codice di impegno per il sistema principale. All'interno di una rete, i codici per l'impegno del trunk, i codici di impegno del percorso e il secondo codice CO devono essere configurati in modo uniforme. Il valore predefinito in Germania è 0.
Posizione del gateway	
Codice paese	Visualizza il codice paese della posizione del proprio gateway. Da impostare tramite Impostazioni di base/Gateway/Posizioni gateway
Prefisso locale	Visualizza il prefisso locale della posizione del proprio gateway. Da impostare tramite Impostazioni di base/Gateway/Posizioni gateway
Numero PABX	Visualizza il numero PABX della posizione del proprio gateway. Da impostare tramite Impostazioni di base/Gateway/Posizioni gateway
Numero stazione di sistema - in entrata	

Parametri	Descrizione
Codice paese	Utilizzato per l'analisi delle cifre delle chiamate in entrata. Codice paese senza zeri iniziali (ad esempio, 1 negli Stati Uniti, 49 in Germania)
Prefisso locale	Utilizzato per l'analisi delle cifre delle chiamate in entrata. Prefisso locale senza zeri iniziali (ad esempio, 89 per Monaco di Baviera)
Numero PABX	Utilizzato per l'analisi delle cifre delle chiamate in entrata. Numero PABX (numero di telefono centrale dell'azienda, ad esempio 777)
Numero di posizione	Utilizzato per l'analisi digitale dei numeri di telefono pubblici per le connessioni in uscita. Verifica le informazioni di composizione per determinare se il numero di destinazione chiamato si trova nel proprio sistema.
Numero della stazione di sistema - in uscita Informazioni: Le modifiche ai numeri PABX in uscita devono essere coordinate con i fornitori di rete. (Clip senza screening)	
Codice paese	Utilizzato per l'identificazione del chiamante nelle chiamate in uscita. Il codice paese senza zeri iniziali (ad esempio, 1 negli Stati Uniti, 49 in Germania) viene trasmesso alla rete. Se non viene inserito alcun "numero PABX in uscita", viene utilizzato automaticamente il "numero PABX in entrata".
Prefisso locale	Utilizzato per l'identificazione del chiamante nelle chiamate in uscita. Il prefisso locale qui specificato (senza zeri iniziali, ad esempio 89 per Monaco) viene trasmesso alla rete. Se non viene inserito alcun "numero PABX in uscita", viene utilizzato automaticamente il "numero PABX in entrata".
Numero PABX	Utilizzato per l'identificazione del chiamante nelle chiamate in uscita. Il numero PABX specificato qui (numero di telefono centrale dell'azienda, ad esempio 777) viene trasmesso alla rete. Se non viene inserito alcun "numero PABX in uscita", viene utilizzato automaticamente il "numero PABX in entrata".
Soppressione staz. N. di chiamata	Attivando questo flag, si nasconde il numero DID nell'ID chiamante.
Percorso di overflow	
Percorso di overflow	Se tutte le linee del percorso configurato sono impegnate, è possibile impostare un overflow su un altro percorso. Il percorso di overflow si applica solo quando LCR è disabilitato.
Trasmissione delle cifre	
Trasmissione delle cifre	Il tipo di trasmissione delle cifre viene determinato qui per il percorso selezionato e viene visualizzato come testo statico (ad esempio, tabella dei percorsi 6: invio in blocco) in Impostazioni | Instradamento a minor costo | Piano di composizione dopo aver selezionato la tabella dei percorsi (vedere l'elenco a discesa Tabella dei percorsi).
Trasmissione delle cifre: Cifra per cifra	Le cifre vengono trasmesse in sincronia con la composizione del numero.

Parametri	Descrizione
Trasmissione delle cifre: invio in blocco	Durante la trasmissione in blocco delle cifre (composizione in blocco per percorso), le cifre composte vengono memorizzate dal sistema di comunicazione. La composizione avviene solo quando è trascorso un determinato tempo dall'ultima cifra digitata, quando è stato inserito il codice di fine composizione # o se viene trovata una corrispondenza esatta nella regola di composizione. Nel caso del PRI negli Stati Uniti, la composizione a blocchi verso l'ufficio centrale è obbligatoria. Per poter selezionare la trasmissione di cifre in blocco, è necessario attivare LCR. Il tipo di trasmissione delle cifre viene impostato automaticamente sulla trasmissione delle cifre in blocco nella tabella dei percorsi se almeno un percorso della tabella dei percorsi LCR è configurata con la trasmissione delle cifre in blocco.
Numero di estensione mobile (MEX)	
Numero MEX	Se l'ITSP utilizzato supporta la funzione "Estensione mobile (MEX)", è necessario inserire qui il numero MEX (8 cifre, solo numeri) fornito dall'ITSP. Questa funzione può essere utilizzata solo con una connessione DID per telefonia Internet (SIP come ISDN). Viene utilizzato per integrare telefoni cellulari/smartphone nel sistema di comunicazione. L'utente del telefono cellulare può essere raggiunto tramite il servizio One Number Service con un unico numero di telefono, che viene comunicato anche all'altra parte. Quando un abbonato effettua una chiamata con il proprio telefono cellulare, l'interlocutore visualizza il numero dell'ufficio dell'abbonato, quindi il numero del telefono cellulare dell'abbonato rimane sconosciuto. Inoltre, gli altri abbonati interni possono verificare lo stato di presenza di tali abbonati anche se stanno parlando al cellulare.
Utente esterno affidabile	
Utente esterno affidabile	Utente che può essere assegnato a piattaforme di collaborazione esterne come MS Teams per effettuare chiamate telefoniche.

Descrizione dei parametri delle schede:

- **Modifica dei parametri di instradamento**

Parametri	Descrizione
Flag di instradamento	
Ripetizione di cifre su	Quando viene impegnato un percorso in uscita con la ripetizione delle cifre attivata, il codice di instradamento viene inviato prima del numero di chiamata. Questo vale solo se LCR è disattivato (vedere Impostazioni | Instradamento a minor costo).
Analisi del secondo tono di linea/Monitoraggio trunk	L'analisi del secondo tono di linea avvisa il sistema di comunicazione di rilevare un segnale di linea aggiuntivo. Questa funzione viene utilizzata con applicazioni di sistemi di comunicazione tandem. Questa valutazione dipende dal Paese, ad esempio in Belgio dopo lo 00 e in Francia dopo il 16 o il 19. Non è rilevante in Germania. Vale solo per i fornitori di rete che inviano un secondo tono di linea per le chiamate internazionali.

Parametri	Descrizione
Intercettazione per direzione	Questo flag è necessario per la connessione di rete QSIG. Quando questo flag è impostato, il sistema di comunicazione verifica se la stazione remota ha ricevuto una richiesta di deviazione o se il sistema di comunicazione ha implementato il trasferimento in avanti alla posizione di intercettazione centrale. La stazione remota riceve un messaggio che indica se è necessario o meno attuare una deviazione per questa chiamata. Se l'intercettazione è attivata per un percorso, tutte le chiamate inoltrate a questo percorso vengono intercettate in questa posizione di intercettazione. Per implementare questa funzione, è necessario configurare i numeri diurni e notturni per ciascun percorso (vedere Assegnazione suonerie per linea). Inoltre, non è necessario inserire una posizione di intercettazione per il servizio diurno/notturno (vedere Intercettazione/Attendant).
Audio Over. service 3.1 kHz	Per tutte le chiamate in uscita su ISDN, Audio Over. service 3.1 kHz è l'impostazione predefinita. Si tratta del tipo di trasmissione standard per le chiamate in uscita su una linea ISDN (Integrated Services Digital Network). Una connessione dal sistema di comunicazione a un CO digitale con un modem analogico deve essere identificata come servizio dati. Questo flag deve essere impostato per evitare problemi durante il funzionamento del FAX. In alcuni casi, un operatore di rete potrebbe non supportare il servizio dati audio a 3,1 kHz. Ciò può causare il mancato invio dei fax a determinati numeri di telefono esterni. Una possibile soluzione è disabilitare il flag **Audio Over. service 3.1 kHz**.
Aggiunta prefisso di direzione in entrata	Quando questa opzione è attivata sui telefoni di sistema con impegno in entrata, oltre al numero di chiamata viene visualizzato anche il codice del percorso.
Aggiunta prefisso di direzione in uscita	Quando questa opzione è attivata con impegno in uscita, oltre al numero di chiamata viene visualizzato anche il codice di accesso. Informazioni: la modifica di questo parametro influisce sull'identificazione del chiamante e deve quindi essere coordinata con i fornitori di rete. (Clip senza screening)
N. di chiamata con prefisso internazionale/nazionale	Se questo flag è abilitato, il codice nazionale o internazionale del numero di telefono (ad esempio, 02302…., 00492302...) deve essere aggiunto come prefisso per l'ITSP. Impostazione predefinita: funzione attivata
Tono di richiamata verso CO	Se questo flag è impostato, verrà inviato un "tono di richiamata" alla centrale ISDN in caso di chiamata in entrata. Si tratta di un protocollo speciale necessario per i provider Global One e Sovintel.
Segmentazione	Quest'area definisce il comportamento del sistema durante l'invio di messaggi ISDN in cui viene superata la lunghezza massima dei dati utente del livello 2 (260 byte).
Segmentazione: sì	Il messaggio da inviare viene suddiviso in segmenti da 260 byte e inviati singolarmente. Il sistema di comunicazione ricevente deve supportare la segmentazione e raccogliere e organizzare i singoli segmenti in un messaggio.
Segmentazione: no	La segmentazione non è necessaria, poiché il livello 2 sottostante è in grado di trasportare messaggi di qualsiasi lunghezza.

Parametri	Descrizione
Segmentazione: Tronca messaggio	Il messaggio da inviare viene troncato a meno di 260 byte eliminando le parti meno importanti (come ad esempio i nomi) e quindi inviato.
Disattiva UUS per percorso	La segnalazione da utente a utente (UUS) può essere disattivata con questo flag. In tal modo si sopprime la trasmissione del nome e del numero di telefono della stazione A nell'elemento UUI (informazioni da utente a utente, UUI) per l'inoltro delle chiamate esterne (inoltro esterno). Questo flag deve essere disattivato manualmente per Telefonica.
Usa sempre DSP	Se questo flag è impostato, la connessione al provider di servizi di telefonia Internet è possibile solo tramite un DSP (processore di segnale digitale). Se questo flag non è impostato, esiste una connessione Direct Payload al provider di servizi di telefonia Internet. Questo flag deve essere impostato per il percorso della rete OpenScape Voice. Questo flag non può essere impostato nel caso di trasmissioni fax (T.38) tramite un dispositivo esterno (ad esempio, Mediatrix 4102).
Nome in CO	Questo flag è configurato per i CO che supportano il nome del chiamante.
Impegno trunk analogico	Qui è possibile selezionare diversi intervalli di tempo che determinano l'inizio della composizione del numero quando si utilizzano linee di composizione analogiche (MSI). Se non è impostata alcuna pausa, il sistema di comunicazione attende fino a quando non riconosce il tono di composizione. Nota per il Brasile: Quando si utilizza la segnalazione DTMF da terminali analogici in combinazione con trunk analogici e impulso digitale dopo il rilevamento del tono di composizione, potrebbero verificarsi problemi con la restrizione delle chiamate interurbane quando il codice paese è impostato su Brasile. In questo caso, i segnali DTMF provenienti dai terminali analogici vengono inviati direttamente ai trunk analogici (la "procedura 1A" non viene utilizzata). Per questo motivo, i segnali DTMF digitati prima della ricezione del tono di composizione vengono persi. Di conseguenza, in questi casi, è necessario abilitare l'instradamento al minor costo (LCR) affinché il metodo di composizione e la restrizione delle chiamate a pagamento funzionino correttamente sul dispositivo.
Pausa chiamata trunk	La pausa della chiamata CO determina il periodo di tempo che trascorre prima che una chiamata venga riconosciuta come completata una volta che l'utente ha riagganciato. Questa opzione è valida solo per le linee MSI. Per una chiamata interurbana con, ad esempio, 1 secondo di attivazione e 4 secondi di disattivazione, è necessario configurare una pausa di 6 secondi. In alcuni CO, tuttavia, è prevista una pausa di 10 secondi tra uno squillo e l'altro. In questi casi, è necessario programmare una pausa di 13 secondi per le chiamate trunk. In caso contrario, non sarà possibile implementare la deviazione di chiamata. Negli Stati Uniti, questo ciclo dura due secondi acceso e due secondi spento, per un totale di sei secondi. L'opzione di sei secondi è quella predefinita, quindi non è necessario apportare alcuna modifica. Intervallo di impostazione: da 2 a 13 secondi.
Tipo di impegno	Questo campo specifica i criteri da applicare nel caso in cui il sistema di comunicazione abbia necessità di impegnare una linea in uscita.
Tipo di impegno: ciclico	Il sistema di comunicazione avvia la ricerca ciclica di una linea libera con il numero di linea successivo in base all'ultima linea in uscita impegnata in questo percorso.

Parametri	Descrizione
Tipo di impegno: lineare	Il sistema di comunicazione inizia sempre la ricerca dal numero di linea più basso assegnato a questo percorso.
Tipo di percorso	Ci sono due opzioni per il tipo di percorso. Il tipo di percorso può essere impostato come CO (Central Office) o come PABX (Private Automatic Branch Exchange).
Tipo di percorso: CO	Le linee assegnate a questo percorso sono soggette a restrizioni per le chiamate a pagamento. Quando LCR è attivo, la restrizione delle chiamate a pagamento è regolata dal piano di composizione (colonna COS).
Tipo di percorso: PABX	La restrizione per le chiamate a pagamento viene applicata solo se a questo percorso è assegnato un secondo codice CO. Quando LCR è attivo, la restrizione delle chiamate a pagamento è regolata dal piano di composizione (colonna COS). Il tipo di percorso influisce anche sul testo predefinito del nome del percorso (vedere Percorsi) e sulla procedura utilizzata per riconoscere il tono di composizione sulle linee MSI.
N. e tipo, in uscita	L'amministratore può configurare separatamente il "numero PABX in entrata" e il "numero PABX in uscita", suddivisi in parti per il prefisso internazionale, il prefisso locale e il numero PABX (= numero di connessione nella rete locale). Ciò è necessario per l'implementazione della funzione "CLIP senza screening". Se non è stato configurato alcun "numero PABX in uscita", il sistema di comunicazione utilizzerà sempre i dati dell'impostazione "numero PABX in entrata". In caso di un impegno in entrata su una linea ISDN, il sistema di comunicazione tronca il numero PABX (allineato a sinistra) dal numero di telefono ricevuto e interpreta la parte restante come numero di selezione diretta interna. Per le informazioni relative al numero di chiamata verso la rete PSTN, il sistema di comunicazione inserisce automaticamente il numero PABX (o la parte definita nella configurazione) come parte iniziale del numero di chiamata. Ciò non si applica alle informazioni di composizione (indirizzo di destinazione). I numeri di chiamata delle stazioni interne inviati alla stazione remota possono essere composti come segue:
N. e tipo, in uscita: Sconosciuto	solo numero DID (impostazione predefinita)
N. e tipo, in uscita: Numero PABX	numero PABX + numero DID
N. e tipo, in uscita: Prefisso locale	+ Prefisso locale + Numero PABX + Numero DID
N. e tipo, in uscita: Codice paese	Prefisso internazionale + Prefisso locale + Numero PABX + Numero DID
N. e tipo, in uscita: Interna	Solo per sistemi in rete: non è possibile aggiungere prefissi numerici per piani di numerazione chiusi. I prefissi dei numeri di chiamata sono stati omessi.
Tipo di numero di chiamata	Le impostazioni nell'area "N. e tipo, in uscita" influiscono anche sulle chiamate provenienti da un interno in un sistema partner (un nodo in rete). A causa di questa impostazione, il numero del chiamante ricevuto dal nodo in rete e inoltrato al Central Office viene esteso per il percorso in uscita.

Parametri	Descrizione
Tipo di numero di chiamata: Interna	In questo caso viene trasmesso solo il numero di chiamata interno. Se la destinazione è una stazione esterna, non viene trasmesso alcun numero oppure viene trasmesso solo quello dell'Attendant Console. Il numero di chiamata interno può essere visualizzato quando la destinazione è una stazione interna su un altro nodo.
Tipo di numero di chiamata: Selezione passante	In questo caso viene trasmesso solo il numero DID. Il numero di chiamata interno non viene fornito per la visualizzazione presso destinazioni interne in altri nodi. Le informazioni relative al numero di chiamata sono sufficienti per le destinazioni esterne.
Tipo di numero di chiamata: Interno/DID	Questa impostazione è utile per scopi di connessione in rete. Sia il numero di chiamata interno che il numero di chiamata DID vengono trasmessi alla stazione di destinazione. Se viene chiamata una stazione interna all'interno della rete, è possibile visualizzare il numero di chiamata interno del chiamante per questa stazione. Se la stazione di destinazione interna ha attivato l'inoltro delle chiamate verso una destinazione esterna, ad esempio, anche in questo caso è possibile trasmettere il numero DID.
Reinstradamento	
Cambia percorso	Quando questo flag è attivato, è anche possibile instradare le informazioni del canale D tramite altri percorsi. Questa opzione consente di impostare percorsi alternativi tramite altri percorsi. L'opzione può essere attivata solo quando il piano di numerazione delle chiamate è inequivocabile. (Numerazione chiusa o codici di impegno univoci in una rete. Anche il sistema che effettua la richiesta deve supportare questa funzione.). Se viene implementato il reindirizzamento, è necessario impostare anche il reindirizzamento con modifica percorso attiva per il percorso corrispondente. Questa opzione è disponibile solo per il collegamento in rete CorNet NQ e deve essere attivata allo stesso modo in entrambi i sistemi di comunicazione in rete.
Ottimizzazione percorso attiva	Per ottimizzare l'uso del canale B, il trasferimento di chiamata può essere eseguito sulla base del protocollo in conformità con la specifica "Inoltro di chiamata/Reindirizzamento parziale". Se il reindirizzamento parziale viene rifiutato, viene utilizzato il trasferimento in avanti.
Ottimizzazione percorso attiva: No	Quando si seleziona questa opzione, il reindirizzamento viene disattivato. Per l'inoltro delle chiamate, la connessione viene sempre stabilita tramite due canali B.
Reinstradamento attivo: Se il percorso è noto	Quando si seleziona questa opzione, il reindirizzamento è attivo solo se il percorso è noto e se viene eseguita con successo una procedura di "handshake" tra i due sistemi di comunicazione in rete.
Ottimizzazione percorso attiva: Sempre	Se la configurazione per la chiamata in entrata è impostata sullo stesso percorso della destinazione di inoltro della chiamata, la chiamata verrà rifiutata (viene utilizzata la funzione di deviazione delle chiamate) dal sistema di comunicazione se questa opzione è attivata. Nel caso di sistemi collegati in rete, questa opzione deve essere attivata sempre allo stesso modo in entrambi i sistemi di comunicazione in rete.

Descrizione dei parametri delle schede:

- **Modifica parametro speciale**

Parametri	Descrizione
Piano di numerazione Definisce il parametro Piano di numerazione nei messaggi in uscita	
Numero del destinatario della chiamata	Verifica di sistema = definita dal sistema; piano di numerazione ISDN, piano di numerazione privato, piano di numerazione sconosciuto = preimpostato manualmente
Tutti gli altri	ad esempio, numero del chiamante, numero di reindirizzamento, ecc. Verifica di sistema = definita dal sistema. Piano di numerazione ISDN, piano di numerazione privato, piano di numerazione sconosciuto = preimpostato manualmente
Sito	Il parametro Sito (posizione) determina come viene impostato il parametro Posizione nell'elemento informativo CAUSE e nell'indicatore di avanzamento del Q931. Verifica di sistema = definita dal sistema; in alternativa, è possibile impostare manualmente "Rete privata e stazione" o "Sempre stazione".
COLP	Se questo flag è impostato, il numero del destinatario della chiamata verrà mostrato al chiamante in caso di connessione CO esterna in entrata. Il chiamante può vedere se la chiamata è stata inoltrata o risposta da qualcun altro. Questa funzione deve essere attivata anche dall'ufficio centrale. Se il flag è impostato e una chiamata esterna in entrata viene inoltrata o intercettata, il numero di chiamata aggiornato viene segnalato al CO nel messaggio di connessione emesso dal sistema di comunicazione. Se la funzione COLP è attivata nel CO, viene visualizzato anche il numero di chiamata aggiornato per il chiamante. Informazioni: Questo flag non influisce sulla visualizzazione del numero di chiamata per le connessioni in uscita esterne.
Invio notifica	Questo messaggio viene utilizzato per la trasmissione delle informazioni di stato relative alla connessione corrente. Il messaggio può essere inviato sia dalla rete che dall'abbonato per avvisare l'altra parte (rete o abbonato) di un'interruzione della connessione, ad esempio, o dell'attivazione dell'inoltro di chiamata. Se la funzione di notifica non è supportata dal CO, il messaggio di notifica può essere soppresso reimpostando questo flag. Se questa opzione è attivata, viene trasmesso un messaggio di "Notifica" se una chiamata è in attesa o parcheggiata, ad esempio. L'invio della notifica viene valutato solo nei protocolli DSS1, NI1 e MCI. Nei protocolli SIP-Q, CorNet-NQ e QSIG la notifica viene sempre inviata.
senza CLIP	Se questo flag è impostato, le informazioni sul chiamante verso la rete pubblica saranno soppresse per le chiamate in uscita su una linea BRI o PRI. Questo flag può essere attivato o disattivato in base ai percorsi. Inoltre, la stazione ha la possibilità di sopprimere le informazioni relative al destinatario della chiamata per ogni singola chiamata tramite un codice di accesso o il menu telefonico del sistema.
Nessun SETUP ACK.	Se questo flag è impostato, il messaggio di conferma della configurazione dal sistema di comunicazione al Central Office e viene soppresso. Rilevante per CO speciali. Esempio: CO Fetex150 di Fujitsu.

Parametri	Descrizione
nessuna informazione DIV.LEG	Se questo flag è impostato, il segnale standard di informazione sul LEG di deviazione (numero di chiamata della parte che effettua il reindirizzamento) non viene inviato al CO. Le informazioni DIV. LEG devono essere soppresse se si verificano problemi nel caso di inoltro di chiamata esterno (inoltro di chiamata esterno).
Con invio completato	Se questo flag è impostato, il sistema emette l'informazione opzionale "Tutte le cifre inviate" una volta che tutte le cifre composte sono state trasmesse.
Chiamata interna come esterna	Se questo flag è impostato, le chiamate interne alla rete vengono segnalate acusticamente allo stesso modo delle chiamate esterne.
Senza CCNR	Se questo flag è impostato, una chiamata ISDN in entrata con CCNR (completamento della chiamata in caso di mancata risposta) viene segnalata in modo che il sistema possa accettare una richiesta di richiamata. Ciò significa che il chiamante può avviare una richiamata se la stazione non risponde. In alcuni casi il messaggio non è supportato dal provider ISDN. In questo caso è necessario attivare l'interruttore per impedire al sistema di inviare CCNR.

28.3.10.3 Linee/Rete > Servizi QSIG

In una rete composta da più sistemi di comunicazione, i dati delle chiamate (dati GEZ) dei sistemi parziali vengono trasmessi a un determinato sistema di comunicazione della rete. A tale scopo, in ogni sistema di comunicazione viene configurato il numero di telefono del sistema di destinazione (numero di telefono del posto di documentazione centralizzata) al quale trasmettere i dati delle chiamate.

Descrizione dei parametri delle schede:

- **Cambia servizi QSIG**

Parametri	Descrizione
Dati del proprio sistema	
Numero del sistema	Questi dati consentono l'identificazione del proprio sistema di comunicazione nel collegamento in rete. Tali dati sono validi sia per la segnalazione centrale di occupato che per il routing dei dati di connessione. In un collegamento in rete con più sistemi di comunicazione, ogni sistema presenta un numero univoco. Se il sistema di comunicazione è collegato in rete con tali sistemi e si desidera utilizzare i servizi QSIG, per motivi di compatibilità deve essere possibile gestire il numero del sistema anche in tale contesto. Valori consentiti: da 1 a 255
Numero del gruppo	Nei sistemi di comunicazione, gli utenti possono essere classificati in gruppi, che quindi ricevono un numero di gruppo univoco. Nel singolo sistema di comunicazione tale possibilità di raggruppamento non esiste. Tuttavia, per motivi di compatibilità, il numero di gruppo deve essere amministrato anche in quel caso. Valori consentiti: da 1 a 40

Parametri	Descrizione
Segnalazione di occupato su più sistemi	
Nr. di sistema Sistema di dest.	Questi dati definiscono un sistema di comunicazione in cui è utilizzata la segnalazione centrale di occupato. Questo può essere il sistema principale o un sottosistema. Numero del sistema di comunicazione configurato per la segnalazione di occupato centralizzata. Valori consentiti: da 1 a 255
Nr. di tel. sistema di dest.	Numero di telefono del sistema di comunicazione configurato per la segnalazione di occupato centralizzata. Qui è necessario inserire solo il numero di telefono del sistema, non un numero di telefono utente. In Piano di selezione LCR occorre assicurarsi che, dopo l'immissione del numero di telefono del sistema, non venga effettuata alcuna ulteriore selezione. Esempio: il numero del sistema di destinazione è: 999. La voce del piano di composizione deve quindi essere: -999 (e non-999XXX e non-999Z).
Routing dati di collegamento	
Nr. di tel. sistema di dest.	Questi dati definiscono un sistema di comunicazione in cui è utilizzata la registrazione dei dati di connessione. Questo può essere il sistema principale o un sottosistema. Numero del sistema di comunicazione impostato come sistema di registrazione centrale (vedere anche le istruzioni per il sistema di destinazione nr. di tel.).

28.3.10.4 Linee/Rete > Assegna MSN

Descrizione dei parametri delle schede:

- **Visualizza MSN**
- **Modifica MSN**

Parametri	Descrizione
MSN	Visualizzazione o immissione del numero MSN (collegamento a più terminali).
Linea	Visualizzazione dell'assegnazione della linea sulla quale è attivo l'MSN.

28.3.10.5 Linee/collegamenti in rete > Parametri ISDN

Con il clock di riferimento (clock ISDN) vengono sincronizzati i processi sulle linee esterne all'interno di una rete specifica o della connessione alla rete esterna. Normalmente, il sistema di comunicazione seleziona automaticamente la linea da utilizzare come clock di riferimento per tutti i sistemi di comunicazione di una rete o della connessione alla linea esterna. Tuttavia, se una linea utilizzata come clock di riferimento non è più operativa, occorre configurare altre linee come clock di riferimento.

Il sistema di comunicazione seleziona la linea secondo il seguente ordine:

1) Lista nr. permessi
2) Linea esterna S_{2M}
3) Linea esterna S_0
4) Linea verticale S_{2M} (solo configurazione slave)
5) Linea verticale S_0

Descrizione dei parametri delle schede:

- **Orologio ISDN**

Parametri	Descrizione
Indice	Le posizioni rispecchiano le priorità 1-4 (per la lista numeri permessi) o 1-16 (per la lista numeri vietati).
Liste nr.permessi	Se la lista nr. permessi contiene delle voci, la selezione automatica della linea prevista dal sistema di comunicazione viene ignorata. Per la ricerca, le porte ISDN inserite nella lista nr. permessi (max. 4 consentite) vengono utilizzate per prime dopo la linea di riferimento.
Liste nr.vietati	Per la ricerca, le porte ISDN inserite nella Lista nr. vietati (max. 16 consentite) vengono ignorate dopo la linea di riferimento.

28.3.11 Autorizzazioni

In **Abilitazioni** sono raggruppate le funzioni relative all'abilitazione delle linee esterne. Regolano l'accesso dell'utente a connessioni esterne che possono generare costi.

28.3.11.1 Classi di autorizzazione > Utenti

Descrizione dei parametri della scheda:

- **Visualizza tutti gli utenti**

Parametri	Descrizione
N° tel., **Numero di telefono**	Numero di telefono dell'utente
Nome	Nomi utente.
Giorno	Gruppo di abilitazione selezionato per il giorno.
Notte	Gruppo di abilitazione selezionato per la notte.
Gruppo di abilitazione Giorno	Scelta del gruppo di abilitazione per il giorno. La selezione effettuata si riferisce alla tabella delle **abilitazioni giorno** tramite la quale il gruppo di abilitazione viene collegato effettivamente alla relativa abilitazione.
Gruppo di abilitazione Notte	Scelta del gruppo di abilitazione per la notte. La selezione effettuata si riferisce alla tabella delle **abilitazioni notte** tramite la quale il gruppo di abilitazione viene collegato effettivamente alla relativa abilitazione.

Nota: I testi dei gruppo di abilitazione vengono generati in base alla procedura guidata **Configurazione di base** > **Prefisso internazionale del sistema**.

28.3.11.2 Classi di autorizzazione > Giorno: Gruppi di abilitazione

Descrizione dei parametri delle schede:

- **Modifica nome**
- **Modifica gruppo di abilitazione**
- **Giorno: Mostra membri del gruppo**

Parametri	Descrizione
Gruppo di abilitazione	Nome liberamente scelto per i gruppi di abilitazione 1-15. Assegnazione dei privilegi centralino per fascio, per i servizi giorno e notte. Quando si configurano gli utenti, l'accesso ai numeri di telefono esterni può essere limitato mediante assegnazione di gruppi di abilitazione.
Abilitazione	Assegnazione delle abilitazioni ai singoli gruppi di abilitazione per il servizio giorno. Tutte le limitazioni sono effettive solo sulle linee di un fascio di tipo linea urbana.
Gruppo di abilitazione: Interna	L'utente può fare solo telefonate interne. Valore predefinito: predefinito nel gruppo di abilitazione 1
Gruppo di abilitazione: Semiabilitato	L'utente può solamente rispondere a chiamate esterne. Valore predefinito: predefinito nel gruppo di abilitazione 2
Gruppo di abilitazione: Lista nr. permessi	L'utente può comporre solo i numeri di telefono esterni definiti nella lista nr. permessi. In caso non sia stato inserito nessun numero, si applica la semiabilitazione alla linea urbana. Valore predefinito: predefinito nel gruppo di abilitazione 4
Gruppo di abilitazione: Lista nr. vietati	L'utente non può comporre i numeri di telefono esterni definiti nella lista nr. vietati. In caso non sia stato inserito nessun numero, si applica l'abilitazione alla linea urbana. Valore predefinito: predefinito nel gruppo di abilitazione 3, 5, 6
Gruppo di abilitazione: Abilitato	L'utente può ricevere ed effettuare chiamate senza restrizioni. Valore predefinito: predefinito nel gruppo di abilitazione da 7 a 15
Mostra membri del gruppo	Visualizzazione del numero di telefono e del nome dei membri del gruppo di abilitazione selezionato.

28.3.11.3 Classi di autorizzazione > Notte: Gruppi di abilitazione

Descrizione dei parametri delle schede:

- **Modifica nome**
- **Modifica gruppo di abilitazione**
- **Notte: Mostra membri del gruppo**

Parametri	Descrizione
Gruppo di abilitazione	Nome liberamente scelto per i gruppi di abilitazione 1-15. Assegnazione dei privilegi centralino per fascio, per i servizi giorno e notte. Quando si configurano gli utenti, l'accesso ai numeri di telefono esterni può essere limitato mediante assegnazione di gruppi di abilitazione.
Abilitazione	Assegnazione delle abilitazioni ai singoli gruppi di abilitazione per il servizio notte. Tutte le limitazioni sono effettive solo sulle linee di un fascio di tipo linea urbana.
Gruppo di abilitazione: Interna	L'utente può fare solo telefonate interne. Valore predefinito: predefinito nel gruppo di abilitazione 1
Gruppo di abilitazione: Semiabilitato	L'utente può solamente rispondere a chiamate esterne. Valore predefinito: predefinito nel gruppo di abilitazione 2
Gruppo di abilitazione: Lista nr. permessi	L'utente può comporre solo i numeri di telefono esterni definiti nella lista nr. permessi. In caso non sia stato inserito nessun numero, si applica la semiabilitazione alla linea urbana. Valore predefinito: predefinito nel gruppo di abilitazione 4
Gruppo di abilitazione: Lista nr. vietati	L'utente non può comporre i numeri di telefono esterni definiti nella lista nr. vietati. In caso non sia stato inserito nessun numero, si applica l'abilitazione alla linea urbana. Valore predefinito: predefinito nel gruppo di abilitazione 3, 5, 6
Gruppo di abilitazione: Abilitato	L’utente può ricevere ed effettuare chiamate senza restrizioni. Valore predefinito: predefinito nel gruppo di abilitazione da 7 a 15
Mostra membri del gruppo	Visualizzazione del numero di telefono e del nome dei membri del gruppo di abilitazione selezionato.

28.3.11.4 Classi di autorizzazione > Liste nr. permessi

Descrizione dei parametri delle schede:

- **Visualizza destinazioni di selezione breve**
- **Aggiungi numero di telefono**

Parametri	Descrizione
Lista 1-6	Visualizza/Aggiungi/Modifica/Cancella un numero permesso. La lista nr. permessi contiene i numeri di telefono che possono essere chiamati dall'utente. Possono essere create fino a 6 liste nr. permessi. La prima Lista nr. permessi può contenere 100 voci, le restanti 5 liste fino a 10 voci ciascuna.
Numero di telefono	I singoli numeri di telefono possono comprendere fino a 26 caratteri (numeri da 0 a 9 e caratteri * e #). L'elenco non deve necessariamente mostrare il numero di telefono completo. Ad esempio, per permettere agli utenti di comporre numeri 0800xxx (numeri verdi), occorre inserire qui solo 0800. Poiché gli elenchi si riferiscono solo alle chiamate in uscita, non è necessario indicare il codice di impegno della linea con il numero di telefono inserito.

28.3.11.5 Autorizzazioni > Liste nr. vietati

Descrizione dei parametri delle schede:

- **Visualizza destinazioni di selezione breve**
- **Aggiungi numero di telefono**
- **Modifica filtri di analisi**

Parametri	Descrizione
Lista 1-6	Visualizza/Aggiungi/Modifica/Cancella un numero di telefono vietato. La lista nr. vietati contiene i numeri di telefono che non possono chiamati dagli utenti. Possono essere create fino a 6 liste numeri vietati. La prima Lista nr. vietati può contenere 50 voci, le restanti 5 liste fino a 10 voci ciascuna.
Numero di telefono	I singoli numeri di telefono possono comprendere fino a 26 caratteri (numeri da 0 a 9 e caratteri * e #). L'elenco non deve necessariamente mostrare il numero di telefono completo. Ad esempio, al fine di evitare la selezione di numeri 0900xxx (a pagamento) da parte degli utenti, occorre inserire qui solo 0900. L'immissione del carattere # al primo posto della lista di un numeri non consentiti impedisce il bypass del controllo composizione per i telefoni di sistema, se una linea esterna analogica viene impegnata con il tipo di selezione DTMF e si commuta su DTMF durante la composizione. Poiché gli elenchi si riferiscono solo alle chiamate in uscita, non è necessario indicare il codice di linea urbana con il numero di telefono inserito.
Modifica filtri di analisi Mediante speciali filtri di analisi, è possibile determinare per qualsiasi lista dei numeri vietati, quali cifre digitate non devono essere confrontate con la relativa lista dei numeri vietati. Il sistema di comunicazione nasconde l'area delle cifre prima dell'analisi del numero composto.	
Dalla cifra Alla cifra	In questa sequenza di cifre (1-25) il filtro di analisi è attivo nell'ambito del numero di telefono.
Carattere	Proibendo i caratteri * e #, gli utenti possono inserire tali caratteri per bypassare il controllo della selezione.

28.3.11.6 Classi di servizio > Lista nera

Descrizione dei parametri delle schede:

- **Mostra lista**
- **Aggiungi numero di telefono**

Parametri	Descrizione
Numero di telefono	I singoli numeri di telefono possono comprendere fino a 25 caratteri (numeri da 0 a 9 e il carattere +). Il carattere "+" si riferisce al prefisso internazionale che è configurato nel sistema e deve essere inserito nella prima posizione. Il primo carattere di ogni voce può essere "+" o qualsiasi cifra. I numeri di telefono sono ordinati numericamente nella Lista nera. Le voci della lista nera devono essere inserite in formato internazionale (ad es. 004989) o canonico (ad es. +4989).
Blocca chiamate anonime	L'abilitazione di questo flag blocca le chiamate senza numero del chiamante o con il numero del chiamante esistente ma con presentazione limitata.

Parametri	Descrizione
Funzione lista nera attiva	Abilitando questo flag si bloccano i numeri di chiamata aggiunti. La funzione di lista nera si basa solo sul numero chiamante fornito dal provider.

28.3.11.7 Classi di autorizzazione > Servizio notturno

Descrizione dei parametri della scheda:

- **Modifica servizio notte**

Parametri	Descrizione
Utente abilitato per il servizio notte	Se determinati utenti devono avere la possibilità di portare il sistema di comunicazione in modalità notte, tali utenti devono essere inseriti nell'elenco Utente abilitato per il servizio notte. È possibile inserire un massimo di 5 utenti. Valore predefinito: 100
Utente	Elenco di tutti gli utenti disponibili nel sistema di comunicazione.
Utente abilitato	Elenco di utenti utenti autorizzati che possono attivare il servizio notte.
Aggiungi >>	Aggiunge l'utente selezionato agli utenti abilitati.

28.3.11.8 Classi di autorizzazione > Assegnazione gruppi VBZ

Descrizione dei parametri delle schede:

- **Modifica assegnazioni gruppi**
- **Linea a gruppo**
- **Intervallo selezione breve gruppo**

Parametri	Descrizione
Assegnazione dei gruppi VBZ	Assegnazione a un gruppo con restrizioni di traffico (1-64) di un utente. Tramite l'assegnazione a un gruppo con restrizioni di traffico, è possibile assegnare ai singoli utenti del sistema di comunicazione un gruppo con restrizioni di traffico. Codificando la matrice di collegamento, è possibile quindi accedere a questi gruppi per definire quali utenti possono accedere a quali altri utenti. Per impostazione predefinita, tutti gli utenti sono assegnati al gruppo con restrizioni di traffico 1. In questo modo tutti gli utenti hanno accesso illimitato agli altri utenti. Valori consentiti: da 1 a 64

Parametri	Descrizione
Linea a gruppo	Assegnazione di una linea al gruppo con restrizioni di traffico. Tramite Assegnazione gruppi con restrizioni di traffico, è possibile assegnare alle singole linee del sistema di comunicazione un gruppo con restrizioni di traffico. Codificando la matrice di collegamento, è possibile quindi accedere a questi gruppi per definire quali utenti possono accedere a quali linee. Per impostazione predefinita, tutte le linee urbane sono assegnate al gruppo con restrizioni di traffico 1. In questo modo tutti gli utenti hanno accesso illimitato a tutte le linee, sia in entrata che in uscita. Valori consentiti: da 1 a 64
Intervallo selezione breve gruppo	A ogni gruppo con restrizioni di traffico viene assegnato un intervallo di numeri di selezione breve. Se un utente seleziona un numero di selezione breve, il sistema determina se l'utente è abilitato o meno a utilizzare tale sistema di selezione breve valutando il gruppo di selezione breve (KWZ) associato. Se la selezione breve del sistema rientra nell'intervallo di selezioni brevi del sistema assegnato a tale gruppo con restrizioni di traffico, la chiamata viene effettuata. Se la selezione breve del sistema non corrisponde all'area assegnata viene generato un messaggio di errore. Nei gruppi con restrizioni di traffico, gli intervalli dei numeri brevi di sistema possono sovrapporsi. Tuttavia, non è permesso inserire singoli numeri di selezione breve nei gruppi con restrizioni di traffico o più sistemi di numeri di selezione breve in un gruppo con restrizioni di traffico. Ad esempio, sono consentiti i seguenti: 1: 0-99; 2: 50-150; 3: 200-500. Invece non sono consentiti i seguenti: 1: 0, 5, 10; 2: 50-100, 300-500. Valori consentiti: 0-7999

28.3.11.9 Classi di autorizzazione > Matrice VBZ

Descrizione dei parametri delle schede:

- **Modifica matrice VBZ**

Parametri	Descrizione
Matrice Col	Per modificare in modo specifico una possibilità di connessione tra due gruppi con restrizioni di traffico, fare clic sul campo nel punto di incrocio di questi gruppi con restrizioni di traffico nella matrice Col. Fare ripetutamente clic su tale campo per attivare o bloccare le possibilità di connessione per un fascio, per l'altro fascio o per entrambi i fasci. Per utilizzare la matrice di collegamento, è innanzitutto necessario che ogni utente sia assegnato a un gruppo tramite Assegnazione gruppi con restrizioni di traffico. Per impostazione predefinita, tutti gli utenti e tutte le linee sono assegnati al gruppo 1. Consentendo al gruppo 1 un accesso illimitato, per impostazione predefinita, ogni utente potrà contattare ogni altro utente e utilizzare tutte le linee.

Parametri	Descrizione
Griglia	Nella matrice viene visualizzato un elenco di gruppi in orizzontale lungo il bordo superiore e in verticale lungo il bordo sinistro. Nei punti di contatto si trova una casella di controllo. La freccia nella relativa casella di controllo indica la relazione esistente tra i due gruppi. Una casella vuota indica che non è possibile alcuna connessione. Una matrice di collegamento in cui non sia presente alcuna freccia ha come conseguenza un blocco completo del sistema di comunicazione.
Bloccare tutto	La matrice Col sopprime il traffico tra gli utenti/le linee di un gruppo (sottosistema) e tra i gruppi.
Rilasciare tutto	La matrice Col consente il traffico tra gli utenti/le linee di un gruppo (sottosistema) e tra i gruppi.
Solo interno al gruppo	La matrice Col consente il traffico solo tra gli utenti/le linee di un gruppo (sottosistema).

28.3.11.10 Classi di autorizzazione > Servizio notte auto

Descrizione dei parametri delle schede:

- **Visualizza tutti i giorni**
- **Modifica giorno**

Parametri	Descrizione
Lunedì, Martedì, Mercoledì, Giovedì, Venerdì, Sabato, Domenica	Il giorno configurato tramite il servizio notte automatico. La pianificazione comprende l'intera settimana (da lunedi a domenica) e i giorni speciali. I giorni speciali sono giorni di vacanza o particolari, ad esempio feste aziendali.
Zona	La pianificazione di un giorno può essere suddivisa in un massimo di 4 zone (intervalli di tempo). Le zone possono essere configurate sequenzialmente e senza interruzioni. In questo modo, ad esempio, l'ora finale del primo intervallo può essere identica all'ora di inizio del secondo intervallo. Un intervallo non può avere la stessa ora di inizio e di fine. La lunghezza minima di un intervallo corrisponde a 15 minuti. Valori consentiti: 1-4
Inizio	Ora di inizio per la zona. Inizia il primo intervallo di un giorno alle 0.00, l'ora di inizio deve essere inserita nel formato 00:00.
Fine	Ora fine per la zona. Termina l'ultimo intervallo di un giorno alle 24.00, l'ora di fine deve essere inserita nel formato 23:59.
Nr. tel. Notte	Numero di telefono servizio notte per la zona. Se per il numero di telefono notte non viene inserito alcun numero, nel sistema viene attivato il servizio notte per linea. Le destinazioni vengono configurate in **Linee/Rete** > **Cambia linea** > **Assegnazione linea**. I tempi inseriti tramite il servizio notte automatico si applicano a tutte le linee.
OK	La zona viene configurata.
Elimina	La zona definita viene eliminata.

Parametri	Descrizione
Copia servizio	È possibile copiare le zone impostate su uno o più altri giorni selezionando il giorno desiderato, sul giorno speciale selezionando il rispettivo flag, semplicemente selezionando **Seleziona tutto**. Premendo **Applica**, le impostazioni delle zone nei giorni selezionati verranno sovrascritte con le zone impostate nel giorno corrente.

28.3.11.11 Classi di autorizzazione > Giorni speciali

Descrizione dei parametri della scheda:

- **Modifica giorni speciali**

Parametri	Descrizione
Giorno	Quando si seleziona una data nel calendario, questa viene automaticamente inserita qui.
Nome	Nome per questo giorno speciale (ad esempio, Lunedi di Pentecoste)

28.3.12 Interfacciamenti

Le funzioni per le apparecchiature ausiliarie, come la Musica su attesa (MoH), la configurazione degli annunci o il collegamento di un telefono d'ingresso come apriporta alle porte del sistema (trunk), sono raggruppate sotto la voce **Apparecchiature ausiliarie**.

28.3.12.1 Apparecchiature ausiliarie > Musica su attesa

Descrizione dei parametri delle schede:

- **Modifica musica su attesa**

Parametri	Descrizione
Tipo di MOH	Il parametro Tipo di MOH consente di scegliere tra tre possibili opzioni. La musica per questa funzione può essere fornita internamente o esternamente.
Tipo di MOH: Nessuna musica su attesa	Se si seleziona questa opzione, la funzione Musica su attesa viene disattivata completamente. Ciò non si applica quando una chiamata esterna viene trasferita da un trasferimento prima della risposta; il chiamante sente quindi la suoneria.
Tipo di MOH: MOH senza tono suoneria	Se questa opzione è selezionata, nel caso di un trasferimento non mascherato, il chiamante sentirà la musica su attesa durante il trasferimento, così come durante il trasferimento della chiamata da parte del trasferente e mentre la connessione esterna squilla alla destinazione trasferita.

Parametri	Descrizione
Tipo di MOH: MOH con tono suoneria	Se questa opzione è selezionata, nel caso di un trasferimento non mascherato, il chiamante sentirà la musica su attesa mentre avviene il trasferimento. Non appena la chiamata viene trasferita dall'interlocutore e la connessione esterna squilla alla destinazione trasferita, il chiamante sente un tono di chiamata. L'opzione MOH con tono suoneria dovrebbe essere sempre impostata in un sistema di rete, al fine di fornire al cliente un ambiente uniforme. |Se il chiamante raggiunge il sistema tramite un provider di servizi di telefonia Internet (ITSP), questa opzione non si applica e il chiamante sentirà la musica in attesa durante il trasferimento.

Accesso e attivazione del tipo tramite Manager E.

Il formato di ingresso per la musica su attesa è un file wave con PCM e 16 bit. Le frequenze di campionamento supportate sono 8, 22,05, 24, 32, 40, 44,1 e 48 kHz in mono o stereo. Il formato preferito è PCM, 16 bit, 8 kHz, mono. Si consiglia di utilizzare il formato di ingresso preferito e di limitare la lunghezza dei file wave a circa 2 minuti. È possibile impostare un MOH per il giorno e uno per la notte. È necessario un ripristino.

28.3.12.2 Apparecchiature ausiliarie > Segreteria telefonica

Descrizione dei parametri delle schede:

- **Modifica segreteria telefonica**

Parametri	Descrizione
Segreteria telefonica Accesso in richiamata	Impostare il **Numero di chiamata** e il **Nome** del dispositivo.
Dispositivo per la registrazione dal vivo	Impostare il **Numeri di chiamata** del dispositivo.

28.3.12.3 Apparecchiature ausiliarie > Annunci

Descrizione dei parametri delle schede:

- **Modifica annunci**

Parametri	Descrizione
File WAVE	Qui è possibile selezionare il WAVE (.wav) per un annuncio specifico (vedere la sezione Configurazione > Annunci > Caricamento sul gateway).

Parametri	Descrizione
Accesso	La connessione viene definita tramite l'accesso. Qui è possibile selezionare la porta (analogica SLA o EVM) a cui è collegato il dispositivo. **Suggerimento:** Alle porte analogiche impostate come porte di annuncio deve essere assegnato il valore "Segreteria telefonica", in **Modalità Esperto** > **Server telefonia** > **Stazione** > **Stazioni analogiche** > **Modifica** > **Tipo di interno**, come descritto in Parametri della stazione. Le destinazioni esterne possono essere utilizzate per indirizzare i dispositivi di annuncio in un altro nodo del sistema. A tal fine, il dispositivo di annuncio viene identificato come esterno. Il numero di chiamata di una porta di annuncio in un altro nodo del sistema viene inserito qui. **Suggerimento:** Questo elenco di apparecchiature si riferisce all'impostazione **Annuncio**, in **Modalità Esperto** > **Server telefonia** > **Chiamate in entrata** > **UCD** > **Modifica parametri gruppo UCD**, come descritto in Chiamate in entrata > UCD. Se si seleziona **Destinazione esterna**, appaiono i due campi seguenti: • **Percorso** (gruppi trunk) • **Numero di chiamata** (dispositivo)

Parametri	Descrizione
Tipo	Dal menu a discesa è possibile selezionare uno dei seguenti tipi di annunci: • **Nessuno**: l'apparecchiatura per l'annuncio non è collegata. • **Annuncio**: consente di collegare un solo dispositivo di annuncio esterno tramite porte SLA o schede EVM. L'annuncio fornito dal dispositivo di annuncio attivato deve avere un inizio e una fine fissi. Questo dispositivo non deve inoltrare la chiamata dopo la fine dell'annuncio (non deve essere inserita una destinazione di commutazione). La porta del dispositivo di annuncio corrispondente viene inserita in **Accesso**). Equivale ad **avvio/ interruzione** per i dispositivi di destinazione esterni. • **Musica su attesa**: un annuncio o un brano musicale vengono ripetuti continuamente. Le chiamate in coda possono essere collegate anche durante la riproduzione della musica o dell'annuncio. La connessione può avvenire tramite porte SLA o schede EVM. La porta del dispositivo di annuncio corrispondente viene inserita in **Accesso**. Equivale a **continuo** per i dispositivi di destinazione esterni. • **Musica interna**: attiva la musica di attesa interna al sistema nel sistema di comunicazione. Per questa opzione, è necessario inserire **Nessuno** in **Accesso**. L'MOH esterno (configurazione Manager E) viene ascoltato se definito come destinazione nel sistema di comunicazione. Le voci in **Accesso** non hanno effetto su nessuna variante. • **PC multimediale**: questa impostazione è predefinita. Il PC multimediale o l'applicazione di controllo controlla se il chiamante sente l'annuncio dall'inizio o è collegato a un annuncio in corso. • **Lettore di annunci**: il lettore di annunci è un programma software interno disponibile insieme alla funzionalità UC Booster (UC Booster Card o UC Booster Server). **Nota:** La funzionalità di lettore di annunci è disponibile solo in modalità UC Suite.
Modalità	È possibile selezionare una delle due opzioni seguenti: • **avvio/interruzione**: riproduzione singola • **continuo**: riproduzione continua

Nota: La procedura guidata **Musica in attesa/Annunci** può essere utilizzata anche per configurare gli **Annunci**. Per maggiori informazioni, vedere Come configurare gli annunci.

28.3.12.4 Apparecchiature ausiliarie > Apriporta

Descrizione dei parametri delle schede:

- **Modifica apriporta**

Parametri	Descrizione
Utente	Selezione del numero di telefono/della porta di connessione del telefono d'ingresso. Il tipo di porta della stazione deve essere P.O.T. o Nessuna porta.

Parametri	Descrizione
Destinazione	Selezione del numero di telefono/della porta di connessione della destinazione della suoneria del telefono d'ingresso. È possibile specificare un numero di stazione o un numero di gruppo come destinazione dello squillo a cui viene segnalato uno squillo speciale quando si preme il tasto del campanello. La chiamata viene segnalata in base agli algoritmi di inoltro delle chiamate definiti in "Impostazioni - Chiamate in arrivo".
Apriporta	Attiva la funzione di apertura della porta. Impostando questo flag, è possibile attivare un apriporta collegato alla TFE-S per le stazioni.
DTMF	L'impostazione di questo flag consente di attivare l'apriporta a distanza con un trasmettitore DTMF.
FWD	L'impostazione di questo flag abilita l'inoltro esterno della destinazione della suoneria del telefono d'ingresso.

28.3.12.5 Interfacciamenti > SmartVM

Descrizione dei parametri delle schede:

- **Modifica caselle postali SmartVM**

Parametri	Descrizione
Numero mailbox	Immissione del numero della mailbox. Le mailbox vengono identificate sulla base del numero mailbox. Se occorre assegnare una mailbox a un utente, è assolutamente necessario che entrambi abbiano lo stesso numero di telefono.
Nome	Visualizzazione del nome della mailbox. Il nome corrisponde al nome dell'utente (se disponibile). Nel caso dei gruppi viene visualizzato il nome assegnato.
messaggio di saluto	Scelta dell'annuncio di benvenuto. La possibilità di utilizzare le voci disponibili dipende dal menu del telefono selezionato (TUI). Con la TUI OSO è supportato solo l'annuncio di benvenuto 1 per le mailbox standard.
Annuncio: **Annuncio 1-4**	La scelta degli annunci di benvenuto 1-4 dipende dal tipo di mailbox: Mailbox predefinito: messaggio di benvenuto 1 o 2 (TUI OSO solo 1) Mailbox console posto operatore: annuncio di benvenuto 1, 2, 3 o 4
Annuncio: **Giorno/Notte**	L'annuncio di benvenuto dipende dalla modalità giorno/notte: Giorno - Annuncio di benvenuto 1 / notte - Annuncio di benvenuto 2
Annuncio: **Tipo chiamata**	Solo per mailbox predefinito: l'annuncio dipende dallo stato dell'utente: Chiamata non risposta - annuncio di benvenuto 1 / Occupato - annuncio di benvenuto 2
Annuncio: **Nessuno**	Non viene riprodotto alcun annuncio di benvenuto. La mailbox rimane attiva, ad esempio per inoltrare la chiamata al posto di rinvio.

Parametri	Descrizione
Registrazione	Se questo flag è attivato, la mailbox è di tipo standard. Non può più essere una mailbox posto operatore. Se il flag è disattivato (opzione predefinita), la mailbox non offre la possibilità di lasciare un messaggio. L'utente può, al primo accesso alla propria mailbox, attivare la registrazione. Tramite ciò viene garantito che prima della messa in funzione ad opera dell'utente non possano essere registrati messaggi. Impostazione predefinita: funzione attivata
AutoAttendant	Se questo flag è attivato, la mailbox è di tipo posto operatore (AutoAttendant). Non può più essere una mailbox standard. Possono essere configurate fino a 100 mailbox di servizio. Passando dalla mailbox standard a quella AutoAttendant vengono cancellati tutti i messaggi registrati. Impostazione predefinita: funzione disattivata
Reset password	Se il flag è attivato, la password per la mailbox viene reimpostata su `123456`. Al successivo accesso, l'utente deve modificare la password per la propria mailbox. Impostazione predefinita: funzione disattivata

Descrizione dei parametri delle schede:

- **Modifica parametri SmartVM**

Parametri	Descrizione
Parametri generali	
Lungh. max. numero mailbox	Lunghezza massima del numero mailbox. Valori consentiti: 2-16 posizioni; valore predefinito: 3 posizioni
Lunghezza mass.messaggio (min)	Lunghezza massima della durata della registrazione di un messaggio. Intervallo di valori: 1 o 2 minuti; valore predefinito: 2 minuti
Limite numero chiamata	Nelle connessioni in uscita attivate mediante SmartVM (post-selezione e selezione breve AutoAttendant) possono essere composti solo numeri di telefono la cui lunghezza non superi quella specificata. Se vengono configurati numeri di telefono più lunghi, non viene stabilita alcuna connessione. La lunghezza predefinita corrisponde a quella del numero di telefono della mailbox (lunghezza del numero interno) per cui è consentita la sola selezione di numeri interni. Valori consentiti: da 2 a 30, valore predefinito: 3
Dest. rinvio fax generale	Immissione della destinazione di rinvio fax verso la quale SmartVM deve di regola inoltrare i fax in entrata. Se non è indicata alcuna destinazione di rinvio fax, i fax in entrata saranno rifiutati. Valori consentiti: max. 16 cifre
Lingua standard	Scelta della lingua della guida utente. Vale per tutte le mailbox. Se la guida utente non è disponibile nella propria lingua, viene impostata la versione in inglese britannico.
Interfaccia utente telefono	Scelta della struttura menu del telefono per la casella vocale (interfaccia utente dei telefoni, TUI). La scelta si applica a tutte le mailbox.

Parametri	Descrizione
Interfaccia utente telefono (TUI): **SmartVM**	SmartVM TUI, EVM TUI (predefinito).
Interfaccia utente telefono (TUI): **OSO**	TUI OSO, simile alla TUI della UC Suite.
Ordine annuncio data	visibile solo con la TUI SmartVM: Impostazione della sequenza degli annunci per il messaggio, data di registrazione e numero del chiamante (se noto).
Ordine annuncio data: **Data dopo messaggio**	visibile solo con la TUI SmartVM: Messaggio - Data registrazione - Numero di telefono del chiamante (se noto).
Ordine annuncio data: **Data prima del messaggio**	visibile solo con la TUI SmartVM: - Data registrazione - Numero di telefono del chiamante (se noto) -- Messaggio. Per i messaggi di utenti interni vale quanto segue: Nome dell'utente interno (se disponibile) - Data registrazione - Numero di telefono del chiamante (se noto) -- Messaggio.
Numero di messaggi per casella postale	Numero massimo di messaggi per una mailbox. Valori consentiti: da 0 a 100, valore predefinito: 30
Disattivazione EVM	Se questo flag è attivato, SmartVM è disattivato. Impostazione predefinita: funzione disattivata
Consenti richiamata da casella vocale solo a numeri noti	Quando l'utente A chiama l'utente B, l"utente B ha un inoltro di chiamata sulla casella vocale, l'utente A esterno lascia un messaggio vocale, l'utente B chiama SmartVM, immette la password e mentre ascolta il messaggio compone la cifra "8". Componendo questo numero, viene richiamato l'utente B. Se questo flag è attivato, la richiamata avviene se il numero dell'utente B fa parte dei numeri conosciuti. I numeri conosciuti sono il numero di cellulare e il numero di telefono abitazione/esterno dei dettagli del profilo della gestione utenti (Applicazioni-UC Smart-Gestione utenti) Impostazione predefinita: funzione attivata
Comportamento AA VP Definire se in alcuni casi AutoAttendant deve riprodurre automaticamente gli annunci.	
VP - Prima del trasferimento	Se questo flag è attivato, in caso di "VP - Prima del trasferimento" viene riprodotto il seguente messaggio: "Attendere prego, sta per rispondere uno dei nostri operatori..." Impostazione predefinita: funzione disattivata

Parametri	Descrizione
VP - Risultato trasferimento	Se questo flag è attivato, in caso di "VP - Risultato trasferimento" viene riprodotto il seguente messaggio: „Il numero chiamato è inesistente.“ “Il numero da Lei chiamato è al momento occupato.” „L'utente non risponde.“ Impostazione predefinita: funzione attivata
VP - Rinvio	Se questo flag è attivato, in caso di "VP - Rinvio" viene riprodotto il seguente messaggio: "Le risponderà uno dei nostri operatori. Attendere prego." „Le risponderà la mailbox dell'utente.“ "Attendere prego, sta per rispondere uno dei nostri operatori..." Impostazione predefinita: funzione attivata
VP - Prima del rilascio	Se questo flag è attivato, in caso di "VP - Prima del rilascio" viene riprodotto il seguente messaggio: “Riprovare a chiamare in un secondo momento.” „Grazie. Arrivederci.“ “Il numero della mailbox non è valido.” Impostazione predefinita: funzione attivata

Descrizione dei parametri delle schede:

- **Modifica parametri posto operatore automatico**

Parametri	Descrizione
Numero di chiamata	Numero dell'AutoAttendant (predefinito: 352).
Intercetta dopo annuncio	Se questo flag è attivato, dopo la riproduzione dell'annuncio di benvenuto viene eseguita la deviazione della chiamata al posto di rinvio (ad esempio console posto operatore). Durante l'annuncio di benvenuto non è possibile chiamare le destinazioni di selezione rapida. Impostazione predefinita: funzione disattivata
nessuna selezione suffisso	Se questo flag è attivato, il chiamante può essere inoltrato verso altre destinazioni soltanto selezionando le destinazioni di selezione breve. Il chiamante può comporre qualsiasi numero di telefono di più cifre. Impostazione predefinita: funzione disattivata

Descrizione dei parametri delle schede:

- **Modifica destinazioni selez. breve/rinvio Giorno**
- **Modifica destinazioni selez. breve/rinvio Notte**
- **Modifica destinazioni selez. breve/rinvio 3**
- **Modifica destinazioni selez. breve/rinvio 4**

Parametri	Descrizione
Seleziona	Selezione di un utente interno (prima metà dell'elenco) o di una casella vocale (seconda metà dell'elenco) come destinazione di selezione breve o posto di rinvio.
Azione	Visualizzazione di 10 possibili destinazioni di selezione breve e del posto di rinvio.
Numero di chiamata	Numero di telefono dell'utente selezionato o della casella vocale selezionata.
Nome	Nome dell'utente selezionato o della casella vocale selezionata.
Tipo	Scelta del tipo di numero di telefono.
Tipo: **Numero di chiamata**	Qui, è possibile chiamare l'utente selezionato con la destinazione di selezione breve assegnata.
Tipo: **Mailbox**	Qui, è possibile chiamare la casella vocale selezionata con la destinazione di selezione breve assegnata.

28.3.13 Payload

In **Payload** sono riunite le funzioni che vengono utilizzate per visualizzare e configurare i tipi di collegamento e i protocolli.

28.3.13.1 Payload > Periferiche

Descrizione dei parametri delle schede:

- **Mostra impostazioni globali della periferica**
- **Ripristina impostazioni iniziali della periferica**

Parametri	Descrizione
Gateway globale del tipo G.711	"Periferica" è la denominazione generale per utenti, servizi e funzioni che richiedono l'uso di canali. Vengono visualizzati il tipo di codec del gateway globale, il numero massimo di canali B disponibili per i quali si dispone di licenza, nonché il numero massimo di client LAN per un canale per Musica su attesa (le chiamate in soprannumero non vengono connesse).
Numero max. di canali B dell'HW	
Numero di client della LAN su un canale di MoH	

Per ripristinare le impostazioni del dispositivo è necessario il riavvio del sistema di comunicazione.

28.3.13.2 Payload > Media Stream Control (MSC)

Descrizione dei parametri delle schede:

- **Modifica i parametri del jitter di MSC**

Parametri	Descrizione
	Il controllo di flusso multimediale (MSC) effettua il monitoraggio e la valutazione dei flussi multimediali gestiti tramite il sistema di comunicazione. Provvede alla trasmissione di dati multimediali tra le reti mediante il gateway (TDM/IP).
Statistica del traffico (soltanto SNMP)	Accesso ai dati delle statistiche per chiamate del sistema riuscito tramite SNMP.
Intervallo per la generazione di pacchetti RTCP (sec.)	L'intervallo di reporting espresso in secondi per pacchetti RTCP (Real Time Control Protocol) gestisce e assicura la conformità dei parametri QoS (Quality of Service) mediante scambi periodici di messaggi di controllo tra mittente e destinatario. Valori consentiti: da 5 a 10, valore predefinito: 5

Descrizione dei parametri delle schede:

- **Ripristina le impostazioni iniziali di MSC**

Parametri	Descrizione
Ripristina le impostazioni iniziali di MSC	Ripristinare tutte le impostazioni MSC originali.

28.3.13.3 Payload > Moduli HW

Gestione dei moduli DSP del sistema di comunicazione.

Descrizione dei parametri delle schede:

- **Mostra tutti i moduli HW**
- **Modifica le impostazioni di DSP**
- **Modifica le impostazioni del jitter di DSP**

Parametri	Descrizione
Tipo HW	Visualizzazione dei DSP (Digital Signal Processor) utilizzati nel sistema di comunicazione. Le opzioni possibili sono: • **Onboard** = DSP della scheda madre integrato • **OCCB X-1** = DSP di un sottomodulo OCCB (OCCB1 o OCCB3)
Versione del firmware	Versione corrente del firmware di ogni singolo DSP
Versione API	Versione API (Application Programming Interface) corrente di ogni DSP
Generale	
Indirizzo IP	Indirizzo IP del modulo DSP (modificabile se l'indirizzo IP è già assegnato). ***Nota:*** L'ultimo ottetto dell'indirizzo IP non può essere .1 (xxx.xxx.xxx.1)
Porta	Numero di porta del modulo DSP
Visualizzazione stato	Utilizzato per il riconoscimento della disponibilità dei DSP Valore predefinito: Messaggi di stato

Parametri	Descrizione
Riduzione eco	Se il flag è attivato, nelle trasmissioni vocali viene soppresso il feedback audio (effetto eco). Valore predefinito: Attivato
Segnalazioni DTMF fuori banda	Se il flag è attivato: i segnali DTMF vengono trasmessi tramite un canale di segnalazione separato (outband). Valore predefinito: Disattivato
Parametri fax	
Numero di pacchetti ridondanti	Definizione del numero di pacchetti ridondanti: maggiore è questo valore, più robusta è la trasmissione fax in termini di perdita di pacchetti. Lo svantaggio di valori più elevati è l'aumento della larghezza di banda richiesta. Valore predefinito: 2
Jitter di rete massimo (hex ms)	Definizione del jitter di rete massimo espresso in millisecondi: più alto è il valore, maggiore è la probabilità di varianza del runtime per i pacchetti dati nelle reti. Sono ammessi solo i valori esadecimali, rappresentati da cifre da 0 a 9 e da A a F. Questo parametro non deve essere modificato. Valore predefinito: 00C8
Timeout del rilevamento del tono Fax/modem (sec)	Definizione del tempo in secondi per l'identificazione del tono fax durante una connessione: in questo modo si garantisce la commutazione al protocollo fax T.38. Una volta trascorso il tempo qui configurato, non verranno più riconosciuti i toni fax. Il valore 0 indica l'attivazione del rilevamento del tono per l'intera durata della connessione. Valore predefinito: 0
Jitter DSP	
Tipo di buffer del jitter	Definizione del tipo di buffer jitter Valore predefinito: Adattivo
Tipo di buffer del jitter: statico	Il ritardo medio del buffer jitter è sempre lo stesso.
Tipo di buffer del jitter: Adattivo	Alla ricezione dei dati, il buffer jitter modifica il ritardo medio in base alla situazione. Cerca di ridurre al minimo sia il ritardo che la perdita di pacchetti dati.
Ritardo medio voce (ms)	Definizione del tempo di permanenza, espresso in millisecondi, di un pacchetto nel buffer jitter in caso di trasmissioni vocali tramite IP. ***INFO:*** nel caso del **Tipo di buffer del jitterAdattivo** il valore definito qui è solo il valore iniziale. Valore predefinito: 40

Parametri	Descrizione
Ritardo massimo voce (ms)	Definizione del tempo massimo in millisecondi di ritardo per la voce **Tipo di buffer del jitter Statico**: indicare il massimo ritardo effettivamente misurato in millisecondi prima che il buffer del jitter intervenga nel flusso di dati quando riceve pacchetti IP nell'ambito di una trasmissione vocale. Nel buffer jitter statico, il valore consigliato per la maggior parte degli ambienti è 80. **Tipo di buffer del jitter Adattivo**: Indicare il massimo numero di millisecondi per il ritardo vocale medio. Se il ritardo effettivamente misurato è superiore, i pacchetti vanno persi. Nel buffer jitter adattivo, il valore consigliato per la maggior parte degli ambienti è 120. ***Nota:*** Il valore deve essere sempre maggiore rispetto al valore specificato nel campo “Ritardo medio voce (ms)”. Valore predefinito: 120
Ritardo minimo voce (ms)	Definizione del tempo minimo in millisecondi di ritardo per la voce **Tipo di buffer del jitter Adattivo**: indicare il numero minimo di millisecondi consentiti per il ritardo medio vocale. Il ritardo medio deve essere sempre superiore o uguale a questo valore. Valore predefinito: 20
Perdita di pacchetti / preferenza ritardo	Viene definito il rapporto tra perdita di pacchetti e ritardi di propagazione per i pacchetti dati **Tipo di buffer del jitter Adattivo**: indicare un valore compreso tra 0 e 8, a seconda di cosa sembri più accettabile in caso di ritardi consistenti: la perdita di pacchetti o un ritardo ancora maggiore. Un valore di 0 indica la minima perdita di pacchetti, con lo svantaggio di un ritardo di propagazione più consistente. Un valore di 8 indica il minimo ritardo di propagazione, con lo svantaggio di una possibile perdita di pacchetti. Il valore consigliato per la maggior parte degli ambienti è 4. Valore predefinito: 4
Ritardo medio dati (ms)	Definizione del ritardo medio per i dati in millisecondi Qui viene indicato il numero medio di millisecondi durante i quali il pacchetto dati viene trattenuto nel buffer jitter per la trasmissione dei dati. Il valore consigliato per la maggior parte degli ambienti è 60. Valore predefinito: 60
Ritardo massimo dati (ms)	Definizione del ritardo massimo per i dati in millisecondi Qui viene indicato il massimo ritardo effettivamente misurato in millisecondi che intercorre da quando si riceve un pacchetto IP all'intervento del buffer jitter. Il valore consigliato per la maggior parte degli ambienti è 200. ***INFO:*** Valori più elevati (da circa 2000) non hanno alcun effetto. Una volta ricevuto per intero il pacchetto nel buffer, tale pacchetto lascia il buffer. Sono certamente possibili valori inferiori a 100, tuttavia nella pratica sono sconsigliati. Valore predefinito: 200

28.3.14 Statistiche

In **Statistiche** sono riunite le funzioni che vengono utilizzate per la visualizzazione delle statistiche.

28.3.14.1 Statistiche > Statistiche gateway > Scheda madre > Statistiche periferiche

Descrizione dei parametri delle schede:

- **Mostra statistica SCN**
- **Mostra statistica LAN**

Parametri	Descrizione
Tipo di dispositivo	Consente di visualizzare i componenti LAN e SCN (Switched Circuit Network) esistenti.
Risorse al momento occupate	Consente di visualizzare le risorse attualmente assegnate di un componente (canali configurati e utilizzati).
Totale	Consente di visualizzare la somma delle risorse attualmente assegnate.
Aggiornamento autom.	La visualizzazione viene aggiornata automaticamente ogni 60 secondi.
Secondi fino al prossimo aggiornamento	Consente di visualizzare il timer conteggio alla rovescia che parte da 60 secondi.
Utente DDS1	Non appena un telefono cellulare entra nell'area di una posizione di passaggio radio differente ("moduli cordless posizione attuale"), una connessione a un interno viene modificata utilizzando una connessione DSS1 inizializzata dal modulo cordless. Pertanto, l'utente DSS1 fa riferimento al numero o ai telefoni cellulari o alle connessioni DSS1 stabiliti nel passaggio.
HFA / Lingua dei servizi di rete IP	Il componente SCN visualizza il numero di canali DSP occupati quando vengono stabilite le chiamate gateway.
Musica su attesa	Quando la funzione di interlavoro DMC è attiva in una rete IP, le connessioni gateway vengono impostate sui canali DMC. Dalla prospettiva dell'utente, un canale DMC è un canale gateway che fornisce una connessione gateway.
SIU	SIU riserva un canale DSP utilizzato per rilevare o generare toni di sistema, come i toni DTMF
DMC	Consente di visualizzare il timer conteggio alla rovescia che parte da 60 secondi.
H.323 (RTP)	Consente di visualizzare le risorse utilizzate in caso di chiamata vocale.
Fax T.38	Consente di visualizzare le risorse utilizzate in caso di connessione fax.
PPP	Consente di visualizzare le risorse utilizzate in caso di punto-punto.

28.3.14.2 Statistiche > Statistiche gateway > Scheda madre > Statistiche MSC

Descrizione dei parametri delle schede:

- **Mostra statistica complessiva**

  Le statistiche MSC sono le statistiche di conversione media stream utilizzate nei processori di segnali digitali tra IP e TDM (Media Stream Control). La statistica complessiva MSC mostra una panoramica comprendente dati statistici relativi a tutte le comunicazioni registrate. Fornisce informazioni sui pacchetti RTP/TCP inviati e non inviati, sui pacchetti ricevuti e non ricevuti e sul numero di byte inviati e ricevuti.

Descrizione dei parametri delle schede:

- **Mostra statistica chiamate singole**

  La Statistica chiamate singole MSC elenca in formato tabellare, per ogni connessione con conversione mediante processori di segnali digitali, i dati di connessione e i parametri usati. Tali dati sono usati dagli esperti per le analisi degli errori.

28.3.14.3 Statistiche > Statistiche SNMP

Descrizione dei parametri delle schede:

- **Mostra tabella statistica**
- **Mostra statistica**

Parametri	Descrizione
Statistica tabelle if	Statistiche SNMP sulle singole interfacce (se = interfaccia) nel sistema di comunicazione, ad esempio interfacce Ethernet.
Statistica IP	Dettagli ed errori associati al routing IP
Statistica TCP	Dettagli ed errori associati al Protocollo TCP
Statistica UDP	Dettagli ed errori associati al Protocollo UDP

28.3.14.4 Statistiche > Statistiche di telefonia > Testi di sistema

Descrizione dei parametri delle schede:

- **Visualizza testi di sistema**

Parametri	Descrizione
Lingue disponibili	Visualizzazione delle lingue disponibili nel sistema di comunicazione per il display del telefono

28.3.14.5 Statistiche > Statistiche di telefonia > Agenti UCD

Descrizione dei parametri delle schede:

- **Visualizza agenti UCD**

Parametri	Descrizione
Numero agenti UCD	

Parametri	Descrizione
Totale	Numero totale di agenti UCD connessi al sistema di comunicazione
Disponibile	Numero di agenti UCD disponibili
Stato agenti UCD	
Numero di telefono	Numero di telefono dell'agente UCD
Servizio	Nome dell'agente UCD
ID	ID dell'agente UCD
Gruppo UCD	Gruppo UCD a cui è assegnato l'agente UCD.
Stato	Stato dell'agente UCD

28.3.14.6 Statistiche > Statistiche di telefonia > Stato linea

Descrizione dei parametri delle schede:

- **Visualizza stato linea**

Parametri	Descrizione
Data	Data dell'interrogazione sullo stato dell'ultimo cambiamento di stato della linea
Ora	Ora dell'interrogazione sullo stato dell'ultimo cambiamento di stato della linea
Slot / porta	Visualizzazione dei moduli, degli slot e delle porte o dell'interfaccia LAN
Route	Visualizzazione del nome delle route, per capire meglio a quale ITSP appartiene una linea.
Numero linea	Codice della linea
Commento	Stato della linea (viene visualizzato l'ultimo stato della linea). Sono disponibili i seguenti stati della linea: • **Inattività** (linea in stato di quiete) • **In allarme** (è presente una chiamata) • **Collegato a:** (connessione al numero di telefono visualizzato) • **Linea bloccata** • **Linea caduta**

28.3.14.7 Statistiche > Statistiche di telefonia > Inoltro

Descrizione dei parametri delle schede:

- **Visualizza inoltro**

Parametri	Descrizione
Inoltro di chiamata	

Parametri	Descrizione
Stato	Stato della deviazione di chiamata: • **Off**(nessun inoltro di chiamata attivo) • Se la deviazione di chiamata è attiva viene visualizzato il tipo di deviazione di chiamata e la destinazione di inoltro.
Destinaz.di deviazione da	Indicazione se l'utente della destinazione di inoltro dell'inoltro chiamata è un altro utente. Vengono visualizzati il numero di telefono e il nome dell'utente che effettua l'inoltro.
Segnalaz. ampliata	
utent. incl. segnal.chiam.	Numero di telefono e nome utente a cui è applicabile la segnalazione chiamate
Segnalazione da	Indicazione se l'utente della destinazione di inoltro di chiamata è un altro utente. Vengono visualizzati il numero di telefono e il nome dell'utente a cui è applicabile la segnalazione di chiamata.

28.3.14.8 Statistiche > Statistiche di telefonia > Utenti

Descrizione dei parametri delle schede:

- **Visualizza parametri utente**
- **Visualizza funzioni attivate**

Parametri	Descrizione
Numero di telefono	Numero di telefono dell'utente
Servizio	Nome dell’utente
Selezione passante	MSN (Interno) dell'utente
Tipo di dispositivo	Tipo di telefono, ad esempio, OpenStage 60
Clip/Lin	LIN (Location Identification Number) Solo per USA e Canada: il servizio di emergenza avanzato E911 trasmette, in caso di chiamata di emergenza, informazioni sulla posizione geografica del chiamante, oltre al suo numero di telefono. A ogni utente con un numero MSN valido viene assegnato un LIN.
Accesso	Per i telefoni analogici e $U_{P0/E}$ vengono visualizzati la scheda, lo slot e il numero di porta. Solo sui telefoni $U_{P0/E}$ viene visualizzata anche l'impostazione master o slave. Con i telefoni IP, indicazione dell'interfaccia LAN, del tipo e del numero
Parametri	
Tipo di periferica	Tipo di periferica, ad esempio predefinita o fax Valore predefinito: Predefinito
Lingua	Impostazione della lingua del telefono

Parametri	Descrizione
Segnalazione di chiamate interne	Tipo chiamata per la segnalazione di chiamate interne Valore predefinito: Suoneria 1
Segnalazione di chiamate esterne	Tipo chiamata per la segnalazione di chiamate esterne Valore predefinito: Suoneria 1
Abilitazione (LCR)	Classe di autorizzazione dell'utente per Least Cost Routing (LCF) Valore predefinito: 15
Tipo di licenza	Tipo di licenza dell'utente
Caratteristiche	
Non disturbare	Stato della funzione Non disturbare Valore predefinito: Off
Messaggio di risposta	Stato della funzione Messaggio di risposta Valore predefinito: Off
Chiave elettronica	Stato della funzione Chiave elettronica Valore predefinito: Off
Disattivazione della visualizzaz. del nr. di telefono on	Stato della funzione Disattivazione della visualizzaz. del nr. di telefono Valore predefinito: Off
Segnalaz. ampliata	Stato della funzione Segnalazione delle chiamate Valore predefinito: Off
Attivare il silenzio	Stato della funzione Chiamata senza suoneria/Silenzio Valore predefinito: Off
Passo multiplo/chiamata di gruppo	Stato della funzione Gruppo di ricerca/Chiamata di gruppo Valore predefinito: Off
Avviso di chiam. in attesa senza segnalazione acustica	Stato della funzione Avviso di chiam. in attesa senza segnalazione acustica Valore predefinito: Off
Risposta tramite altoparlante	Stato della funzione Risposta tramite altoparlante Valore predefinito: Off
Rilascio avviso chiamata in attesa	Stato della funzione Rilascio avviso chiamata in attesa Valore predefinito: Off
Deviazione chiamata dopo intervallo	Stato della funzione Deviazione chiamata dopo intervallo Valore predefinito: Off
AUL	Stato della funzione Deviazione di chiamata (AUL) Valore predefinito: Off

28.4 Applicazioni

In **Applicazioni** sono riportate le funzioni per la configurazione del server applicazioni per la comunicazione unificata e Web Services.

28.4.1 Selezione applicazione

In **Selezione applicazione** sono riunite le funzioni utilizzate per la scelta della soluzione di comunicazione unificata utilizzata.

28.4.1.1 Selezione applicazione

Descrizione dei parametri delle schede:

- **Selezione applicazione**

Parametri	Descrizione
Seleziona pacchetti applicazioni	Selezione del pacchetto applicazioni con UC Smart o con UC Suite. Nel pacchetto applicazioni con UC Suite su OpenScape Business UC Booster Server, è necessario inoltre l'indirizzo IP dell'UC Booster Server (l'indirizzo IP del server Linux).
Selezione applicazione	Visualizzazione dei componenti supportati per il pacchetto applicazione selezionato, incluso l'indirizzo IP del server utilizzato.

28.4.2 Servizio di integrazione Active Directory

Le funzioni rilevanti per l'integrazione di Active Directory sono raggruppate sotto **Servizio di integrazione Active Directory**.

28.4.2.1 Servizio di integrazione Active Directory

Descrizione dei parametri delle schede:

- **Servizio di integrazione Active Directory**

Parametri	Descrizione
Tipo sincronizzazione	I valori possibili per il tipo sincronizzazione sono i seguenti: • **Libero** Non viene eseguita nessuna sincronizzazione dell'utente con il servizio Active Directory. • **did** Sincronizzazione automatica dell'utente con Active Directory. Il numero DID è utilizzato come chiave di sincronizzazione. • **forzata** Sincronizzazione manuale dell'utente con Active Directory. Con la sincronizzazione forzata, è possibile sincronizzare l'utente Active Directory con più utenti OpenScape Business. • **membro_mulap** L'utente sincronizzato automaticamente è membro di un gruppo MULAP.
Cerca	I campi liberi nella parte superiore dello schermo possono essere usati per ricercare un utente specifico quando il numero di utenti è troppo grande per entrare in una sola schermata. Nei campi **Nome**, **Cognome**, **Nome visualizzato** e **DID** viene eseguita una ricerca "inizia con". Nel campo **Utente Active Directory** viene eseguita una ricerca "contiene". La ricerca inizia dopo aver premuto il pulsante **Cerca**.
Modifica	Questo pulsante può essere utilizzato per configurare la sincronizzazione di un utente specifico. Le azioni disponibili quando si seleziona **Modifica** sono i seguenti pulsanti che appaiono.
Salva i dati	Si può selezionare un utente AD specifico e forzare la sincronizzazione con un utente OpenScape Business specifico. In questo modo si possono sincronizzare diversi numeri DID con lo stesso utente AD.
Reimposta	Tentativo di sincronizzazione di un utente OpenScape Business con qualsiasi utente Active Directory. Quest'azione può essere usata, ad esempio, se la sincronizzazione utente si arresta.
Non sincronizzare	Arresta la sincronizzazione di un utente OpenScape Business specifico. I dati utente già sincronizzati non vengono eliminati ma viene interrotta qualsiasi sincronizzazione ulteriore.

28.4.3 UC Smart

UC Smart comprende diverse funzioni di comunicazione unificata.

28.4.3.1 UC Smart > Impostazioni di base

Descrizione dei parametri delle schede:

- **Impostazioni di base**

Parametri	Descrizione
Attiva/disattiva UC Smart	

Parametri	Descrizione
Attiva	UC Smart e la UC Suite non possono essere attivi contemporaneamente. (Dopo l'attivazione, vengono visualizzati altri parametri)
Attiva/disattiva CloudService	
Attiva	Questo flag controlla lo stato della funzionalità CloudService. Si noti che attivando la funzione CloudService, WebServices verrà riavviato.
Impostazioni di accesso	
HTTP	I client UC Smart possono accedere al sistema tramite HTTPS (connessione crittografata, opzione consigliata) o HTTP (connessione non crittografata, opzione non consigliata). La selezione viene effettuata all'interno dell'applicazione stessa. Qui viene definita l'abilitazione per uno o entrambi i protocolli.
HTTPS	
Politica per le password	
L'utente deve immettere una password sicura	Criteri per l'impostazione della password nei client UC Smart. La password predefinita deve essere cambiata al primo accesso e la nuova password deve corrispondere ai criteri qui definiti (vedere il pulsante del punto esclamativo). La password viene memorizzata nel client, altrimenti viene richiesta ogni volta che si avvia il client.
Salvare i dati di accesso nel terminale	I dati di accesso sono inoltre memorizzati nel telefono.
Password iniziale UC Smart a livello di sistema	La password iniziale comune a livello di sistema si applica a tutti gli utenti UC Smart configurati che non hanno ancora effettuato l'accesso a UC Smart e non hanno ancora cambiato tale password iniziale. Successivamente, ogni utente in questione deve essere inserire una password personalizzata. ***INFO***: L'assegnazione di una password iniziale comune a livello di sistema in UC Smart pone un rischio per la sicurezza nel caso in cui i singoli utenti non utilizzino successivamente una password personale. In alternativa, si consiglia l'assegnazione di password iniziali individuali per ciascun utente.
Orario d'ufficio	
Ora inizio	È possibile configurare l'orario d'ufficio selezionando di conseguenza due valori dagli elenchi a discesa Ora inizio e Ora fine. L'orario d'ufficio predefinito è dalle 08:00 alle 20:00
Ora fine	
Presenza	
Nascondi stato con errori	È possibile nascondere l'opzione dello stato di presenza "Malattia" agli utenti dei client UC.

28.4.3.2 UC Smart > Gestione utenti

Descrizione dei parametri delle schede:

- **Gestione utenti**

Parametri	Descrizione
Utente	Elenco di tutti gli utenti presenti; gli utenti selezionati devono ottenere una licenza Utente UC
Impostazioni	
Utenti	Visualizzazione del numero interno dell'utente.
Servizio	Visualizzazione del nome dell'utente.
Password	Qui è possibile definire la password del client UC Smart.
Lingua	Lingua di UC Smart Assistant
L'utente deve indicare una nuova password	(solo visualizzazione)
Accesso UC Smart Assistant	Abilitazione all'accesso a UC Smart Assistant tramite l'utente
Configurato come utente Mobility	(solo visualizzazione)
Licenza casella vocale	(solo visualizzazione)
Servizi associati	(solo visualizzazione)
Dettagli del profilo	
Numero del cellulare	Numero di cellulare del partecipante in formato canonico (ad es. `+39 173 1234567`).
Numero di telefono privato/ esterno	Numero di telefono aggiuntivo dell'utente in formato canonico (ad es. `+39 051 987654321`).
Indirizzo e-mail	Indirizzo e-mail dell'utente
Da casella vocale a e-mail	Attivazione/disattivazione dell'avviso tramite e-mail all'arrivo di un nuovo messaggio vocale.
Visibilità presenza	Consente di impostare se lo Stato presenza deve essere visibile per partecipanti interni ed esterni o solo per gli interni o per nessun tipo di partecipante.
Informazioni sulla licenza	Visualizzazione delle licenze disponibili nel sistema per la particolare applicazione

28.4.3.3 UC Smart > Stato

Descrizione dei parametri delle schede:

- **Stato**

Parametri	Descrizione
Server applicazioni	Visualizzazione lo stato del server applicazioni UC Smart integrato.
Connessioni attive	Visualizzazione del numero di connessioni attive per client UC Smart.

28.4.4 OpenScape Business, UC Suite

In **OpenScape Business UC Suite** sono presenti funzioni di comunicazione unificata, quali Conferenza in corso, Reparti e Gruppi, Configurazione della rubrica esterna, Pianificazioni normali e di vacanze nonché le impostazioni dei server e del Contact Center per la UC Suite.

28.4.4.1 OpenScape Business, UC Suite

Parametri	Descrizione
OpenScape Business, UC Suite	Configurazione della UC Suite, comprensiva dei client myPortal, myAgent, myAttendant e myReports, messaggi vocali e fax e conferenze.

28.4.4.2 OpenScape Business UC Suite > Rubrica utente

Se si desidera modificare il proprio nome e cognome, questa operazione deve essere eseguita dall'amministratore. In caso contrario, le modifiche non saranno mantenute dopo la sincronizzazione. La sincronizzazione avviene quando il sistema si riavvia o qualsiasi impostazione viene modificata dall'amministratore.

Se un utente è membro di un gruppo MULAP, non è visualizzato nella rubrica utente. Se un utente è membro di un gruppo di ricerca, è visualizzato nella rubrica utente.

Parametri	Descrizione
Cerca	Ricerca di un utente UC Suite.
Icona dello stato presenza	L'amministratore può modificare lo stato di presenza per ogni utente e impostare la relativa data e ora di ritorno nel formato Giorno-Mese-Anno (GG/MM/AA) e 24 ore (HH:MM), rispettivamente. Un'icona grigia non è attualmente connessa alla UC Suite. **Nota:** Ogni membro di un gruppo di ricerca è considerato come un utente della rubrica del sistema ed è visualizzato in grigio.
Modifica	Modifica delle impostazioni dell'utente UC Suite selezionato. **Nota:** A causa di un noto problema di compatibilità del browser, la configurazione della finestra **Modifica utente** può essere diversa quando si utilizza Firefox. La configurazione è coerente con IE/Chrome/Edge.

Parametri	Descrizione
Reimposta utente	Le impostazioni di un utente vengono riportate ai valori predefiniti. Durante il processo vengono cancellati i messaggi vocali, i messaggi personali della casella vocale, le voci del diario, le conferenze pianificate, le e-mail e i messaggi fax dell'utente. **Nota:** In questo caso, la password predefinita è impostata su 4 caratteri (1234).
Sblocca utente	Gli utenti bloccati (ad esempio dopo diversi tentativi errati di inserire la password) possono essere sbloccati, visualizzazione icona lucchetto. L'amministratore può essere informato della revoca via e-mail.
Dati personali	Dati personali dell'utente
Dati personali: I miei dati personali	Nome di accesso, Password, Cognome, Interno, Nome, Numero casella vocale, Numero fax, Numero assistente, E-mail, Reparto, Numero cellulare, Numero esterno 1/2, Numero abitazione (in formato canonico, es. +49 89 700798765). La password è valida per i client UC Suite.
Dati personali: La mia immagine	Viene dimensionato automaticamente Formati file supportati: BMP, JPG/JPEG/JFIFI, PNG. Dimensione massima del file: 10 MB
Dati personali: Livello utente	Configurabile solo dall'amministratore per il Contact Center: se l'agente deve essere permanentemente disponibile, selezionare la casella di controllo **Agente sempre disponibile**. L'agente rimane disponibile per chiamate, fax e e-mail, anche se non ha risposto a una chiamata, fax o e-mail. Quando si configura un utente come agente, vengono definiti i diritti di agente selezionando l'appropriata classe di servizio per quell'agente (ossia il livello di autorizzazione come agente, supervisore o amministratore) dall'elenco a discesa **Livello**. I supervisori e gli amministratori possiedono un livello di autorizzazione superiore.
Preferenze	Impostazioni del client specifiche per l'utente.
Preferenze: Aspetto	Colori delle skin dell'interfaccia utente; lingua dell'interfaccia utente; utilizzo o meno del classico tray pop.
Preferenze: Avvisi	Impostazioni delle finestra popup.
Preferenze: Presenza	Impostazioni dello stato di presenza.
Preferenze: Connettività Outlook	Generazione di appuntamenti calendario: acquisizione dello stato presenza nell'integrazione calendario di Outlook: controllo dello stato presenza tramite appuntamenti Outlook/iCal (la prima parola chiave nella riga dell'Oggetto controlla lo stato presenza)
Preferenze: Tasti di scelta rapida	Definizione dei tasti di scelta rapida per le funzioni di chiamata.

Parametri	Descrizione
Preferenze: Varie	Reimpostazione automatica dello stato di presenza allo stato "Ufficio" al termine dell'appuntamento, abilitazione della registrazione dei registri dei client, definizione del metodo di trasmissione, tempo di conservazione delle voci del registro (il valore massimo è di 30 giorni), programmazione dei tasti funzione del telefono, abilitazione della ricerca live e inclusione dei contatti LDAP nella ricerca live nelle directory, definizione di un messaggio di risposta.
Regole di chiamata	Regole per chiamate in entrata
Regole di chiamata: Destinazioni di inoltro	Definizione delle destinazioni di inoltro per ogni stato presenza (deviazione di chiamata basata sullo stato)
Regole di chiamata: Motore regole	Definizione di regole di chiamata complesse in funzione dello stato presenza (deviazione di chiamata basata su regole)
Comunicazioni	Gestione dei messaggi di utenti specifici
Comunicazioni: Impostazioni casella vocale	Registrazione di messaggi vocali in ogni stato presenza; impostazione della lingua della casella vocale Valore predefinito: disattivato
Comunicazioni: Avviso VM	Per il servizio informativo per nuovi messaggi vocali e e-mail, vedere I miei dati personali. Requisito: il server di posta e il proprio indirizzo di posta elettronica sono configurati in Service Center > Inoltro e-mail". "In uscita" crea una User Outcall al numero di telefono indicato (formato canonico). Per i numeri di telefono SMS, vedere I miei dati personali. Per il contenuto dell'SMS, vedere Modelli.
Comunicazioni: Avviso fax	Per il servizio informativo per nuovi messaggi fax e e-mail, vedere I miei dati personali. Requisito: il server di posta e il proprio indirizzo di posta elettronica sono configurati in Service Center > Inoltro e-mail". L'opzione "In uscita" genera una chiamata in uscita da parte dell'utente al numero di telefono specificato (in formato canonico) solo entro l'orario lavorativo oppure 24 ore al giorno. Per i numeri di telefono SMS, vedere I miei dati personali. Per il contenuto dell'SMS, vedere Modelli.
Comunicazioni: Notifiche di chiamata senza risposta	Per il servizio di notifica per nuove chiamate perse, vedere l'indirizzo e-mail in I miei dati personali. Requisito: il server di posta e il proprio indirizzo di posta elettronica sono configurati in Service Center > Inoltro e-mail".
Profili	profilo per AutoAttendant personale
Occupato, Nessuna risposta, In riunione, In malattia, In pausa, Fuori sede, In vacanza, A pranzo, A casa	Un chiamante può essere trasferito digitando una cifra da 0 a 9 a una destinazione di inoltro o può lasciare un messaggio. A tal fine è richiesto un annuncio per stato presenza.
Profili: Ignora annuncio dinamico	L'annuncio automatico dello stato presenza non viene riprodotto e al suo posto per il chiamante viene riprodotto solo l'annuncio del nome e quindi l'AutoAttendant personale
Sensibilità	Impostazioni per salvaguardare la riservatezza dei dati

Parametri	Descrizione
Sensibilità: Protezione e accesso	Rilascio di messaggi vocali per myAttendant; controllo della casella vocale dal proprio telefono senza alcuna password; visibilità delle persone con cui si sta parlando e copia del proprio layout BLF.
Sensibilità: Visibilità presenza	Definizione della visibilità del proprio stato presenza per gli utenti interni
Sensibilità: Presenza casella vocale	Annuncio del proprio stato presenza per chiamante esterno. Immissione di numeri di telefono interni bloccati, è possibile utilizzare caratteri jolly.
myAttendant	Visualizzazione solo per utenti che dispongono di licenza per myAttendant
myAttendant: Messaggi LAN	Moduli di testo per messaggi istantanei di myAttendant, liberamente scelti, selezione nella finestra chat del client
myAttendant: DID	Immissione di numeri di selezione passante; in caso myAttendant venga utilizzato da più aziende, può essere visualizzata una finestra "Per"
myAttendant: Comunicazioni	Immissione di un numero interno per gli inoltri chiamata in caso di emergenza o per la mancata accettazione (Inoltro non presidiato) da parte di myAttendant (per gli USA)

28.4.4.3 OpenScape Business UC Suite > Reparti

Descrizione dei parametri delle schede:

- **Reparti**

Parameters	Descrizione
Nome reparto	I reparti raggruppano gli utenti presenti nella rubrica interna in base alle rispettive organizzazioni. In questo modo è possibile eseguire ad esempio l'assegnazione automatica degli utenti ai reparti con myAttendant.
Gruppo di ricerca	(Numerazione interna non rilevante)
Add	Add a new department.
Modifica	Edit a selected department.
Rimuovi	Remove the selected departments.

28.4.4.4 OpenScape Business UC Suite > Gruppi

Attraverso un gruppo Casella vocale (segreteria telefonica) è possibile consentire l'accesso a messaggi vocali a uno specifico gruppo di utenti. Il numero di telefono del gruppo Casella vocale non consente di chiamare i membri di questo gruppo, ma di raggiungere direttamente la segreteria telefonica (ovvero la casella vocale) del gruppo.

Attraverso un gruppo fax (gruppo Casella fax) è possibile consentire l'accesso a messaggi fax a uno specifico gruppo di utenti. Il numero di telefono del gruppo fax consente di raggiungere direttamente la casella fax del gruppo.

I gruppi Preferiti consentono di creare gruppi con contatti e assegnarli agli utenti.

Descrizione dei parametri delle schede:

- **Gruppi vocali**
- **Fax group**
- **Gruppi Preferiti**

Tabella 64:

Parameters	Descrizione
VoiceMail groups	
Modifica	Edit the selected voicemail group
Rimuovi	Remove the selected voicemail groups
VoiceMail groups	Nome gruppo casella vocale
Pilota	Numero di telefono del gruppo casella vocale
Tipo	Tipo di gruppo casella vocale
N. utenti	Numero di membri di un gruppo casella vocale
N. messaggio	Numero di nuovi messaggi vocali per il gruppo casella vocale
Utenti	Membri del gruppo casella vocale
Fax group	
Modifica	Edit the selected fax group
Fax Group	Name of the fax group
Pilota	Call number of the fax group
N. utenti	Number of members in the fax group
N. fax	Number of new fax messages for the fax group
Multiutenti	If it is a fax group, **Yes** is displayed. Otherwise **No** is displayed.
Gruppi Preferiti	
Add	Add a new favourite group
Modifica	Edit the selected favourite group
Rimuovi	Remove the selected favourite groups
Nome gruppo	Nome del gruppo Preferiti
Numero di contatti	Numero dei contatti che sono stati aggiunti al gruppo

Parameters	Descrizione
Modificabile	Selezionare se l'utente può modificare o meno il gruppo Preferito.

28.4.4.5 OpenScape Business UC Suite > Modelli

Descrizione dei parametri delle schede:

- **Provider SMS**

Parameters	Descrizione
Add	Add a new Template. Enter the Template's name and the author's name. Placeholders, which can be selected individually under "VSL Fields", can be inserted into the Recipient, Subject or Body fields, respectively.
Modifica	Edit the selected Template. Change the Template's name and the author's name. Edit also Recipient, Subject and Body fields. Placeholders, which can be selected individually under "VSL Fields", can be inserted into the Recipient, Subject or Body fields, respectively.
Rimuovi	Remove the selected Template.
Set To Default	Set the selected Template as default.

28.4.4.6 OpenScape Business UC Suite > External Directory

Descrizione dei parametri delle schede:

- **Rubrica esterna**

Parameters	Descrizione
Add	Aggiunta manuale di singoli contatti alla rubrica esterna. I caratteri devono essere nel formato UTF-8
Modifica	Edit a selected contact of the external directory.
Rimuovi	Remove the selected contacts of the external directory

Descrizione dei parametri delle schede:

- **Importa rubrica esterna**

Parameters	Descrizione
Importa da	Choose whether the import of contacts information will be done from a local file or from a public Windows folder.
Carica file	Click **Choose File** to select the file to be uploaded to the system.
Cartella di Windows pubblica	Enter the **Filename**, **Username**, **Domain**, **Password** of the public windows folder to be uploaded to the system and click **Test** to test it.

Parameters	Descrizione
Opzioni	This area offers various options regarding the formatting of the csv file that is going to be imported. Additionally there is an option that clears the existing data before executing the import. Finally, another one option declares the way that duplicates are handled during an import.

Descrizione dei parametri delle schede:

- **Esporta directory esterna**

Parameters	Descrizione
Esporta in	Choose where the exported file will be saved, locally or in a public Windows folder.
Cartella di Windows pubblica	Enter the **Filename**, **Username**, **Domain**, **Password** of the public windows folder to be uploaded to the system and click **Test** to test it.

28.4.4.7 OpenScape Business UC Suite > Config provider esterni

Descrizione dei parametri delle schede:

- **Fornitori LDAP**

Parametri	Descrizione
Aggiungi/Modifica/Rimuovi	Aggiungere, modificare o rimuovere i dati di accesso del server LDAP.
Nome	Nome per questa rubrica esterna non in linea
Server/Indirizzo del server	Nome DNS o indirizzo IP del server LDAP.
Porta	Numero di porta del server LDAP esterno
Nome utente	Nome utente per l'accesso al server LDAP remoto.
Password	Password per l'accesso al server Exchange remoto.
Nome distinto base LDAP	Nome distinto base LDAP, ad es.: dc=esempio-di-dominio, dc=rete.
TLS	Abilitare l'uso solo di connessioni sicure al server LDAP.
Titolo, **Nome**, **Cognome**, **Ufficio 1**, **Ufficio 2**, **Num. abitazione**, **Cellulare**, **Società**, **Num. società**, **Indirizzo postale**, **Stato o provincia**, **Paese**, **Codice postale**, **E-mail**, **Cercapersone**, **Numero di fax** e **Città**	In fase di configurazione di una rubrica esterna non in linea, l'amministratore può adattare la mappatura dei campi ai nomi del server LDAP utilizzato. Durante la ricerca del nome tramite il numero di telefono, i campi eliminati vengono ignorati. La ricerca viene sempre eseguita sulle ultime 4 posizioni del numero di telefono, precedute dal carattere jolly predefinito. È possibile disattivare la ricerca del nome mediante il numero di telefono all'arrivo delle chiamate. Immettere la designazione del campo corrispondente del server LDAP. **Nota:** La mappatura campo LDAP dipende dal nome del campo corrispondente in base all'uso del server LDAP esterno.

Descrizione dei parametri delle schede:

- **PST scambio**

Parametri	Descrizione
Aggiungi/Modifica/Rimuovi	Aggiungere, modificare o rimuovere i dati di accesso del server Exchange. In un ambiente Microsoft, Active Directory Server (ADS) ovvero il server Exchange funge anche da server LDAP.
Nome	Nome di questa rubrica esterna non in linea.
Metodo di autenticazione	Metodo di autenticazione da utilizzare per l'accesso al server Exchange remoto. È possibile scegliere tra **Di base** e **OAuth 2.0**.
Server/Indirizzo del server	Nome DNS o indirizzo IP del server Exchange.
Nome utente	Nome utente per l'accesso al server Exchange remoto.
Password	Password per l'accesso al server Exchange remoto. Visibile solo se il metodo di autenticazione selezionato è **Di base**.
ID tenant, **ID applicazione**, **ID client**, **Ambito**	**ID tenant**, **ID applicazione** e **ID client** corrispondenti all'applicazione registrata in Azure AD per l'integrazione della directory di Exchange. Possono essere ottenuti dall'amministratore di Azure AD. **Ambito** richiesto dall'applicazione (facoltativo). Valore predefinito: https://outlook.office365.com/.default Visibile solo se il metodo di autenticazione selezionato è **OAuth 2.0**.

Descrizione dei parametri delle schede:

- **Integrazione del calendario di Exchange**

Parametri	Descrizione
Integrazione del calendario di Exchange	In Windows, l'integrazione calendario viene utilizzata per la creazione automatica di appuntamenti di Outlook in caso di assenza. Se gli appuntamenti di Outlook non vengono memorizzati nel file PST locale, ma sul server di Exchange, i dati di accesso devono essere inseriti qui.
Attiva integrazione del calendario di Exchange	Attivazione dell'integrazione calendario di Exchange
Metodo di autenticazione	Metodo di autenticazione da utilizzare per l'accesso al server Exchange remoto. È possibile scegliere tra **Di base** e **OAuth 2.0**.
Server	Per maggiori dettagli sull'uso delle diverse versioni del server Microsoft Exchange, consultare il sito Unify Experts Wiki all'indirizzo: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.
Nome utente	Nome utente per l'accesso al server Exchange remoto.
Password	Password per l'accesso al server Exchange remoto. Visibile solo se il metodo di autenticazione selezionato è **Di base**.

Parametri	Descrizione
ID tenant, **ID applicazione**, **ID client**, **Ambito**	**ID tenant**, **ID applicazione** e **ID client** corrispondenti all'applicazione registrata in Azure AD per l'integrazione del calendario di Exchange. Possono essere ottenuti dall'amministratore di Azure AD. **Ambito** richiesto dall'applicazione (facoltativo). Visibile solo se il metodo di autenticazione selezionato è **OAuth 2.0**.

28.4.4.8 OpenScape Business UC Suite > Contact Center

Descrizione dei parametri delle schede:

- **Pianificazione**
- **Coda**
- **Livello di servizio**
- **Priorità chiamante VIP**
- **Elenco chiamate VIP**
- **Agenti preferiti**
- **Pause del Contact Center**
- **Elaborazione semplice**
- **Elaborazione multipla**
- **Associazioni coda**

Pianificazione

Le pianificazioni definiscono come devono essere trattate le chiamate, in giorni e in orari specifici. Le pianificazioni e le regole ivi contenute (Call Control Vector, CCV) consentono di definire per ogni coda d'attesa come le chiamate in arrivo verranno gestite in giorni o orari specifici. A una pianificazione deve essere assegnata almeno una regola (Call Control Vector CCV). Le regole determinano, per il periodo di validità di una pianificazione, come vengono gestite le chiamate in entrata di una coda di attesa. Le regole si applicano solo alle chiamate e non ai fax e alle e-mail.

Per informazioni dettagliate sulla configurazione di pianificazioni, vedere Procedura di configurazione

Parametri	Descrizione
Pianificazione	Nome pianificazione
Coda	Nome della coda d'attesa associata alla pianificazione.
Gruppo di ricerca	Identificatore gruppo di ricerca del gruppo UCD, impostato durante la configurazione di base del Contact Center.
Pianificazione	
Nome pianificazione	Nome pianificazione

Parametri	Descrizione
CCV predefinito	Viene visualizzata la regola predefinita per questa pianificazione, valida dopo l'assegnazione a una coda di attesa 24 ore al giorno e 365 giorni all'anno. Se in occasioni e orari specifici (pausa, fine settimana, giorno festivo, vacanza ecc.) sono valide altre regole, è possibile assegnarvi una pianificazione corrispondente sotto forma di regole eccezione (CCV eccezione).
Code	
Nome coda	Nome della coda d'attesa associata alla pianificazione.
Coda attiva	Indica se la coda d'attesa è attiva o inattiva.
Eccezioni	
CCV	Nome della regola eccezione (eccezione CCV) Definire le regole eccezione, ovvero come verranno gestite le chiamate in arrivo in ore specifiche (pausa, fine settimana, ferie, vacanza, ecc.). In questo caso le pianificazioni vacanze hanno la priorità rispetto alle altre pianificazioni e regole di una coda d'attesa.
Descrizione	Testo descrittivo per la regola eccezione
Tipo	Tipo di regola eccezione
Data inizio	Data di inizio della regola eccezione
Data fine	Data di fine della regola eccezione
Ora di inizio	Ora di inizio della regola eccezione
Ora fine	Ora di fine della regola eccezione
Si verifica	La frequenza con la quale è stata pianificata la regola di eccezione

Coda

Le code d'attesa sono alla base del Contact Center. Le chiamate, i fax e le e-mail di una coda d'attesa vengono gestiti in base al livello di competenza degli agenti, alla priorità e al tempo d'attesa. Per le chiamate in attesa è possibile riprodurre annunci.

Per informazioni dettagliate sulla configurazione di code d'attesa, vedere Procedura di configurazione

Parametri	Descrizione
Coda	Nome coda
Coda attiva	Indica se la coda d'attesa è attiva o inattiva.
Gruppo di ricerca	Identificatore gruppo di ricerca del gruppo UCD, impostato durante la configurazione di base del Contact Center.
Impostazioni generali	
Nome coda	Nome coda
Coda attiva	Definizione dello stato della coda d'attesa

Parametri	Descrizione
Coda attiva: Inattivo	La coda d'attesa non è attiva.
Coda attiva: Attivo	La coda d'attesa è attiva.
Gruppo di ricerca	Identificatore gruppo di ricerca del gruppo UCD, impostato durante la configurazione di base del Contact Center.
Switch telefono	Viene visualizzata la voce CSP
Pianificazione	Viene visualizzata la pianificazione assegnata
Conteggio allarmi coda	Valore soglia di allarme Se il numero qui indicato supera il numero di chiamate in coda d'attesa, l'icona della coda d'attesa visualizzata dall'agente passa da verde ad arancione. Valore predefinito: 0 chiamate
Ora allarme coda	Valore soglia di allarme in secondi Se il tempo in coda d'attesa per una chiamata qui indicato viene superato, la corrispondente voce nell'elenco di chiamate del Contact Center dell'agente diventa rossa. Valore predefinito: 0 secondi
Timeout chiamate perse	Timeout per chiamate perse in secondi Trascorso il tempo qui specificato una chiamata senza risposta da parte dell'agente viene inoltrata al successivo agente libero. Valore predefinito: 10 secondi
Soglia chiamate abbandonate	Tempo limite per chiamate interrotte in secondi Sulla base del tempo qui indicato, viene definito se una chiamata abbandonata viene inclusa nelle statistiche. Verranno incluse nelle statistiche le chiamate che vengono abbandonate una volta trascorso il tempo indicato. Valore predefinito: 0 secondi
Finestra popup attivata	Se il flag è attivato: in myAgent viene visualizzata una finestra popup all'arrivo delle chiamate per visualizzare e inserire i dati dei clienti. Le finestre popup sono necessarie per accettare ed eseguire richiamate, nonché per accettare fax e e-mail. Valore predefinito: Disattivato **Nota:** Le notifiche relative alle opzioni tramite **myAgent** > **Configurazione** > **Notifiche** > **Applicazione popup su chiamate in entrata** vengono sovrascritte dall'attivazione della screen pop **WBM** > **Modalità esperti** > **OpenScape Business UC Suite** > **Contact Center** > **Coda** > **Impostazioni generali** > **Screen pop abilitata**.
Modalità elaborazione	Definizione della modalità elaborazione

Parametri	Descrizione
Modalità elaborazione: Nessuna elaborazione	Per le code d'attesa non possono essere definiti motivi per l'elaborazione.
Modalità elaborazione: Elaborazione semplice	Per le code d'attesa possono essere definiti uno o più motivi per l'elaborazione.
Modalità elaborazione: Elaborazione multipla	Per le code d'attesa è possibile definire uno o più motivi per l'elaborazione e riunirli in gruppi o sottogruppi.
Timeout finestre popup	Timeout screenpop in secondi Se è impostato a 0, myAgent richiederà automaticamente 20 secondi di durata della finestra popup. Valore predefinito: 20 secondi
Priorità	Se un agente è assegnato a più code d'attesa, tramite la priorità delle code d'attesa è possibile definire se le chiamate per una coda d'attesa con priorità più alta devono essere inoltrate a questo agente con precedenza sulle chiamate di altre code d'attesa.
Modalità lunghezza coda di attesa	Definizione della modalità lunghezza coda di attesa
Modalità lunghezza coda di attesa: Statica	Se la modalità lunghezza coda di attesa è impostata a Statica, è possibile configurare WLS e la lunghezza della coda di attesa.
Modalità lunghezza coda di attesa: Nessuno	Se la modalità lunghezza coda di attesa è impostata a Nessuna, è possibile configurare il parametro WLS, che influenza anche la configurazione UCD. Tuttavia il parametro lunghezza coda di attesa non può essere configurato.
Piloti coda	
Piloti fax in arrivo	Numeri di telefono (piloti) per fax in arrivo I fax destinati a questi numeri vengono inseriti nella coda d'attesa e trattati come una chiamata in arrivo.
Servizio e-mail in arrivo	Indirizzi e-mail per e-mail in arrivo Le e-mail a questi indirizzi vengono inserite nella coda d'attesa e trattate come una chiamata in arrivo.
Aggiungi	Consente di aggiungere un nuovo servizio di e-mail in entrata
Modifica	Consente di modificare il servizio di e-mail in entrata selezionato
Rimuovi	Consente di rimuovere il servizio di e-mail in entrata selezionato
Metodo di autenticazione	Metodo di autenticazione da usare per accedere al servizio di e-mail in entrata È possibile scegliere tra **Basic** e **OAuth 2.0**.
Server	Nome DNS o indirizzo IP del servizio e-mail in entrata
Porta	Numero di porta del servizio e-mail in entrata
Nome utente	Nome utente per accedere al servizio e-mail in entrata

Parametri	Descrizione
Password	Password per accedere al servizio e-mail in entrata Modificabile solo se il metodo di autenticazione selezionato è **Basic**.
Utilizza connessioni SSL	Consente di abilitare o disabilitare l'uso delle connessioni SSL in base alla configurazione del servizio e-mail in entrata
ID tenant, **ID applicazione**, **Segreto client**, **Ambito**	**ID tenant**, **ID applicazione** e **Segreto client** corrispondenti all'applicazione registrata in Azure AD per le code e-mail. Si possono ottenere dall'amministratore di Azure AD. **Ambito** richiesto dall'applicazione (facoltativo). Valore predefinito: https://outlook.office365.com/.default Visibile solo se il metodo di autenticazione selezionato è **OAuth 2.0**.
Varie	
Indirizzo e-mail del mittente	Indirizzo e-mail del mittente dell'e-mail inviata Quando l'agente invia un'e-mail, l'indirizzo e-mail qui indicato viene visualizzato dal destinatario.
Routing chiamate intelligente	Se il flag è attivato: le chiamate in arrivo vengono automaticamente deviate all'agente che per ultimo è stato in contatto con il chiamante. Ciò è possibile se per il chiamante non è stato definito alcun agente preferito. Valore predefinito: Disattivato

Livello di servizio

Sulla base del livello di servizio, è possibile eseguire valutazioni sulla qualità di risposta in una coda d'attesa. Questo è possibile tramite il confronto dei tempi di attesa dei chiamanti in una coda d'attesa con i valori soglia che possono essere qui definiti per ogni coda d'attesa.

Per di ogni chiamata alla rispettiva coda di attesa, al termine della chiamata viene rilevato il grado di servizio e acquisito nella database. L'analisi del livello di servizio può essere eseguita dagli agenti con il livello di autorizzazione "Supervisore" o "Amministratore" tramite l'applicazione myAgent.

Per informazioni dettagliate sulla definizione dei valori soglia per il livello di servizio, vedere Procedura di configurazione

Parametri	Descrizione
Coda	Nome coda
Coda attiva	Indica se la coda d'attesa è attiva o inattiva.
Gruppo di ricerca	Identificatore gruppo di ricerca del gruppo UCD, impostato durante la configurazione di base del Contact Center.
Livello di servizio	L'asse orizzontale mostra il tempo di attesa nella coda a intervalli di 10 secondi, l'asse verticale la soglia per il livello di servizio espressa in valori percentuali. I punti rossi indicano la soglia per la qualità di commutazione nella coda d'attesa. Confrontando i valori soglia con i tempi d'attesa effettivi dei chiamanti, è possibile valutare la qualità.

Priorità chiamante VIP

Sulla base della priorità chiamante VIP, è possibile definire in modo indipendente per ciascuna coda d'attesa se i chiamanti contenuti nell'Elenco chiamate VIP devono essere trattati con priorità.

I valori per la Priorità chiamante VIP possono essere liberamente definiti in base al tempo di attesa del chiamante nella coda d'attesa. In questo modo, si determina il livello di priorità di chiamanti VIP rispetto ai chiamanti normali.

Se un chiamante VIP attiva una richiamata agente (registrazione di un messaggio vocale con richiesta di richiamata), la richiamata agente prende il posto del chiamante VIP nella coda d'attesa. Non viene quindi trasmessa la priorità chiamante VIP.

Per informazioni dettagliate sulla definizione di priorità chiamante VIP, vedere Procedura di configurazione

Parametri	Descrizione
Coda	Nome coda
Coda attiva	Indica se la coda d'attesa è attiva o inattiva.
Gruppo di ricerca	Identificatore gruppo di ricerca del gruppo UCD, impostato durante la configurazione di base del Contact Center.
Priorità chiamante VIP	L'asse orizzontale mostra il tempo di attesa nella coda a intervalli di 30 secondi, l'asse verticale la priorità normale del chiamante che non appartiene all'Elenco chiamate VIP. I punti rossi consentono di definire la priorità tra chiamanti normali e chiamanti VIP.

Elenco chiamate VIP

I chiamanti (rubrica esterna) già registrati nel sistema di comunicazione possono essere inseriti nell'Elenco chiamate VIP. Oltre a ciò, è possibile l'inserimento di tipi di numeri di telefono. I tipi di numeri di telefono sono costituiti da una sequenza specifica di cifre e caratteri jolly (segnaposto). In questo modo è ad esempio possibile inserire tutti i collaboratori di un'azienda nell'elenco chiamate VIP.

Per informazioni dettagliate sulla configurazione di elenchi chiamati VIP, vedere Procedura di configurazione

Parametri	Descrizione
Coda	Nome coda
Coda attiva	Indica se la coda d'attesa è attiva o inattiva.
Gruppo di ricerca	Identificatore gruppo di ricerca del gruppo UCD, impostato durante la configurazione di base del Contact Center.
Elenco chiamate VIP	Vengono visualizzati i chiamanti contenuti nell'elenco chiamate VIP e i modelli di numero di telefono. È possibile aggiungere, modificare o rimuovere chiamanti e schemi di numeri di chiamata dall'Elenco chiamate VIP. Più a destra si trova la barra di scorrimento per un chiamante o modello di numero di telefono, maggiore è la sua priorità rispetto agli altri chiamanti contenuti nell'elenco chiamate VIP o agli altri modelli di numeri di telefono.

Agenti preferiti

A ogni chiamante, è possibile assegnare uno o più agenti preferiti di una coda d'attesa. In questo caso, il sistema di comunicazione tenta innanzitutto di inoltrare le chiamate e le prenotazioni di chiamata del cliente a un agente preferito. Se sono definiti più agenti preferiti, è possibile definire una priorità (sequenza) in base alla quale il chiamante verrà connesso agli agenti preferiti.

Se non è disponibile nessuno degli agenti preferiti, la chiamata verrà inoltrata a uno qualsiasi degli agenti disponibili.

Per informazioni dettagliate sulla definizione di agenti preferiti, vedere Procedura di configurazione

Parametri	Descrizione
Coda	Nome coda
Coda attiva	Indica se la coda d'attesa è attiva o inattiva.
Gruppo di ricerca	Identificatore gruppo di ricerca del gruppo UCD, impostato durante la configurazione di base del Contact Center.
Agenti preferiti	Vengono visualizzati gli agenti preferiti indicati nell'elenco clienti di ogni chiamante indicato. È possibile aggiungere, rimuovere e modificare la priorità di un agente. Se per un chiamante sono stati definiti più agenti preferiti, la posizione nell'elenco mostra la priorità rispetto agli altri agenti preferiti. Più in alto nell'elenco si trova un agente, più elevata è la sua priorità.
Visualizza solo clienti con associazioni ad agenti	Se il flag è attivato: nella lista clienti vengono visualizzati solo i chiamanti per i quali è stato definito almeno un agente preferito. Valore predefinito: Disattivato

Pause del Contact Center

Per prevedere pause definite per ciascun agente, è possibile impostare pause del Contact Center di diversa durata. Le pause del Contact Center sono impostate nel sistema e possono all'occorrenza essere selezionate da un agente tramite myAgent.

Per informazioni dettagliate sulla definizione delle pause del Contact Center, vedere Procedura di configurazione

Parametri	Descrizione
Aggiungi	Consente di aggiungere una nuova pausa al Contact Center
Modifica	Consente di modificare una pausa del Contact Center
Rimuovi	Consente di rimuovere la pausa del Contact Center selezionata
Nome	Nome della pausa del Contact Center
Durata	Durata della pausa del Contact Center in minuti
Attivo	Indica se la pausa del Contact Center è attiva o inattiva.

Elaborazione semplice

Per le code d'attesa con la modalità elaborazione "Elaborazione semplice", è possibile definire qui uno o più motivi per l'elaborazione.

Mediante l'uso dei motivi per l'elaborazione, è possibile assegnare alle chiamate in arrivo argomenti specifici (ad esempio ordine, reclamo, assistenza, ecc.). L'assegnazione a un'agente della fine della conversazione (entro il tempo di lavoro) tramite myAgent, selezionando il codice di elaborazione corrispondente.

Per informazioni dettagliate sulla definizione dei codici di elaborazione, vedere Procedura di configurazione

Parametri	Descrizione
Aggiungi	Consente di aggiungere una nuova elaborazione semplice
Modifica	Consente di modificare l'elaborazione semplice selezionata
Rimuovi	Consente di rimuovere l'elaborazione semplice selezionata
Coda	Nome della coda d'attesa, configurato per l'elaborazione semplice.
Descrizione	Testo descrittivo per il motivo per elaborazione

Elaborazione multipla

Per le code d'attesa con la modalità elaborazione "Elaborazione multipla", è possibile definire qui uno o più motivi per l'elaborazione e riunirli in gruppi o sottogruppi.

Mediante l'uso dei motivi per l'elaborazione, è possibile assegnare alle chiamate in arrivo argomenti specifici (ad esempio ordine, reclamo, assistenza, ecc.). L'assegnazione a un'agente della fine della conversazione (entro il tempo di lavoro) tramite myAgent, selezionando il codice di elaborazione corrispondente.

Per informazioni dettagliate sulla definizione dei codici di elaborazione, vedere Procedura di configurazione

Parametri	Descrizione
Coda	Nome della coda d'attesa, configurato per l'elaborazione multipla. Vengono visualizzati i gruppi e i sottogruppi già definiti per questa coda d'attesa.
Descrizione	Testo descrittivo per il motivo per elaborazione

Associazioni coda

Mediante le associazioni coda d'attesa, è possibile assegnare gli agenti a una o più code d'attesa.

Per informazioni dettagliate sull'assegnazione di agenti alle code d'attesa, vedere Procedura di configurazione

Parametri	Descrizione
Coda	Nome coda
Coda attiva	Indica se la coda d'attesa è attiva o inattiva.

Parametri	Descrizione
Gruppo di ricerca	Identificatore gruppo di ricerca del gruppo UCD, impostato durante la configurazione di base del Contact Center.
Associazione agente	
Interno	Visualizzazione del numero di interno dell'utente
Nome	Visualizzazione del nome dell'utente.
Agente	Agente assegnato alla coda d'attesa.
Tipo	Tipo agente Sono disponibili le opzioni seguenti: • Agente primario: l'agente riceve chiamate indipendentemente dal volume della coda d'attesa. • Agente di overflow: l'agente riceve chiamate solo in caso di overflow della coda d'attesa.
Livello interfaccia	Visualizzazione del livello di competenza in percentuale Il livello di competenza controlla la distribuzione delle chiamate agli agenti in una coda di attesa. Gli agenti con un livello di competenza più alto hanno la priorità nella distribuzione delle chiamate. Se tutti gli agenti hanno lo stesso livello interfaccia, l'agente che è libero da più tempo riceve la chiamata.
Attiva richiamata agente	Se il flag è attivato: l'agente riceve prenotazioni per richiamate sotto forma di messaggi vocali.
Orario lavorativo	Orario lavorativo automatico in secondi
Overflow dopo secondi in coda	Solo per l'agente di overflow: tempo superam. in secondi Trascorso il tempo di overflow, una chiamata viene inoltrata a un agente di overflow.
Overflow dopo chiamate in coda	Solo per l'agente di overflow: Numero chiamate Le chiamate che superano questo numero massimo vengono deviate a un agente di overflow.

28.4.4.9 OpenScape Business UC Suite > Pianificazione

Descrizione dei parametri delle schede:

- **Modifica/Aggiungi**

Parameters	Descrizione
Posto operatore automatico	Configurazione della funzione AutoAttendant della UC Suite (Company AutoAttendant)
Pianificazione	Nome pianificazione
Coda	Nome della coda d'attesa associata alla pianificazione.

Parameters	Descrizione
Gruppo di ricerca	Hunt group identifier of the UCD group, which was set up during the basic configuration of the Contact Center.
Edit / Add / Remove	Edit or remove the selected rule or add a new rule (via the rule editor)
Nome pianificazione	La pianificazione può essere salvata con un nome liberamente definito dall'utente. Si consiglia di scegliere un nome significativo.
CCV predefinito	Alla pianificazione deve essere assegnata almeno una regola (Call Control Vector CCV). Le regole determinano come vengono gestite le chiamate in entrata per il periodo in questione. Le regole si applicano solo alle chiamate e non ai fax e alle e-mail. Le regole vengono create con l'Editor regole grafico (Editor CCV) collegando oggetti CCV predefiniti. Sono disponibili più modelli predefiniti e standardizzati che è possibile modificare e adattare in base a esigenze specifiche.
Queues	Si raccomanda di attivare solo una coda d'attesa per pianificazione (inserire un segno di spunta).
Nome coda	La coda d'attesa può essere salvata con un nome liberamente definito dall'utente. Si consiglia di scegliere un nome significativo.
Coda attiva	La coda d'attesa può essere attivata o disattivata.
Pianificazione	Selezione della pianificazione associata
Pilota	Numero di telefono della relativa porta virtuale nel sistema di comunicazione.
Eccezioni	Una pianificazione con una regola predefinita diventa valida dopo l'assegnazione a una coda di attesa di 24 ore al giorno e 365 giorni all'anno. Se in occasioni e orari specifici (pausa, fine settimana, giorno festivo, vacanza ecc.) sono valide altre regole, è possibile assegnarvi una pianificazione corrispondente sotto forma di regole eccezione (CCV eccezione). In questo modo, è possibile definire come devono essere gestite ad esempio le chiamate in arrivo durante il periodo di vacanza. In questo caso le pianificazioni vacanze hanno la priorità rispetto alle altre pianificazioni e regole.
CCV	Selezione della regola eccezione (eccezione CCV)
Descrizione	Inserimento di una descrizione libera per la pianificazione delle eccezioni
Type	Nell'arco di uno o più giorni della settimana / liberamente definibile entro l'intervallo di date/ore / Pianificazioni vacanze per un intervallo di date
Data inizio	Inizio dell'eccezione (data)
Data fine	Fine dell'eccezione (data)
Start Time	Inizio dell'eccezione (ora)
Ora fine	Fine dell'eccezione (ora)
(Giorno della settimana)	L'eccezione si applicherà a uno o più giorni della settimana
Si verifica	The frequency the exception is scheduled

28.4.4.10 OpenScape Business UC Suite > Carica file

Descrizione dei parametri delle schede:

- **Gestione file audio**

Parameters	Descrizione
Destinazione caricamento	Applicazione per cui viene utilizzato il nuovo annuncio
Destinazione caricamento: Posto operatore automatico	Annunci per commutazione automatica
Destinazione caricamento: Profili	Annunci per tutti gli utenti o singoli utenti della UC Suite
Destinazione caricamento: Annuncio casella vocale	Annunci di benvenuto della casella vocale per tutti gli utenti della UC Suite o per singoli utenti della stessa La durata massima dell'annuncio è di 1 minuto.
Destinazione caricamento: Annuncio di gruppo VM	Annuncio di benvenuto per una casella vocale di gruppo
no key for: uploader	Per l'upload, l'annuncio è salvato in un file PCM con le seguenti caratteristiche: 8 kHz, 16 bit, mono. Il nome del file audio può avere una lunghezza massima di 30 caratteri.
Registratore	L'annuncio viene registrato tramite il telefono di un interno
File wave	
Download	Annunci scaricati.
Delete	Eliminare gli annunci scaricati.
Rinomina	Rinominare gli annunci scaricati.
Registratore	
Nome file	Indicazione del nome file dell'annuncio da registrare.
Extension	Scelta del telefono con cui deve essere registrato l'annuncio.
Esegui chiamata	Chiama il telefono con cui deve essere registrato l'annuncio.
Riproduci	Riproduce il messaggio registrato.
Registra	Avvia la registrazione dell'annuncio.

Descrizione dei parametri delle schede:

- **Carica copertina fax centralizzata**

Parameters	Descrizione
Carica copertina fax centralizzata	
File ocp	La copertina fax è disponibile come file .ocp
Name	The name of the central fax cover page
Descrizione	A description for central fax cover page

Parameters	Descrizione
Carica	Upload the central fax cover page file
Modifica	Edit the selected central fax cover page file
Rimuovi	Remove the selected central fax cover page file
Set To Default	Set the selected central fax cover page file as default
Nome file	Species the file name of the announcement to be uploaded.
Data di creazione	The creation date of the central fax cover page file

28.4.4.11 OpenScape Business UC Suite > Conferenza in corso

Descrizione dei parametri delle schede:

- **Conferencing**

Parameters	Descrizione
Name	Nome conferenza (assegnato dall'utente)
Proprietario	Nome dell'utente che ha avviato la conferenza
Successivo pianificato	Prossima ora inizio pianificata
Active	
N. membri	Numero di partecipanti alla conferenza incluso il supervisore
Display	Utenti della conferenza selezionata
Delete	Delete the selected conferences

28.4.4.12 OpenScape Business UC Suite > Elenco sedi

Descrizione dei parametri delle schede:

- **Elenco sedi**

Parametri	Descrizione
Nome sede	Sedi del sistema di comunicazione connesso in rete (vedere Impostazioni di base > Proprietà del gateway)
Indirizzo sede	Indirizzo IP della UC Booster Card, dell'UC Booster Server o del sistema di comunicazione
Porta sede	Porta server
Linee IP sede	Linee IP sede, se disponibili
Stato online	Stato di connessione del sistema di comunicazione presso la sede

28.4.4.13 OpenScape Business UC Suite > Server

Descrizione dei parametri delle schede:

- **Impostazioni generali**
- **Registra conversazione**
- **Registrazione**
- **Avvisi**
- **Manutenzione**
- **Casella vocale**
- **Contact Card Mapping**

Parametri	Descrizione
Orario d'ufficio	
Ora di inizio	Inizio dell'orario d'ufficio giornaliero (orario di lavoro) Impostazione dello stato presenza dei client UC Valore predefinito: 07:00 **Nota:** Il valore inserito deve essere nel formato 24 ore (HH:MM).
Ora fine	Fine dell'orario d'ufficio giornaliero (orario di lavoro) Impostazione dello stato presenza dei client UC Valore predefinito: 19:00 **Nota:** Il valore inserito deve essere nel formato 24 ore (HH:MM).
Lunghezza password	
Lunghezze	Lunghezza della password per il client UC. Il valore minimo è 6. ***NOTA:*** Modificando la lunghezza delle password si reimposteranno le password di tutti gli utenti. Valore predefinito: 6
Numero di telefono del posto di rinvio	
Numero di destinazione	Numero di telefono del posto di rinvio ***INFO:*** è necessario immettere il numero di telefono configurato nel sistema di comunicazione per il posto di rinvio.
Messaggio istantaneo	
Disabilita messaggio immediato	Se il flag è attivato: non è possibile l'invio di messaggi istantanei. Valore predefinito: Disattivato
Estensioni analogiche	

Parametri	Descrizione
Modalità utente analogico	Definizione della visualizzazione di un utente analogico nella rubrica interna Valore predefinito: Mostra tutto
Modalità utente analogico: **Mostra tutto**	Tutti gli utenti analogici vengono visualizzati nella rubrica interna
Modalità utente analogico: **Mostra solo utenti con nome**	Nella rubrica interna vengono visualizzati solo gli utenti analogici con un nome.
Modalità utente analogico: **Non mostrato**	Nella rubrica interna non viene visualizzato alcun utente analogico.
Estensione	
Lunghezza interna max.	Max. cifre consentite per numeri interni Per prevenire frodi tariffarie, viene impedita la composizione di numeri di telefono interni più lunghi. Valore predefinito: 4
Lunghezza esterna min.	Numero min. di cifre consentite per numeri esterni Valore predefinito: 3
Trasferisci	
SST AutoAttendant normale	Se il flag è attivato, la chiamata viene trasferita indipendentemente dal fatto che la destinazione sia libera, occupata o non disponibile. Valore predefinito: Attivata
Diario	
Consenti eliminazione voci del diario	Questo flag consente o impedisce a un utente di eliminare o meno una voce del diario.
Lunghezza esterna min.	
Formato Fax	
Usa PDF come formato fax	Se il flag è selezionato, il fax ricevuto può essere salvato in formato PDF, in caso contrario viene salvato in formato TIFF.
Server dei directory	
Provider esterno lento	Questo flag migliora il tempo di risposta mediante il pulsante destro del mouse a un'e-mail. Inoltre, quando viene attivato, le ricerche dei contatti vengono eseguite solo nella directory superiore di Exchange e non nelle sottodirectory.
Lunghezza della verifica	In myPortal for desktop e myPortal for Outlook, per definire la lunghezza dei numeri CLI per la ricerca in rubriche LDAP, occorre inserire una cifra da 4 a 8. Il numero più alto (8) può essere utilizzato per assicurare una ricerca più accurata e per migliorare le prestazioni del sistema Valore predefinito: 4

Parametri	Descrizione
Seleziona con ricerca nominale solo l'interno locale	Quando questo flag è selezionato, la funzione "Componi per nome" è limitata al nodo attivo (funzione locale). Quando questo flag non è selezionato, è ancora disponibile la funzione precedente, che considera tutti gli utenti nella rete, ma riproduce l'annuncio solo dopo la selezione di un utente locale.
La cache di ricerca in rubrica scade tra	Impostare il numero di minuti o un intervallo di minuti utilizzati dalla memoria cache durante la ricerca dei contatti. L'intervallo di minuti che è possibile impostare è 1-60 minuti. Quando il valore è "0", questa funzione è disattivata.
Cerca per numero di telefono	Quando questo contrassegno è selezionato, è possibile cercare nelle directory per numero di telefono.
TLS	
Uso di TLS per connessioni client	A causa di motivi di rete, può essere necessario disattivare la connessione client server sicura. Per modificare questa impostazione, è necessario riavviare l'applicazione UC. Ciò deve essere effettuato esclusivamente in casi specifici!
Presenza	
Nascondi stato con errori	Quando questo flag è attivato, lo stato di presenza "malato" non è disponibile per l'uso. Valore predefinito: Disattivato
Nome utente	
Disattiva modifica nome	Quando questo flag è attivato, gli utenti non possono modificare il proprio nome e cognome configurati. Valore predefinito: Disattivato
Bacheca	
Disattiva bacheca	Quando questo flag è attivato, Bacheca non è disponibile.
Visualizza nomi agenti nell'associazione coda myAgent	Quando questo flag è impostato, insieme al numero di interno di un agente, viene visualizzato anche un nome che l'utente può configurare. Un utente visualizzerà "Hotdesk" quando utilizza un interno diverso dal proprio. Valore predefinito: Disattivato.
Registra conversazione	
Registra conversazione	Se il contrassegno è attivato, è possibile la registrazione di chiamate. Valore predefinito: Attivata
Riproduci prompt prima della registrazione	Se il flag è attivato: verrà riprodotto un messaggio prima dell'inizio della registrazione. Valore predefinito: Disattivato
Riproduci tono durante la registrazione	Per OpenScape Business S, se il flag è attivato verrà riprodotto un segnale acustico durante la registrazione. Valore predefinito: Attivata

Parametri	Descrizione
Disponibilità della registrazione della conferenza dal vivo	Se il contrassegno è attivato, è possibile la registrazione di conferenze. Valore predefinito: Disattivato
Registrazione sistema	
Registra messaggi traccia (estesi)	Se il flag è attivato: i messaggi traccia vengono registrati quotidianamente in un file di registro. Valore predefinito: Disattivato
Registri client	
Percorso registro del client	Percorso dell'archivio per file di registro del client (file di registro UC Suite)
Attiva caricamento registro	Se il flag è attivato: i registri del client vengono salvati su disco rigido della UC Booster Card (OCAB), dell'UC Booster Server o del sistema di comunicazione OpenScape Business S. Valore predefinito: Attivata
Abilita logging dei client	Se il flag è attivato: i registri del client vengono registrati. Valore predefinito: Attivata
Avvisi e-mail	
Attiva avvisi e-mail sugli errori di sistema	Se il flag è attivato: vengono inviati avvisi e-mail per avviare uno o più destinatari configurati, ad esempio del livello critico di riempimento di un disco rigido o di un errore. Valore predefinito: Attivata
Abilita e-mail di invito myPortal	Se il contrassegno è attivato, agli utenti UC Suite verrà inviato per e-mail un invito a installare o aggiornare il client myPortal. Questa e-mail viene inviata normalmente a tutti gli utenti UC Suite che hanno un indirizzo e-mail valido nella Directory utenti in una nuova installazione, quando un indirizzo e-mail viene aggiunto o modificato per un utente UC Suite nella Directory utenti o dopo che è stato aggiornato il software OpenScape Business ed è disponibile una nuova versione del client. Valore predefinito: Attivata
Destinatari	Indirizzi e-mail ai quali verranno inviati avvisi e-mail.
Condizioni	
Invia messaggi critici	Se il flag è attivato, viene inviata una notifica via e-mail in caso di messaggi di importanza critica, come ad esempio un errore di sistema Valore predefinito: Attivata
Invia avvisi sull'arresto imprevisto del sistema	Se il flag è attivato, viene inviata una notifica via e-mail in caso di crash del sistema. Valore predefinito: Attivata
Alla notifica di un errore, invia le ultime righe del file di registro	Definizione del numero di righe di un file di registro che devono essere inviate in un messaggio e-mail. Valore predefinito: 100

Parametri	Descrizione
Manutenzione	
Inizia la manutenzione del sistema alle	Definizione dell'ora in cui verrà avviata la cancellazione dei seguenti dati che hanno superato i rispettivi tempi di conservazione previsti: • Messaggi • Informazioni sulle chiamate nel diario delle chiamate (cronologia chiamate) • Chiamate registrate con myAgent (Contact Center) • Fax e e-mail ricevuti e inviati per il Contact Center • File di registro Valore predefinito: 2.00 ore
Messaggio	
Conserva messaggi in Posta in arrivo per	Tempo di conservazione in giorni per i messaggi vocali in posta in arrivo Valore predefinito: 60
Conserva messaggi riprodotti / letti per	Tempo di conservazione in giorni per i messaggi vocali riprodotti/letti Valore predefinito: 30
Conserva messaggi salvati per	Tempo di conservazione in giorni per messaggi vocali salvati Valore predefinito: 365
Conserva messaggi eliminati per	Tempo di conservazione in giorni per i messaggi vocali eliminati Valore predefinito: 30
Fax	
Conserva i fax in Posta in arrivo per	Tempo di conservazione in giorni per i messaggi fax in posta in arrivo Valore predefinito: 30
Conserva i fax letti per	Tempo di conservazione in giorni per i messaggi fax letti Valore predefinito: 30
Conserva i fax eliminati per	Tempo di conservazione in giorni per i messaggi fax eliminati Valore predefinito: 30
Conserva i fax inviati per	Tempo di conservazione in giorni per i messaggi fax inviati Valore predefinito: 30
Manutenzione informazioni sulle chiamate	
Conserva cronologia chiamate per	Tempo di conservazione in giorni per le chiamate nel diario Valore predefinito: 30

Parametri	Descrizione
Chiudi conversazione dopo	Tempo di conservazione in giorni per le chiamate aperte nel diario. Tutte le chiamate senza risposta da/allo stesso contatto durante questo periodo verranno aggiunte alla scheda delle chiamate aperte, collegata alla stessa conversazione. Alla fine di questo periodo, tutte le chiamate in una conversazione sono contrassegnate come completate ed eliminate dalla scheda delle chiamate aperte. Valore predefinito: 3 Valore massimo: 30
Contact Center	Tempo di conservazione in giorni per le chiamate registrate con myAgent e per i fax e le e-mail ricevuti e inviati per il Contact Center Valore predefinito: 30
Mantieni record CC live/ richiamate/e-mail/chiamate fax per	Periodo di conservazione per tutti i dati di comunicazione associati alle chiamate, come messaggi di richiamata, chiamate registrate live, chiamate fax ed e-mail. Valore predefinito: 30
Manutenzione file di registro	
Conserva informazioni del registro per	Tempo di conservazione in giorni per i file protocollo Valore predefinito: 10
Messaggio istantaneo	
Conserva messaggi istantanei per	Tempo di conservazione in giorni per messaggi istantanei. Valore predefinito: 30
Rapporti	
Reimposta password	Reimpostazione della password amministratore di myReports alla password predefinita.
Reimposta tutte le password utente	
Reimposta tutte le password utente	Reimposta le password per tutti gli utenti, consente password composte da un massimo di 6 caratteri. **Nota:** In questo caso, la password predefinita è impostata su 6 caratteri (123456).
Casella vocale	
Lingua della casella vocale	Lingua predefinita della casella vocale per il menu e gli annunci interni del sistema
Ordine di riproduzione messaggi vocali	definizione dell'ordine di riproduzione dei messaggi vocali Valore predefinito: Prima i più recenti
Ordine di riproduzione messaggi vocali Prima i più recenti	Il nuovo messaggio vocale viene presentato per primo.

Parametri	Descrizione
Ordine di riproduzione messaggi vocali Prima i meno recenti	Il messaggio vocale più vecchio viene presentato per primo.
Durata di registrazione messaggio vocale	Definizione del tempo massimo di registrazione per un messaggio vocale in secondi Valore predefinito: 900
Modalità casella vocale	Definizione delle funzionalità della casella vocale Valore predefinito: Completo
Modalità casella vocale Completo	È disponibile l'intera gamma di funzioni per la propria casella vocale
Modalità casella vocale Menu abbreviato	Dopo l'annuncio basato sullo stato o personale, la connessione viene segnalata alla destinazione.
Modalità casella vocale Nessun menu casella vocale	Dopo l'annuncio di benvenuto, il chiamante viene inoltrato direttamente alla registrazione vocale.
Consenti richiamata da casella vocale solo a numeri noti	Se il flag è attivato: viene impedito l'accesso alla casella vocale ai chiamanti i cui numeri non sono memorizzati nel client UC. Valore predefinito: Attivata
Ignora la richiesta "Lasciare un messaggio dopo il segnale"	Se questo contrassegno è attivato, la finestra "Lasciare un messaggio dopo il segnale acustico" non viene visualizzata. Valore predefinito: Disattivato
Contact Card Mapping	
Microsoft: Disponibile (verde)	Lo stato UC di presenza di questa riga è assegnato allo stato Outlook Disponibile (Verde).
Microsoft: Non al lavoro (giallo)	Lo stato UC di presenza di questa riga è assegnato allo stato Outlook Fuori lavoro (Giallo).
Microsoft: Occupato (rosso)	Lo stato UC di presenza di questa riga è assegnato allo stato Outlook Occupato (Rosso).
Microsoft: Fuori servizio (grigio)	Lo stato UC di presenza di questa riga è assegnato allo stato Outlook Fuori servizio (Grigio).

28.4.4.14 OpenScape Business, UC Suite > Profili

Descrizione dei parametri delle schede:

- **Aggiungi / Modifica**

Parametri	Descrizione
Profili	I profili utente memorizzano le impostazioni degli utenti della UC Suite. A un profilo utente possono essere assegnati più utenti (membri). A tutti i membri di un profilo si applicano (prima) le stesse impostazioni. È possibile creare più profili che permettono di eseguire diverse impostazioni per i vari gruppi di utenti.
Nome	Nome del profilo (liberamente scelto)
Dati personali	
I miei dati personali	Dati personali selezionati per gli utenti assegnati. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Preferenze	
Aspetto	Interfaccia e lingua del client UC dell'utente assegnato. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Avviso	Avvisi per l'utente assegnato. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Connettività Outlook	Integrazione del calendario per l'utente assegnato. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Tasti di scelta rapida	Attivazione e impostazione di combinazioni di tasti per accedere a varie funzionalità comunemente usate tramite la tastiera. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Varie	Ripristino automatico dello stato presenza "Ufficio", metodo di trasferimento e tempo di conservazione nel diario delle chiamate per l'utente assegnato. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Regole di chiamata	
Destinazioni di inoltro	Destinazioni per l'inoltro chiamate in arrivo in funzione dello stato presenza dell'utente assegnato. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Comunicazioni	
Impostazioni casella vocale	Registrazione di messaggi vocali in funzione della stato presenza dell'utente assegnato. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Avviso VM	Notifica di nuovi messaggi vocali per gli utenti assegnati. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Avviso fax	Notifica di nuovi fax per gli utenti assegnati. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Notifiche di chiamata senza risposta	Notification Service for Missed Calls.
Profili	

Parametri	Descrizione
Profili	AutoAttendant personale per l'utente assegnato. I relativi utenti devono registrare un annuncio a seconda delle esigenze. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Sensibilità	
Protezione e accesso	Consentire l'ascolto di messaggi vocali con myAttendant e il controllo della casella vocale dal proprio telefono senza una password. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Visibilità presenza	Utenti interni autorizzati a visualizzare lo stato presenza. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Presenza casella vocale	Chiamanti interni o esterni che devono essere informati sullo stato presenza tramite annunci automatici della casella vocale. L'icona del lucchetto indica se l'utente è abilitato a modificare queste impostazioni.
Preferiti	
Preferiti	Gruppi Preferiti con un elenco di contatti che possono essere assegnati all'utente.

Descrizione dei parametri delle schede:

- **Assegna utenti**

Parametri	Descrizione
Utenti assegnati	Utente a cui si deve applicare il profilo
Utenti disponibili	Users to whom the profile can be applied

Descrizione dei parametri delle schede:

- **Rimuovi**

Parameters	Descrizione
Name	Nome del profilo (liberamente scelto)
Users	Utente a cui si deve applicare il profilo

28.4.4.15 OpenScape Business UC Suite > Intestazione fax

Descrizione dei parametri delle schede:

- **Modifica**
- **Add**
- **Rimuovi**

Parameters	Descrizione
Template Name / Name	Nome della riga di intestazione (deve essere univoco).
Text	È possibile aggiungere segnaposto per Data/Ora, Nome società, Nome utente, Numero società, Numero pagina e Conteggio pagine.

28.4.5 Web Services

In **Web Services** sono riunite funzioni utilizzate per la configurazione dell'interfaccia Web, quali ad esempio la Web Collaboration.

28.4.5.1 Servizi Web > Web Collaboration

Per l'integrazione di Web Collaboration su un server pubblico (server di Web Collaboration come servizio Internet) o tramite un server personalizzato (server di Web Collaboration integrato nella LAN del cliente o presso un partner).

Descrizione dei parametri delle schede:

- **Server di Web Collaboration**

Parametri	Descrizione
Tipo di server	Selezione del server di Web Collaboration.
Tipo di server: **Server pubblico**	Il server di Web Collaboration è un server pubblico che si trova su Internet. Per questo motivo viene utilizzata una connessione HTTPS sicura. È inoltre richiesto un numero di licenza e una password. Per impostazione predefinita, a questo scopo viene utilizzata la porta TCP 5100.
Tipo di server: **Server pubblico (Modalità demo/ Modalità valutazione)**	Web Collaboration può essere testato per 5 minuti. Per questo non richiede l'immissione di un indirizzo IP, né di un numero di licenza o di una password.
Tipo di server: **Server personalizzato**	Il server di Web Collaboration è un server personalizzato che si trova sulla rete del cliente o presso un partner. Per questo può essere utilizzata una connessione sicura HTTPS o normale HTTP. Nel caso venga utilizzata una connessione tramite https è necessario un numero di licenza e una password. Per impostazione predefinita, a questo scopo viene utilizzata la porta TCP 5004.
Tipo di server: **Nessun server di collaborazione Web**	Non viene utilizzato alcun server di Web Collaboration. L'opzione per l'avvio di una sessione di Web Collaboration nel client UC è disattivata.

URL / Indirizzo IP	Immissione dell'URL/indirizzo IP del corrispondente server di Web Collaboration. Server pubblico tramite https e server personalizzato tramite https o http.
	Esempio:
	`http://<Indirizzo IP del server Web Collaboration>:5004/OscInterface`
	`https://<Indirizzo IP del server Web Collaboration>:5100/XMLRPSecure`

Numero di licenza	Numero di licenza per la connessione sicura al server di Web Collaboration.
Password	Password per la connessione sicura al server di Web Collaboration.

28.4.6 Open Directory Service

In **Open Directory Service** sono riunite le funzioni per la configurazione di Open Directory Service.

28.4.6.1 Open Directory Service > Impostazioni di base

Parametri	Descrizione
Attiva/disattiva Open Directory Service	Valore predefinito: disattivato
Credenziali di accesso al server LDAP	Dati di accesso del server database esterno. Open Directory Service deve essere autorizzato ad accedere al database esterno; se necessario, a tal fine deve essere aggiunto un account utente nel server.

28.4.6.2 Open Directory Service > Origini dati > Utenti OpenScape Business

Descrizione dei parametri delle schede:

- **Panoramica delle origini dati configurate**

Parametri	Descrizione
Utenti OpenScape Business	Directory interna della UC Suite. La directory è assegnata in modo permanente a Open Directory Service e non può essere cancellata o modificata.
Rubrica esterna UC Suite	Origine dati esterna per i sistemi UC Suite. La directory è assegnata in modo permanente a Open Directory Service e non può essere cancellata o modificata.
Directory globale	Origine dati della directory globale per sistemi diversi da UC Suite. La directory è assegnata in modo permanente a Open Directory Service e non può essere cancellata o modificata.
Destinazioni di selezione breve	Numeri centrali di selezione rapida. La directory è assegnata in modo permanente a Open Directory Service e non può essere cancellata o modificata.
Aggiungi/Modifica/Elimina	Origini dati esterne per informazioni di contatto da database con accesso in lettura tramite ODBC.

Descrizione dei parametri delle schede:

- **Modifica origine dati**

Parametri	Descrizione
Nuova origine dati	Qui è possibile modificare i parametri delle origini dati aggiunte.

28.4.6.3 Servizio Open Directory > Origini dati > LXV3

Parametri	Descrizione
Destinazioni di selezione breve	Numeri di selezione breve centralizzati. La rubrica Open Directory Service è assegnata in modo permanente e non può essere eliminata o modificata.

28.4.6.4 Servizio Open Directory > Origini dati > LXV3

Parametri	Descrizione
Panoramica delle origini dati configurata	Una mappatura uscita dati definisce quali campi dello schema dati di Open Directory Service devono essere inviati tramite LDAP, ad esempio, per client LDAP specifici o per gruppi diversi di utenti che non devono visualizzare tutti i dettagli ma solo una parte predefinita. Per impostazione predefinita, la mappatura uscita dati Web è disponibile e non può essere eliminata o modificata. Qui sono assegnati all'output LDAP in modo fisso tutti i campi dello schema dati di Open Directory Service. È possibile configurare ulteriori mappature uscita dati LDAP.
Aggiungi	Aggiungere altre mappature di output dei dati. I client LDAP possono accedere a mappature uscita dati specifiche accedendo a LDAP tramite il parametro dc, ad esempio, dc=web.

28.4.6.5 Open Directory Service > Manutenzione

Descrizione dei parametri delle schede:

- **Manutenzione**

Parametri	Descrizione
Controlla/riavvia Open Directory Service	Visualizzazione dello stato di Open Directory Service (grigio = disattivato, rosso = errore di configurazione o origine dati non disponibile, verde = attivato)
Riavvia	Riavvio del servizio Open Directory Service

28.4.7 Application Launcher

In **Application Launcher** sono riunite le funzioni per la configurazione dell'Application Launcher.

28.4.7.1 Application Launcher

Parametri	Descrizione
Upload del file di configurazione	Profilo con i dati di configurazione di Application Launcher per una rapida configurazione di Application Launcher su tutti i PC client. Una volta completamente configurata l'Application Launcher per un utente iniziale, l'amministratore può rendere tale profilo, unitamente ai dati di configurazione dell'Application Launcher, disponibili nel sistema di comunicazione. Successivamente tutti gli utenti possono eseguire la configurazione dell'Application Launcher mediante l'importazione di questo profilo.
Profilo	È consentito il tipo di file .xml

28.5 Middleware

Le funzioni per la configurazione del middleware sono raggruppate sotto **Middleware**.

28.5.1 Lettore di annunci

Descrizione dei parametri delle schede:

- **Impostazioni del lettore di annunci**
- **Statistiche del lettore di annunci**

Parametri	Descrizione
Attivazione	
Il servizio verrà avviato automaticamente	Attivazione o disattivazione del dispositivo di riproduzione degli annunci.
Statistiche del lettore di annunci	Qui viene visualizzato lo stato del dispositivo per gli annunci. I dati vengono aggiornati automaticamente ogni 5 minuti. Tuttavia, la pagina può essere aggiornata anche manualmente.

28.5.2 Csta Message Dispatcher (CMD)

Descrizione dei parametri delle schede:

- **Impostazioni Csta Message Dispatcher (CMD)**
- **Statistiche - Csta Message Dispatcher (CMD)**

Parametri	Descrizione
Attivazione	
Il servizio verrà avviato automaticamente	Attivazione o disattivazione del CSTA Message Dispatcher (CMD). Il CMD assicura la connessione tra i client OpenScape Business TAPI 120 e il sistema di comunicazione ed è necessario per l'uso delle funzionalità.
Registrazione automatica	

Parametri	Descrizione
Registrazione automatica client abilitata	Attivazione o disattivazione dell'accesso automatico dei client. Registrazione automatica significa che sono consentite nuove voci nell'elenco del firewall CTI. In questo modo, il firewall CTI viene automaticamente configurato. Se sono stati connessi tutti i client abilitati, è possibile eliminare il segno di spunta e impedire la creazione di nuove voci nel firewall CTI. Un PC può essere autorizzato a controllare un interno specifico. Devono inoltre essere assegnate le licenze TAPI/CTI.
Firewall CTI	
Elimina	Le voci con un segno di spunta nella colonna Elimina vengono eliminate dall'elenco dei client autorizzati non appena si preme il pulsante **Applica**. L'accesso sarà rifiutato a meno che sia stata attivata la registrazione automatica.
ID applicazione	Nome del PC da cui è possibile controllare un interno. Mediante l'uso del nome del PC, è possibile utilizzare il DHCP anche per i PC OpenScape Business TAPI 120.
Numero di telefono	Numero di telefono dell'interno che deve essere controllato.
Statistiche - Csta Message Dispatcher (CMD)	Qui viene visualizzato lo stato del CMD. Durante l'uso è possibile controllare quali OpenScape Business TAPI 120 sono collegati al CMD che potrebbero richiedere l'assegnazione di licenze. I dati vengono aggiornati automaticamente ogni 5 minuti. La pagina può essere aggiornata anche manualmente.

28.5.3 Provider di servizi CSTA (CSP)

Descrizione dei parametri delle schede:

- **Impostazioni Csta Service Provider (CSP)**
- **Statistiche Csta Service Provider (CSP)**

Parametri	Descrizione
Attivazione	
Il servizio verrà avviato automaticamente	Attivazione o disattivazione del CSTA Service Provider (CSP). Il CSP è necessario per la UC Suite, per il server DSS (Presence Manager, solo in rete), per OpenScape Business TAPI 170 e per le applicazioni CSTA esterne.
Accesso CSTA	
ID utente CSTA/Password utente CSTA	OpenScape Business TAPI 170 e le applicazioni CSTA esterne possono accedere al CSP solo con l'account utente qui configurato. Se non è stato configurato alcun utente CSTA, non è possibile usare OpenScape Business TAPI 170 o applicazioni CSTA esterne nel CSP.

Parametri	Descrizione
Statistiche Csta Service Provider (CSP)	Qui viene visualizzato lo stato del CSP. È possibile visualizzare quante e quali applicazioni sono associate al CSP. Le applicazioni sconosciute vengono contrassegnate con "Predefinito". È possibile visualizzare lo stato di connessione ai singoli nodi della rete/locali. I dati vengono aggiornati automaticamente ogni 5 minuti. La pagina può essere aggiornata anche manualmente.

28.5.4 Server DSS

Descrizione dei parametri delle schede:

- **Impostazioni server DSS**
- **Statistiche - Server DSS**

Parametri	Descrizione
Attivazione	
Il servizio verrà avviato automaticamente	Attivazione o disattivazione del server DSS.
Statistiche - Server DSS	Qui viene visualizzato lo stato del server DSS. I dati vengono aggiornati automaticamente ogni 5 minuti. La pagina può essere aggiornata anche manualmente.

28.5.5 Media Extension Bridge (MEB)

Descrizione dei parametri delle schede:

- **Impostazioni Media Extension Bridge (MEB)**
- **Statistiche Media Extension Bridge (MEB)**

Parametri	Descrizione
Attivazione	
Il servizio verrà avviato automaticamente	Attivazione o disattivazione del Media Extension Bridge.
Statistiche Media Extension Bridge (MEB)	Qui viene visualizzato lo stato del MEB. I dati vengono aggiornati automaticamente ogni 5 minuti. La pagina può essere aggiornata anche manualmente.

29 Appendice

Questa appendice riporta informazioni di riferimento, quali ad esempio, le lingue e gli standard supportati, i limiti di configurazione e le capacità, i servizi Euro ISDN, i codici per attivare e disattivare i servizi, i codici dei servizi via DTMF nonché i protocolli IP e i numeri di porte utilizzati.

29.1 Standard supportati

Qui sono fornite informazioni sugli standard supportati.

Ethernet

- RFC 894 Ethernet II Encapsulation
- IEEE 802.1Q VLAN
- IEEE 802.2 Logical Link Control
- IEEE 802.3u 100BASE-T
- IEEE 802.3ab Gigabit Ethernet
- IEEE 802.3x Full Duplex Operation

Routing IP

- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 2822 Internet Message Format
- RFC 826 ARP
- RFC 2131 DHCP
- RFC 1918 IP Addressing
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1334 PPP Authentication Protocols
- RFC 1618 PPP over ISDN
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1877 PPP Internet Protocol Control Protocol
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 2516 Method for Transmitting PPP Over Ethernet (PPPoE)
- RFC 3544 IP Header Compression over PPP

NAT

- RFC 2663 NAT

IPSec

- RFC 2401 Security Architecture for IP
- RFC 2402 AH - IP Authentication Header
- RFC 2403 IPsec Authentication - MD5
- RFC 2404 IPsec Authentication - SHA-1
- RFC 2405 IPsec Encryption - DES
- RFC 2406 ESP - IPsec encryption

- RFC 2407 IPsec DOI
- RFC 2408 ISAKMP
- RFC 2409 IKE
- RFC 2410 IPsec encryption - NULL
- RFC 2411 IP Security Document Roadmap
- RFC 2412 OAKLEY

SNMP

- RFC 1213 MIB-II

QoS

- IEEE 802.1p Priority Tagging
- RFC 1349 Type of Service in the IP Suite
- RFC 2475 An Architecture for Differentiated Services
- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding (EF) PHB (Per-Hop Behavior)

Servizi

- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding (EF) PHB (Per-Hop Behavior)

Codec

- G.711
- G.729

VoIP via SIP

- RFC 2198 RTP Payload for Redundant Audio Data
- RFC 2327 SDP Session Description Protocol
- RFC 2617 HTTP Authentication: Basic and Digest Access Authentication
- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 3261 SIP Session Initiation Protocol
- RFC 3262 Provisional Response Acknowledgement (PRACK) Early Media
- RFC 3263 SIP Locating Servers
- RFC 3264 An Offer/Answer Model with the Session Description Protocol
- RFC 3310 HTTP Digest Authentication
- RFC 3311 Session Initiation Protocol (SIP) UPDATE Method
- RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
- RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3489 STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515 The Session Initiation Protocol (SIP) Refer Method
- RFC 3550 RTP: Transport Protocol for Real-Time Applications
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3581 An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing

- RFC 3891 The Session Initiation Protocol (SIP) Replaces Header

Altri

- RFC 959 FTP
- RFC 1305 NTPv3
- RFC 1951 DEFLATE

29.2 Servizi Euro ISDN

I servizi Euro ISDN possono essere utilizzati con qualsiasi linea Euro ISDN, a condizione che l'hardware esistente (ad es. telefono o scheda ISDN) sia adeguato a tale scopo. I servizi sono resi disponibili continuamente per la linea urbana oppure vengono attivati o disattivati tramite un codice.

La disponibilità dei servizi dipende dal gestore di rete. Alcuni dei servizi indicati generano addebiti.

Argomento	Spiegazione
Numero di telefono multiplo (MSN = Multiple Subscriber Number)	Ad ogni connessione punto - multipunto possono essere assegnati più numeri di telefono. L'assegnazione di questi numeri di telefono ai singoli terminali può essere eseguita direttamente dall'utente a livello dei terminali.
Trasmissione del numero di telefono (CLIP = Calling Line Identification Presentation)	Il numero di telefono personale viene trasmesso all'utente chiamato e viene visualizzato sul display del telefono oppure viene salvato nella lista delle chiamate in caso di mancata risposta. I numeri di telefono errati non possono essere trasmessi. Tuttavia, la selezione passante degli impianti TK non può essere controllata. La trasmissione del numero di telefono personale può essere disattivata per tutte le chiamate oppure solo per determinate chiamate.
Disattivazione della visualizzazione del numero di telefono (CLIR = Calling Line Identification Restriction)	La trasmissione del numero di telefono può anche essere disattivata in modo permanente o valutando caso per caso. La visualizzazione del numero di telefono per gli utenti B sarà possibile solo per i collegamenti appositamente configurati (chiamata d'emergenza, polizia, vigili del fuoco).
Identificazione delle chiamate di disturbo (MCID = Malicious Call Identification)	Il chiamato può identificare il chiamante anonimo mediante il centralino anche se l'opzione di trasmissione del numero di telefono è disattivata. Questo servizio è a pagamento.
Cambiamento del bus (TP = Terminal Portability)	Questo servizio consente di collegare il terminale ISDN utilizzato ad un'altra presa ISDN durante una chiamata, continuando la conversazione. La conversazione deve essere parcheggiata prima di effettuare il cambiamento.

Argomento	Spiegazione
Sottoindirizzamento (SUB = Subadressing)	Questa funzione può essere utilizzata a pagamento in aggiunta al normale numero di telefono e consente, a seconda del chiamante, di utilizzare un terminale che è possibile chiamare (ad es. un programma sul PC).
Segnalazione utente-utente (USS = User to User Signalling)	Durante la creazione e l'interruzione della connessione è possibile scambiare informazioni mediante il canale D. La trasmissione è possibile in entrambe le direzioni.
Gruppo utenti chiuso (CUG = Closed User Group)	Se questo servizio è attivo, non sono possibili conversazioni al di fuori del gruppo di utenti (ad eccezione delle chiamate d'emergenza al 110 e 112). Tuttavia, è possibile bloccare anche i chiamanti dall'esterno.
Deviazione di chiamata su occupato (CFB = Call Forwarding Busy)	Questo inoltro di chiamata devia le chiamate su occupato a qualsiasi collegamento telefonico raggiungibile. L'inoltro di chiamata viene eseguito sul centralino. Entrambi i canali restano quindi liberi.
Deviazione di chiamata incondizionata (CFU = Call Forwarding Unconditional)	Questo inoltro di chiamata devia immediatamente le chiamate a qualsiasi collegamento telefonico raggiungibile. L'inoltro di chiamata viene eseguito sul centralino. Entrambi i canali restano quindi liberi.
Deviazione di chiamata su mancata risposta (CFNR = Call Forwarding No Reply)	Questo inoltro di chiamata devia le chiamate a qualsiasi collegamento telefonico raggiungibile dopo 20 secondi (in caso di mancata risposta) L'inoltro di chiamata viene eseguito sul centralino. Entrambi i canali restano quindi liberi.
Avviso di chiamata in attesa (CW = Call Waiting)	Durante una chiamata viene segnalato un ulteriore chiamante. Nel frattempo, al chiamante viene trasmesso il segnale di libero. La chiamata in attesa può essere accettata, respinta oppure semplicemente ignorata.
Richiamata alternata (Hold = Call Hold)	La funzione Consultazione consente di instaurare una seconda chiamata durante una chiamata in corso. Il passaggio da una chiamata all'altra è chiamato "richiamata alternata". L'utente della conversazione in attesa non può sentire l'altra conversazione attiva.
Conferenza a tre (3PTY = Three Party Service)	Due chiamate esistenti possono essere collegate. In questo modo è possibile creare una conferenza a 3 utenti.
Richiamata automatica su occupato (CCBS = Completion of Calls to Busy Subscriber)	Questo servizio può essere attivato se l'utente chiamato è occupato. Non appena il collegamento di questo utente risulta nuovamente libero, il chiamante riceve un segnale. Il collegamento viene instaurato non appena viene sollevato il ricevitore.

Argomento	Spiegazione
Visualizzazione del costo al termine della conversazione (AOCE = Advice of Charge (End))	Se lo si desidera, è possibile visualizzare il costo della chiamata alla fine della conversazione. Eventuali sconti e tariffe non vengono considerati.
Visualizzazione del costo durante la conversazione (AOCD = Advice of Charge (During))	Se lo si desidera, è possibile visualizzare il costo della chiamata durante la conversazione. Eventuali sconti e tariffe non vengono considerati.

29.3 Porte usate

I componenti del sistema OpenScape Business utilizzano porte diverse, che potrebbero dover essere aperte nel firewall in base alle necessità. Per le porte dei client basati sul Web (ad esempio, myPortal to go), è necessario configurare l'inoltro delle porte nel router.

L'elenco completo di tutte le porte utilizzate da OpenScape Business è disponibile nel "Database di gestione delle interfacce" (IFMD), accessibile tramite il Portale partner di Unify (https://unify.com/en/partners/partner-portal.

Nota: Le porte identificate nell'elenco seguente con "O" sono opzionali, cioè non sono aperte in modo permanente nel firewall.

Descrizione	TCP	UDP	Numero di porta	OpenScape Business X	Scheda UC Booster	OpenScape Business S	Server UC Booster
Componenti del sistema							
Portale di amministrazione (https)	X		443	X	X	X	X
Verifiche CAR Alive	X		12062	X		X	
CLA	X		61740	A		A	A
CLA Auto Discovery		X	23232	X		X	X
CLS	X		7780, 7790 (fino alla versione V3R3) 7780, 7791 (dalla versione V3R3.1 in poi)	A		A	
Programma di installazione del client di comunicazione	X		8101	X	X	X	X
Csta Message Dispatcher (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	

Descrizione	TCP	UDP	Numero di porta	OpenScape Business X	Scheda UC Booster	OpenScape Business S	Server UC Booster
Csta Service Provider (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	A		A	
FTP Passive	X		40000-40040	A		A	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Messaggistica istantanea (http)	X		8101	X	X	X	X
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS Cloud Service	X		8602	X			
Server LDAP	X		389		X	X	X
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
NAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
Openfire Admin (https)	X		9091		X	X	X
OpenScape Business Auto Update Service (http)	X		8101	X	X	X	X
OpenScape Business Multisite	X		8778		X	X	X
OpenScape Business myReports (http)	X		8101		X	X	X
Server stato OpenScape Business	X		8808	X		X	X
Portale utenti OpenScape Business	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (integrato)		X	29100-30530	X	X	X	X
RTP (server)		X	29100-30888	X	X	X	X
SIP (server)	X	X	5060	X		X	
SIP TLS SIPQ (server)	X		5061	X		X	

Descrizione	TCP	UDP	Numero di porta	OpenScape Business X	Scheda UC Booster	OpenScape Business S	Server UC Booster
SIP TLS Subscriber (server)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (traps)		X	162	X		X	
VSL	X		8770-8780		X	X	X
Webadmin per client	X		8803	X	X	X	X
Client basati sul Web							
Client basati sul Web (http)	X		8801	X	X	X	X
Client basati sul Web (https)	X		8802	X	X	X	X

Nota: Per motivi di sicurezza, si consiglia di utilizzare solo https per i client basati sul Web e di impostare l'inoltro delle porte da TCP/443 esterno a TCP/8802 interno.

Certificato CLS

A partire dalla V3R3.1, viene fornito un nuovo certificato CLS con un nome comune (CN) aggiornato tramite una porta di nuova introduzione. Ciò offre un algoritmo digest migliorato e più forte, nonché entità legali aggiornate. I sistemi con licenza online tramite la modalità CLS Connect richiedono i seguenti due prerequisiti:

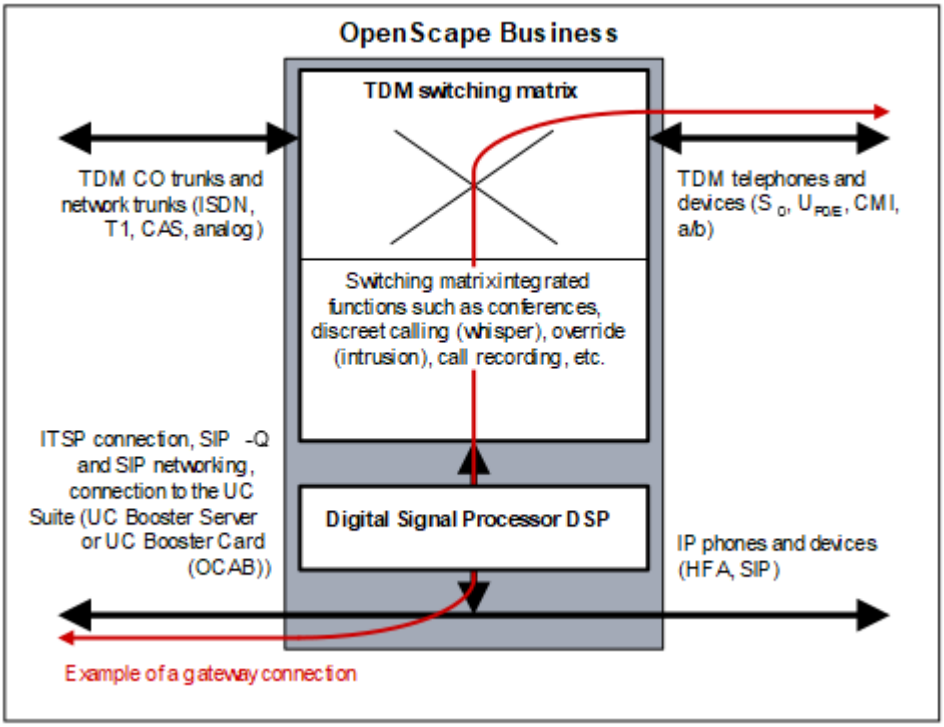
- L'indirizzo IP 188.64.16.4 è abilitato per il traffico in uscita nel firewall.
- Le porte 7780 e 7791 sono abilitate per il traffico in uscita nel firewall.

La porta 7790 usata in precedenza può essere rimossa dalla configurazione del firewall dopo l'aggiornamento alla V3R3.1 per aumentare la sicurezza.

29.4 Progettazione dei canali DSP per i sistemi di comunicazione OpenScape Business X3/X5/X8

Le connessioni tra telefoni/linee IP e TDM sono connessioni "gateway", per le quali è sempre necessario un canale DSP (Digital Signal Processor). Oltre a ciò, i canali DSP sono necessari per l'attivazione della funzione Crittografia segnalazione e payload (SPE).

Nessun canale DSP necessario per connessioni TDM pure e connessioni solo IP.



La scheda madre dei sistemi di comunicazione OpenScape Business X3/X5/X8 mettono a disposizione fino a otto canali DSP.

Se i canali DSP di una scheda madre non sono sufficienti, è possibile aggiungere altri canali collegando una Voice Channel Booster Card (sottomodulo OCCB1 o OCCB3):

- OCCB1 fornisce fino a 40 canali DSP supplementari.
- OCCB3 fornisce un massimo di 120 canali DSP supplementari.

Il numero di canali DSP disponibili per le connessioni al gateway si riduce grazie all'uso del codec G.729 e della Crittografia segnalazione e payload (SPE).

In ultima analisi, il numero di connessioni simultanee del gateway (connessioni voce simultanee con transizione TDM-IP) determina se e quale sottomodulo OCCB deve essere utilizzato.

In caso di conferenze UC Suite e telefoni IP, un sistema di comunicazione OpenScape Business X3/X5/X8 è in grado di includere fino a otto canali DSP. Per impostazione predefinita, ai 3 codec predefiniti per Musica su attesa sono assegnati tre canali DSP. Questo numero può essere diminuito se si usano meno codec per Musica su attesa. Inoltre, due canali DSP sono riservati per la configurazione della crittografia segnalazione e payload (SPE). Il resto dei canali DSP possono essere assegnati a telefoni IP (un canale DSP per telefono IP). Quando si esauriscono i canali DSP disponibili, il numero di canali DSP può essere aumentato con l'uso delle corrispondenti schede OCCB (OCCB1 o OCCB3 come precedentemente indicato).

Suggerimento: Per maggiori informazioni sul numero massimo di canali DSP disponibili sulla scheda madre e di sottomoduli OCCB, consultare Limiti di configurazione in funzione del sistema.

In caso di sottodimensionamento dei canali DSP, possono verificarsi colli di bottiglia DSP che si manifestano ad esempio mediante lo stato di occupato durante la connessione (tono di occupato mentre viene stabilita la connessione, indicazione a display `Attualmente impossibile`).

Quando si verifica un collo di bottiglia DSP, viene creata la relativa voce nel file di registro eventi (log eventi) del sistema di comunicazione.

Se si verificano frequentemente colli di bottiglia DSP, occorre adottare le seguenti misure:

Se	Allora
Vengono utilizzati i canali DSP della scheda madre.	Inserire il sottomodulo OCCB1 o OCCB3 nella scheda madre.
I canali DSP della scheda madre sono sufficienti. Non è richiesto alcun modulo OCCB1.	Inserire il sottomodulo OCCB3 nella scheda madre.
I canali DSP della scheda madre sono sufficienti. Non è richiesto alcun modulo OCCB3.	Occorre verificare se il sistema di comunicazione può essere utilizzato solo con il codec G.711. In questo modo il numero di canali DSP viene portato al massimo. ***INFO:*** l'opzione **Usa solo G.711** può essere attivata da un amministratore con il profilo **Expert** tramite la **Modalità esperti** (**Telefonia** > **Gateway voce** > **Parametri Codec**).

La seguente tabella fornisce valori orientativi sul sottomodulo OCCB da utilizzare all'occorrenza.

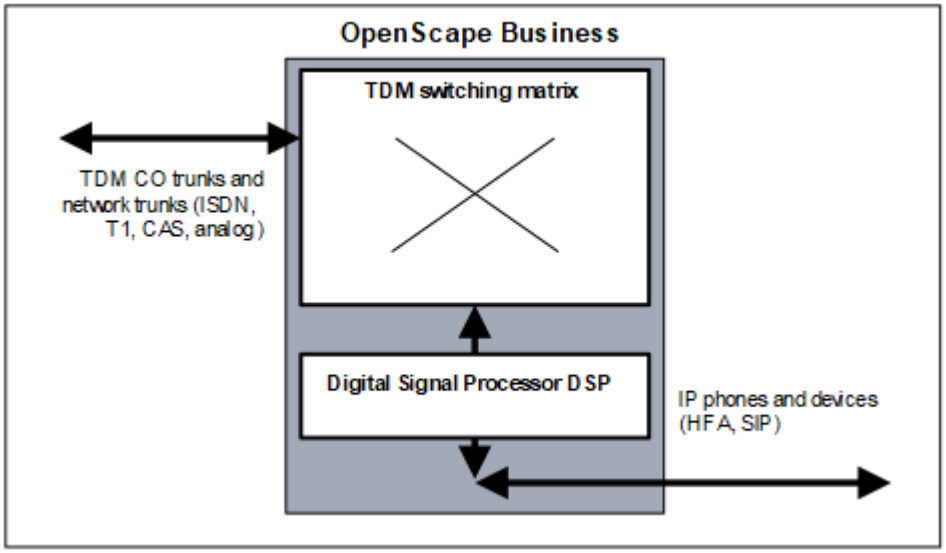
Totale dei canali TDM: Linee esterne e connessioni di rete (ISDN, T1, CAS, analogica)	Totale dei canali IP: Collegamento ITSP, connessione in rete SIP-Q e SIP, collegamento alla UC Suite (UC Booster Server o UC Booster Card (OCAB))	**Totale dei telefoni TDM e dei dispositivi TDM (S_0, $U_{P0/E}$, CMI, a/b)**	**Totale dei telefoni IP e dei dispositivi IP (HFA, SIP)**	**Quale sottomodulo OCCB?**	**Note**
un numero a piacere di	annunci (fino a 16) 0	un numero a piacere di	0	Nessuno modulo secondario OCCB	Smart VM e le conferenze di sistema vengono elaborati tramite la rete.

Totale dei canali TDM: Linee esterne e connessioni di rete (ISDN, T1, CAS, analogica)	Totale dei canali IP: Collegamento ITSP, connessione in rete SIP-Q e SIP, collegamento alla UC Suite (UC Booster Server o UC Booster Card (OCAB))	**Totale dei telefoni TDM e dei dispositivi TDM (S_0, $U_{P0/E}$, CMI, a/b)**	**Totale dei telefoni IP e dei dispositivi IP (HFA, SIP)**	**Quale sottomodulo OCCB?**	**Note**
			fino a 8	Nessuno modulo secondario OCCB	Indipendentemente dai canali TDM. Per l'uso di Smart VM e conferenze di sistema in combinazione con telefoni IP e di dispositivi IP sono necessarie risorse DSP.
			9 - 100	OCCB1	Indipendentemente dai canali TDM. Per l'uso di Smart VM e conferenze di sistema in combinazione con telefoni IP e di dispositivi IP sono necessarie risorse DSP, fino a 40 contemporaneamente.
			> 100	OCCB3	Indipendentemente dai canali TDM. Per l'uso di Smart VM e conferenze di sistema in combinazione con telefoni IP e di dispositivi IP sono necessarie risorse DSP, fino a 120 contemporaneamente.
	> 0	fino a 8		Nessuno modulo secondario OCCB	
	> 0	9 - 100		OCCB1	fino a 40 contemporaneamente

Totale dei canali TDM: Linee esterne e connessioni di rete (ISDN, T1, CAS, analogica)	Totale dei canali IP: Collegamento ITSP, connessione in rete SIP-Q e SIP, collegamento alla UC Suite (UC Booster Server o UC Booster Card (OCAB))	**Totale dei telefoni TDM e dei dispositivi TDM (S_0, $U_{P0/E}$, CMI, a/b)**	**Totale dei telefoni IP e dei dispositivi IP (HFA, SIP)**	**Quale sottomodulo OCCB?**	**Note**
	> 0	> 100		OCCB3	fino a 120 contemporaneamente
> 0	fino a 8			Nessuno modulo secondario OCCB	La combinazione è rilevante soprattutto per SIP-Q e la UC Suite.
> 0	fino a 9			OCCB1	La combinazione è rilevante soprattutto per SIP-Q e la UC Suite.
> 0	> 40			OCCB3	La combinazione è rilevante soprattutto per SIP-Q e la UC Suite.

Gli esempi seguenti forniscono valori orientativi sul sottomodulo OCCB da utilizzare all'occorrenza.

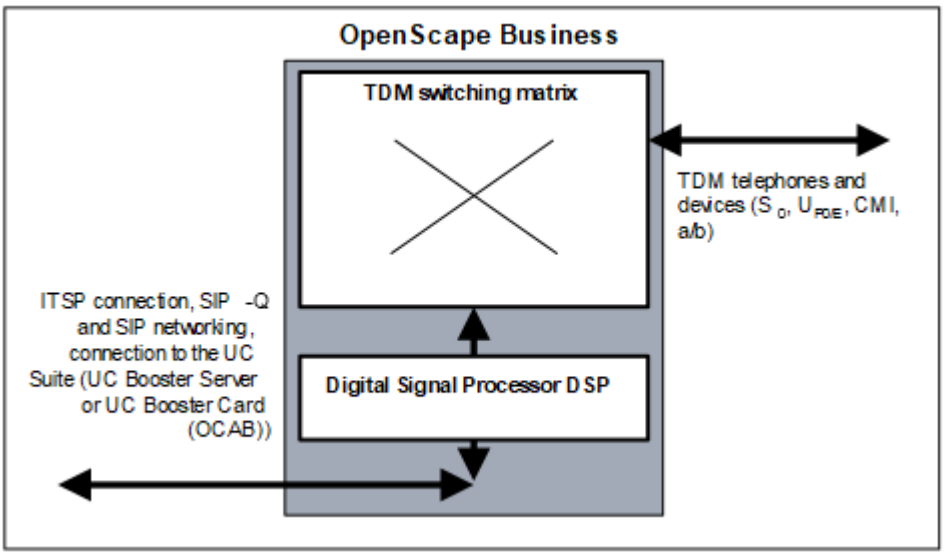
Esempio 1: OpenScape Business con linee esterne TDM e telefoni e dispositivi IP



Se	Allora
OpenScape Business con: • 1 x Linee esterne TDM (ISDN) • 20 x Telefoni IP (HFA, SIP)	I canali DSP sulla scheda madre sono sufficienti. Non è richiesto alcun modulo OCCB.
OpenScape Business con: • 1 x Linee esterne TDM (ISDN) • 100 x Telefoni IP (HFA, SIP)	Il sottomodulo OCCB1 è obbligatorio. In alternativa, è possibile utilizzare il sottomodulo OCCB3.
OpenScape Business con: • 2 x Linee esterne TDM (ISDN) • 100 x Telefoni IP (HFA, SIP)	Il sottomodulo OCCB3 è obbligatorio.
OpenScape Business con: • 4 x Linee esterne TDM (ISDN) • 500 x Telefoni IP (HFA, SIP)	Il sottomodulo OCCB3 è obbligatorio. ***NOTA:*** per ottenere il numero massimo di canali DSP, nella configurazione del sistema può essere usato solo il codec G.711.

Se il sistema di comunicazione è provvisto anche di telefoni e dispositivi TDM (S_0, $U_{P0/E}$, CMI, a/b), occorre tenere in considerazione ulteriori canali DSP.

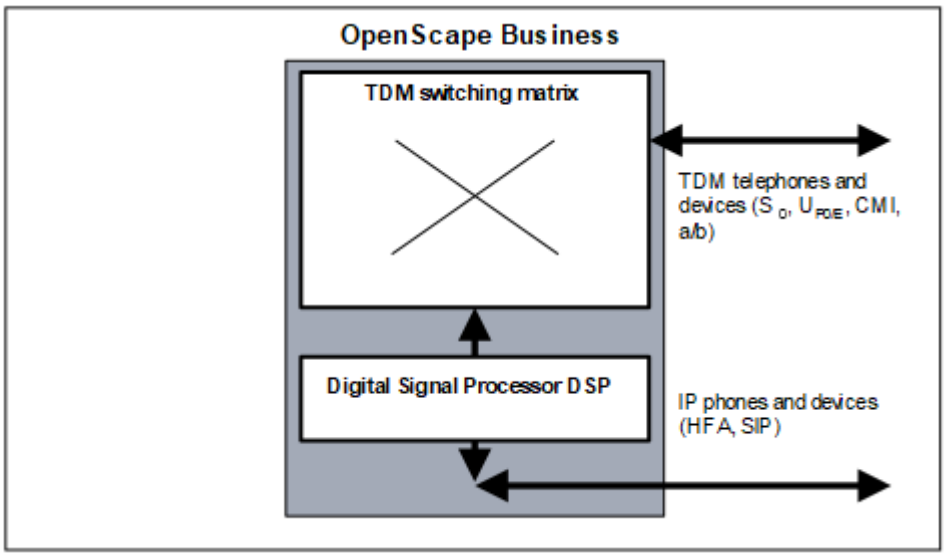
Esempio 2: OpenScape Business con connessione ITSP, telefoni e dispositivi TDM



Se	Allora
OpenScape Business con: • 6 x Connessioni ITSP (6 canali B) • 20 x Telefoni TDM (S_0, $U_{P0/E}$, CMI, a/b)	I canali DSP sulla scheda madre sono sufficienti. Non è richiesto alcun modulo OCCB.
OpenScape Business con: • 30 x Connessioni ITSP (30 canali B) • 100 x Telefoni TDM (S_0, $U_{P0/E}$, CMI, a/b)	Il sottomodulo OCCB1 è obbligatorio. In alternativa, è possibile utilizzare il sottomodulo OCCB3.

Se il sistema di comunicazione è provvisto di telefoni e dispositivi IP (HFA, SIP), occorre tenere in considerazione ulteriori canali DSP.

Esempio 3: OpenScape Business con telefoni e dispositivi TDM e telefoni e dispositivi IP



Se	Allora
OpenScape Business con: • 6 x Telefoni TDM (S_0, $U_{P0/E}$, CMI, a/b) • 6 x Telefoni IP (HFA, SIP)	I canali DSP sulla scheda madre sono sufficienti. Non è richiesto alcun modulo OCCB.
OpenScape Business con: • 100 x Telefoni TDM (S_0, $U_{P0/E}$, CMI, a/b) • 100 x Telefoni IP (HFA, SIP)	Il sottomodulo OCCB3 è obbligatorio.

Se il sistema di comunicazione è provvisto anche di linee TDM o IP, occorre tenere in considerazione ulteriori canali DSP.

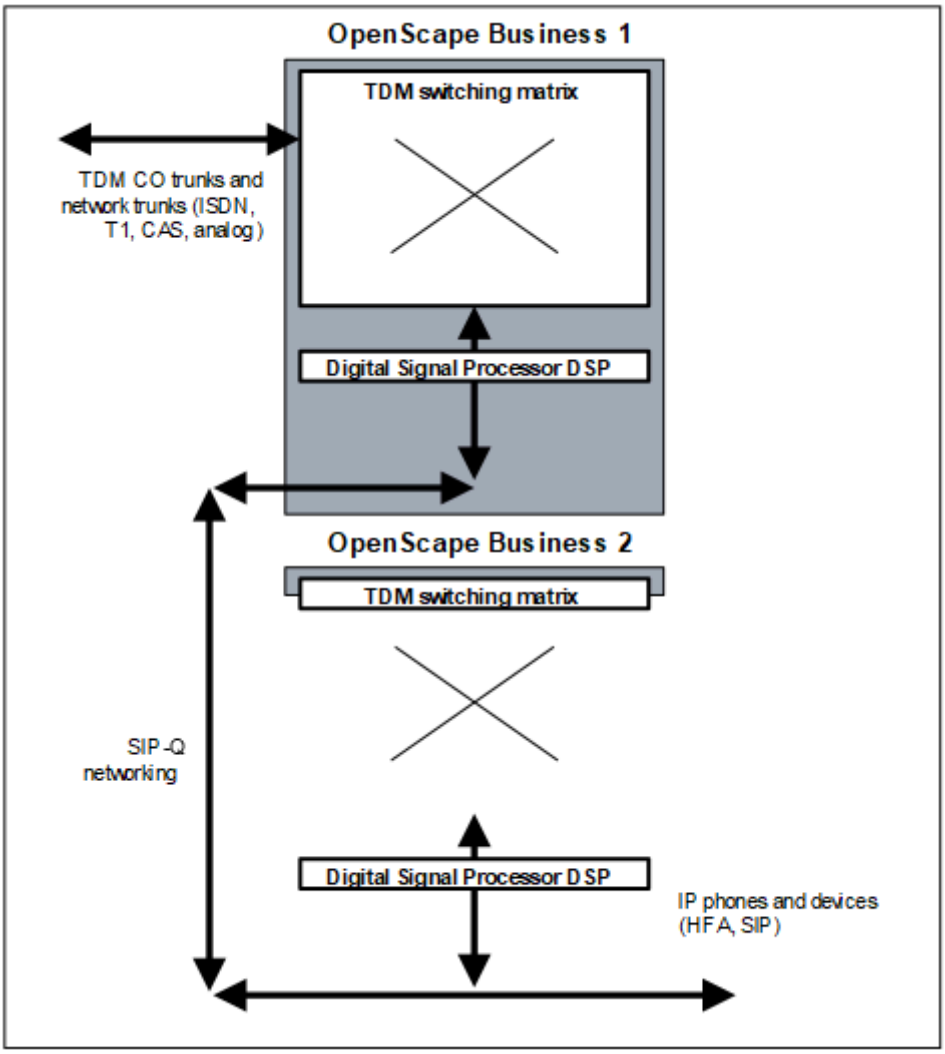
Esempio 4: Collegamento in rete SIP-Q di OpenScape Business

Nota: Questo esempio illustra i requisiti di un secondo sistema OpenScape Business connesso in rete. Per semplificare, in questo esempio non verranno illustrate le connessioni del primo sistema. Tuttavia, occorre tenere in considerazione anche i requisiti del primo sistema come indicato negli esempi 1, 2 e 3.

Il sistema di comunicazione OpenScape Business 1 funge da gateway per le linee TDM.

I telefoni IP (HFA, SIP) sono collegati esclusivamente al sistema di comunicazione OpenScape Business 2.

Sulla base del numero di telefoni IP nel sistema di comunicazione OpenScape Business 2 devono essere pianificati i canali DSP per il sistema di comunicazione OpenScape Business 1. I canali DSP sono richiesti solo con gateway TDM.



Se	Allora
OpenScape Business 1 con: • 1 x Linee esterne TDM (ISDN) OpenScape Business 2 con: • 100 x Telefoni IP (HFA, SIP)	In OpenScape Business 1 è richiesto il sottomodulo OCCB1. In alternativa, è possibile utilizzare il sottomodulo OCCB3. Nessun sottomodulo OCCB in OpenScape Business 2.
OpenScape Business 1 con: • 2 x Linee esterne TDM (ISDN) OpenScape Business 2 con: • 100 x Telefoni IP (HFA, SIP)	In OpenScape Business 1 è richiesto il sottomodulo OCCB3. Nessun sottomodulo OCCB in OpenScape Business 2.
OpenScape Business 1 con: • 4 x Linee esterne TDM (ISDN) OpenScape Business 2 con: • 500 x Telefoni IP (HFA, SIP)	In OpenScape Business 1 è richiesto il sottomodulo OCCB3. ***NOTA:*** per ottenere il numero massimo di canali DSP, nella configurazione del sistema può essere usato solo il codec G.711. Nessun sottomodulo OCCB in OpenScape Business 2.

Se il sistema di comunicazione OpenScape Business 2 è provvisto anche di linee o telefoni e dispositivi TDM (S_0, $U_{P0/E}$, CMI, a/b), occorre tenere in considerazione ulteriori canali DSP.

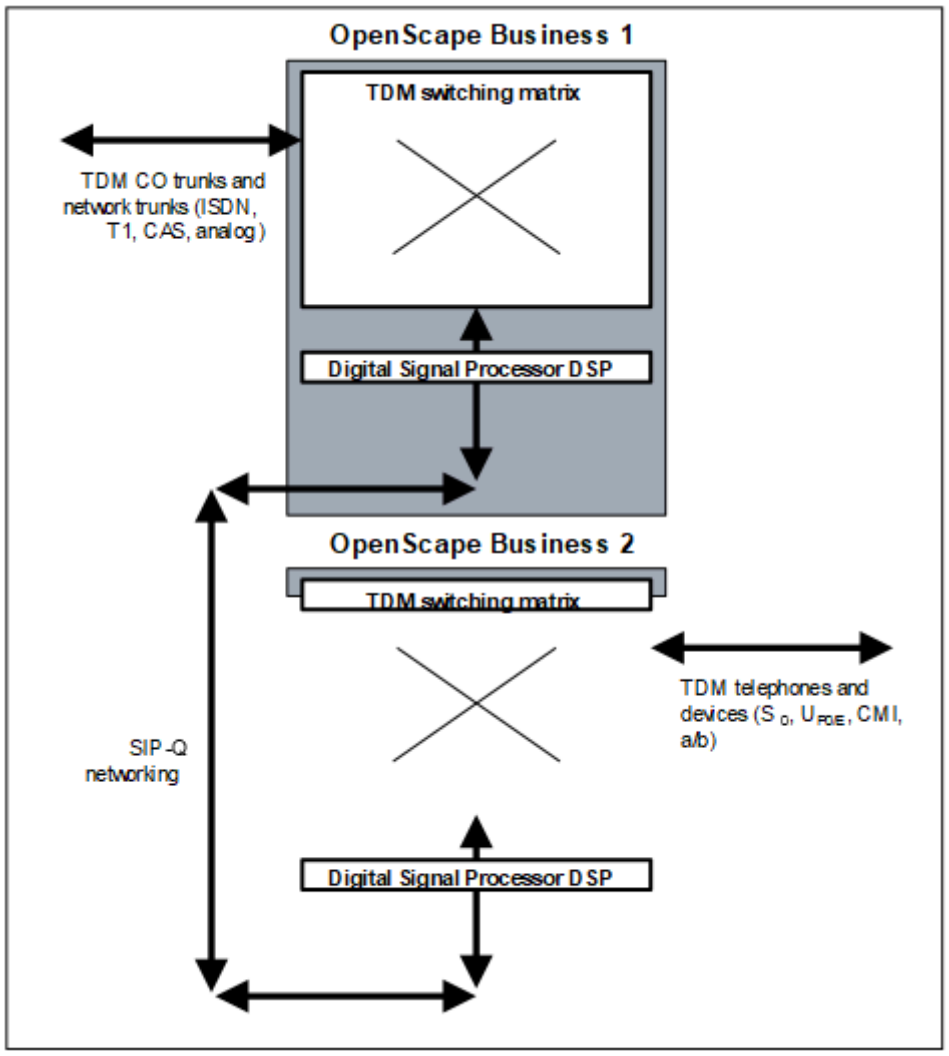
Esempio 5: Collegamento in rete SIP-Q di OpenScape Business

Nota: Questo esempio illustra i requisiti di un secondo sistema OpenScape Business connesso in rete. Per semplificare, in questo esempio non verranno illustrate le connessioni del primo sistema. Tuttavia, occorre tenere in considerazione anche i requisiti del primo sistema come indicato negli esempi 1, 2 e 3.

Il sistema di comunicazione OpenScape Business 1 funge da gateway per le linee TDM.

I telefoni TDM (S_0, $U_{P0/E}$, CMI, a/b) sono collegati esclusivamente al sistema di comunicazione OpenScape Business 2.

Poiché in entrambi i sistemi di comunicazione, sono necessarie connessioni gateway (OpenScape Business 1: linea TDM <-> rete SIP-Q, OpenScape Business 2: rete SIP-Q <-> telefono TDM), entrambi richiedono canali DSP.



Se	Allora
OpenScape Business 1 con: • 1 x Linee esterne TDM (ISDN) OpenScape Business 2 con: • 100 x Telefoni TDM (S_0, $U_{P0/E}$, CMI, a/b)	In OpenScape Business 1 e in OpenScape Business 2 è richiesto il sottomodulo OCCB1. In alternativa, è possibile utilizzare il sottomodulo OCCB3 in entrambi i casi.
OpenScape Business 1 con: • 2 x Linee esterne TDM (ISDN) OpenScape Business 2 con: • 100 x Telefoni TDM (S_0, $U_{P0/E}$, CMI, a/b)	In OpenScape Business 1 e in OpenScape Business 2 è richiesto il sottomodulo OCCB3.

Se il sistema di comunicazione OpenScape Business 1 è provvisto anche di telefoni e dispositivi TDM (S_0, $U_{P0/E}$, CMI, a/b), occorre tenere in considerazione ulteriori canali DSP.

Esempio 6: OpenScape Business con telefoni e dispositivi IP

Nota: Questo esempio illustra i requisiti di un secondo sistema OpenScape Business connesso in rete. Per semplificare, in questo esempio non verranno illustrate le connessioni del primo sistema. Tuttavia, occorre tenere in considerazione anche i requisiti del primo sistema come indicato negli esempi 1, 2 e 3.

Se	Allora
OpenScape Business X3/X5/ X8 con: • 7 x Telefoni IP (HFA, SIP)	I canali DSP sulla scheda madre sono sufficienti. Non è richiesto alcun modulo OCCB.
OpenScape Business: • 30 x Telefoni IP (HFA, SIP)	Il sottomodulo OCCB1 è obbligatorio. In alternativa, è possibile utilizzare il sottomodulo OCCB3.
OpenScape Business con: • 100 x Telefoni IP (HFA, SIP)	Il sottomodulo OCCB3 è obbligatorio.

30 Glossario

Nel glossario vengono riportate brevi spiegazioni sui termini utilizzati (ad esempio, per i protocolli e gli standard).

30.1 Glossario

10BaseT, 100BaseT, 1000BaseT

Si tratta della specifica (IEEE 802.3i) per le reti con banda di trasmissione base 10 MBit/s su un cavo simmetrico da 100 Ohm a quattro conduttori. 100BaseT indica una larghezza di banda fino a 100 MBit/s e 1000BaseT fino a 1000 MBit/s.

AES (Advanced Encryption Standard, standard di crittografia avanzato)

AES è un sistema di crittografia simmetrico considerato dal National Institute of Standards and Technology come il successore dei precedenti standard DES e 3DES. È utilizzato ad es. con VPN.

ADSL con indirizzo IP dinamico

ADSL è l'acronimo di Asymmetric Digital Subscriber Line e significa che le larghezze di banda da Internet (Download, Downstream) e per Internet (Upload, Upstream) sono diverse. L'ADSL corrisponde alla classica connessione DSL. Un indirizzo IP dinamico è sufficiente se i servizi Web e E-mail vengono messi a disposizione da un Internet Service Provider.

ADSL con indirizzo IP fisso

ADSL è l'acronimo di Asymmetric Digital Subscriber Line e significa che le larghezze di banda da Internet (Download, Downstream) e per Internet (Upload, Upstream) sono diverse. L'ADSL corrisponde alla classica connessione DSL. L'ADSL con indirizzo IP fisso è necessaria se occorre gestire in loco alcuni server Web ed E-mail.

AF-EF (Expedited Forwarding - Assured Forwarding)

I punti codice "Expedited Forwarding" (EF) e "Assured Forwarding" (AF) definiscono le diverse priorità dei pacchetti IP in Quality of Service (QoS).

AF: garantisce una larghezza di banda minima per i dati.

EF: garantisce una larghezza di banda costante per i dati.

ARP (Address Resolution Protocol)

L'ARP è un protocollo di rete che viene utilizzato per l'assegnazione di indirizzi di rete a dispositivi hardware. Nonostante non si limiti ai protocolli Ethernet e IP, viene quasi esclusivamente utilizzato insieme all'assegnazione di indirizzi IP sulle reti Ethernet.

Autenticazione

L'autenticazione è la verifica dell'identità di una persona o di un PC. Tale verifica può avvenire semplicemente con un nome utente oppure in modo più complesso, ad esempio tramite le impronte digitali.

Autorizzazione

L'autorizzazione è la concessione di diritti (ad esempio dei diritti di accesso).

Canale B

Il canale B è una via di trasmissione per i dati utili (lingua, informazioni) di una chiamata ISDN.

BLF Campo lampade occupato

myPortal offre un cosiddetto Campo lampade occupato (BLF) per visualizzare in modo ottimale lo stato di conversazione degli utenti.

Broadcast

Un broadcast è un messaggio inviato a tutti gli elementi collegati a una rete informatica. In questo modo un messaggio (un pacchetto dati) viene trasmesso da un singolo punto a tutti gli utenti di una rete. Un broadcast viene utilizzato prevalentemente nelle reti di dati quando gli indirizzi dei destinatari del messaggio non sono ancora noti.

CA (Certification Authority, autorità di certificazione)

CA è un'organizzazione che emette certificati con firme digitali. Le firme digitali sono utilizzati ad esempio in una VPN (Virtuale Private Network).

Interfaccia CAPI (Common Application Programming Interface)

CAPI è un'interfaccia software conforme ISDN che consente lo sviluppo di software per ISDN senza conoscenze dell'hardware ISDN specifico di un produttore.

Centrex

Centrex (Central Office Exchange) mette a disposizione le funzioni di un centralino telefonico tramite PSTN o tramite ITSP. È detto anche centralino telefonico virtuale, Hosted PBX (Private Branch Exchange) o NetPBX designato.

CHAP (Challenge Handshake Authentication Protocol)

CHAP è un protocollo di autenticazione che viene introdotto nell'ambito del protocollo Point to Point.

COS (Classi di Servizio)

QoS è un metodo che viene utilizzato per valutare la qualità della trasmissione di dati su reti IP.

CLIP (Calling Line Identification Presentation)

La trasmissione del numero di telefono consente di visualizzare il numero telefonico del chiamante. In questo modo l'utente chiamato può identificare il chiamante prima di iniziare la conversazione.

CLIR (Calling Line Identification Restriction)

Il chiamante nasconde il proprio numero di telefono all'utente chiamato. Pertanto l'utente chiamato non può identificare l'autore della chiamata.

COLP (Connected Line Identification Presentation)

La trasmissione del numero di telefono consente all'utente chiamato di visualizzare il numero di telefono del chiamante quando si instaura la connessione.

COLR (Connected Line Identification Restriction)

Se l'utente chiamante ha scelto di nascondere il proprio numero di telefono all'utente chiamato, questo numero non viene comunque visualizzato nonostante l'attivazione del servizio COLP.

Comfort User

Comfort User è l'utente standard del sistema di comunicazione.

Comfort Plus

Comfort Plus User è l'utente avanzato del sistema di comunicazione. A differenza del Comfort User, il Comfort Plus User dispone di più servizi (come Fax, Mobilità, Conferenze).

CorNet

CorNet è un protocollo proprietario per la connessione in rete dei sistemi di comunicazione HiPath e OpenScape. Anziché un supporto generale per QSIG, CorNet integra tutti i servizi specifici del produttore dei sistemi di comunicazione HiPath e OpenScape.

CorNet-IP

CorNet-IP è una variante del protocollo CorNet, che consente una rete di giunzione di impianti o il collegamento di sistemi di telefonia (ad es. optiPoint) tramite IP.

CorNet-NQ

Un protocollo di segnalazione proprietario basato su QSIG, per la connessione dei sistemi di comunicazione con uno o più impianti QSIG.

CSTA (Computer Supported Telecommunications Applications)

CSTA è un'interfaccia per applicazioni che supporta lo standard European Computer Manufacturers Association (ECMA). Tramite CSTA è possibile controllare e monitorare le attività di telecomunicazione su SIP.

CSV (Character Separated Values)

Un file CSV è un file di testo che consente di memorizzare e scambiarsi facilmente dati strutturati. CSV è l'acronimo di Character Separated Values, Comma Separated Values o Colon Separated Values, poiché i singoli valori possono essere separati da specifici caratteri, ad esempio la virgola o il punto e virgola. I file CSV devono essere in formato ANSI/ASCII.

CRL (Certificate Revocation List)

Una CRL è la pubblicazione di certificati pubblici revocati. Le CRL possono sempre essere generate dalle autorità di certificazione prima dell'emissione del certificato.

Delay

Nel campo delle telecomunicazioni, un delay ha due significati:

- L'intervallo di tempo di cui viene ritardato un evento.
- Il tempo che trascorre fra il verificarsi di un evento e le conseguenze dell'evento stesso.

Dedicated Gateway (gateway dedicato, assegnato in modo fisso)

Se nell'LCR è configurato un gateway dedicato per un fascio, tale dispositivo verrà immediatamente utilizzato per il routing. Eventuali regole in conflitto relativamente al routing non saranno valide.

DHCP (Dynamic Host Configuration Protocol)

DHCP è il metodo con cui si assegnano, all'avvio di un PC, determinate configurazioni IP (indirizzo IP, maschera di sub-rete, ecc.).

DS (DiffServ, Differentiated Services)

DS è un metodo di gestione dei pacchetti nelle reti di dati. Stabilisce come deve essere trasmesso/inoltrato un pacchetto dati e fornisce uno specifico livello di servizio in merito a larghezza di banda, gestione delle code e scelta/rifiuto dei pacchetti.

Algoritmo di Diffie-Hellman

L'algoritmo di Diffie-Hellman provvede allo scambio delle chiavi su una VPN. I dati ottenuti con questo algoritmo sono configurati con un set specifico di parametri matematici. Poiché lo scambio di codici funziona in modo ordinato, entrambi gli utenti devono presentare gli stessi valori per questi parametri.

DLI (Deployment License Service Integrated)

Tramite DLI è possibile installare e configurare automaticamente telefoni IP di sistema.

DMZ (Demilitarized Zone)

Una DMZ (zona demilitarizzata) indica una rete di computer con opzioni di accesso protette ai nodi della rete (computer, router, ecc).

DNS (Domain Name Service)

Risoluzione dei nomi in Internet e nella LAN. I nomi dei PC o delle pagine Web vengono tradotti negli indirizzi IP corrispondenti utilizzando DNS.

DSL (Digital Subscriber Line)

DSL è una tecnologia che consente l'accesso a Internet a banda larga. Grazie alla tecnologia DSL viene superato il percorso fra il centralino del provider e la presa telefonica del cliente.

DSS (Direct Station Selection)

I tasti funzione di un telefono o di un modulo aggiuntivo possono essere configurati come tasti per la chiamata diretta (DSS). A tale scopo i tasti vengono programmati con il numero di telefono di un utente interno o di un gruppo. Premendo un tasto DSS viene effettuata immediatamente una chiamata alla destinazione programmata.

DTMF (Dual Tone Multifrequency)

Vedere DTMF, Selezione multifrequenza.

EIM (Enterprise Instant Messaging)

EIM è un servizio di messaggistica istantanea che viene eseguito su server privati in un'azienda, su piattaforme quali Live Communications Server o Office Communications Server 2007 di Microsoft.

Switch Enterasys

Gli switch Enterasys sono soluzioni di rete sicure prodotte da Enterasys Networks. Gli switch impilabili, riconoscono le funzioni QoS, classificano e assegnano priorità ad applicazioni vocali, video e dati.

ESP (Encapsulating Security Payload))

Si tratta di un protocollo IPSec che consente di garantire l'integrità e l'autenticità dei pacchetti grazie alla crittografia degli stessi. La verifica di integrità e di autenticità non viene eseguita sull'intestazione IP ma solo sui dati veri e propri (Payload).

FoIP (Fax over IP)

FoIP è un metodo di trasmissione dei messaggi fax sulla rete IP.

FTP

Il File Transfer Protocol (protocollo di trasferimento dati) FTP è un protocollo di rete specificato in RFC 959 per la trasmissione dei dati su reti TCP/IP.

Codici funzione

I codici funzione sono numeri MSN/interni o numeri pilota ad esempio per parcheggio, conferenze e AutoAttendant. I codici funzione corrispondono agli utenti virtuali. In un sistema di reti, i codici funzione devono essere sempre univoci.

G.711

G.711 è uno standard per la digitalizzazione dei segnali audio. Viene utilizzato nella telefonia classica su rete fissa (tecnica PCM). G.711 è una possibile codifica voce anche per VoIP.

G.729AB

G.729 indica un Codec per la compressione voce nei segnali digitali e viene integrato nella telefonia IP. G.729 richiede molta potenza di elaborazione. Una variante leggermente semplificata, qualitativa ma solo limitatamente inferiore è G.729AB, che richiede una potenza di calcolo più ridotta.

Gateway / Modulo gateway

Un gateway rappresenta un ingresso o un'uscita per i dati da una rete di comunicazione che dispone di due diversi flussi di traffico.

GSM (Global System for Mobile Communications)

GSM è lo standard per le reti mobili digitali utilizzato principalmente per la telefonia ma anche per la trasmissione di dati a commutazione di linea o di pacchetto, nonché per i messaggi SMS.

Handover (passaggio)

Per handover, che letteralmente significa passaggio, si intende un processo in una rete di comunicazione mobile, in cui, durante una conversazione o una connessione dati, il telefono mobile passa da una cella radio all'altra. Quando si passa da una rete GSM a una UMTS e viceversa con un telefono cellulare dual mode si parla di handover.

Valore hash

Si tratta di valori per la maggior parte scalari, da un sottoinsieme di numeri naturali. Un valore hash viene definito anche "impronta digitale". Come per gli esseri umani le impronte digitali, il valore hash rappresenta un identificativo univoco degli insiemi.

H.323

H.323 è un gruppo di standard che definisce una serie di tipi di supporti per le reti a pacchetti. Gli standard coprono voce, dati, fax e video e definiscono come deve avvenire la conversione del segnale da analogico a digitale e quali tipi di segnalazione devono essere utilizzati.

OpenScape Business Assistant

OpenScape Business Assistant viene utilizzato per l'amministrazione del sistema di comunicazione. Qui sono disponibili tutte le procedure guidate per un rapido supporto alle attività di amministrazione.

Servizi hosted

I servizi hosted sono servizi IT tradizionali come posta elettronica, invio messaggi immediato (IM) e Unified Communications (UC), che un provider Internet mette a disposizione di un'azienda da una sede remota; in questo modo non è necessario per l'azienda eseguire e mantenere questi servizi su server locali.

ICMP (Internet Control Message Protocol)

ICMP viene utilizzato in una rete informatica per lo scambio di messaggi informativi e di errore tramite il protocollo Internet IP.

IDS (Intrusion Detection System)

IDS è un sistema di protezione che sorveglia tutte le attività di rete, in ingresso e in uscita, per identificare i possibili problemi di protezione. In questi problemi rientrano anche gli attacchi (dall'esterno dell'organizzazione) e l'utilizzo improprio (attacchi dall'interno dell'organizzazione).

Standard IEEE

Lo standard IEEE è una serie di specifiche definite dall'Institute of Electrical and Electric Engineers (IEEE) (ad esempio, Token Ring, Ethernet), per creare uno standard di rete comune destinato ai produttori.

IEEE 802.1p

IEEE 802.1p è uno standard IEEE, che regola il trasporto dei pacchetti dati con diversa priorità nelle reti informatiche. I pacchetti di dati vengono suddivisi in classi di priorità da 1 a 7. Lo standard definisce solo priorità crescenti da 1 a 7, senza fornire ulteriori informazioni su come i singoli pacchetti di dati devono essere trattati.

Protocollo IKE

Il protocollo IKE svolge due funzioni distinte. Per prima cosa crea una SA (Security Association) utilizzata esclusivamente dal protocollo IKE (IKE-SA). Quindi la utilizza per proteggere tutte le trasmissioni successive di dati payload che richiedono SA (Payload-SA).

IM (Invio messaggi immediato)

IM è una procedura per lo scambio in tempo reale di messaggi di testo tramite Internet con il supporto di PC, Pocket-PC e telefoni cellulari. I moderni servizi di IM consentono VoIP, videoconferenze, trasferimento di dati e condivisione di applicazioni desktop.

IP PBX

IP PBX è un impianto di comunicazione che supporta sia le connessioni VoIP che le connessioni voce tramite le linee telefoniche esistenti.

IPSec

IPSec è uno schema di standard aperti comunicazioni su reti IP protette e con garanzia di riservatezza, grazie all'introduzione di vari servizi e protocolli di sicurezza.

ISP (Internet Service Provider)

Un ISP è un'azienda, una persona, un'organizzazione che offre servizi per il collegamento a Internet. Alcuni ISP sono grandi aziende nazionali o internazionali che offrono l'accesso da numerose località, mentre altri sono limitati a regioni o paesi specifici.

ITSP (Internet Telephony Service Provider)

Un ITSP è un'azienda, una persona, un'organizzazione che offre servizi di telefonia via Internet.

DP (Selezione a impulsi)

DP è il più vecchio metodo di selezione per le trasmissioni telefoniche automatiche. Oggi è quasi completamente sostituita da DTMF (segnalazione a toni).

Jitter

Per Jitter si intende un ritardo dei pacchetti di dati durante la trasmissione vocale. Un ritardo eccessivo fra l'invio dei pacchetti dati e la ricezione a destinazione può rendere la comunicazione vocale irregolare e di difficile comprensione.

Selezione breve personale

Grazie alla selezione breve personale è possibile salvare sul proprio telefono 10 numeri esterni di selezione breve aggiuntivi oltre a quelli offerti a livello centrale dal sistema.

Selezione breve del sistema

I numeri telefonici esterni più spesso utilizzati possono essere salvati in nella memoria del sistema di comunicazione. Ciascun numero viene rappresentato da un numero di selezione breve che può essere utilizzato al posto del numero telefonico completo.

Latenza

Per latenza si intende il tempo necessario per il trasporto di un pacchetto dati da un'applicazione a un'altra, inclusi la durata della trasmissione in rete e il tempo necessario per la preparazione e l'elaborazione dei dati sull'apparecchio del mittente e del destinatario.

LCR (Least Cost Routing)

Con il supporto di LCR (Least Cost Routing) è possibile definire con quale operatore effettuare una chiamata a un cellulare o internazionale. Tramite il sistema di comunicazione si definisce un operatore conveniente, quindi si effettuano tutte le conversazioni corrispondenti con questo operatore.

LIN (Location Identification Number)

Il LIN è un numero univoco composto da non oltre 16 cifre che corrisponde al NANP (North American Numbering Plan) composto da 10 cifre.

LWCA (Leightweight CA)

LWCA è una funzione di certificazione limitata.

Media Stream Channel

Un Media gateway può terminare i canali B ISDN della linea e creare canali di streaming per le reti a pacchetti basate su IP con le informazioni voce trasmesse. I Media Stream Channel contengono una combinazione di supporti audio, video e T.120.

DTMF (Dual Tone Multiple Frequency)

La selezione DTMF (a toni) è il tipo di selezione della telefonia analogica e risulta oggi predominante nella tecnica di trasmissione dei numeri sulle reti telefoniche.

MIM (Invio messaggi immediato mobile)

MIM è un servizio presenza/invio messaggi immediato per i telefoni mobili.

Mobilità

Per "mobilità" si intende l'utilizzo di Pocket-PC e telefoni mobili, nonché la loro integrazione nel sistema di comunicazione di un'azienda.

MOH (Music on Hold)

È possibile riprodurre una musica di attesa (MOH, Music on Hold) per gli utenti quando non possono essere connessi immediatamente con la destinazione.

MSN (Multiple Subscriber Number)

Collegando telefoni ISDN tramite un bus S0 (Connessione punto - multipunto) ciascun telefono ISDN (utente ISDN) viene assegnato a un Multiple Subscriber Number (MSN) univoco. Gli utenti ISDN sono raggiungibili tramite il loro MSN.

MULAP (Multiple Line Appearance)

I MULAP sono gruppi specifici in cui più telefoni vengono riuniti. Un membro del gruppo può essere assegnato a vari telefoni sotto un solo numero (Basic MULAP).. Inoltre è possibile definire per alcuni gruppi speciali servizi utilizzabili per la comunicazione fra dirigenti e segretarie o nel team (Direttore MULAP, Team MULAP).

Gateway multiplo

In caso di collegamento in rete a gateway multiplo, le chiamate vengono istradate tramite più gateway.

myAttendant

myAttendant è la console del sistema di comunicazione.

myPortal

myPortal è il portale utenti basato su Java che consente l'accesso alle funzioni di comunicazione unificata. Oltre alle informazioni sullo stato di presenza e a comodi ausili per la selezione come le liste dei preferiti e la rubrica, l'utente ha accesso, ad es., ai messaggi vocali e ai fax.

myPortal per Outlook

myPortal for Outlook è il portale utente integrato in Microsoft Outlook per l'accesso degli utenti alle funzioni di comunicazione unificata (Unified Communications), analogo a myPortal. Inoltre offre la comoda funzione Dialer sul desktop.

NAC (Network Admission Control)

NAC è una tecnologia che protegge dagli attacchi di virus e worm sulla rete. Con NAC, durante l'autenticazione, i terminali verificano anche la conformità alle regole. Se ad esempio il programma antivirus non è aggiornato o se nel sistema operativo del client manca la più recente patch di sicurezza, tale terminale viene messo in quarantena e fornito degli aggiornamenti necessari fino a quando non viene ripristinata la conformità alle regole.

NAT, Network Address Translation

NAT è una procedura che consente di sostituire un indirizzo IP in un pacchetto dati con un altro. Viene utilizzata per rappresentare indirizzi IP privati come indirizzi IP pubblici. Il masking o PAT (Port Address Translation) si applica quando anche i numeri di porta vengono riscritti.

NTBA (Network Termination for ISDN Basic Access)

NTBA (Network Termination for ISDN Basic Access), noto anche come NT (Network Termination), è il dispositivo di terminazione per l'accesso base ISDN. Si tratta della porzione di congiunzione fra la rete digitale del gestore e i dispositivi ISDN sul lato dell'utente.

NTPM (Network Termination for Primary Rate Multiplex Access)

NTPM (Network Termination for Primary Rate Multiplex Access) è il dispositivo di terminazione per l'accesso multiplex ISDN principale. Si tratta della porzione di congiunzione fra la rete digitale del gestore e i dispositivi ISDN sul lato dell'utente.

OLSR

OLSR è uno specifico protocollo Ad-hoc che consente di ottimizzare le capacità mancanti di routing OSI Livello 2 su OSI Livello 3.

ONS (One Number Service)

Numero di telefono assegnato direttamente a un utente. A un utente possono essere assegnate più risorse (telefoni). Se l'utente viene chiamato con il numero ONS, la chiamata viene inoltrata al telefono attualmente utilizzato dall'utente (ad esempio un telefono cellulare).

PAP (Password Authentication Protocol)

PAP è una procedura per l'autenticazione sul protocollo Point-to-Point. Viene utilizzata per l'accesso a un ISP. Nella procedura PAP la password per l'autenticazione viene trasmessa in formato testo insieme a un ID utente.

PBX (Public Branch Exchange)

Un PBX (impianto telefonico) è un dispositivo di trasmissione che collega più terminali (ad es. telefoni, fax, segreterie telefoniche) fra loro e alla rete telefonica pubblica.

Peer

Con peer si intende il terminale di comunicazione in una rete Peer-to-Peer. Ciascun peer mette a disposizione i propri servizi e utilizza quelli dell'altro peer.

Peer-to-Peer

In una rete peer to peer, tutti i PC dispongono degli stessi diritti e possono pertanto utilizzare e usufruire dei servizi sulla rete.

Autenticazione istanza peer

L'autenticazione dell'istanza peer in una connessione garantisce che questa corrisponda ai requisiti.

PKI (Public Key Infrastructure)

Con PKI si identifica un sistema di crittografia e crittologia che consente di emettere, distribuire e verificare certificati digitali. I certificati emessi nell'ambito di un PKI vengono utilizzati per la protezione delle comunicazioni via computer.

PPP (Point to Point Protocol)

Il PPP è lo standard IETF per la trasmissione di pacchetti IP su collegamenti seriali. PPP viene utilizzato principalmente per l'accesso a Internet.

PPPoE (Point-to-Point Protocol over Ethernet)

Il protocollo PPPoE (PPP over Ethernet) è l'applicazione del protocollo di rete Point-to-Point su una connessione Ethernet

Chiave precondivisa

Si tratta di una chiave che viene definita durante la configurazione del tunnel VPN. Poiché i partner VPN che comunicano tramite tunnel possono autenticarsi, per entrambi i terminali del tunnel è necessario utilizzare la stessa chiave.

PPTP (Point-to-Point Tunneling Protocol)

PPTP è una tecnologia che può essere configurata con una rete privata virtuale (VPN). Poiché Internet fondamentalmente è una rete aperta, grazie a PPTP si garantisce che i messaggi trasmessi da un nodo VPN a un altro siano protetti. Con PPTP gli utenti possono accedere alla rete aziendale tramite Internet.

Presenza

Il termine "presenza" indica la capacità dei sistemi di comunicazione unificata di stabilire la posizione e lo stato dell'utente in qualsiasi momento. In questo modo è possibile comunicare con l'utente tramite telefono, posta elettronica, invio messaggi immediato o fax, come desiderato.

Server Proxy

Il server proxy è l'elemento di congiunzione tra un'applicazione client e il server Web. Il suo compito è filtrare le richieste delle applicazioni client e alleggerire il carico del server Web.

PSTN (Public Switched Telephone Network)

PSTN rappresenta una rete telefonica pubblica via cavo. Le reti pubbliche possono essere fornite da enti sia privati che pubblici.

QOS (Quality of Service)

Per il Voice over IP è importante garantire una larghezza di banda minima per la durata della trasmissione. Se più applicazioni con gli stessi diritti stanno utilizzando l'IP, la larghezza di banda disponibile per la trasmissione viene suddivisa. In questo caso una connessione voce può evidenziare la perdita di pacchetti e, di conseguenza, una ridotta qualità. Esistono varie procedure per garantire la massima qualità di trasmissione; questa procedura viene definita Quality of Service (QoS).

RAS (Remote Access Service)

Un utente RAS è un utente IP (ad es. un collaboratore in remoto) che accede al sistema in remoto e si comporta come un utente IP interno. In questo modo può utilizzare la gamma completa di servizi del sistema di comunicazione.

RJ45 (Registered Jack 45)

RJ45 è un connettore a otto poli utilizzato ad esempio per la connessione di cavi 10BaseT in un ambiente di rete.

Roaming

Il roaming è la capacità dei terminali di una rete mobile connessi a una rete di un paese straniero di poter telefonare o accedere ai servizi di telefonia mobile come se fossero nel proprio paese di origine.

RTCP (Real Time Control Protocol)

Il Real Time Control Protocol (RTCP) provvede alla gestione e assicura la conformità ai parametri QoS (Quality of Service) mediante scambi periodici di messaggi di controllo tra mittente e destinatario.

RTP (Real-Time Transport Protocol)

RTP è lo standard IETF per lo streaming di dati multimediali in tempo reale tramite il protocollo IP. RTP si basa di norma sul protocollo UDP e utilizza porte UDP dinamiche, che negoziano specifici flussi multimediali fra mittente e destinatario.

RTT (Round Trip Time)

RTT è l'intervallo di tempo richiesto da un pacchetto dati per passare dall'origine alla destinazione.

SA (Security Association)

SA (connessione di sicurezza) è un accordo fra due entità comunicanti in una rete informatica. Descrive come entrambe le parti possano utilizzare i servizi di protezione per poter comunicare fra loro.

SDSL (Symmetric Digital Subscriber Line)

SDSL è particolarmente adeguato per la telefonia Internet, le applicazioni Internet in aziende con rete locale, le videoconferenze e, ad esempio, per il telelavoro grazie all'invio e alla ricezione con la stessa larghezza di banda. A differenza dell'ADSL le larghezze di banda di SDSL presentano quindi la stessa ampiezza su Internet.

Secure CLI

Secure CLI è una funzione di sicurezza che offre un'interfaccia per riga di comando e per il trasferimento di dati tramite SFTP (Secure File Transfer Protocol).

SFTP (Secure File Transfer Protocol)

SFTP è un protocollo di sicurezza per la trasmissione di record di dati di connessione.

Client VPN ShrewSoft

Il client VPN ShrewSoft è un client VPN open source e gratuito con interfaccia grafica. Include tra l'altro ISAKMP, il supporto per Xauth e RSA, AES, Blowfish e protocolli di crittografia 3DES.

Gateway singolo

In caso di collegamento in rete a gateway singolo, tutte le chiamate vengono istradate tramite un solo gateway.

SIP (Session Initiation Protocol)

SIP è un protocollo Internet standard secondo RFC 3261 per l'istaurazione e il controllo di connessioni voce e videoconferenze tramite una rete IP.

SNMP (Simple Network Management Protocol)

SNMP è una procedura per ottenere informazioni sullo stato dei componenti di rete e PC.

SPE (Crittografia segnalazione e payload)

La crittografia segnalazione e payload (SPE) serve a garantire la sicurezza della trasmissione di dati voce. Vengono crittografati i flussi di dati d'uso e di segnalazione VoIP da e al gateway e tra telefoni IP.

SRTP (Secure Real-Time Transport Protocol)

SRTP è un protocollo RTP crittografato. È particolarmente adatto per la trasmissione di dati di comunicazione tramite Internet ed è principalmente utilizzato in applicazioni di telefonia basate sul protocollo IP.

SSH (Secure Shell)

SSH è un protocollo che supporta l'accesso remoto, il trasferimento dati e la connessione TCP/IP protetta. È possibile crittografare, autenticare e comprimere automaticamente i dati trasmessi.

SSL (Secure Socket Layer)

SSL è un protocollo per la trasmissione di documenti via Internet. Con SSL i dati vengono crittografati con chiavi private prima di essere trasmessi. Gli URL che richiedono una connessione SSL iniziano con https: anziché con http:.

Stato

Insieme alla "presenza", indica lo stato di un utente (disponibile, occupato, non in linea, ecc.), in modo che un altro utente nel sistema di comunicazione possa sapere se l'utente desiderato è raggiungibile.

STUN (Simple Traversal of UDP over NAT)

STUN è un protocollo di rete che consente di rilevare la presenza, identificare e bypassare il firewall e il router NAT.

Funzione survivability

La funzione survivability è la capacità di un sistema di reti di mantenere il servizio anche in presenza di errori nella rete.

TAE (Telekommunikations-Anschluss-Einheit, unità colleg. telecom.)

TAE è un tipo di connessione analogica telefonica con interfaccia a/b e connessioni ISDN per collegare l'NTBA alla linea. Si possono collegare telefoni analogici, fax e telefoni ISDN.

TCP (Transmission Control Protocol)

TCP è un protocollo che definisce quali dati verranno scambiati tra i PC e in che modo. Tutti i sistemi operativi dei PC moderni supportano TCP e lo utilizzano per lo scambio dei dati con altri PC.

TFTP (Trivial File Transfer Protocol)

TFTP è un protocollo di trasmissione dei dati che supporta la lettura o la scrittura di file. Molte delle funzioni dei protocolli FTP di livello più alto non sono disponibili nel TFTP, ad esempio l'assegnazione di diritti, la visualizzazione dei file esistenti o l'identificazione dell'utente.

Telnet

Un protocollo che collega due PC per stabilire una connessione terminale al PC remoto. L'utente non si registra nel PC, la connessione avviene tramite Internet/Telnet. L'utente avvia la sessione Telnet, stabilisce al connessione all'host Telnet e accede. Tramite la connessione l'utente è in grado di utilizzare il PC remoto e il suo sistema viene visualizzato su quel PC come un terminale locale collegato.

TOS (Type of Service)

TOS è un campo nell'intestazione di pacchetti di dati che viene utilizzato per l'assegnazione e la valutazione della priorità dei pacchetti stessi (ad esempio per la funzione Quality of Service).

UCD (Uniform Call Distribution)

UCD consente la distribuzione uniforme a un gruppo di utenti (gruppo UCD) delle chiamate in arrivo nel sistema di comunicazione.

UDP, User Datagram Protocol

UDP è un protocollo di rete appartenente allo stato di trasporto della famiglia IP. UDP è responsabile per l'instradamento dei dati alle applicazioni corrette tramite Internet.

UMTS (Universal Mobile Telecommunications System)

UMTS è uno standard per reti di telefonia mobile di terza generazione con una velocità di trasmissione dati decisamente superiore (384 Kbit/s a 7,2 Mbit/sec), rispetto agli standard di seconda generazione o allo standard GSM.

Comunicazione unificata

Unified Communications consente l'integrazione di diversi sistemi, mezzi, dispositivi e applicazioni di comunicazione in un ambiente (ad es. telefonia IP, telefonia fissa e mobile, posta elettronica, invio messaggi immediato, applicazioni desktop, casella vocale, fax, conferenze e Unified Messaging).

Unified Messaging

Unified Messaging consente l'integrazione di diversi flussi di dati di comunicazione, quali posta elettronica, SMS, fax, telefonia, ecc. in una sola memoria messaggi. Questa memoria messaggi è accessibile da numerosi dispositivi esterni di diverso tipo.

VAD (Voice Activity Detection)

VAD (Voice Activity Detection) indica un riconoscimento automatico delle pause della voce nella trasmissione digitale dei dati audio.

Interfaccia VCAPI

VCAPI è un'interfaccia CAPI virtuale che emula la presenza di una scheda ISDN locale. Se in un PC della rete interna è presente una scheda ISDN, tutti gli utenti della rete possono usufruire di questa scheda ISDN tramite l'interfaccia VCAPI.

VDSL (Very High Speed Digital Subscriber Line)

VDSL deve essere introdotta se occorre trasmettere grandi flussi di dati, simmetrici o asimmetrici, rapidamente a breve distanza. VDSL rappresenta un'alternativa ad ADSL ed SDSL, che presenta una velocità di trasmissione superiore.

VoIP (Voice over IP)

VoIP consente la trasmissione di dati voce su reti IP.

VPN (Virtual Private Network)

VPN offre l'infrastruttura pubblica di Internet per il collegamento di siti e l'accesso di operatori remoti. I sistemi di crittografia e autenticazione consentono un accesso sicuro alla rete dati interna da parte degli utenti esterni.

WAN (Wide Area Network)

WAN è l'abbreviazione utilizzata in riferimento a una rete geografica, ad esempio, Internet.

WBM (Web Based Management)

WBM è un'interfaccia utente che viene visualizzata in un browser Internet tramite pagine HTML o JAVA e un protocollo Web.

Standard X.509 (certificato VPN)

X.509 è uno standard per un'infrastruttura PKI e al momento lo standard più importante per i certificati digitali.

XMPP (Extensible Messaging and Presence Protocol)

Standard Internet utilizzato principalmente per i messaggi istantanei. XMPP supporta l'interazione con utenti di altre reti quali, ad esempio, AIM, ICQ o Windows Live Messenger (WLM). XMPP e le relative ottimizzazioni supportano tra l'altro le conferenze con molteplici utenti (ad es. Multi User Chat) e la visualizzazione dello stato online.

Secondo grado

Secondo grado significa che un utente effettua una chiamata mentre ha già una seconda chiamata in attesa.

Indice analitico

A

Abilitazione alla linea urbana 752
  aggiungere un numero di telefono alla lista dei numeri permessi 756
  aggiungere un numero di telefono alla lista dei numeri vietati 757
  configurare 755, 756, 761, 763, 763
  modifica del filtro lista nr. vietati 758
  visualizzazione delle liste di numeri permessi 757
  visualizzazione delle liste di numeri vietati 757
Abilitazioni, Modalità esperti 1608, 1697
Accesso a distanza al sistema di comunicazione 1362
Accesso a Internet 364
  configurazione 365
  configurazione tramite ISP pre-configurato 371
  configurazione tramite un ISP PPPoE standard 374
  configurazione tramite un ISP standard PPTP 376
  tramite modem Internet esterno 370
  tramite router esterno 366
accesso mobile 960
Accesso remoto 1362
  attiva, tramite Internet con indirizzo IP fisso 206, 208, 208, 209, 257, 259, 259, 260, 1366
  attivare, tramite Internet senza indirizzo IP fisso 1367
  attivazione, tramite ISDN 1363
  configurazione PC 1364
  configurazione PC con Windows 7 1365
  disattiva 1368
accesso utente mobile 960
Accetta accesso in scrittura, Modalità esperti 1510
Addebiti - Coefficienti, Modalità esperti 1546
Addebiti - Formato di output, Modalità esperti 1545
Addebiti chiamata - Codici di addebito, Modalità esperti 1547
Agente relè DHCP:configurazione 349
Agenti UCD, Modalità esperti 1717
aggiornamenti automatici 541
aggiornamenti software 1246
aggiornamento 1246
Aggiornamento
  personalizzato 1255
Aggiornamento della licenza 334
aggiornamento software (vedere aggiornamento) 1246
Aggiornamento tramite Carica file, Modalità esperti 1479
Aggiornamento tramite chiave USB, Modalità esperti 1479
Aggiornamento via Internet, Modalità esperti 1478
aggiornamento, completo
  avvio in background 1253
Aggiornamento, completo
  avvio con visualizzazione dello stato di avanzamento 1251, 1260
Altoparlante 439
ambiente elettrico
  OpenScape Business S 84
  OpenScape Business UC Booster Server 84
Ambienti Terminal Server/Citrix Server 532
annunci di stato casella vocale 599
Annunci nella distribuzione delle chiamate 749
annunci per la casella vocale 599
Apparecchio porta/Apriporta 1149
Apparecchio, profilo 469
Application Launcher 1187, 1757
  profilo per i dati di configurazione 1188
Application Launcher, Modalità esperti 1756
Applicazione UC
  riavvio 1266, 1266
Applicazioni, Modalità esperti 1721
Applicazioni, Modalità Esperto 1757
Appuntamento 672
Argomenti, tipi 72
Arresto
  PIN per l'attivazione 1264
Arresto del sistema di comunicazione 1263
Arresto di OpenScape Business X 1263
Ascolto chiamate, Modalità esperti 1492
Assegna MSN, Modalità esperti 1696
Assegnazione delle chiamate 656
Assegnazione gruppi VBZ, Modalità esperti 1701
attiva licenze 308
Attivazione / Disattivazione del tono di conferenza 654, 655
attivazione del software 1246
Attivazione licenza 318
autenticazione
  partecipante alla conferenza 516
AutoAttendant 598
Avvertimento 74
  avviso 77
Avviso
  messaggi fax 611
  messaggi vocali 528, 611
Avviso di chiamata in attesa/Segnalazione della chiamata 661
Azione automatica 1273
  arresta notifica DLS 1277
  arresto Garbage Collection 1275
  attiva Garbage Collection 1275
  attiva notifica DLS 759, 760, 761, 1276, 1279, 1279, 1281
  Garbage Collection 1273
  modifica Garbage Collection 1274
  modifica notifica DLS 1276
  notifica DLS 1275
Azione manuale 1302
Azioni
  Azioni automatiche, Modalità esperti 1508, 1508
  Azioni manuali, Modalità esperti 1506

Azioni, Modalità esperti 1506

B

Backup - immediato 1243
Backup (vedi Salvataggio) 1238
Backup dei dati (vedi Salvataggio) 1238
Basic MULAP
  aggiunga un membro 727
  aggiungere 725
  aggiungi 730
  cancella 727
  cancella un membro 727
  modifica 726
  modifica un membro 728
  visualizza 726
Blocco del telefono 770
Blocco servizi (solo LX) 993
Branding, Modalità esperti 1477

C

CA Lightweight 1009
CA Lightweight, Modalità esperti 1560
Cablaggio per interfacce LAN e WAN 85
CallMe 554
capacità della casella vocale 599
Carica file, Modalità esperti 1743
Carica nel gateway, Modalità esperti 1472
caricamento sul gateway, modalità Esperto 1473
Carrier Select Override 773
casella fax 606
casella vocale 599, 599
  rispondere alla chiamata 599
Casella vocale (UC Smart) 521
casella voicemail, vedere casella vocale 599
CDP (Certificate Distribution Point) 1030
Certificati attivi, Modalità esperti 1561
Certificati CA SPE, Modalità esperti 1559
Certificati configurati, Modalità esperti 1563
Certificati Peer, Modalità esperti 1563
Certificati server, Modalità esperti 1577
Certificati VPN
  generazione certificati CA Lightweight 1010
  generazione richiesta di certificato 1012, 1013
  importazione 1013
  importazione certificato CA attendibile 1012
  visualizzazione 1011
Certificato autorità di certificazione DLSC, Modalità esperti 1557
Certificato client DLSC, Modalità esperti 1555
Certificato Secure Trace, Modalità esperti 1490
Certificato SPE, Modalità esperti 1559
chiamata
  persa 578
  pianificata 578
Chiamata altoparlante discreta) 646
chiamata di gruppo 680
  casella vocale 681
  di tipo Avviso di chiamata in attesa, aggiungere 697
  di tipo Gruppo, aggiungere 689
  di tipo libero, aggiungere 698
  DND per i membri del gruppo 681
  Telefoni SIP 683
  tipo chiam. 683
Chiamata di gruppo
  attiva il rifiuto dell'avviso di chiamata per i membri del gruppo 700
  cancella tipo gruppo 691
  cancellazione tipo avviso di chiamata in attesa 699
  cancellazione tipo libero 699
  disattiva il rifiuto dell'avviso di chiamata per i membri del gruppo 700
  modifica del tipo avviso di chiamata in attesa 698
  modifica del tipo libero 698
  modifica tipo gruppo 690
  tipo avviso di chiamata in attesa, aggiungi membro 699
  tipo avviso di chiamata in attesa, cancella membro 699
  tipo gruppo, aggiungi membro 692
  tipo gruppo, cancella membro 692
  tipo libero, aggiungi membro 699
  tipo libero, cancella membro 699
  visualizzazione del tipo avviso di chiamata in attesa 698
  visualizzazione del tipo libero 698
Chiamata diretta 633
Chiamata diretta per gruppi 737
Chiamata in preselezione 625
Chiamate di emergenza
  requisiti 811
Chiamate in entrata
  Gruppi/Gruppi di ricerca, modalità Esperto 1669
  Inoltri, Modalità esperti 1681
  Membri Gruppi, Modalità esperti 1673
  Risposta per assente, Modalità esperti 1678
  Team/Top, Modalità esperti 1675
  UCD, Modalità esperti 1678
Chiamate in entrata, Modalità esperti 1669
Chiave elettronica singola 770
Chiavi precondivise 1008
circuito di alimentazione e collegamento
  OpenScape Business S 84
  OpenScape Business UC Booster Server 84
Classi di autorizzazione
  Assegnazione gruppi VBZ, Modalità esperti 1701
  Giorni speciali, Modalità esperti 1704
  Giorno: Gruppi di abilitazione, Modalità esperti 1698
  Liste nr. permessi, Modalità esperti 1699
  Liste nr.vietati, Modalità esperti 1700, 1700
  Matrice VBZ, Modalità esperti 1702
  Notte: Gruppi di abilitazione, Modalità esperti 1698
  Servizio notte auto, Modalità esperti 1703
  Servizio notturno, Modalità esperti 1701
Classi di priorità 428

Classi di servizio
Utenti, Modalità esperti 1697
Classi di Servizio, Modalità esperti 1604
Client (UC Smart) 485
Client (UC Suite) 532
Client di distribuzione e licenze (DLSC), Modalità esperti 1555
Client di sistema 431
Client IP (vedi Utente IP) 431
Client IP, Modalità esperti 1663
Client IP, modalità Esperto 1637
Client NCP
attivare, disattivare 1018
preparare 1017
Client PC 108
Client SIP 431
Client UC Smart 485
Client UC Suite 532
Client, requisiti hardware e software 535, 843, 867, 871
CLIP - Trasmissione del numero di telefono del chiamante 636
CLIP no screening 640
CLIR - Disattivazione della visualizzazione del numero di telefono del chiamante 637
CMD (CSTA Message Dispatcher) 1757
Codec audio 425
assegnare i parametri a una destinazione 426
configurare i parametri 425
Codice di autorizzazione per la licenza (LAC) 308, 318
codici di servizio, modalità esperti 1537, 1537
Collegamento in rete
eterogenea, ibrida 1046
COLP - Presentazione dell'identificazione delle linee connesse 639
COLR - Disattivazione della visualizzazione del numero di telefono del chiamato 639
Combinazioni di tasti per dialer sul desktop 580
componente di traccia
modifica 1324
Componente di traccia 1311
arrestare 1323
arresto di tutti i componenti 1324
avviare 1323
modifica 1324
visualizza 1322
visualizzare dettagli 1323
Componente di traccia M5T
arresta 1317
avvia 1317
modifica 1317
visualizza 1317
Componente di traccia M5T, Modalità esperti 1489
Componente traccia M5T 1307
Componenti di traccia, Modalità esperti 1495
Comportamento nelle emergenze 82, 82
Composizione a cifre 625
Comunità di lettura, Modalità esperti 1504
Comunità di scrittura, Modalità esperti 1504
Comunità trap, Modalità esperti 1504
Comunità, Modalità esperti 1503
Concetti 72
Condivisione desk 960
condizione
inoltro di chiamata basato su regole 555
Condizioni di servizio (climatiche, meccaniche)
OpenScape Business S 90
OpenScape Business UC Booster Server 90
OpenScape Business X3, X5, X8 89
conferenza 516, 592, 592
Conferenza 583
AdHoc 589
aperta 593
autenticazione 583
controllo da applicazione 583
controllo tramite telefono 583
invita per appuntamento di Outlook 583
invita tramite e-mail 583
numero di accesso 583
partecipante 583
pianificata 590
prolungamento 583
registrazione 583
sala conferenze virtuale 583
supervisore conferenza 583
tipi di conferenze 583
tono di conferenza 583
utente Mobility Entry 583, 589, 590, 593
Conferenza (UC Suite) 583
conferenza AdHoc 516
Conferenza AdHoc 589
Conferenza aperta 593
conferenza controllata da applicazioni 516
Conferenza controllata da applicazioni 584
Conferenza controllata telefonicamente 584
Conferenza in corso, Modalità esperti 1744
conferenza permanente 516, 592
conferenza pianificata 516
Conferenza pianificata 590, 590
conferenza, controllo tramite telefono 516
conferenze 592
configurazione
annunci, modalità esperto 1473
Indirizzo IP del gateway, Modalità esperti 1477
SmartVM, Modalità esperti 1474, 1474, 1475
Configurazione
Branding, Modalità esperti 1477
Configurazione porta, Modalità esperti 1473
Musica su attesa (MoH), Modalità esperti 1472
Configurazione dell'hardware OpenScape Office MX
visualizza 479
Configurazione dell'inoltro chiamate 523, 651
Configurazione della linea esterna ISDN 403
Configurazione di canali DSP 1766
Configurazione Direttore/Segretaria 705
aggiungere 712

aggiungere un membro 718
aggiungere una casella fax 719
cancellare 714
casella fax 707
elimina un membro 718
modifica delle proprietà di un membro 719
modifica un membro 718
modificare 713
Telefoni SIP 708
tipo chiam. 707
Configurazione eventi, Modalità esperti 1499
Configurazione formato traccia, Modalità esperti 1486
Configurazione porta, Modalità esperti 1473
Configurazione provider esterni, Modalità esperti 1731
Configurazione team 701
aggiungere 709
aggiungere una casella fax 717
aggiungi membro 715
cancella membro 715
casella fax 703
modifica delle proprietà di un membro 716
modifica l'assegnazione tasti sul telefono 717
modifica un membro 716
modificare 711
tipo chiam. 703
Configurazione Team
cancellare 712
Configurazione, Modalità esperti 1472, 1505
Conformità
norme canadesi 88
norme internazionali 89
Conformità CE 88
Connessione a banda larga 364
Connessione al CLA centrale;CLA
connessione centralizzata 337
Connessione al CLA locale;CLA
connessione locale 326, 327, 337
connessione al sistema 1188
Connessione LDAP 1188
Connessione via cavo 364
Contact Center 830, 831, 831, 831, 865, 881, 882, 882, 882
:eliminazione di un agente dalla coda di attesa 937
add a break 932
add a queue 922
agente 874
agenti preferiti 875
aggiungere una pianificazione 916
assegnazione dell'agente alla coda d'attesa 936
attivazione della coda di attesa 928
client 865
coda d'attesa 879
condizioni per l'uso 938
configurazione del gruppo UCD 913
configurazione di un utente come agente 914
define preferred agents 931
definizione del valore soglia per il livello di servizio 929
definizione priorità del chiamante VIP 930
delete a break 933
disattivazione della coda di attesa 928
display a parete 892
download rule 922, 922
edit a queue 926
elaborazione 891
elaborazione multipla, aggiunta del motivo per l'elaborazione 934
elaborazione multipla, eliminazione del motivo per l'elaborazione 936
elaborazione multipla, modifica del motivo per l'elaborazione 935
elaborazione semplice, aggiunta motivo per l'elaborazione 933
elaborazione semplice, modifica del motivo per l'elaborazione 934
elenco chiamate VIP 893
eliminare una pianificazione 921
eliminazione dell'agente preferito 932
grado di servizio 892
limitazioni dei servizi del sistema 939
livelli di autorizzazione di un agente 874
livello di autorizzazione di un agente 874
load announcement 915
modelli di rapporti predefiniti 943
modifica dell'elenco chiamate VIP 930
modifica di una pausa 933
modificare una pianificazione 919
motivo dell'elaborazione 891
myAgent 866
myReports 869
myReports user roles 869
pausa 876
print rule 921, 922, 922
priorità chiamante VIP 893
procedura di configurazione 913
rapporti 942
record announcement 915
richiamata agente 892
save rule as PDF file 921
simple wrapup, delete wrapup reason 934
soluzione secondaria 894
uso di telefoni DECT 941
visualizzazione dei dettagli coda 892
Contact Center, Modalità esperti 1733
Contact Center: Esempio per la configurazione di un Contact Center 897
Contact Center:Configurazione 897
Contact Center:configurazione di un pilota per i fax di arrivo 929
contatto 577
Convenzioni di visualizzazione/rappresentazione 73
Conversione dei numeri in nomi 641
Cordless
Multi-SLC, Modalità esperti 1668
Per tutto il sistema, Modalità esperti 1665
SLC, Modalità esperti 1667

Stazione base, Modalità esperti 1668
Corporate Network 782
Cover Page Editor 608
Creazione certificati, Modalità esperti 1576
Crittografia segnalazione e payload (SPE) 993
attivazione del supporto SPE 995
disattivazione del supporto SPE 995
Crittografia segnalazione e payload (SPE), Modalità esperti 1558
CRL (Certificate Revocation List) 1010, 1030
CSP (Csta Service Provider) 1758
Csta Message Dispatcher (CMD) 1757

D

Da e-mail a SMS 613
Daemon RPCAP 1328
attivare 1329
disattivare 1329
Daemon RPCAP, Modalità esperti 1497
Data e Ora, Modalità esperti 1542
Dati del registro Admin, Modalità esperti 1505
Dati di configurazione 1238
dati di configurazione per funzioni diagnostiche 1336
genera 1337
Dati prestazionali 1433
Dati utente
importazione 423
Destinazioni di selezione breve, Modalità esperti 1535, 1756
Deviazione chiamata a tempo 655
Deviazione di chiamata 653
in base allo stato 554
Diagnosi IP
Scheda madre, Modalità esperti 1510, 1511, 1511
Diagnosi IP, Modalità esperti 1510
Diagnostica applicazione
Impostazioni sviluppatore, Modalità esperti 1509, 1510
Scheda madre, Modalità esperti 1510
Diagnostica applicazione, Modalità esperti 1509
Diagnostica piattaforma, Modalità esperti 1509
Dial In Control Server 782
Dialer degli appunti 580
dialer sul desktop 533
Dialer sul desktop 580
diario
tempo di conservazione 578
Diario (UC Smart) 514
diario (UC Suite) 578
Differimento delle chiamate in entrata 659
Directory di backup 1239
Direttore MULAP 723
aggiungere 728
aggiungere un membro 729
cancella 729
cancella un membro 730
modifica 729
modifica un membro 730
Telefoni SIP 724
tipo chiam. 724
visualizzazione 729
Direttore/Segretaria (vedere Configurazione Direttore/Segretaria) 705
DISA, Modalità esperti 1529
Disattivazione della visualizzazione del numero di telefono del chiamante - CLIR 637
Disattivazione della visualizzazione del numero di telefono del chiamato - COLR 639
Display, Modalità esperti 1526
Distribuzione delle chiamate
accettazione automatica chiamate UCD 745
accettazione automatica chiamate UCD, disattiva 745
accettazione automatica chiamate UCD; attiva 745
agente UCD 741
aggiunta agente UCD 743
AICC (Automatic Incoming Call Connection) 745
annunci 749
cancellazione agente UCD 743
coda d'attesa 746
configurazione 739
gruppo UCD 739
modifica annunci 749
modifica coda d'attesa 746
modifica del tempo di post-elaborazione 744
modifica la musica (musica su attesa, MoH) 750
modifica overflow 748
modifica priorità chiamate esterne 745
modifica priorità chiamate interne 745
overflow 747
priorità chiamate esterne 744
priorità chiamate interne 744
rilascio di chiamate UCD su linee analogiche 751
rilascio di chiamate UCD su linee analogiche, modifica tempo di rilascio 751
servizio notturno 748
stato utente 741
tempo di post-elaborazione 743
trasferimento a gruppo UCD 750
trasferimento a gruppo UCD, modifica tempo di attesa/ripresa 750
Distribuzione delle chiamate (UCD) 739, 739
configura 740
configurazione di gruppi UCD 740
DNS (Domain Name Service)
definire il server 356
download (vedere aggiornamento) 1246
DSL (Digital Subscriber Line) 364
DynDNS 355
DynDNS (Dynamic Domain Name Service) 378

E

e-mail
invito alla conferenza 516

E-mail
avviso 528, 611
E-mail, Modalità esperti 1499
eccezione
inoltro di chiamata basato su regole 555
Editor regole 831, 882
Editor tabelle NAT 989
elenco dei Preferiti 577
Elenco dei Preferiti
messaggio istantaneo 519
Elenco dei Preferiti (UC Smart) 507
Elenco sedi, Modalità esperti 1744
Emissione di interferenze 87
Esegui traceroute, Modalità esperti 1511
Estensioni selezione passante, Modalità esperti 1660
Eventi
Configurazione eventi, Modalità esperti 1499
E-mail, Modalità esperti 1499
Registri di diagnostica, Modalità esperti 1501
Registro eventi, Modalità esperti 1499
segnalazione allarmi, Modalità esperti 1501
Tabella delle reazioni, Modalità esperti 1500
Eventi, Modalità esperti 1498
evento 1329, 1330, 1330, 1331, 1331
modifica impostazioni e-mail 1333
Evento
cancellazione registro 1332
modifica delle impostazioni di reazione a più eventi 1334
modifica delle impostazioni di reazione agli eventi 1333
modificare la registrazione eventi tramite LAN 1332
scaricamento del protocollo 1332
visualizzazione della tabella delle reazioni 1333
EVM, Modalità esperti 1645

F

Fasci 401, 407
assegnazione del codice 411
assegnazione nomi 411
configura il tipo di numero in uscita 413
configurazione del fascio di overflow 411
configurazione del tipo di numero di telefono 413
inserimento del numero di telefono del sistema 412
inserimento del prefisso in entrata 409, 413
inserimento del secondo codice di linea 414
FastViewer 518, 593, 594
fax 599
Fax
T.38 615
Fax di gruppo 3 439
Fax di gruppo 4 436
Fax Printer 533, 608
Fax T.38 615
file audio 1234
File audio 1231
File CSV 421
file di licenza 308
File di licenza 318
file di registro 1330
file immagine 1247
File PDF
avviso 611
messaggio fax 606
File TIFF
avviso 611
messaggio fax 606
File WAV
avviso 528, 611
file Wave 1234
File wave 1231
firewall 1188
Firewall 985
Firewall delle applicazioni, modalità Esperto 1553
Firma digitale 1008
Flag di sistema
numero chiamante in gruppi di risposta / gruppi di segnalazione chiamate / CFN / RNA 696
RPA alla richiamata 697, 1057
squillo di avviso in gruppi RPA 697
supporto SPE 995
Flag LCR, Modalità esperti 1603
Flag Sistema, Modalità esperti 1512
Flag utente
rifiuto chiamata su altoparlante Off 634
rifiuto dell'avviso di chiamata in attesa 700
Flex Call 669
Formato classico dei numeri di telefono 514
Formato dei numeri di telefono 514
Formato dei numeri di telefono selezionabile 514
Funzione direttore (vedere Configurazione Direttore/Segretaria) 705
Funzione segretaria (vedere Configurazione Direttore/Segretaria) 705
Funzione Team (vedere Configurazione team) 701
funzioni
myPortal 532
myPortal for Outlook 533
Funzioni
myPortal Smart 487

G

Garbage Collection, Modalità esperti 1508
Gateway vocale
Interconnessione SIP, modalità Esperto 1629
Gateway voce
Interconnessione SIP, Modalità esperti 1627
Parametri Codec di destinazione, Modalità esperti 1614
Parametri codec, Modalità esperti 1612
Parametri SIP, Modalità esperti 1609
Provider di servizi di telefonia Internet, Modalità esperto 1615
Servizi di rete, Modalità esperti 1626, 1627
Gateway voce, Modalità esperti 1609
Gateway, Modalità esperti 1538

Gestione basata sul Web 113
Gestione certificati, Modalità esperti 1561, 1577
gestione conferenze 516
Gestione conferenze 584
Gestione dei messaggi 857
Gestione della porta, Modalità esperti 1543
Gestione inventario 1267
Gestore di rete 782
Gestore di rete principale 782
Giorni speciali, Modalità esperti 1704
Giorno
  Gruppi di abilitazione, Modalità esperti 1698
Gruppi 678
Gruppi con restrizioni di traffico 767, 767
  assegnazione dei numeri di selezione breve del sistema 768
  assegnazione della linea 769
  assegnazione utenti 768
Gruppi, Modalità esperti 1728
Gruppi/Gruppi di ricerca, modalità Esperto 1669
Gruppo Casella fax 732
  add a member 737
  configura 735, 737
  delete a member 737
  modifica 736
  visualizzazione 736
Gruppo Casella vocale 732
  aggiungere 733
  aggiungere un membro 734
  cancella 734
  cancella un membro 734
  modifica 734
  modifica un membro 735
  visualizzazione 734
gruppo di ricerca 684
  casella vocale 685
  Telefoni SIP 687
  tipo chiam. 686
Gruppo di ricerca
  aggiungere 692
  aggiungi membro 695
  cancella membro 695
  cancellare 695
  modificare 694
Gruppo di risposta per assente 678
  aggiungi membro 688
  attivazione risposta per assente da richiamata 697, 1057
  attivazione tono di avviso 697
  attivazione visualizzazione nome del chiamante 696
  attivazione visualizzazione numero di telefono del chiamante 696
  cancella membro 689
  configura 688
  disattivazione risposta per assente da richiamata 697, 1057
  disattivazione tono di avviso 697
  disattivazione visualizzazione nome del chiamante 696
  disattivazione visualizzazione numero di telefono del chiamante 696
  risposta esterna a un gruppo di risposta per assente 679
  risposta per assente da richiamata 679
  telefoni SIP 679
  tono di avviso 679
  visualizzazione nome del chiamante 679
  visualizzazione numero di telefono del chiamante 679
Gruppo fax (vedere Gruppo Casella fax) 732
Gruppo segreteria telefonica (vedere gruppo Casella vocale) 732
Gruppo Team 701
  aggiungere 709
  aggiungere un membro 715
  aggiungere una casella fax 717
  cancella 712
  cancella un membro 715
  casella fax 703
  modifica 711
  modifica delle proprietà di un membro 716
  modificare l'assegnazione tasti sul telefono 717
  modificare un membro 716
  tipo chiam. 703
Gruppo Top 705
  aggiungere 712
  aggiungere un membro 718
  aggiungere una casella fax 719
  cancella 714
  cancella un membro 718
  casella fax 707
  modifica 713
  modifica delle proprietà di un membro 719
  modificare un membro 718
  Telefoni SIP 708
  tipo chiam. 707

H

Hot Desking 960
Hotline 812
Hotline a tempo 812

I

ICMP (Internet Control Message Protocol) 1287
IKE-SA 1008
Immagine del software
  Software di sistema, Modalità esperti 1478, 1479, 1479
Immagine del software, Modalità esperti 1477, 1482
Immagine telefono
  Carica, Modalità esperti 1480
  Distribuire per terminale, Modalità esperti 1481
  Distribuire, Modalità esperti 1480
Implementazione parametri telefoni, Modalità esperti 1548

Impostazioni di base 1512
Addebiti, Modalità esperti 1545, 1546, 1547
Classi di Servizio, Modalità esperti 1541
Data e Ora, Modalità esperti 1542, 1543, 1543
DynDNS, Modalità esperti 1540, 1541
Gateway, Modalità esperti 1537, 1538
Gestione della porta, Modalità esperti 1543
Implementazione parametri telefoni, Modalità esperti 1548
Player, Modalità esperti 1548
Risparmio energia, Modalità esperti 1551
Sistema, Modalità esperti 1520, 1526, 1529, 1530, 1533, 1535, 1535, 1535, 1537
Impostazioni di base, Modalità esperti 1512, 1755
Impostazioni di Secure Trace, Modalità esperti 1490
Impostazioni di SNTP, Modalità esperti 1543, 1543
impostazioni e-mail 1331
In attesa 641
Incidenti, segnalazione 82
Inclusione 663
Indirizzi IP 1268
visualizzazione elenco 1269
Indirizzi IP statici, modalità Esperto 1590
Indirizzo IP del gateway, Modalità esperti 1477
Inoltri, Modalità esperti 1681
inoltro di chiamata
basato su regole 555
Inoltro di chiamata a tempo 649
Inoltro di chiamata fisso 649
Inoltro di chiamata nella linea urbana 656
Inoltro di chiamata su occupato 650
Inoltro, Modalità esperti 1718
installazione 133, 218, 271
Interconnessione SIP, Modalità esperti 1627
Interfacce di output traccia, Modalità esperti 1487
Interfacce di rete
Scheda applicazioni, Modalità esperti 1593, 1593, 1594
Scheda madre, Modalità esperti 1579, 1584, 1586, 1586, 1587, 1592
Interfacce di rete, Modalità esperti 1579
Interfacce urbane 1587
Scheda madre, modalità Esperto 1580, 1589, 1590, 1592
Interfaccia Web Services 1172
Interfacciamenti
Musica su attesa, modalità Esperto 1704
SmartVM, Modalità esperti 1708
Interfacciamenti, Modalità esperti 1665
Interferenza radio 87
Internet Telephony Service Provider (ITSP) 179, 242, 381, 383
Intestazione ESP 999
Intestazione fax, Modalità esperti 1753
Inventario OpenScape Business S
interrogazione 1273
Inventario OpenScape Business X3/X5/X8
interrogazione 1271
Inventario OpenScape Office LX/HX
interrogazione 339, 339
Inventario OpenScape Office MX
controllo 338
inventario, OpenScape Business S 1271
inventario, OpenScape Business X 1270
Invio per e-mail 612
invito
conferenza 516
IP Mobility 960
Istruzioni di sicurezza 73
Istruzioni di sicurezza per Brasile 78
Istruzioni di sicurezza per Canada 81
Istruzioni di sicurezza per l'Australia 78
Istruzioni di sicurezza per USA. 78
Istruzioni operative 72
ITSP (Internet Telephony Service Provider) 381

J

Java 1188
Java Runtime Environment (JRE) 135, 219

K

Kernel Crash Data Service
avvio 1325
stop 1326

L

LAN 1 (WAN), modalità Esperto 1580
LAN 1, Modalità esperti 1593
LAN 2, Modalità esperti 1584, 1594
LAN 3 (Admin), Modalità esperti 1586
Larghezza di banda - LAN 1054
LCR
Abilitazioni, Modalità esperti 1604
Flag LCR, Modalità esperti 1603
Multisito, Modalità esperti 1608
Piano di composizione, Modalità esperti 1604
Regola di composizione, Modalità esperti 1606
Tabella delle rotte, Modalità esperti 1605
LCR (Least Cost Routing) 771
abilitazione 779
assegnazione/modifica dell'autorizzazione 779
funzionalità 771, 772
modifica il piano di composizione 776
modifica la tabella delle rotte 777
modifica le regole di composizione 781
piano di composizione 775
regole di composizione 779
tabella delle rotte 777
LDAP, Modalità esperti 1533
lettore di annunci 1757

Licenza
aggiornamento 335
attivazione tramite i file della licenza 310
visualizzazione informazioni 330, 339
Licenze 294
Attivare con il codice di autorizzazione della licenza 309, 1408
visualizzare le informazioni 328, 329, 329, 330
Limiti prestazionali 1433
Linea esterna
configurazione della linea esterna ISDN 403
Linea ISDN
impegno mirato 783
Linea privata 636
Linee 401
assegnazione MSN 406
configurazione del tipo di impegno 412, 415, 417
modifica del codice 405, 405, 405
modifica del fascio 410
modifica del protocollo 406, 406, 407
tipo di impegno 408
Linee, Modalità esperti 1684
Linee/Rete
Assegna MSN, Modalità esperti 1696
Linee, Modalità esperti 1684
Parametri ISDN, Modalità esperti 1696
Servizi QSIG, Modalità esperti 1695
Linee/Rete, Modalità esperti 1683
lingua di sistema per la casella vocale 599
Lingue 109
Lista di controllo di sicurezza 985
Lista di numeri vietati
visualizzare 757
Liste nr. permessi, Modalità esperti 1699
Liste nr.permessi, visualizzare 757
Liste nr.vietati, Modalità esperti 1700, 1700
logo telefono
Carica, Modalità esperti 1481
Loopback digitale 1306
Loopback digitale, Modalità esperti 1488
LXV3, Modalità esperti 1756

M

Mail Exchanger 378, 378
definire 381
Manager E 131
Manutenzione DLI, Modalità esperti 1507
Manutenzione, Modalità esperti 1756
Manutenzione, Modalità Esperto 1472
Mappatura (stato presenza UC Suite) 551
Marchio CE 87
Matrice VBZ
modificare 769
Matrice VBZ, Modalità esperti 1702
MCL Single Stage 782
MCL Two Stage 782
MEB (Media Extension Bridge) 1759
Media Extension Bridge (MEB) 1759
Media Stream Control (MSC), Modalità esperti 1712
Mediatrix 4102S 108
Membri Gruppi, Modalità esperti 1673
Menu Flexible, Modalità esperti 1535
messaggi fax 599, 858
Messaggi istantanei 597, 858, 858
messaggi vocali
annunci stato 599
salva 599
Messaggi vocali 599, 858
Messaggi vocali (UC Smart) 521
messaggio istantaneo 597
Messaggio istantaneo 519, 519, 519, 519, 597, 597
Mobilità
cancella utente 959
mobility
configurare telefoni cellulari per GSM 955
Mobility Entry 948
codici di servizio 949
Mobility Entry, Modalità esperti 1661
Modalità esperti, Modalità esperti 1471
Modelli, Modalità esperti 1730
Modello SMS 613
Modem 439
Modem Internet 370
Modem ISDN 436
Modifica d.selez 626
Modo DHCP, Modalità esperti 1587
Moduli HW, Modalità esperti 1713
MoH 1234
MULAP di base 720
tipo chiam. 722
Multi Location 1047
Multi-SLC, Modalità esperti 1668
musica su attesa 1234
Musica su attesa 1231, 1231, 1231
Musica su attesa (MOH) 749
Musica su attesa (Music on Hold MoH), UCD 749
Musica su attesa interna 1234
Musica su attesa, modalità Esperto 1704
myAgent
requisiti 867
myPortal
funzioni 532
stato presenza 532
myPortal for Outlook
funzioni 533
myPortal Smart
Funzioni 487
myPortal to go
requisiti 947
myReports
reset administrator password 871
user roles 869

N

NAT (Network Address Translation) 988
NAT, Modalità esperti 1597
Nodi, Modalità esperti 1626
Nome dell'Host, Modalità esperti 1579, 1593
Nome DNS 378
Non disturbare 659
note sull'utilizzo simultaneo di myAgent e client UC Suite 873
Notifica con SMS 613
Notifica DLS, Modalità esperti 1508
Notte
    Gruppi di abilitazione, Modalità esperti 1698
Numerazione
    aperta 1055
    nascosta, chiusa 1055
Numerazione E.164 1056
Numeri di telefono
    importazione 423
Numeri di telefono di rete pubblica nella rete 1056
numero di accesso
    conferenza 516

O

Oggetti CCV 831, 882
Open Directory Service 1188
    Manutenzione, Modalità esperti 1756
    Origini dati, modalità Esperto 1755
Open Directory Service, Modalità esperti 1755, 1756
OpenScape Business Assistant 113, 115
OpenScape Business X3R
    Messa a terra di protezione 1403, 1405, 1406
OpenScape Business X5R
    Messa a terra di protezione 1403, 1405, 1406
OpenScape Office, modalità Esperto 1755
OpenScape Personal Edition 108
OpenStage 108
OpenStage Attendant 840
optiPoint 108
Ora di aggiornamento del nome di DNS, Modalità esperti 1541
Ottimizzazione delle rotte 1056
Out of Service, Modalità esperti 1485
Output console traccia, Modalità esperti 1509

P

Padding 999
Paging interno al gruppo 738, 738
    trasferisci chiamata 738
Panoramica messaggi 857
Parametri Codec di destinazione, Modalità esperti 1614
Parametri codec, Modalità esperti 1612
Parametri di rete (LAN, WAN) 1053
Parametri ISDN, Modalità esperti 1696
Parametri SIP, Modalità esperti 1609
Parametri utente, Modalità esperti 1647
Parametro globale, modalità Esperto 1587
Parcheggio 642
Partner PSTN, Modalità esperti 1599
Path Replacement 1056
Pausa nella selezione 632
Payload
    Media Stream Control (MSC), Modalità esperti 1712
    Moduli HW, Modalità esperti 1713
    Periferiche, Modalità esperti 1712
Payload SA 1008
Payload, Modalità esperti 1712
Per tutto il sistema, Modalità esperti 1665
Percorso, modalità Esperto 1687
Periferiche, Modalità esperti 1712
permanente 592
Pianificazione 830, 881
Pianificazione vacanze 831, 882
Pianificazioni, Modalità esperti 1741
Piano di composizione 136, 222, 419, 775
    cancellazione 422
    importazione 423
    modifica 423
Piano di composizione, Modalità esperti 1604
Piano di rete 1046
PIN mobile 669
PIN per attivare un arresto 1264
Ping, Modalità esperti 1511
Player, Modalità esperti 1548
Pool di indirizzi IP, modalità Esperto 1589
porta 1188
Porte 986
    configurazione dell'abilitazione della porta 987, 1138
    gestione delle porte 987
post-selezione 628
Postazione di lavoro alternativa 554
Prenotazione linea 635
prerequisiti per l'uso di Application Launcher 1188
prerequisiti richiesti per l'uso di myReports 871
Presentazione dell'identificazione delle linee connesse - COLP 639
Presenza (UC Smart) 504, 504
Presenza (UC Suite) 551, 551
Primary Rate Interface 782
Priorizzazione delle linee urbane 418
Procedure guidate 122
Processo di concessione delle licenze 316
profili
    creare nuovo profilo 469
    modifica 473
Profili di traccia, Modalità esperti 1495
Profili utente della UC Suite 547
Profili/Modelli, Modalità esperti 1659
Profilo
    aggiungi membro 471
    apparecchio 469
    cancella membro 471

esporta singoli profili 472
esporta tutti i profili 474, 981
importa singoli profili 472
importa tutti i profili 474, 981
mostra membri 470
visualizza profilo 470
Profilo di traccia 1309
aggiungere 1322
arrestare 1314
arresto di tutti i profili 1322
avvia 1314
visualizzare dettagli 1321
visualizzazione 1313
Profilo per i dati di configurazione dell'Application Launcher 1188
Profilo, Modalità esperti 1751
Profilo:esporta tutti i profili 474, 981
Profilo:importa tutti i profili 474, 981
programmazione dei tasti 441, 441
Programmazione dei tasti, Modalità esperti 1664
Promemoria 672
Protezione dei dati 87, 942
Protocollo Admin
Configurazione, Modalità esperti 1505
Dati del registro Admin, Modalità esperti 1505
Protocollo Admin, Modalità esperti 1505
Protocollo ARP, Modalità esperti 1510
Protocollo CSTA 1157
Protocollo diagnosi 1302
scarica 1304
Protocollo PPP, Modalità esperti 1599
Provider di servizi CSTA (CSP) 1758
Provider di servizi di telefonia Internet, Modalità esperto 1615
PSTN, Modalità esperti 1598
Public Key Infrastructure (PKI), Modalità esperti 1575
Pulsanti utente 857
layout 857
Punti codice AF/EF 428

Q

Quality of Service (QoS) 428
configurazione 430
Quality of Service, Modalità esperti 1541

R

Record MX 378
registra 581
registrazione delle chiamate (Voice Recording, registrazione vocale) 648
Registri client 1346
scarica 1349
Registri di diagnostica, Modalità esperti 1501, 1506
Registri diagnostica 1302
scarica 1304
Registro Admin 1040
caricare 1040
modifica della lingua 995, 996, 996, 997, 1040
Registro di diagnostica 1331
apertura 1335
cancellazione 1335, 1336
scaricamento 1335
Registro eventi, Modalità esperti 1499
Registro traccia cliente 1307
aprire 1316
cancella 1316
carica 1316
modifica 1315
visualizza 1315
Registro traccia cliente, Modalità esperti 1489
Registro traccia, Modalità esperti 1488
regola 555
Regola di composizione, Modalità esperti 1606
Regola NAT
cancellazione 990
configurazione 988
configurazione con Editor tabelle NAT 989
Regole attive, Modalità esperti 1572
Regole configurate, Modalità esperti 1574
Regole di composizione 779
Regole NAT 988
Regole VPN
aggiunta di regola configurata 1027
aggiunta per direzione opposta 1028
cancellazione 1029
modifica 1028
mostra regole speciali attive 1026
mostra tutte le regole attive 1026
mostra tutte le regole configurate 1027
Reparti 576
Reparti, Modalità esperti 1728
Requisiti antincendio 85
Requisiti di protezione contro i fulmini 86
Requisiti LAN 1053
Requisiti richiesti per l'uso di myAgent 867
requisiti richiesti per myPortal to go 947
Rete
eliminazione di nodi dal sistema di reti 1142
licenze 1052
omogenea, nativa 1046
Riavvia / Ricarica
Riavvia / Ricarica, Modalità esperti 1502
Riavvia / Ricarica, Modalità esperti 1501, 1502
Riavvio di OpenScape Business 1261, 1261
Ricarica della UC Booster Card 1265
Ricarica di OpenScape Business 1262
richiamata
diario 578
Richiamata 644
Richiamata alternata 643
Richiamata automatica 660, 661
Richiamata automatica su dispositivo occupato 661

Riciclaggio 83
Rifiuto chiam.con add.al chiamante per linea esterna 771
Rifiuto chiamata su altoparlante per utenti 633
attivare 634
disattiva 634
Rifiuto delle chiamante 658
Rilascio della linea per una chiamata di emergenza 814
Rinvio/PO/Hotline, Modalità esperti 1530
Ripetizione della selezione 627
Ripristina 1238, 1246
Ripristina (vedi Ripristino) 1246
Risparmio energia, Modalità esperti 1551
risposta a una chiamata dalla casella vocale 599
Risposta per assente, Modalità esperti 1678
Risposta tramite altoparlante 633
Route statiche 357
aggiungere 358, 361, 362, 363
cancella 359
Route statiche, Modalità esperti 1595, 1596
Router Internet 366
Router predefinito 357
configura 357
Router predefinito, Modalità esperti 1596, 1597
Routing 357
NAT, Modalità esperti 1597
PSTN, Modalità esperti 1598, 1599, 1599
Routing IP Modalità esperti 1595, 1596, 1596, 1596
Routing IP, Modalità esperti 1597
Routing, Modalità esperti 1595, 1627
Rubrica
messaggio istantaneo 519
Rubrica di sistema 507
rubrica di sistema (UC Suite) 567
Rubrica esterna 561
Rubrica esterna (LDAP) 565
Rubrica esterna, Modalità esperti 1730
Rubrica interna (UC Smart) 506
Rubrica interna (UC Suite) 559
Rubrica utente, Modalità esperti 1725
rubriche (UC Smart) 505
Rubriche (UC Suite) 556

S

sala conferenze virtuale 516
Salva 1238
Salvataggio
immediato 1243
pianificato 1245
Scambio di numeri 670
Scheda ISDN 436
Scheda madre, Modalità esperti 1510
Scheda madre, modalità Esperto 1587
Schema indirizzi IP 137, 222
Secure Trace 1307
arresto 1318, 1318
avvio 1318
controllo stato 1318
importazione certificato da file X.509 1319
Modifica passphrase 1318
Modifica password 1318
X.509-File Importa 1319
Secure Trace, Modalità esperti 1490
Security Associations SA 1007
Sede operativa, Modalità esperti 1721
Segnalazione allarmi, Modalità esperti 1501
Segnalazione della chiamata/Avviso di chiamata in attesa 661
Segnalazione delle chiamate 657
Segnalazione di chiamate 636
Segreteria telefonica 439
Selez. blocco tasti 625
Selezione applicazione 1721
Selezione breve del sistema (KWZ) 628
Selezione breve individuale (KWI) 632
server delle licenze (CLS) 313
Server delle licenze (CLS) 335
modifica indirizzo IP 207, 258, 315, 323, 326, 331, 332, 332, 333, 336
Server DNS 356
Server DNS, Modalità esperti 1596
Server DSS 1759
Server FTP, Modalità esperti 1586
Server licenze centrale (vedi Server delle licenze) 335
Server PKI
aggiunta 1029
visualizzazione 1029
Server, Modalità esperti 1745
Servizi
voce, in rete 1052
Servizi attivi, Modalità esperti 1564
Servizi configurati, Modalità esperti 1565
Servizi Euro ISDN 1762
Servizi QSIG, Modalità esperti 1695
Servizi remoti 1356
Servizi Web 1188
Web Collaboration, Modalità esperti 1754
Servizio Active Directory 1185
Servizio CallMe 554
Servizio d'emergenza E911 815
Servizio di integrazione Active Directory
configura 1186
Servizio di integrazione Active Directory, Modalità esperti 1721
Servizio DynDNS 378
configura 379
configurazione 398, 399, 399, 401, 984
Servizio DynDNS, Modalità esperti 1540
Servizio informativo 528, 611
Servizio notte auto, Modalità esperti 1703
Servizio notturno, Modalità esperti 1701
Servizio Open Directory
Impostazioni di base, Modalità esperti 1755
Origini dati, Modalità esperti 1756, 1756

Set di backup 1238, 1239, 1239
backup immediato 1244
backup pianificato 1245
Ripristina 1246
visualizza 1239
visualizzazione 1240
Set di backup a scopo di diagnostica 1336, 1337
Sicurezza
Client di distribuzione e licenze (DLSC), Modalità esperti 1555, 1555, 1557
Crittografia segnalazione e payload (SPE), Modalità esperti 1558, 1559, 1559
Firewall delle applicazioni, modalità Esperto 1553
Sicurezza del Web, Modalità esperti 1578
Sicurezza SQL, Modalità esperti 1579
SSL, Modalità esperti 1576, 1577, 1577
VPN, Modalità esperti 1559, 1560, 1561, 1561, 1563, 1563, 1564, 1565, 1566, 1568, 1572, 1574, 1575
Sicurezza dei dati 87
Sicurezza del Web, Modalità esperti 1578
Sicurezza SQL, Modalità esperti 1579
Sicurezza, Modalità esperti 1553
Single Location 1047
Sistema, Modalità esperti 1512
SLC, Modalità esperti 1667
Smaltimento 83
SmartVM, Modalità esperti 1474, 1474, 1475, 1708
SMS
avviso 611
SNMP
Comunità, Modalità esperti 1503, 1504, 1504, 1504
Trap, Modalità esperti 1504
SNMP (Simple Network Management Protocol) 1288
aggiunta di una comunità 1300
cancellazione di una comunità 1301
comunità 1289
Gestione database informazioni MIB 1289
modifica di una comunità 1300
mostra comunità 1300
trap 1289
visualizza i trap 1301
visualizzazione dettagli trap 1302
SNMP Statistiche, Modalità esperti 1717
SNMP, Modalità esperti 1503
software, aggiornamento (vedere aggiornamenti software) 1246
software, attivazione (vedere attivazione del software) 1246
software, trasferimento (vedere trasferimento del software) 1246
Soluzione cordless
struttura del sistema 964
sopravvivenza 1139
Sostituzione dell'hardware 334
SSDP (Smart Services Delivery Platform) 1356
configura PIN per attivazione/disattivazione del plugin Service 1362
configurazione del plugin servizio per una rete del cliente con proxy 1359
disattivazione plugin servizio 1361
reimposta plugin servizio 1361
SSL (Secure Socket Layer) 1030
attivazione certificato 1037
cancellazione certificato 1036
creazione certificato autofirmato 1033
esportazione certificato 1037
generazione di un certificato CA 1032
generazione di una richiesta di certificato 1034
importazione certificato prorogato 1037
importazione di un certificato server 1035, 1035, 1038
visualizzazione certificato 991, 992, 992, 1036
Standard 1760
Statistiche
SNMP Statistiche, Modalità esperti 1717
Statistiche di gateway, Modalità esperti 1716
Statistiche di telefonia, Modalità esperti 1717, 1717, 1718, 1718, 1719
Statistiche gateway, Modalità esperti 1716
Statistiche MSC, Modalità esperti 1716
Statistiche periferiche, Modalità esperti 1716
Statistiche, Modalità esperti 1716
Stato connessione 1267
richiamare 1268
Stato del sistema di comunicazione 1267
Stato ITSP 1267
richiamare 1269
Stato linea, Modalità esperti 1718
Stato modulo, Modalità esperti 1485
Stato porta e modulo, Modalità esperti 1484
stato presenza 532
Stato presenza
deviazione di chiamata 554
Stato presenza (UC Smart) 504
Stato presenza (UC Suite) 551
Stato utente 1267
richiamare 1268
Stato VPN 1267
stazioni 419
Stazioni analogiche, modalità esperti 1640
STUN (Simple Traversal of UDP over NAT) 400
supporto backup (vedi Supporto di backup) 1240
supporto di backup 1240
aggiungere 1241
Cancella 1243
modifica 1242
Supporto di backup 1238

T

tabella delle reazioni 1331
Tabella delle reazioni, Modalità esperti 1500
Tabella delle rotte 777
Tabella delle rotte, Modalità esperti 1605
Tasti funzione 441
programma 442, 503
programmazione 482, 483, 485, 503, 528

Tasto chiamata su altoparlante (diretta) 632
Tasto DSS 632
Team (vedere Configurazione team) 701
Team/Top, Modalità esperti 1675
Telefon-Logo
    Verteilen, Experten-Modus 1482
Telefoni 108
Telefoni cordless 108
Telefoni DECT 108
Telefoni Gigaset 108
Telefoni SIP 108
Telefoni WLAN 109
Telefonia dual mode 954
Telefonia Internet 381
Telefonia, Modalità esperti 1512
Telefono analogico 439
Telefono ISDN 436
Telelavoratore 976
Telelavoro 554
Temporizzazioni
    monitoraggio di una chiamata UCD su una linea analogica 751
    monitoraggio di una trasferta prima della risposta a un gruppo UCD 751
Temporizzazioni, Modalità esperti 1520
Test della connessione di rete 1287
    tramite Ping 1287
    tramite Traceroute 1288
Testi di assenza 665
Testi di sistema, Modalità esperti 1717
Testi messagi 665
Testi, Modalità esperti 1535
Testo in più lingue 1230
Tipo di avvertimento
    Attenzione 76
    Avvertenza 75
    Pericolo 74
Tracce
    Ascolto chiamate, Modalità esperti 1492
    Componente di traccia M5T, Modalità esperti 1489
    Componente licenza, Modalità esperti 1494
    Componenti di traccia, Modalità esperti 1495
    Configurazione formato traccia, Modalità esperti 1486
    Interfacce di output traccia, Modalità esperti 1487
    Loopback digitale, Modalità esperti 1488
    Profili di traccia, Modalità esperti 1495
    Registro traccia cliente, Modalità esperti 1489
    Registro traccia, Modalità esperti 1488
    rpcap Daemon, Modalità esperti 1497
    Secure Trace, Modalità esperti 1490, 1490, 1490
    Tracce server multimediale, modalità Esperti 1498
    Traccia dello stack H.323, Modalità esperti 1491
    Trasferimento TCP, Modalità esperti 1496
Tracce server multimediale, modalità Esperti 1498
Tracce, Modalità esperti 1486
traccia
    cancella il registro 1312
Traccia 1305
    cancella il registro 1312
    download del registro 1311
    modifica interfacce di output traccia 1315
    modifica la configurazione del formato della traccia 1314
    registro 1306
    visualizzare interfacce di output traccia 1315
    visualizzare la configurazione del formato della traccia 1314
Traccia componente licenza 1309
    modifica 1321
Traccia componente licenza, Modalità esperti 1494
Traccia dello stack H.323 1308
    aprire il registro 1320
    cancellare il registro 1321
    caricare il registro 1320
    modifica i moduli 1320
    modificare la configurazione 1319
    visualizza la configurazione 1319
Traccia dello stack H.323, Modalità esperti 1491
Traccia server multimediale
    arresta 1327
    avvio 1326
Traccia:configurazione formato traccia 1305
Traccia:interfacce di output traccia 1306
Trap, Modalità esperti 1504
Trasferimento 670
trasferimento del software 1246
Trasferimento TCP 1327
    arrestare 1328
    avvia 1327
    cancellare 1328
Trasferimento TCP, Modalità esperti 1496
trasferisci chiamate 643
Trasferta al gruppo con paging interno 738
Trasmissione del numero di telefono del chiamante - CLIP 636
Trasmissione di informazioni sul numero di telefono specifiche del cliente 640
Trasmissione selezione 773
    scegliere 774
Trunk server SIP nativo, modalità Esperto 1629
Trunk/Instradamento
    Percorso, modalità Esperto 1687
Tunnel attivi, Modalità esperti 1566
Tunnel configurati, Modalità esperti 1568
Tunnel IPSec 1007
Tutti i lease, Modalità esperti 1592

U

UC Applications, Modalità esperti 1657
UC Booster Card
    riavvio 1264, 1265
UC Smart
    Gestione utenti 1723
    Impostazioni di base 1722

Interrogazione stato 1356
Stato 1355, 1724
UC Smart, Modalità esperti 1722
UC Suite 1725
attivazione della registrazione dei registri dei client dei singoli utenti 1348
Carica file, Modalità esperti 1743
Conferenza in corso, Modalità esperti 1744
Configurare le notifiche e-mail per gli errori di sistema 1352
Configurazione provider esterni, Modalità esperti 1731
configure retention period for contact center data 1355
configure retention period for log files 1354
configure storage path for client log files 1348
configure time for maintenance 1354
Contact Center, Modalità esperti 1733
disable recording of system logs 1347
disable saving of client logs on system hard disk 1349
disattivazione della registrazione dei singoli registri dei client 1347
e-mail notification 1350
Elenco sedi, Modalità esperti 1744
enable recording of system logs 1347
enable saving of client logs on system hard disk 1349
Gruppi, Modalità esperti 1728
Intestazione fax, Modalità esperti 1753
manutenzione 1345
Modelli, Modalità esperti 1730
monitoraggio 1345
performing system maintenance immediately 1355
Pianificazioni, Modalità esperti 1741
Profilo, Modalità esperti 1751
Registri client 1346
Reparti, Modalità esperti 1728
Rubrica esterna, Modalità esperti 1730
Rubrica utente, Modalità esperti 1725
scaricare i registri dei client 1349
Server, Modalità esperti 1745
UC Suite
disable recording of client logs on system-wide basis 1347
enable recording of client logs on system-wide basis 1347
maintenance 1353
notification 1350
system logs 1346
UC Suite, Modalità esperti 1725
UCD (Uniform Call Distribution) (vedere Distribuzione delle chiamate) 739
UCD, Modalità esperti 1678
Ultimi lease attivi, modalità Esperto 1592
upgrade 1246
users of UC Suite
change length of password 547
Modifica password 546
Uso corretto dei sistemi di comunicazione e del server 83
Utente 1634
configurazione tramite la procedura guidata 444
IP 431
ISDN 436
Programmazione dei tasti, Modalità esperti 1664
Utenti, Modalità esperti 1637, 1640, 1641, 1642, 1643, 1645, 1646, 1659, 1660, 1661
Utente di UC Smart
modifica dati 503, 528
Utente di UC Suite
configura come agenti 545
modifica dati 544
reimposta 545
Utente IP 431
utente Mobility Entry 592, 592
Utente Mobility Entry
conferenza 583, 589, 590, 593
Utente online 1368, 1511
avvio 1286, 1369
Utente online, Modalità esperti 1511
Utente RAS 431
utenti
Utente, Modalità esperti 1657
Utenti
analogici 439
Panoramica, Modalità esperti 1663
Utente, Modalità esperti 1647
Utenti base, Modalità esperti 1482, 1482, 1642, 1668
Utenti DECT, Modalità esperti 1643
utenti di UC Smart
modifica dati 503
utenti di UC Suite 541
cambia stato presenza 546
Utenti ISDN 436
Utenti ISDN, Modalità esperti 1641
Utenti Mobility Entry
conferenze 516
Utenti UP0, Modalità esperti 1634
Utenti virtuali, Modalità esperti 1646
Utenti, Modalità esperti 1634, 1634, 1697, 1719

V

valori massimi
Servizi 1441
Visualizzatore eventi 1307
aprire il registro 1316
cancellare il registro 1316
carica il registro 1316
modifica il registro 1315
mostra il registro 1315
Voce Mail Exchange 378
voci registro 1330
VPN
autenticazione 1008
certificati 1009
client 1014
larghezza di banda 998
meccanismi di protezione 1007

VPN - Servizi attivi
mostra tutti i servizi 1020
mostra un servizio speciale 1020
VPN - Servizi configurati
cancellazione 1022
modifica 1021
mostra tutti i servizi 1020
rinomina 1021
VPN - Tunnel attivi
mostra 1022
mostra le regole 1023
VPN - Tunnel configurati
aggiunta 1024
mostra le regole 1024
visualizzazione 1023
VPN (Virtual Private Network) 997
end-to-site 997
site-to-site 997
VPN, Modalità esperti 1559

W

WAN 378
WBM 113
pagina iniziale 113
web collaboration 518
Web Collaboration 593, 594, 594
Web Collaboration, Modalità esperti 1754
Web Services, Modalità esperti 1754

© 2025 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.